ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы
«Ақпараттық қауіпсіздік жүйелері» кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі с.ғ.к., доцент Бердібаев Р. Ш.
_____ «_____» _____ 2019 ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: «Web-қосымшаларды қорғау үшін сканерлерді талдау және зерттеу»
Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Қадыр Айбек Тобы: СИБк-15-1
Ғылыми жетекші: с.ғ.к., доцент Шайкулова А.А.
Кеңесшілер:
Экономикалық бөлім бойынша:
т.ғ.к., профессор Арипбаева Ж.Г.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «04» мамыр 2019 ж.
(қолы)
Тіршілік қауіпсіздігі бөлімі бойынша:
аға оқытушы Тәжиев Э.О.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «28» 05 2019 ж.
(қолы)
Есептеу техникасын қолдану бойынша:
т.ғ.к., доцент Шайкулова А.А.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «21» 05 2019 ж.
(қолы)
Мөлшер бақылаушы:
аға оқытушы Асқарова Ж.Б.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «11» мамыр 2019 ж.
(қолы)
Пікір беруші:
т.ғ.к., ассистент-профессор Сейлова Н.А.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «11» мамыр 2019 ж.
(қолы)

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы

Басқару және ақпараттық технологиялар институты
Ақпараттық қауіпсіздік жүйелері кафедрасы
5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

Дипломдық жобаны орындауға берілген
ТАПСЫРМА

Студент: Қаусар Айбек Бауыржанұлы
(аты-жөні)

Жобаның тақырыбы: Web-қосымшаларды қорғау үшін сканерлерді таңдау және зерттеу.

2018 ж. «26» 10 № 124 университет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «11» 06 2019 ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): „Web-қосымшаларды қорғау үшін сканерлерді таңдау және зерттеу" тақырыбындағы дипломдық жобада осалдықтар қауіптерге, осалдық түрлерінің таңдау жасалады. OWASP қауымдастығының таңдауларына сүйене отырып, қауіпті және жиі кездесетін түрлеріне, осалдық ішінде PHP-инъекция, SQL-инъекция, скриптерді қайтарымсыз орындау, Cross-Site Scripting осалдықтарына қатты түсініктер беріледі. Securitylab.ru жүйесінен соңғы қосымшалар бойынша қауіпсіздік сканерлерінің бірнешеуіне талдау жасалып, осалдық мүмкіндіктері салыстырылады: олар: XSpider, Nessus, Internet Scanner, Retina Network Security сканерлері.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:

1. Web-қосымшалар осалдықтары және олардан төнетін қауіптер
2. PHP-инъекция
3. SQL-инъекция
4. Cross-site Scripting осалдығы
5. XSPIDER-ді қолдану нұсқаулары
6. Техникалық-экономикалық негіздемесі

7. Өмір тіршілік қауіпсіздігі
8. Қорытынды

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі: 1. Қорғалған Web-қосымшаның әзірлеудің және сүйемелдеудің өмірлік циклі
2. Осалдықтар сканерлерін пайдалану диаграммасы
3. Желінің бұзуға төтеп беруштігін тексеру режимінде сканерлерді сынау көрсеткіші
4. Веб-қосымшалар қауіпсіздігіне тонетін қауіптердің жіктелуі

Негізгі ұсынылатын әдебиеттер: 1 Геннадий Б. Защита информации ограниченного доступа от утечки по техническим каналам. -М: Телеком 2014
2. Хорев П. Б., Методы и средства защиты информации в компьютерных системах, -М: Издательский центр „Академия", 2005.
3. Жуков Ю. Основы веб-хакинга. Нападение и защита. - Спб: Питер, 2010.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Есептеу техникасы бойынша Өміртіршілік қауіпсіздігі бөлімі	Шайкулова А.А.	11.02. - 29.05	
	Торгаев Э.Э.	20.05-23.05	
Экономикалық бөлім	Арепаева М.Г.	04.03 -04.05	

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
Кіріспе	14.02.2019	
Web-қосымшалар осал-дықтары және оларға тонетін қауіптер	27.02.2019	
Тестілік және продук-тивті күйлерді са-лыстыру	06.03.2019	
PHP инъекция	12.03.2019	
Қауіпсіздік сканерле-рін зерттеу, талдау	17.03.2019	
Хосттарды тексеру, түйіндердегі осалдық-тарды анықтау	03.04.2019	
Қосымшаны қорғау механизмі	11.04.2019	
XSPIDER-ді қолдану нұсқаулары	26.04.2019	
Web, mail серверлерімен жұмыс істейтін хосттарды қашықтан жіліміндіру	15.05.2019	
Өмір тіршілік қауіпсіздігі	28.05.2019	
Техникалық-экономика-лық негіздемесі	04.06.2019	

Тапсырманың берілген уақыты «21» 01 2019 ж.

Кафедра меңгерушісі _____ (_____)
(қолы) (аты-жөні)

Жобаның
ғылыми жетекшісі _____ (Шаяхметова А.А.)
(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент _____ (Қадыр А.Б.)
(қолы) (аты-жөні)

АҢДАТПА

«Web-қосымшаларды қорғау үшін сканерлерді талдау және зерттеу» тақырыбындағы дипломдық жобада осы саладағы қауіптерге, олардың түрлеріне талдау жасалады. OWASP қауымдастығының талдауларына сүйене отырып, қауіптің жиі туындайтын түрлеріне, олардың ішінде PHP-инъекция, SQL-инъекция, Скриптерді сайтаралық орындау, Cross-Site Scripting осалдықтарына нақты түсініктер беріледі. Securitylab.ru жүргізген сауалнамалар бойынша қауіпсіздік сканерлерінің бірнешеуіне талдау жасалып, олардың мүмкіндіктері салыстырылады, олар: xSpider, Internet Scanner, Nessus, Retina Network Security Scanner сканерлері. Тиімдісін тәжірибе жүзінде қолданып, есеп құрастырылған.

АННОТАЦИЯ

В дипломном проекте "Аанализ и исследование сканеров для защиты Web-приложений" проводится анализ угроз в данной области, их видов. Опираясь на анализы ассоциации OWASP, дается четкое представление о наиболее часто возникающих видах риска, среди которых уязвимости PHP-инъекции, SQL-инъекции, межсистемного выполнения скриптов, Cross-Site Scripting. По проведенным опросам Securitylab.ru был проведен анализ нескольких сканеров безопасности и сопоставлены их возможности: сканеры xSpider, Internet Scanner, Nessus, Retina Network Security Scanner. Составлен отчет по применению на практике.

ANNOTATION

In the diploma project "analysis and research scanners to protect Web-applications" analyzes the threats in this area, their types. Based on the analyses of the Association of OWASP, provides a clear indication of the most frequently encountered types of risk, including vulnerability PHP injection, SQL injection, cross-system scripting, Cross-Site Scripting. Securitylab.ru according to the conducted surveys, several security scanners were analyzed and their capabilities were compared: xSpider, Internet Scanner, Nessus, Retina Network Security Scanner. In practice, we used efficiency, a report was compiled.

Мазмұны

Кіріспе

Қазіргі заманғы өмірлік барлық салалар ақпараттық қауіпсіздіктің түрлі қатерлеріне ұшыраған ақпараттық технологияларды (бұдан әрі АҚ) пайдаланумен тығыз байланысты. Осының салдарынан компания акцияларының құнының төмендеуі, серіктестер/клиенттер және т. б. тарапынан сенім деңгейінің төмендеуі мүмкін. Түрлі ақпараттық ресурстар зиян шегіп, оның салдары әлеуметтік-экономикалық дағдарысын туындатуы да мүмкін. Осындай тәуекелдерді азайту үшін компаниялар АҚ-ны қамтамасыз етуге байланысты мәселелермен айналысуға мәжбүр. Сонымен қатар, бірқатар жағдайларда бұл қажеттілік заңнамалық (ҚШФ, Президент жарлықтары және т.б.), сондай-ақ халықаралық (ISO/IEC 27005:2008, PCI DSS, SOX және т. б.) түрлі өлшемдерге сәйкес келу ниетімен немесе талаптарымен байланысты. АҚ-ны қамтамасыз етуге тиісті назар аударатын Компания өздерінің Ақпараттық активтері мен оларға төнуі мүмкін қауіптерді басқаруы тиіс. Қауіпсіздік сканерлері осы міндетті шешуге көмектесетін құрал болып табылады. Қауіпсіздік сканері бұл зерттелетін объектінің әртүрлі осалдықтарына ұшырағыштығын әр түрлі тексеру арқылы анықтауға мүмкіндік беретін бағдарламалық немесе аппараттық-бағдарламалық құрал. Осалдық – кейбір қауіп-қатерді (мысалы, ақпаратты ұрлауға) іске асыру арқылы қауіпсіздіктің бұзылуына әкелуі мүмкін ақпараттық жүйедегі әлсіз орын. Зерттеу объектісі ретінде ақпараттық жүйенің кез келген компоненті бола алады: web-сервер, web-қосымшалар, ДҚБЖ, әртүрлі желілік жабдық және т. б. Қазіргі нарық компанияның ақпараттық ресурстарының қорғалуын талдауға арналған көптеген шешімдерді ұсынады. Кез келген осындай шешімнің негізі қауіпсіздікті сканерлеуші ядросканер екенін ескеру керек. Қалған модульдер - кейбір функцияларды кеңейту мақсатында қолданылады. Мысалы, шешім Vulnerability Assessmentk, Policy Managementk, Risk Assessmentk және т.б. сияқты көптеген түрлі модульдерді қамтуы мүмкін, бірақ барлық осы модульдердің нақты пайдасы қауіпсіздік сканерінің сканерлеуші ядросы зерттелетін ақпараттық жүйеде бар барлық осалдықтарды дұрыс анықтағанда ғана болады. Компанияның басқарушылары үшін (CEO, топ-менеджмент) қауіпсіздік сканерлерін қолдану компанияның АҚ-ның қолайлы деңгейін қамтамасыз ету мақсатына жетуіне көмектесуге қабілетті әрқашан ашық процесс болып табылмайды. Бұл шын мәнінде ақпараттық қауіпсіздікті басқару жүйесінің жетілу деңгейі төмен компаниялар үшін дұрыс шешім болып табылады. Бірақ жоғары деңгейде кемелденуі бар компаниялар үшін қазіргі заманғы қауіпсіздік сканері АҚ-ны қамтамасыз ету мақсаттарына қол жеткізуге көмектесе алады. Ал АҚ-ны қамтамасыз етудің негізгі мақсаты - компанияның ақпаратты қорғау саласындағы стратегиясын іске асыру, яғни үдерістердің АҚ саясатына сәйкестігі. Қазіргі заманғы қауіпсіздік сканері АҚ стратегиясын іске асыруға қалай көмектесе алады? Бұл сұраққа жауап беру үшін қазіргі заманғы қауіпсіздік сканерлерінің мүмкіндіктерін зерттеу, талдауды және қарастыруды ұсынамын. Қауіпсіздікті кешенді бағалау

қауіпсіздік сканерлері ақпараттық жүйелердегі осалдықтарды уақтылы анықтауға көмектесетін ыңғайлы және қарапайым құрал болып табылады.

1 Web-қосымшалар осалдықтары және оларға төнетін қауіптер

OWASP қауымдастығының ақпарат қауіпсіздігін қамтамасыз етуге байланысты көптеген зерттеулері мен талдаулары осы саладағы мамандар мен компаниялар үшін көптен танымал және осы қауымдастықтың құрамында жұмыс істегісі келетін, осы қауымдастықпен бірлесіп жұмыс істегісі келетін, сонымен қатар қауымдастықтың болжамдарына сүйенетін шағын ұйымдар, жекелеген қолданушылар да жеткілікті. Қауымдастық болжамдары ақпарат қауіпсіздігінің осалдықтарына байланысты көптеген талдаулар жасап, соған сәйкес дұрыс кеңестер ұсынады. OWASP қауымдастығының талдаулары бойынша Веб-қосымшалардың 19%-да зиянкестерге қосымшаның өзіне де, серверге де бақылау жасауға мүмкіндік беретін осалдықтар бар. Егер сервер ұйым желісінің периметрінде болса, қаскүнем компанияның ішкі желісіне кіре алады. Корпоративтік ақпараттық жүйелердің осалдықтарын зерттеу нәтижелері көрсеткендей, АЕЖ ену векторларының 75%-ы веб-қосымшаларды қорғау кемшіліктерімен байланысты. Көптеген жағдайларда веб-қосымшалар кодтағы қателерге байланысты осал болып табылады. Конфигурациядағы өзгерістер осалдықтарының тек 17%-ы ғана жойылуы мүмкін, оның ішінде олардың көпшілігінің тәуекел деңгейі төмен. Қауіпті осалдықтарды жою үшін, әдетте, кодқа түзетулер енгізу қажет.

Әрбір екінші ағып кету есептік деректерді, оның ішінде бөгде ресурстарға қол жеткізу үшін жария етуге әкелуі мүмкін. Мысал ретінде барлық пайдаланушыларға қол жетімді конфигурациялық файлдарды, оларда сақталған парольдерді келтіруге болады.

Қаскүнемдер пайдаланушылардың жеке деректерін өңдеу жүзеге асырылатын веб-қосымшалардың 18%-да ұрлауы мүмкін. Бұл ретте дербес деректер біз зерттеген әрбір веб-қосымшада (91%) сақталады және өңделеді. Орташа есеппен бір веб-қосымшаға 33 осалдықтар келеді, оның алтауы жоғары тәуекелге ие. 2017 жылмен салыстырғанда бір веб-қосымшаға келетін қауіпті осалдықтар саны 3 есеге өскен.

Өнімді жүйелер тестіден аз осалдықтардан тұрады, бірақ бұл оларды қорғау емес. Жоғары деңгейдегі тәуекелдің кем дегенде бір осалдығын қамтитын өнімді жүйелердің үлесі тестіден артық. Тәжірибе көрсеткендей, веб-қосымшаны сәтті бұзу үшін жиі бір сыни қауіпті осалдықтың жеткілікті болуы. Бастапқы кодты талдау тексеру тиімділігін арттырады. Сарапшылардың бастапқы кодқа қол жетімділігі болған жағдайда, тәуекелдің жоғары деңгейіндегі анықталған осалдықтардың орташа саны, статистика бойынша, екі еседен астам өседі екен [1].

1.1 Қауіпті осалдықтары бар веб-қосымшалардың сандық

Жоғары тәуекел деңгейінің осалдығы бар веб-қосымшалардың үлесін төмендетуге арналған шаралар жүзеге асырылғанымен, ол белгілі бір уақыт өте келе қайтадан өсіп отырады. Жеткіліксіз авторизациялаумен, еркін

файлдарды жүктеу немесе оқу мүмкіндігімен, сондай-ақ SQL-кодты енгізу мүмкіндігімен байланысты осалдықтар көп таралған.

Рұқсат етілмеген қол жеткізу - қауіптің тұрақты түрі.

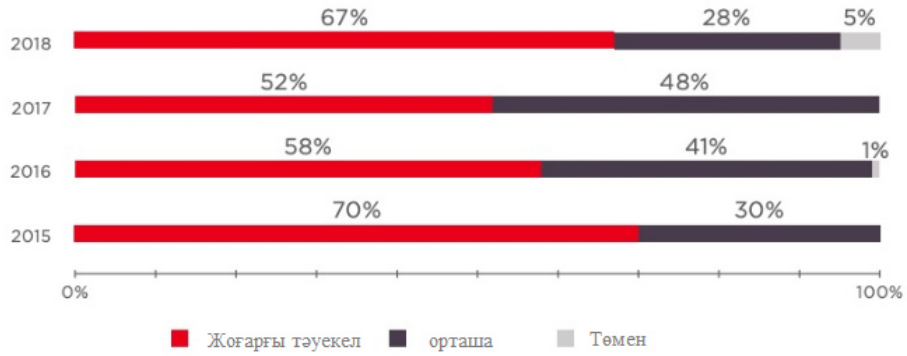
2017 жылы рұқсатсыз қол жеткізу қаупін тудыратын осалдықтармен веб-қосымшалардың үлесі төмендегеннен кейін олардың үлесі 72%-ға дейін өсіп, 2016 жылғы деңгейге жеткен (75%).

Қолданылатын БҚ нұсқалары сирек ашыла бастады.

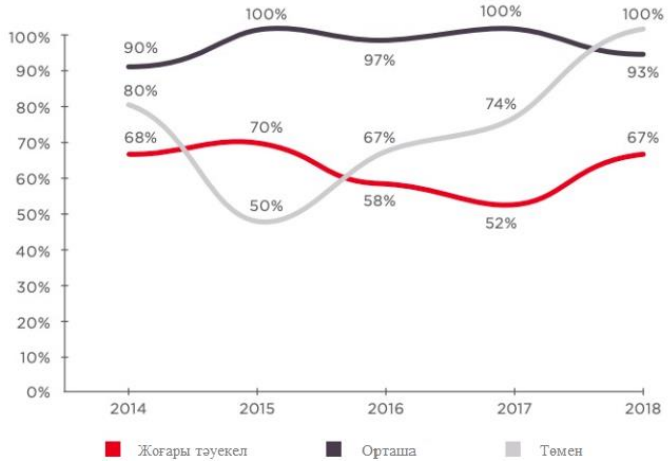
2018 жылы пайдаланылатын БҚ нұсқалары ашылатын веб-қосымшалардың үлесі 42%-ды құрады, бұл 2017 жылға қарағанда (61%) айтарлықтай аз. Мүмкін, мұндай үрдіс осы осалдықтың кең таралуымен және оны жоюдың салыстырмалы қарапайымдылығымен түсіндірілетін болар [1].

Деректердің ағып кетуі мүмкін жүйелердің үлесі өсуде.

Конфигурациялық және баптағыш ақпараттың, бастапқы кодтардың, сессия идентификаторларының, сондай-ақ басқа да сезімтал ақпараттың жылыстауы веб-қосымшалардың 79%-да мүмкін. Салыстыру үшін: 2016 жылы — 60%, 2017 жылы - 70% болған (Сурет 1, 2, 3, 4).



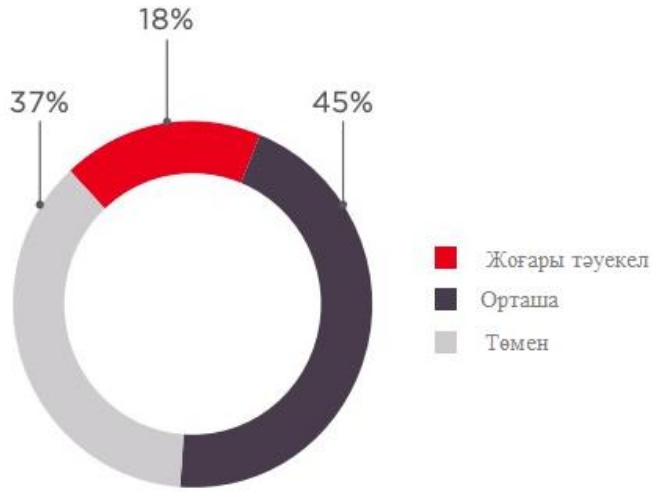
Сурет 1 – Осалдықтар тәуекелінің ең жоғары дәрежесіне байланысты осал сайттар үлесі



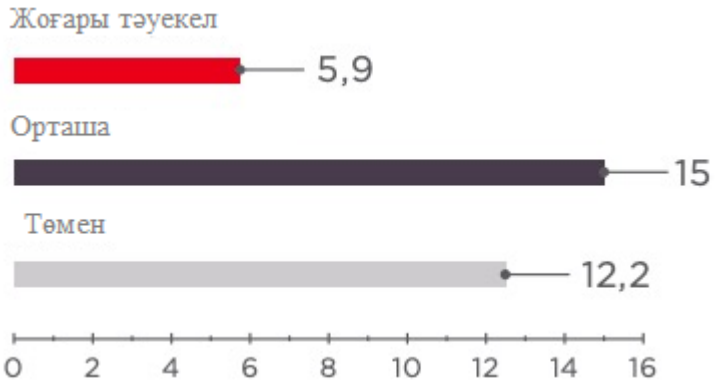
Сурет 2 – Әртүрлі тәуекел дәрежесіндегі осалдықтары бар сайттар үлесі

Веб-қосымшалардың қорғалуын талдау

83% – Зерттелген веб-қосымшалардағы код осалдығының үлесі 3-суретте берілген.



Сурет 3 – Әртүрлі тәуекел дәрежесіндегі осалдықтардың үлесі



Сурет 4 – Бір жүйеге осалдықтардың орташа саны

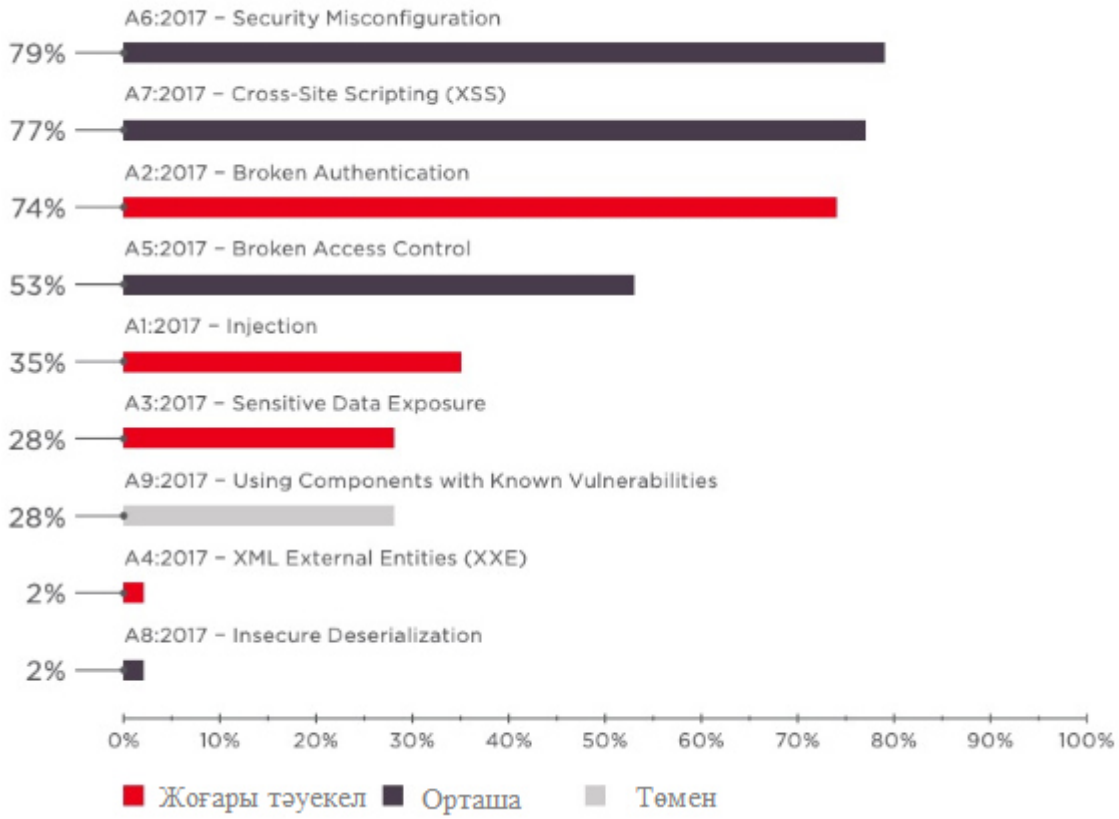
1.2 Ең көп таралған осалдықтар

Веб-серверді, және деректер қорының серверін сауатты конфигурациялау және әзірлеуші арқылы алдын ала орнатылған әдепкі параметрлерді және құпия сөздерді қалдырмау аса маңызды болып табылады.

Соңғы жылдары мамандар веб-қосымшаларда 70 түрлі кемшіліктерді тапты. "Сценарийлердің интернет аралық орындалуы" осалдықтары бар веб-қосымшалардың үлесі әрдайым жоғары (Cross-Site Scripting, XSS). Әрбір бес веб-қосымшалардың төртінде конфигурация қателері белгіленген: әдепкі параметрлер, стандартты парольдер, қолданылатын БҚ нұсқалары ашылатын қателер туралы хабарламалар, орнату жолдары және жүйе туралы ақпаратты жинау кезеңінде және шабуылдарды жоспарлау кезінде қаскүнем үшін құнды басқа да деректер.

Веб-бағдарлама логикасында қарастырылған болмаса, XML парсерлерде сыртқы мәндер мен DTD қолдауын өшіріп отыруға кеңес беріледі.

2018 жылы "XML сыртқы мәнін енгізу" (XML External Entities, XXE) осалдығына ұшыраған веб-қосымшалар үлесі төмендеген. Сонымен қатар, бұны тренд деп айтуға әзір ерте, бәлкім бұл, веб-қосымшаларды іріктеу ерекшелігі болар. Керісінше, веб-осалдықтар туралы айтатын болса, XXE әлі де өзекті. 2017 жылы ол бірінші рет OWASP Top 10 (*Open Web Application Security Project* - бұл веб-қосымшалардың қауіпсіздігін қамтамасыз етудің ашық жобасы. OWASP қауымдастығына корпорациялар, білім беру ұйымдары мен әлемнің жеке тұлғалары кіреді. Қауымдастық еркін қол жеткізудегі мақалаларды, оқу құралдарын, құжаттаманы, құралдар мен технологияларды жасау бойынша жұмыс істейді) рейтингіне еніп, бірден төртінші орынға ие болды (Сурет 5).



Сурет 5 – OWASP тізіміндегі осалдықтар. Top 10−2017 (қосымшалар үлесі)

2018 жылдың сәуір айында Panera Bread кафесінің американдық желісінің сайтында 37 млн клиенттің жеке деректері және олардың төлем карталарының деректері ашық түрде сақталғаны белгілі болды .

Маңызды ақпараттың таралуы 2018 жылы бүкіл әлемде байқалады. Көптеген атышулы оқиғалардың себебі әкімшілік ету және әртүрлі ресурстарға қол жетімділікті шектеудің кемшіліктері болып табылады, бұл ретте зерттеу веб-қосымшаларда маңызды деректерді қауіпсіз сақтау мәселелерін көрсетеді. Мәселен, ағудың 46%-да есептік деректер қауіп-қатерге түседі. Дербес деректер зерттеген веб-қосымшалардың 91%-да

өңделеді, бұл ретте осы жүйелердің 18%-да олардың ағып кетуі мүмкін (барлық ағып кетулердің 19%-ы).

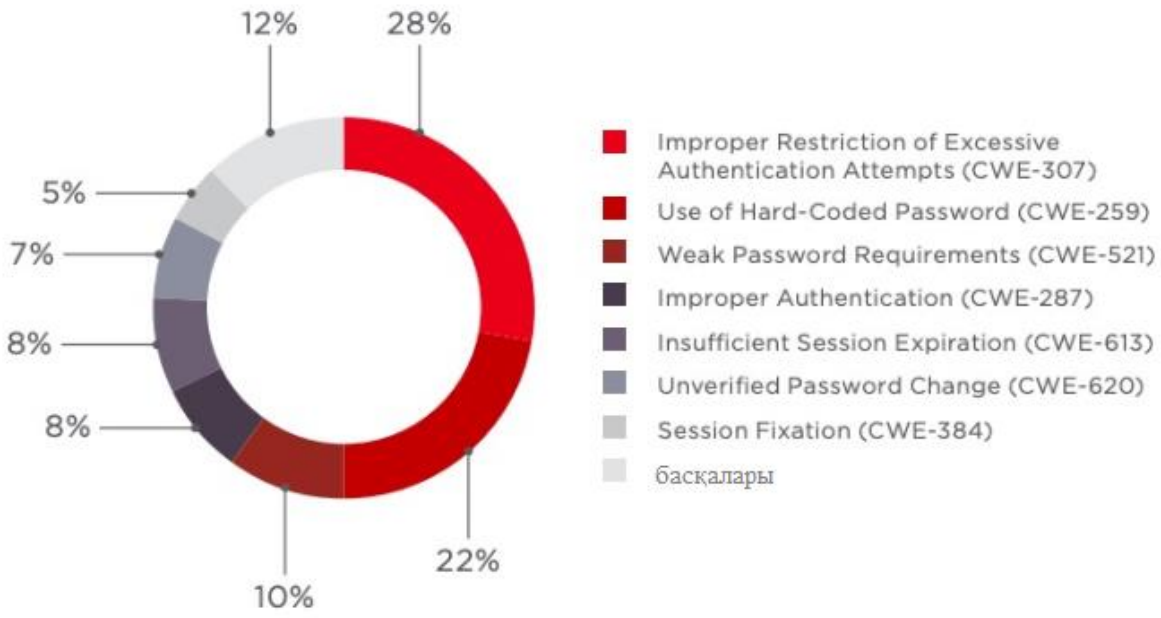
Сезімтал деректер ашық түрде сақталмауы тиіс. Оларды қорғау үшін сенімді криптографиялық алгоритмдерді пайдалануға кеңес беріледі, сонымен қатар сезімтал деректерге қатынауды шектеудің тиімді саясатын қолдану қажеттігі ескертіледі (Сурет 6).

Сурет 6 – Жария сезімтал деректер

Timehop сервисінің 21 млн пайдаланушысы мәліметтерінің жылыстауы әкімшінің есептік деректерін алған қаскүнемнің кінәсінен орын алған. Екі факторлы аутентификацияның болмауына байланысты қаскүнемдердің әрі қарайғы әрекеттері сәтті болып отырған.

Аутентификация және сессияларды басқару тетіктерінің кемшіліктеріне байланысты осалдықтар веб-қосымшаның немесе оның мазмұнының функционалдық мүмкіндіктеріне рұқсатсыз қол жеткізуге себеп болуы мүмкін (Сурет 7).

2018 жылы БАҚ-та айыппұл туралы хабарламалар пайда болды (жалпы сомасы 149 млн. АҚШ доллары), Uber компаниясының қателігінен 50 млн жолаушы және 7 млн жүргізушілердің дербес деректері ұрланған. Ресми мәлімдемеде айтылғандай, қаскүнем GitHub-те корпоративтік репозиторияда сақталған бастапқы кодта базаға қол жеткізу үшін есептік деректерді анықтаған.



Сурет 7 – Аутентификация және сессияларды басқару тетіктерінің осалдығы (Broken Authentication)

Веб-қосымшаларды автоматты түрде талдау кезінде мамандар, мысалы, ДҚБЖ-ға немесе басқа жүйелердің API-не қол жеткізу үшін, кодта берілген қатаң парольдермен жиі кездеседі. Бастапқы кодқа қол жеткізген қаскүнем тиісті жүйелерге рұқсатсыз қол жеткізу және ақпаратты ұрлау үшін осы есептік деректерді пайдалана алады. Сонымен қатар, бірқатар жағдайларда табылған қатаң берілген парольдер тұрақтылыққа қойылатын ең төменгі талаптарға жауап бермейді, демек – брутфорс-шабуыл нәтижесінде сәтті таңдалуы мүмкін. Өз кезегінде, компрометирленген парольді ауыстыру кодқа өзгерістер енгізуді талап етеді.

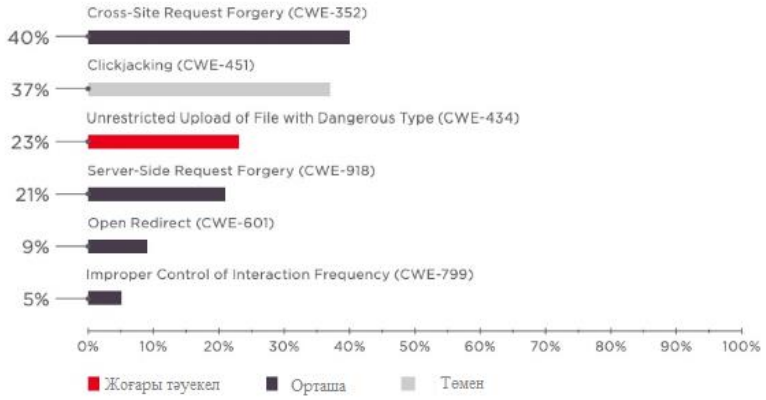
Кодта қатаң берілген парольдерден бас тарту және құпия сөз ретінде таңдауға төзімді таңбалар комбинациясын алған дұрыс (Сурет 8).

Сурет 8 – Веб-қосымшаны автоматтандырылған тестілеу барысында анықталған қатаң берілген парольдің мысалы

OWASP қауымдастығы Top 10-2017 санатының ешқайсысына кірмеген бірқатар осалдықтарды бөліп көрсетеді, олардың болуын тексеру ұсынылады. Бұл тізімде еркін файлдарды жүктеу мүмкіндігі бар - қауіпті осалдық, ол қаскүнемге серверге орындалатын файлдарды жүктеуге және кодты

орындауға мүмкіндік береді, бұл веб-қосымшаны және серверді толық бақылауға алып келуі мүмкін.

Әрбір төртінші зерттелген веб-бағдарламаның еркін файлдарды жүктеуге жол беретіндігі анықталған (Сурет 9).

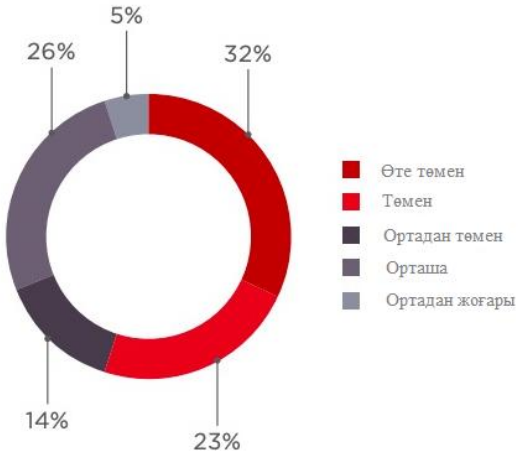


Сурет 9 – OWASP-тағы 2017 жылғы алғашқы ондыққа кірмеген, кең таралған осалдықтар

Жүктелетін файлдар кеңейтімдерін ақ тізім бойынша сүзіп, орындалатын файлдар сақталатын каталогтарға қатынауды шектеу саясатын орнату қажет.

1.3 Қауіптерді талдау және қорғалу деңгейі

Әрбір үшінші веб-бағдарламаның қорғау деңгейі өте төмен. Бұл 2017 жылға қарағанда 15% көп (Сурет 10).

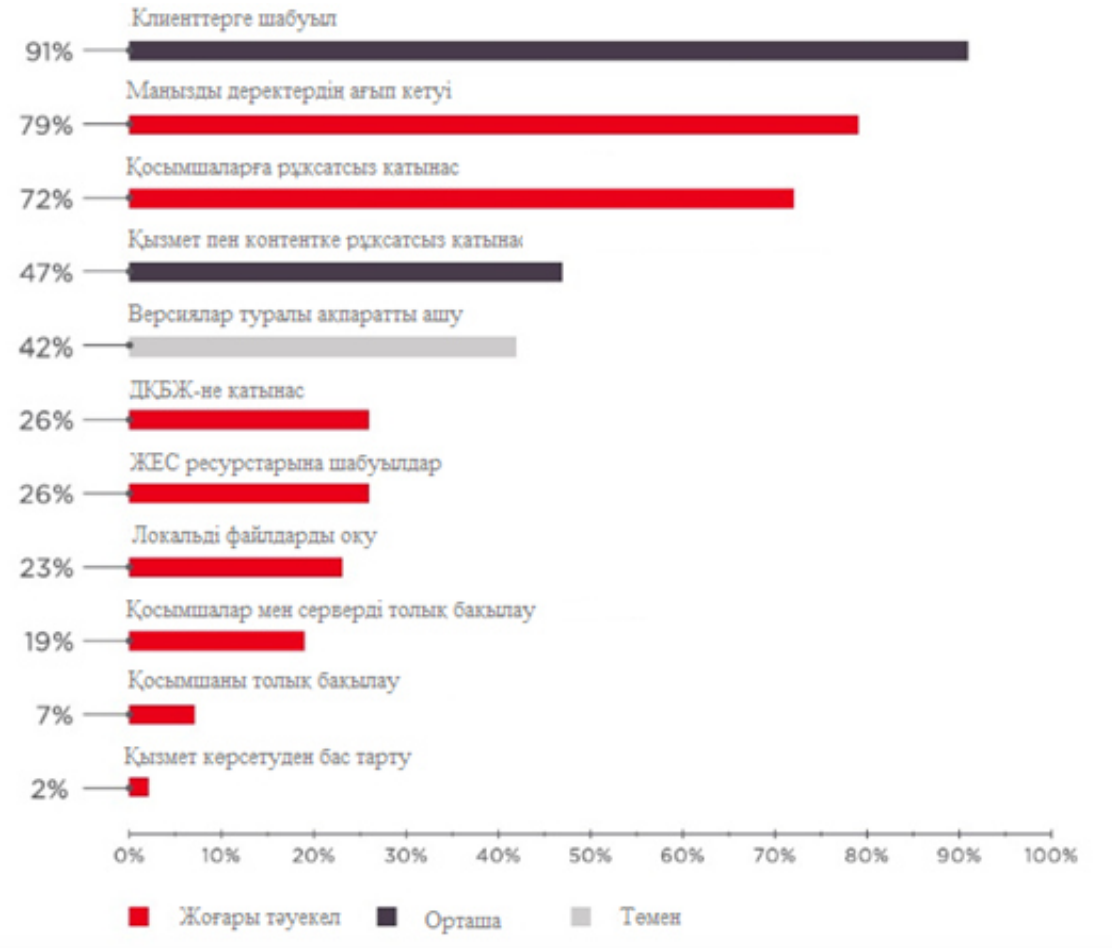


Сурет 10 – Қорғалу деңгейі (веб-қосымшалардың үлесі)

Ақпаратты ұрлаудан басқа, веб-қосымшаға рұқсатсыз кіру оның иесінің беделіне теріс әсер етуі мүмкін

2017 жылы әрбір екінші веб-қосымша (48%) рұқсатсыз қол жеткізу қаупіне ие болды, алайда 2018 жылы мұндай қосымшалардың үлесі 72%-ға дейін өсті. Веб-қосымшалардың 19%-да тек қосымшаны ғана емес, сонымен

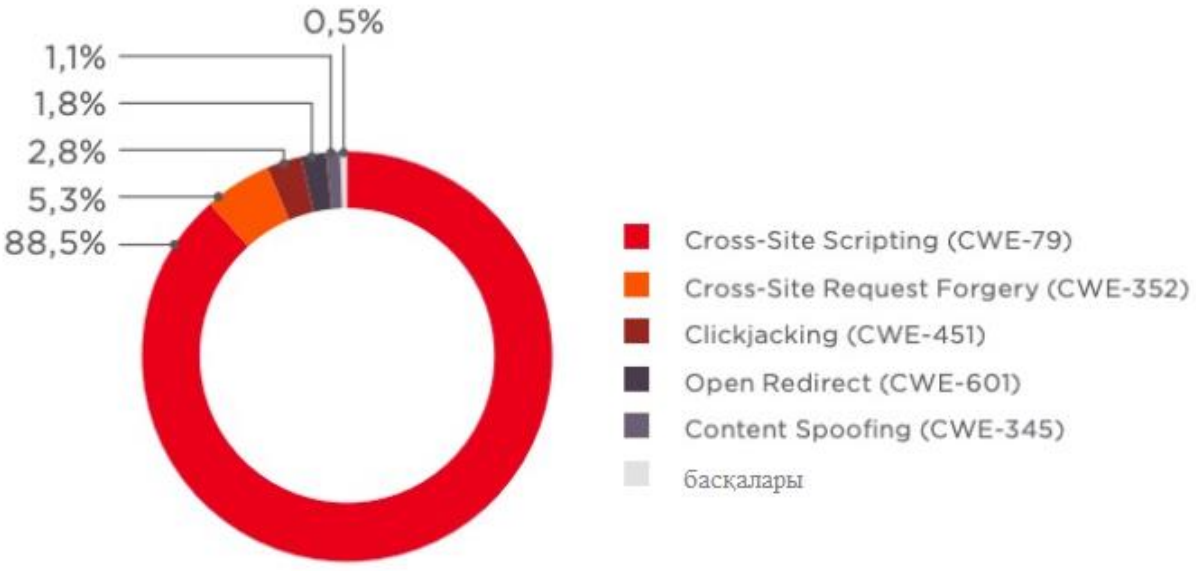
қатар сервер ОЖ үстінен бақылау жасауға мүмкіндік беретін қауіпті осалдықтар табылды. Егер сервер ұйымның желілік периметрінде болса, онда оның компрометациясы корпоративтік ресурстарға шабуыл жасауға мүмкіндік береді. Алайда, ЖЕЖ-ге шабуылдар веб-қосымшаның серверін толық бақылаусыз да жүзеге асырылуы мүмкін. Мысалы, "сервер тарапынан сұранымды қолдан жасау" осалдығы (Server-Side Request Forgery, SSRF) АЖЖ сканерлеуге және ішкі ресурстарға жүгінуге мүмкіндік береді (Сурет 11).



Сурет 11 – Ең кең таралған қауіптер (жүйелер үлесі)

Мысалы, British Airways әуекомпаниясы қосымшасының 380 мың пайдаланушысы төлем карталарының деректері JavaScript тілінде зиянды сценарийді енгізу нәтижесінде ұрланған. Инцидент салдарынан авиатасымалдаушының акциялары 3,8% - ға төмендеді, ал компанияның өзі 500 млн фунт стерлингке дейін айыппұл төлеген [2].

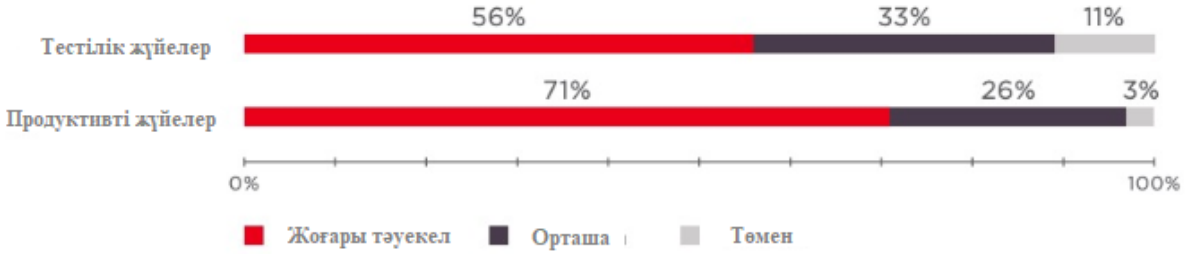
Бұрынғысынша, әрбір веб-қолданбада пайдаланушыларға шабуыл жасауға мүмкіндік беретін осалдықтар бар. Көптеген жағдайларда, бұрынғыдай, бұл "сценарийлердің сайттағы орындалуы" (Cross-Site Scripting, XSS). Алайда, соңғы жылдары бұл осалдықтың үлесі айтарлықтай болды (өткен жылғы 77,9%-ға қарсы 88,5%). Мұндай бір осалдылық ауыр зардаптарға әкелуі мүмкін, бұл бүкіл әлемге таралатыны ақиқат (Сурет 12).



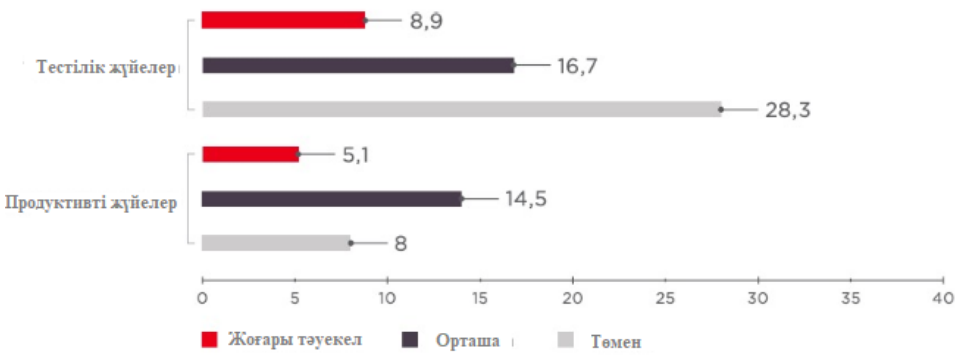
Сурет 12 – Пайдаланушыларға шабуыл жасауға мүмкіндік беретін осалдықтар

1.4 Тестілік және продуктивті жүйелерді салыстыру

Зерттеу нәтижелері бойынша жоғары деңгейдегі тәуекел осалдығы бар өнімді жүйелер үлесінің үш есеге дейін артқанын байқауға болады (2017 жылғы 25%-дан 2018 жылы 71%-ға дейін). Сонымен қатар, бір веб-қосымшадағы осалдықтардың орташа саны бірнеше есе артты; бұл тестілік жүйелерге де, өнімді жүйелерге де қатысты (Сурет 13, 14) [3].



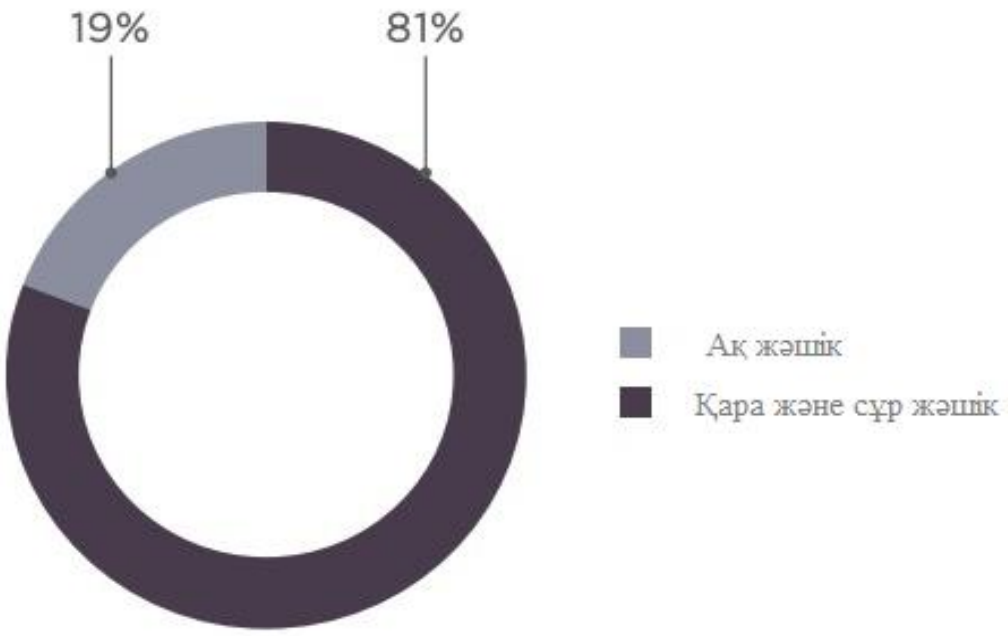
Сурет 13 – Тәуекелдің ең жоғары деңгейі бойынша жүйелердің үлесі



Сурет 14 – Бір жүйеге осалдықтардың орташа саны

1.5 Тестілеу әдістерін салыстыру

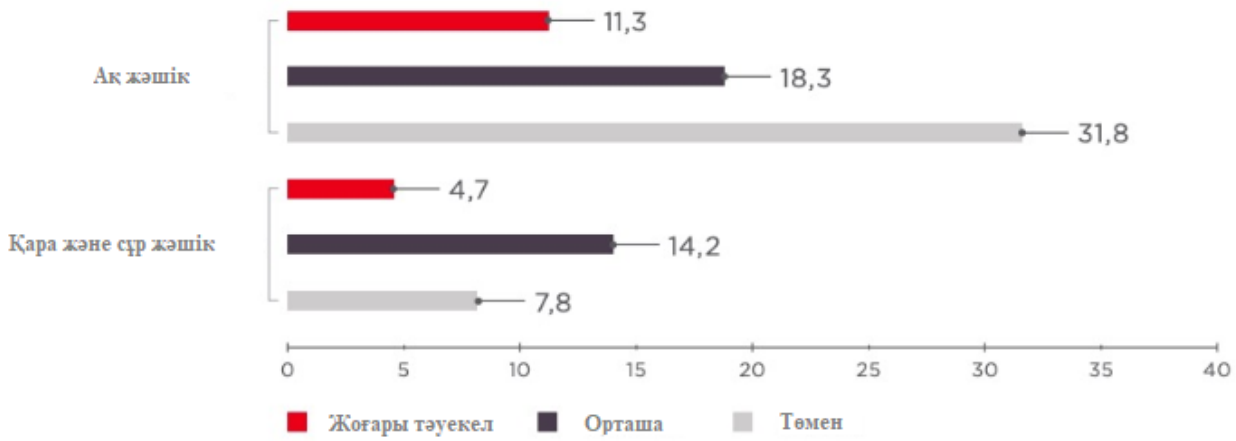
Тестілеу әдістерін салыстыру жыл сайын веб-қосымшаларды ақ жәшік әдісімен талдаудың жоғары тиімділігін растайды. Мысалы, зерттеушілердің бастапқы кодқа қол жеткізуі болған кезде бір жүйеде анықталған қауіпті осалдықтар саны сұр және қара жәшіктің әдістерімен тестілеу кезіндегіге қарағанда айтарлықтай көп. Атап айтқанда, ақ жәшік әдісімен тестілеу кезінде кодты (A1 – Injection) енгізудің анықталған осалдықтарының саны 3 есе өседі (Сурет 15). [3]



Сурет 15 – Тестілеу әдістері

Зерттеу нәтижелері бойынша көптеген веб-қосымшалардың қорғалу деңгейі төмен деген қорытынды жасалған. Бұл ретте қорғалу деңгейі өте төмен веб-қосымшалардың үлесі өткен жылмен салыстырғанда екі есе дерлік өсті, ал осалдықтардың жекелеген санаттары үшін бір жүйедегі осалдықтардың орташа саны бірнеше есеге артқан.

Сайтта тіркеле отырып, пайдаланушы ресурс иелеріне өз деректерін сеніп тапсыруға мәжбүр, ал жеке деректер өңделетін веб-қосымшалардың 18% - да олардың ағып кету қаупі бар (Сурет 16).



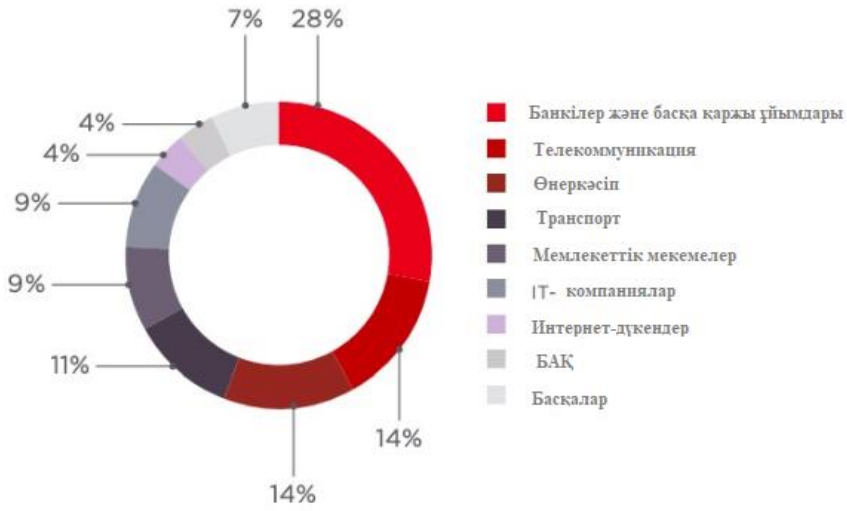
Сурет 16 – Бір жүйеге табылған осалдықтар саны

Веб-қосымшалардың қауіпсіздігін тиімді қамтамасыз ету үшін олардың қорғалуына талдау жасау ұсынылады. Бастапқы кодтың болуы (ақ жәшік әдісімен тестілеу) кибершабуылдарды күтпестен осалдықты анықтауға және одан әрі жоюға мүмкіндік бере отырып, талдауды неғұрлым тиімді етеді. Бұл ретте атап өту қажет: мұндай талдаудың тұрақтылығы маңызды, өйткені тек жүйелі тәсіл жүйедегі осалдықтар санын азайтуға және оларды жоюға арналған ресурстарды оңтайландыруға мүмкіндік береді.

Зерттеу нәтижелері жоғары деңгейдегі тәуекел осалдығы тестілік және өнімді жүйелерде де бар екенін айтады. Веб-қосымшаның қорғалуын талдау оны әзірлеудің ең ерте кезеңдерінен бастап анықталған осалдықтарды жою шығындарын төмендетіп қана қоймай, оның тиімділігін арттырады.

Ең қауіпті осалдықтарды қоса алғанда, 83% осалдықтарды түзету үшін веб-қосымшаны әзірлеуші бағдарламалық кодқа өзгерістер енгізуге тырысады. Веб-бағдарламаны ішінара қайта өңдеу компаниядан Елеулі ресурстарды талап етуі мүмкін. Веб-қосымшалардың жаңа релизін шығаруға қажетті уақыт ішінде бизнес-үдерістерді бұзу тәуекелін төмендету үшін арнайы шешімдерді, атап айтқанда, қосымшалар деңгейіндегі желіаралық экрандарды (web application firewalls, WAF) пайдалануды ұсынады. Тек веб-қосымшаларды қорғаудың кешенді тәсілі табысты кибершабуылдардың тәуекелін барынша азайтып, клиенттердің ақшасын және сенімін сақтауға мүмкіндік береді.

Зерттеу бойынша: 43 веб-қосымшалар 2018 жылы талдаған, өнімді жүйелердің үлесі – 79% -ды құраған (Сурет 17).



Сурет 17 – Зерттеу қатысушыларының портреті

1.6 Осалдықтарды анықтау әдістемелері

Есеп 43 толық функционалды веб-қосымшаларды зерттеу нәтижелерін қамтиды, олар үшін 2018 жылы тексерулердің толық жабындысы бар тереңдетілген талдау жүргізілді. ДБО жүйесіне кіруге тестілеу, аспаптық сканерлеу және зерттеу бойынша жобалардың нәтижелері статистикаға енгізілмеген: бұл ақпарат басқа Талдамалық есептерде ұсынылған. Сонымен қатар, іріктеуде иелері зерттеу мақсаттарында қорғауды талдау нәтижелерін пайдалануға өз келісімін бермеген жүйелер ұсынылмаған.

Қорғауды бағалау қосымша автоматтандырылған құралдарды пайдалана отырып, қара, сұр және ақ жәшіктің әдістерімен жүргізілді. Қара жәшіктің әдісі сыртқы шабуылдаушы тарапынан ол туралы иеленушіден қандай да бір қосымша ақпаратты алдын ала алмай ақпараттық жүйенің қорғалуын бағалау жөніндегі жұмыстарды жүргізу болып табылады. Сұр жәшік әдісі ұқсас, бірақ тәртіп бұзушы ретінде жүйеде белгілі бір артықшылықтары бар пайдаланушы қарастырылады. Ақ жәшік әдісімен талдау кезінде ақпараттық жүйенің қорғалуын бағалау үшін қосымшалардың бастапқы кодын қоса алғанда, ол туралы барлық қолда бар деректер пайдаланылады.

Анықталған осалдықтар Common Weakness Enumeration (CWE) жүйесі бойынша жіктелген. Оқырманның ыңғайлылығы үшін осалдықтардың жоғары дәрежелеріне байланысты олардың ішінен OWASP Top 10-2017 рейтингіне кіретіндерді бөліп, зерттеген веб-қосымшаларда қаншалықты жиі кездесетініне талдау жасалған. [4]

Бұл құжатта тек веб-қосымшалардың коды мен конфигурациясындағы қателерге қатысты осалдықтар ғана бар. Ақпараттық қауіпсіздіктің басқа да кең таралған проблемалары (мысалы, БҚ жаңартуларын басқару процесінің кемшіліктері) қаралмайды. Статистикада OWASP Top 10-2017 рейтингінің A10-Insufficient Logging & Monitoring санатындағы осалдықтар да ескерілмеген, өйткені веб-қосымшалардың қорғалуын талдау бойынша жұмыстарды жүргізу шекаралары шеңберінде журналистиканың және

мониторингтің жеткіліктілігі бағаланбаған. Осалдықтар тәуекелінің дәрежесі Common Vulnerability Scoring System (CVSS v. 3) осалдықты анықтау әдістемесімен талданған; Осы бағалау негізінде жоғары, орташа және төмен тәуекел деңгейлерінің сапалық бағалары бөлінді.

1.7 Веб-қосымшалардың осалдығы және оларға төнетін қауіптер

Қосымшаларды әзірлеу кезінде әзірлеушінің негізгі күш-жігері әдетте талап етілетін функционалдылықты қамтамасыз етуге бағытталған. Бұл ретте бағдарламалық кодтың қауіпсіздігі мен сапасы мәселелеріне жеткілікті көңіл бөлінбейді. Нәтижесінде веб-қосымшалардың басым көпшілігі әртүрлі деңгейдегі сыни осалдықтардан тұрады.

HTTP хаттамасының қарапайымдылығы веб-қосымшаларды автоматты талдаудың және осалдықтарды анықтаудың тиімді әдістерін әзірлеуге мүмкіндік береді. Бұл бұзушының жұмысын айтарлықтай жеңілдетеді, одан кейін олардың ең қызықты шабуыл жасауға осал веб-сайттардың көп санын анықтауға мүмкіндік береді.

Сонымен қатар, кейбір типтегі осалдықтар тек автоматты түрде анықтау ғана емес, сонымен қатар автоматты түрде пайдалануға да жол береді. Осылайша, зиянды кодты веб-ресурстарға жаппай енгізу жүргізіледі, ол содан кейін Интернет желісінің қарапайым пайдаланушыларының жұмыс станцияларынан бот-желілерді құру үшін пайдаланылады. Веб-қосымшаларды пайдаланушылардың жұмыс орындарына шабуыл жасауға арналған платформа ретінде пайдалану мүмкіндігі осы қосымшаларды бұзушының өзі үшін тартымды мақсат етеді.

Осылайша, компанияның ақпараттық инфрақұрылымына шабуыл жасау кезінде тәртіп бұзушылар бірінші кезекте оның веб-қосымшаларын зерттейді. Интернет желісінен қол жетімді веб-қосымшаларда осалдықтар тудыруы мүмкін Тәуекелді жете бағаламау олардың көпшілігінің қорғалуының төмен деңгейінің негізгі себебі болуы мүмкін. [4]

Жоғарыда келтірілген OWASP (коммерциялық емес ұйым – Open Web Application Security Project) өз зерттеуінен кейін он ең қауіпті, бірақ сонымен қатар интернет пен веб-сервистерде бағдарламалық қамтамасыз етуде кең таралған осалдықтардың тізімін ұсынды. OWASP пікірінше, бұл осалдықтарға өзін және өз клиенттерін хакерлерден қорғағысы келетін мемлекеттік және коммерциялық ұйымдарға аса назар аудару керек. Барлық көрсетілген осалдықтар кең таралған, ал оларды тіпті біліктілігі аз хакерлердің күшімен пайдалану жеткілікті, өйткені тиісті бұзу құралдарын Интернет желісінде табу оңай.

1) Injection (кез келген инъекции, олар SQL, LDAP жәгне т.б.);

2) Cross Site Scripting (өзектілігін жоймаған XSS);

3) Broken Authentication and Session Management (аутентификация және сессияларды басқару сәулетіндегі);

4) Insecure Direct Object References (қорғалмаған ресурстар мен объектілер);

5) Cross Site Request Forgery (CSRF);

6) Security Misconfiguration (қоршаған ортаның, әртүрлі фреймворктардың, платформаның қауіпсіз конфигурациясы);

7) Failure to Restrict URL Access (ерекше артықшылықтарды талап ететін функционалға рұқсатсыз қол жеткізу – мысалы, WordPress-тегі блокты басқаруға қолжеткізу үшін URL-де қос «//» слэштің көмегімен тексеруді айналып өту);

8) Unvalidated Redirects and Forwards (ашық редиректтер, нәтижесінде фишинге, HTTP Response Splitting және XSS-ке әкеп соғады);

9) Insecure Cryptographic Storage (маңызды деректерді қауіпсіз сақтау болмайды);

10) Insufficient Transport Layer Protection (транспорттық деңгейде оларды беру кезінде деректерді жеткіліксіз қорғау, мысалы HTTPS –тің орнына HTTP бойынша вместо HTTPS).

Веб-қолданбалар ұшырайтын ең танымал осалдықтар кластарын қарастырайық.

1.7.1 PHP-инъекция

PHP – динамикалық веб-беттерді жасау үшін қолданылатын ең танымал бағдарламалау тілдерінің бірі. PHP-инъекциялар шабуылшыға осал веб-серверде ерікті кодты орындауға мүмкіндік береді. Мысал:

include($page . ‘somefile.php’);

Егер қаскүнем мына түрдегі сұранысты орындайтын болса:

http://victim.com/index.php?page=http://evil.com/

Онда шабуылдаушы бақылайтын веб-серверінің файлы жүктеледі және орындалады.

1.7.2 SQL-инъекция

Мәліметтер базасынан ақпарат алу үшін көптеген қосымшалар SQL тілінде сұраныстарды пайдаланады. Кіріс деректерінің дұрыстығын тексеру дұрыс іске асырылмаған немесе жоқ болған жағдайда, және бұл деректер SQL-сұраныстағы параметр ретінде пайдаланылады, шабуылдаушы ақпаратқа рұқсатсыз қол жеткізе алады немесе аутентификация процесін бұзуы мүмкін. Белгілі бір SQL конфигурацияларында-инъекция қашықтағы жүйеде еркін кодты орындауға әкелуі мүмкін. Кодты қарастырайық:

$query = “SELECT * FROM users WHERE name = ‘” + $user + “’”;

Егер қаскүнем $user параметрі ретінде келесі қатарды берсе:

‘ or ‘a’=’a

Нәтижесінде ДҚБЖ өңдейтін сұраныс мынадай түрге келеді

SELECT * FROM users WHERE name = ‘’ or ‘a’=’a’

бұл аутентификацияны айналып өтуге мүмкіндік береді, өйткені екінші шарт әрдайым ақиқат. [5]

1.7.3 Скриптерді сайтаралық орындау

Зиянкестер белгілі бір веб-ресурста басқа Пайдаланушының құқығын алу үшін қолданатын ең көп таралған әдіс-скрипттерді (cross site scripting, XSS) сайтаралық орындауды пайдалану. Бұл осалдықтар алдыңғы сияқты,

кіріс деректерін жеткіліксіз сүзумен байланысты, бұл жағдайда HTML тілі элементтері мен JavaScript коды.

Мұндай осалдықтардың екі негізгі класы бар: шағылысқан және сақталған. Көрсетілгендер сұранымның мәтініне қосылған шабуыл жасалған код қолданбасының контекстінде (мысалы, мекен-жай URL параметрлерінің бірінде) орындау болып табылады. Шабуыл сәтті орындау үшін зардап шегуші арнайы құрылған сілтеме бойынша өтуі тиіс. Егер қате екіншіге қатысты болса, яғни ең қауіпті класқа жататын жағдайда, зиянкестер енгізген код серверде сақталады және осал бетке кірген әрбір пайдаланушының браузерімен орындалады. [5]

1.7.4 CSRF – Сайттағы сұраныстарды қолдан жасау

CSRF (англ. Cross Site Request Forgery – «Сайттағы сұраныстарды қолдан жасау», XSRF ретінде танымал)

HTTP протоколының кемшіліктерін пайдаланатын, веб-сайттарға келушілерге шабуылдар түрі. Егер жәбірленуші қаскүнем құрған сайтқа кірсе, оның атынан құпия түрде зиянды операцияны жүзеге асыратын басқа серверге (мысалы, төлем жүйесінің серверіне) сұраныс жіберіледі (мысалы, қаскүнем шотына ақша аудару)). [6]

1.7.5 Cross-Site Scripting осалдығы

Бұл бағдарламалық қамтаманың (Web-қосымшалардың) осалдығының бір түрі, бұл ретте сервермен генерацияланған бетте клиенттің шабуыл жасау мақсатында зиянды скрипттер орындалады. Қазір XSS барлық анықталған осалдықтардың 15 % - ын құрайды. Көп уақыт бойы бағдарламашылар оларды қауіпсіз деп санай отырып, оларға тиісті көңіл бөлмеді. Дегенмен, бұл пікір қате: бетте немесе HTTP-Cookie-де өте осал деректер болуы мүмкін (мысалы, әкімші сессиясының идентификаторы). Танымал сайтта скрипт DoS-шабуыл жасай алады (Кесте 1.1).

Кесте 1.1 – Веб-қосымшалар қауіпсіздігіне төнетін қауіптердің жіктелуі

№	Қауіптер түрі	Қауіпке мысалдар	Қауіп салдары
1	Web-қосымша кодындағы осалдықтарды пайдаланумен байланысты қауіптер	SQL-инъекцялар XSS-шабуылдар PHP-инъекция Сайтаралық сұраныстарды қолдан жасау – CSRF	Файлдарға және web-қосымшалар ДҚ-ға рұқсатсыз қол жеткізу, ақпараттың құпиялылығы мен тұтастығын бұзу

1.1-кестенің жалғасы

2	Желілік шабуылдар	Web-қосымша клиентінің браузеріне шабуылдар. Парольдерді іріктеу және пайдаланушыларды аутентификациялау жүйесіне шабуылдар. Web-қосымшалар сервистеріне қызмет көрсетуден бас тарту. Желіні сканерлеу. Ерекше жағдайларды шақыру	Файлдарға және web-қосымшалар ДҚ-ға рұқсатсыз қол жеткізу, пайдаланушының компьютеріне қол жеткізу, ақпараттың қол жетімділігін, құпиялылығын және тұтастығын бұзу
3	Кездейсоқ сипаттағы қауіп	Бағдарламалық-аппараттық құралдардың істен шығуы және бұзылысы шығуы. Табиғи апаттар	Web-қосымшалар ақпараттары мен сервистеріне қол жетімділікті бұзу, қаржылық шығындар
4	Алаяқтық	Спам-тарату. Фишинг. Міндеттемелерден және жасалған әрекеттерден бас тарту. Авторлық құқықты бұзу	Қаржылық және дайындық шығындары

Web-қосымшалардың ең көп таралған шабуылдары желілік шабуылдар болды (web-қосымшалар клиенттерінің браузеріне (26%), web-қосымшалар сервистеріне қызмет көрсетуден бас тарту – (22%), пайдаланушыларды аутентификациялау жүйесі – (18%). Бұл ретте шабуылдардың көпшілігі зиянды бағдарламалық қамтамалар арқылы іске асырылған,

тек Касперский веб-антивирусы 28483783 бірегей зиянды объектілерді тапты: сценарийлер, эксплойттар, орындалатын файлдар және т. б.

Осыған орай, қорғауды келесі бағыттар бойынша құру ұсынылады:

- web-қосымша кодының қауіпсіздігін әзірлеудің барлық өмірлік циклі бойына бақылау;

- клиенттің компьютері мен web-сервер арасында ақпаратты беру кезінде қорғауды қамтамасыз ету;

- ақпаратты клиенттің компьютерінде қорғауды қамтамасыз ету;

- web-сервер деңгейінде ақпаратты қорғаудың мамандандырылған құралдарын пайдалану.

Бұл төмендегілерді қолдану арқылы қол жеткізіледі

қорғау құралдары мен әдістерін:

- әзірлеу кезінде скриптерде қателерге жол бермеу;

- web-қосымшалар;

- осалдықтардың болуына web-қосымшаның кодын сканерлеу және арнайы су белгілерін орнату;

- (мысалы, Trend Micro Deep Security, XSpider көмегімен);

- қолданушыларды көп факторлы аутентификациялау жүйелерін пайдалану (мысалы, құпия коды бар парольдік аутентификация, E-num, сертификаттар, сандық қолдар, биометриялық аутентификация);

- вирусқа қарсы бағдарламалық қамтамасыз етуді қолдану;

Осылайша, Web-қосымшалардағы осалдықтар әлі де ақпаратты қорғауды қамтамасыз етудің кең таралған кемшіліктерінің бірі болып қала береді. Web-қосымшалардың қорғалу проблемасы Web-қосымшаларды әзірлеу кезінде осы жүйелердің ішкі және сыртқы қауіптерден қорғалуымен байланысты мәселелер жиі ескерілмейтінімен де, не осы процеске жеткілікті назар аударылмауымен де күрделене түседі. Бұл өз кезегінде АҚ проблемалары жоба аяқталғаннан кейін жүйе иесінің көзіне түсетін жағдайды туындатады. Ал құрылған Web-қосымшадағы осалдықтарды жою оны әзірлеу мен енгізу кезіндегі бюджеттің неғұрлым Шығыс бабы болып табылады. [6]

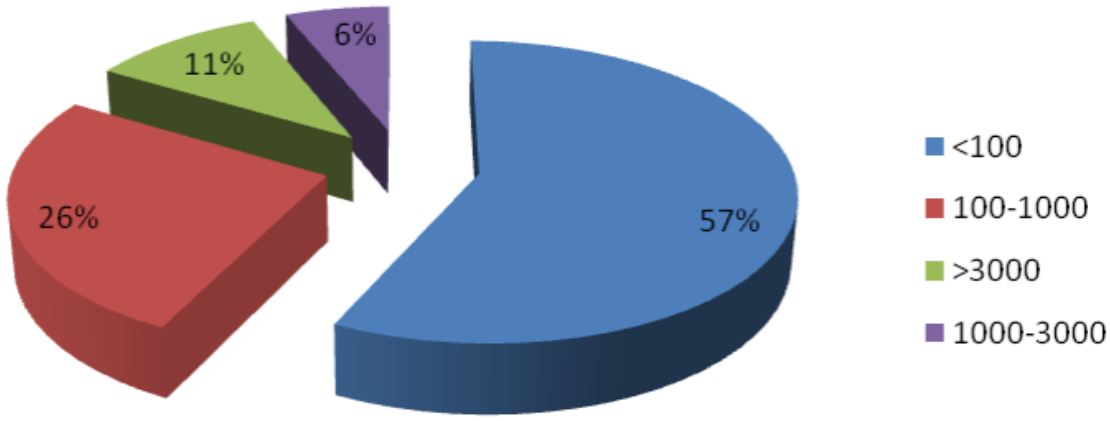
Интернет желісі тарапынан қол жетімді Web-қосымшаларды пайдалана отырып, ақ қауіптерін іске асыру тәуекелінің маңыздылығын жете бағаламау олардың көпшілігінің қорғалу жағдайының ағымдағы төмендігінің негізгі факторы болуы мүмкін.

2 Қауіпсіздік сканерлерін зерттеу, талдау

Қазіргі уақытта көптеген ұйымдардың қызметі олардың ақпараттық жүйелерінің жағдайына байланысты. Ұйымның АТ инфрақұрылымы бизнесті жүргізу тұрғысынан сыни түйіндер мен жүйелерді жиі қамтиды, олардың қол жетімділігін бұзу айтарлықтай зиян келтіруі мүмкін. Мұндай жағдайларда, әдетте, тәуекелдерді тиісті талдаудан кейін өзекті қауіптердің тізбесі қалыптастырылады және оларды бейтараптандыру жөніндегі шаралар кешені әзірленеді. Нәтижесінде ақпараттық қауіпсіздікті басқару жүйесі құрылады,оның құрамына қажетті қорғаныс механизмдерін іске асыратын әртүрлі қорғаныс құралдары кіреді. Кейде ақпараттық қауіпсіздікті басқарудың жалпы жүйесінің құрамына ұйымдық-техникалық іс-шаралар кешені болып табылатын және ақпараттық жүйелердің қорғалуын бақылауға және анықталған осалдықтарды жоюға арналған осалдықтарды анықтау жүйесі кіреді. Қорғалу жағдайын бақылау превентивті қорғаныс механизмдерінің санатына жатады. Оның басты мақсаты – қорғалатын жүйедегі әлсіздікті (осалдықты) уақытылы "байқап отыру", осылайша оны пайдалана отырып, мүмкін болатын шабуылдарды болдырмау. Осалдықтарды іздеуді қолмен немесе автоматтандырылған қауіпсіздік сканерлері арқылы жүзеге асыруға болады. Қазіргі уақытта тексеруді қашықтықтан, желі арқылы орындайтын желілік қауіпсіздік сканерлері кең тараған. [7]

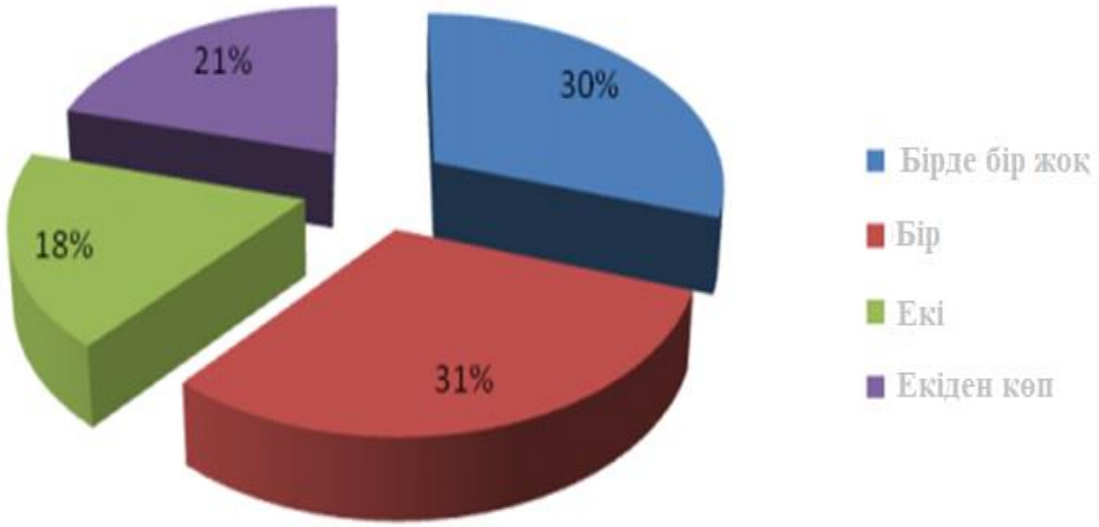
2.1 Қауіпсіздік сканерлерінің қолданылу мақсаты мен міндеттері туралы талдау

Портал арқылы салыстыру алдында Securitylab.ru олар үшін қолданылатын сканерлер мен міндеттер туралы деректерді жинау мақсатында сауалнама жүргізген. Сауалнамаға 500-ге жуық респондент қатысты (Securitylab.ru). Ұйымдағы компьютерлер саны бойынша респонденттердің портретін талдау (сурет. 5) сұралған респонденттердің ең көп үлесі (57%) шағын бизнеске (100 компьютерден кем) қатысты екендігін көрсетті. Саны бойынша екінші топ респонденттер ұйымда 100-ден 1000-ға дейінгі компьютер санатына түсті (26%). Үшінші және төртінші топтар – ірі бизнес пен федералдық мемлекеттік құрылым өкілдері болып шықты. 3 000-нан (11%) астамы үшінші және 1 000 – 3 000 (6%) төртінші топқа арналған компьютерлер. Сауалнамаға қатысқан өте ірі бизнес өкілдері (3000-нан астам компьютер) бизнес көлемі оларға қарағанда азырақтармен (ұйымдағы компьютерлер саны 1000-3000) салыстырғанда 5% - ға артық болды (Сурет 18).



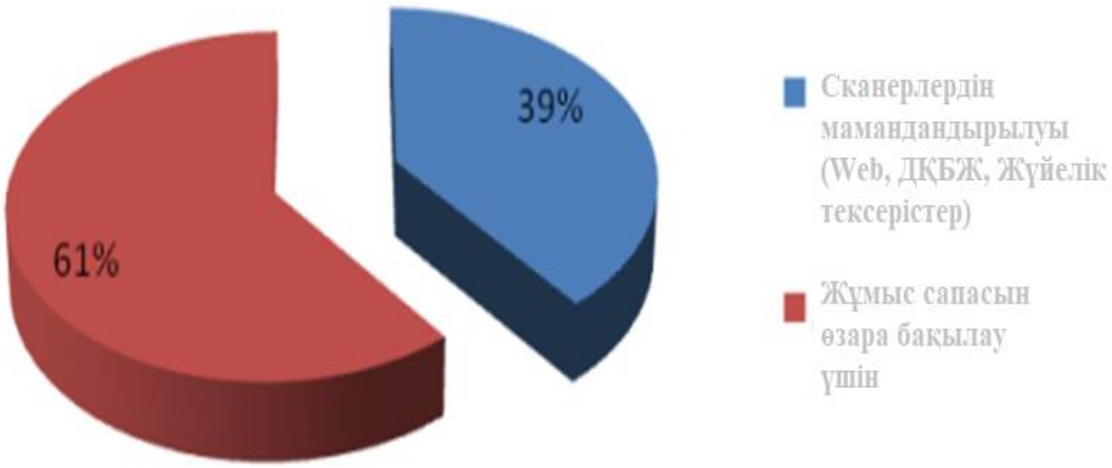
Сурет 18 – Респонденттерді ұйымдағы компьютерлер саны бойынша бөлу

Өз ұйымдарында қолданылатын қауіпсіздік сканерлері туралы сұраққа респонденттердің басым көпшілігі ең болмағанда бір қауіпсіздік сканерін (70%) пайдаланатыны туралы жауап берді. Бұл ретте, өздерінің ақпараттық жүйелерінің қорғалуын талдау үшін қауіпсіздік сканерлерін жүйелі түрде қолдануды тәжірибеге енгізген ұйымдарда осыкластың біреуден артық өнімін пайдалануды қалайды. Респонденттердің 49 % - ы олардың ұйымдарында екі және одан да көп қауіпсіздік сканерлерінің пайдаланылатынын көрсетті. (Сурет 19).



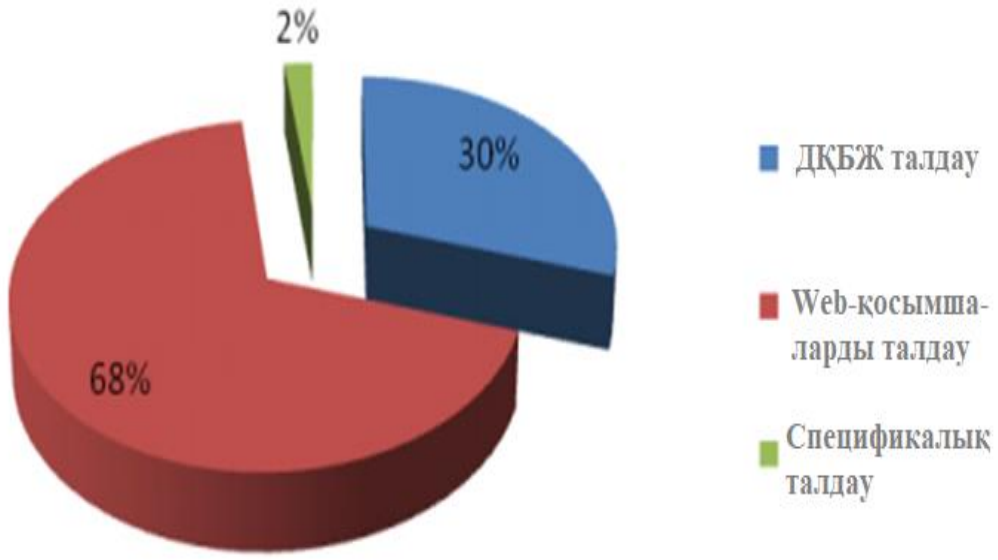
Сурет 19 – Пайдаланылатын қауіпсіздік сканерлерінің саны бойынша сұралған респонденттер ұйымдарын бөлу

Біреуден артық қауіпсіздік сканері пайдаланылатын себептер, ұйымдар бір "вендор" (61%) шешімдеріне , сондай-ақ Кешенді қауіпсіздік сканері орындай алмайтын мамандандырылған тексерулерді орындау қажет болған жағдайларға (39%) сенімсіздікпен қарайды. (Сурет 20).



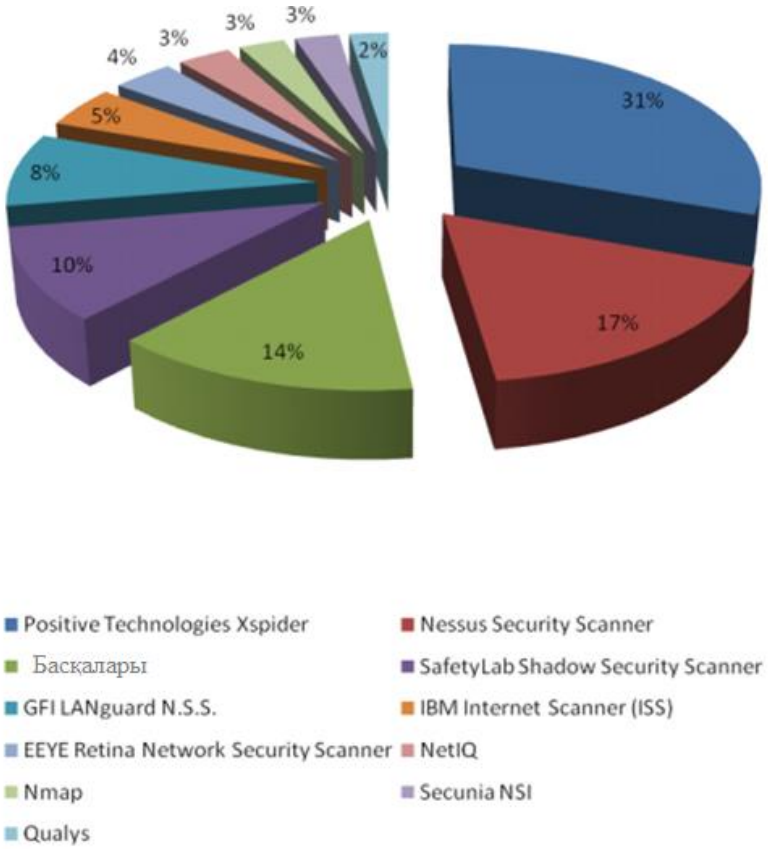
Сурет 20 – Сұралған респонденттердің ұйымдарында біреуден артық қауіпсіздік сканерін пайдалану себептері

Арнайы қауіпсіздік сканерлері қандай мақсаттар үшін пайдаланылатыны туралы сұраққа жауап бере отырып, респонденттердің көпшілігі Web-қосымшалардың қорғалуын талдаудың қосымша құралдары ретінде пайдаланылатынына жауап берді (68%). Екінші орында, ДҚБЖ қауіпсіздігінің мамандандырылған сканерлері (30%), ал үшінші орында (2%) ақпараттық жүйелердің қорғалуын талдау бойынша міндеттердің арнайы шеңберін шешу үшін жеке әзірлеменің утилиттері болды (Сурет 21).



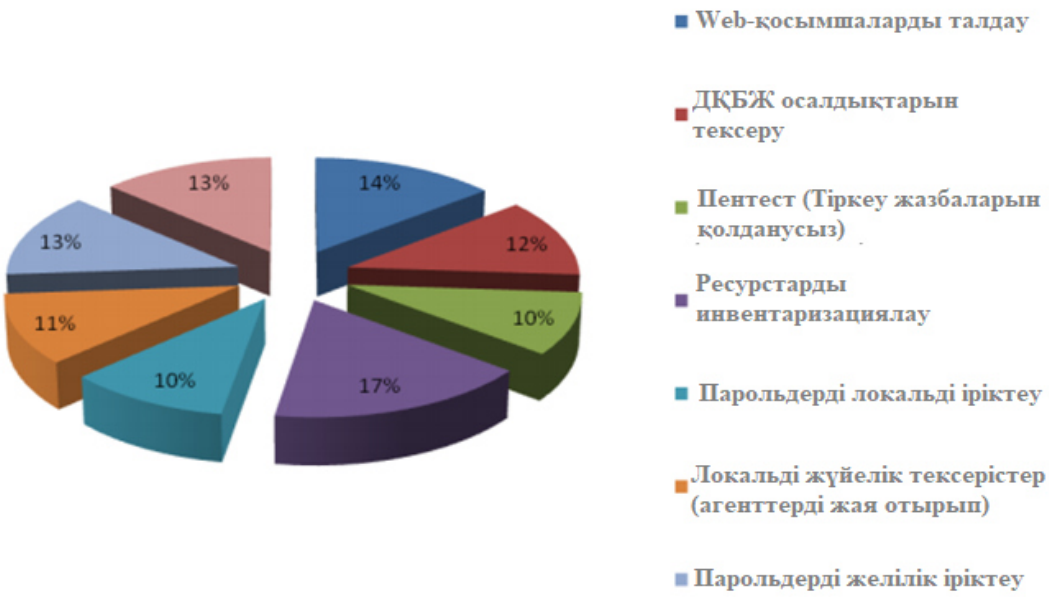
Сурет 21 – Сұралған респонденттер ұйымдарында мамандандырылған қауіпсіздік сканерлерін қолдану мақсаттары

Қауіпсіздік сканерлеріне қатысты соңғы өнімдер туралы респонденттерден сұрау нәтижесі (Сурет 22) көптеген ұйымдардың Positive Technologies XSpider (31%) және Nessus Security Scanner (17%) өнімін пайдалануды қалайтынын көрсетті. [7]



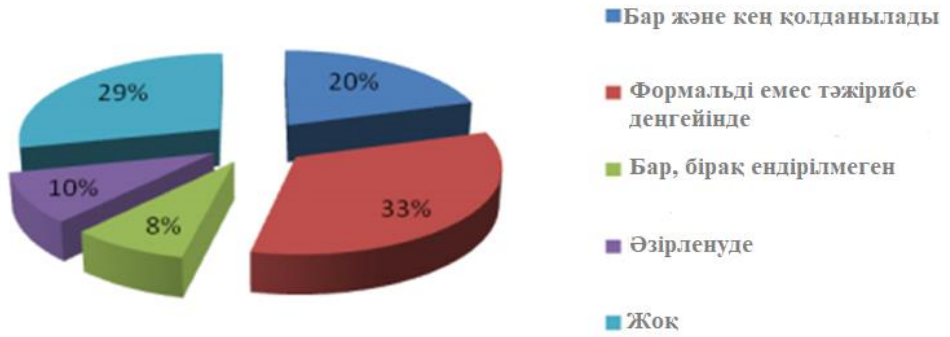
Сурет 22 – Сұралған респонденттер ұйымдарында қолданылатын қауіпсіздік сканерлері

Келесі сұрақ, "сіз қолданатын сканерлеу механизмдері қандай?", қауіпсіздік сканерлері қолданылатын міндеттер шеңберін көрсетеді (Сурет 23).



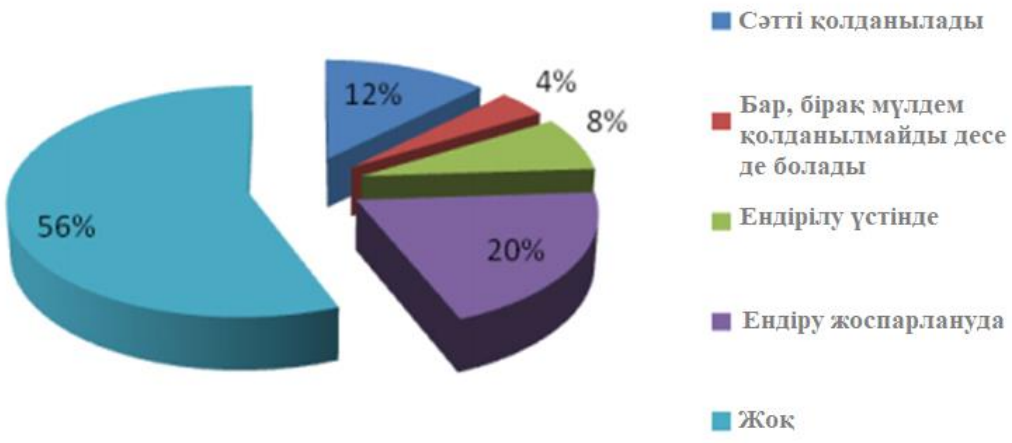
Сурет 23 – Сұралған респонденттер ұйымдарында қолданылатын сканерлеу тетіктері

Ақырында, соңғы екі сұраққа жауаптар стандарттарға (корпоративішілік немесе халықаралық) сәйкестігін бақылау міндетімен жағдайды сипаттайды. Бұл міндет қауіпсіздік сканерлеріне тән емес, бірақ соңғы уақытта оған сұраныс үлкен. "ұйымда жүйелер мен қосымшаларды қауіпсіз күйге келтіру бойынша стандарттар бар ма? сұрағына жауаптар былай беріліп отыр" (Сурет 24).



Сурет 24 – Ұйымдарды жүйелер мен қосымшаларды қауіпсіз күйге келтіру жөніндегі стандарттардың болуы бойынша бөлу

Яғни, көп жағдайларда (71%) қандай да бір стандартқа сәйкес келу әрекеттері жасалады. Ал " ұйымда жүйелер мен қосымшаларды қауіпсіз күйге келтіру бойынша стандарттарға сәйкестікті бақылауды автоматтандыру құралдары пайдаланыла ма?"респонденттердің басым бөлігі (56%) теріс жауап берді (Сурет 25).



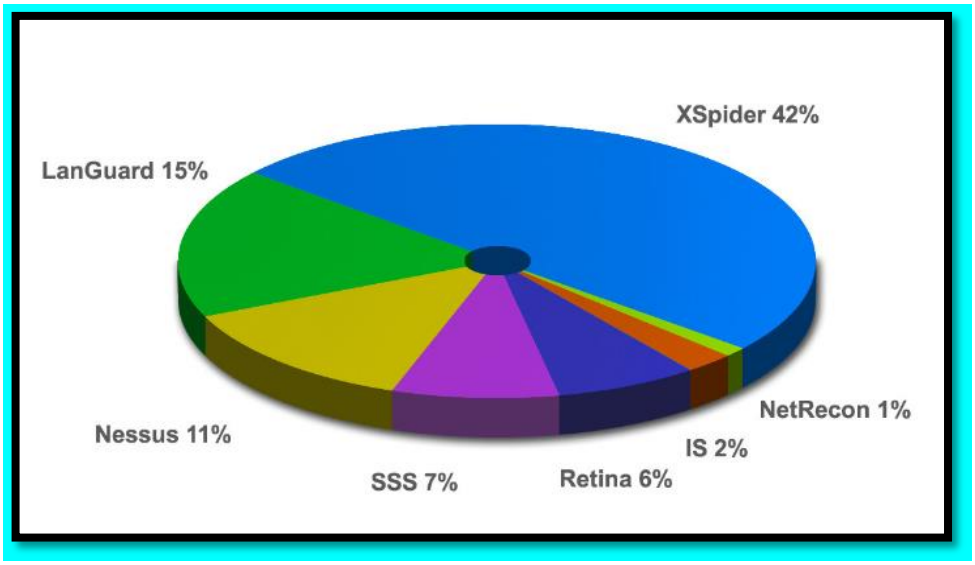
Сурет 25 – Стандарттарға сәйкестікті бақылауды автоматтандыру құралдары пайдаланыла ма? сұрағына диаграмма

Осы ұйымның әр кезеңдегі зерттеулері нәтижесінде xSpider сканерінің қолдану саласы, оның тиімділігі үнемі артық көрсеткіштер беріп отырған.

Сканер тек веб-қосымшаларды тексеріп қана қоймайды, оның жалпы жүйені, әсіресе желіні сканерлеудегі мүмкіндіктері өте үлкен.

үшін оның төрт түрі сынақтан өткізілген (Сурет 26):

- xSpider
- Internet Scanner
- Nessus
- Retina Network Security Scanner



Сурет 26 – Желінің бұзуға төтеп бергіштігін тексеру режимінде сканерлерді сынау көрсеткіші

2.2 Қауіпсіздік сканерлерінің жұмысы, жұмыс нәтижелерін талдау

2.2.1 Төзімділікке желіні тесттен өткізу режимінде салыстыру күрделілігі (ерекшеліктері)

Нақтыға максимальды жуық жағдайда сканерлеуді салыстыру нақты нақты нәтиже берері сөзсіз.

Екінші жағынан, мұндай салыстырудың шектеулі мүмкіндіктерін де түсіну керек. Мысалы, сканерлеу уақыт бойынша созылып кетті, себебі сканерлер кезекпен қолданылуда. Осы уақыт ағымында түйіннің қорғалу деңгейі өзгеріп кетуі мүмкін. Нәтижелердің дұрыстық деңгейін жоғарылату үшін сканер тапқан қызмет түрлерінің тізімі «ортақ» түрге келтіріліп, тек сканерлердің әрқайсысы тапқан желілік қызметтер ғана қалдырылады.

2.2.2 Баллдарды есептеу тәсілі

Барлық сканерлер бірдей тексеру жасай бермейді, сондықтан егер бір сканер осалдықты таппаса, ал екіншісі тапса, онда мынадай тұжырымдар жасалады:

- осал жер бар, және сәйкес тексеру болғанымен, бірінші сканер оны анықтай алмады;
- осал жер бар, және бірінші сканер оны анықтай алмады, себебі оны анықтауға тырысқан да жоқ;

- осал жер табылмады, себебі сканер ондай тексеруге ие емес – (-1 балл);

- осал жер табылмады, бірақ осал жер бар және сәйкес тексеру жүргізілді (осалдықты өткізіп алу, false negative) – (-1 балл);

- осал жер табылды, бірақ шын мәнінде ондай жер жоқ (жалған әрекет, false positive) – (-1 балл). [8]

Осылайша, қателер үшін «айып құндар» есептеледі, сонан соң осал жердің жалпы санынан (барлық сканерлермен табылған) алынып тасталатын болады. Алынған мән сканер сапасының көрсеткіші болып табылады. Сканерлер жалпы бес көрсеткіш бойынша салыстырылады:

- сканерлеу сапасы;

- жалған өңдеулерді алып тастағандағы табылған осал жерлер саны (қате табылған осал жерлер);

- қате табылған осал жерлер саны;

- қате өткізіліп жіберілген осал жерлер саны;

- базада тексерудің болмауы себебінен өткізіліп кеткен осал жерлер саны.

Енді сөзіміз қате болмас үшін баллды есептеуге бірнеше мысалдар келтірелік:

2.3 Хосттарды тексеру, түйіндердегі осалдықтарды анықтау

2.3.1 (host1. test) түйінінің баллдарын есептеуге мысал

Алдымен барлық сканерлермен табылған анық порттарды іріктеп алу керек. Бұл жағдайда барлық төрт сканер тек бір ашық порт – TCP:53 тапқан, яғни тесттен өткізілетін түйін DNS серверін білдіреді.

Барлық сканерлер тапқан осал жерлерді кестеге енгізу қажет (кесте-4). Жалпы сканерлер үш осалдық тапты:

- рекурсивті сұраныстарды қолдау;

- инверсті сұраныстарды қолдау;

- сәйкес сұраныс бойынша зоналарды алу мүмкіндігі.

Кестедегі алғашқы үш қатар – бұл табылған осалдықтар.

Тексергеннен кейін мына жағдай белгілі болды, үш осалдық та шын мәнінде 1.1. түйінінде болып шықты. Сондықтан «нақты (Реально)» бағанында үш осалдықтың әрқайсысы үшін «бірлер» тұрады.

Енді сканерлердің қайсысы «тапсырманы орындады», осыған талдау жасау қажет.

DNS серверінің рекурсивті сұраныстарды қолдайтынын (CVE-1999-0024)XSpider сканері анықтады.

Internet Scanner (IS) мұндай тексеруді орындамайды (бұл үшін оған 1 айып құн есептелген, бұл фактыны жасыл түспен белгілейміз). Nessus және Retina сканерлері бұл тексеруді орындайды, бірақ олар рекурсияны қолдамайды (бұл үшін оған бір айып құ белгіленеді де, бұл факт қызыл түспен белгіленеді). Осылайша, егер сканер осалдықты базада жоқ болу себепті таба алмаса, кестенің сәйкес ұяшығы жасыл түспен белгіленеді. Егер осалдықты

өткізіп алу – қатенің кесірінен болса, кесте ұяшығы қызыл түспен белгіленеді. Кез келген жағдайда, осал жерді өткізіп алуда 1 балл кемиді. Егер сканер осал жер тапса, шын мәнінде онда осал жер болмаса, бұл үшін де 1 балл шегеріледі, ал сәйкес ұяшық сары түспен белгіленетін болады. [8]

Инверсті сұранысты қолдауды (iguery) тек IS сканері тапты, қалған сканерлер мұндай тексеруге ие емес.

DNS серверінен зонаны беру мүмкіндігін тек IS және Nessus тексереді. Осылайша, 4-кестенің алғашқы үш қатары толтырылады. Енді баллдарды есептеу қажет. Бұл үшін осалдықтың жалпы санынан (біздің жағдайымызда) «айып» баллдар азайтылады. XSpider сканері үшін үш мүмкін болатыннан (3-1-1) 1 балл шығады, IS сканері 2 балл алады және т.с.с.

Кестенің тағы бір қатары – «Баллдардың қорытындысы» толтырылады. Нақты, бұл көрсеткіш – әрбір сканердің сканерлеу модулінің сапа көрсеткіші.

Келесі қатарда («Осалдықтар табылды») жалпы қанша осалдықтардың табылғаны жөнінде ақпарат беріледі. Біздің жағдайымызда, нәтиже жалған өңдеулердің жоқтығына байланысты алдыңғы қатармен сәйкес келеді. Жалған өңдеу (False Positives) жоқ, сондықтан кестенің келесі қатары нөлді қамтиды (бұл «сары» ұяшықтар саны). Қателердің кесірінен өткізіп алулар саны келесі қатарда көрсетіледі – бұл «қызыл ұяшықтар» саны.

Соңында, соңғы көрсеткіш – базада тексерудің болмау себебінен өткізіп алулар саны – «жасыл» ұяшықтар саны.

2.3.2 (host2. test) түйінін тексеру

Түйінді тексеруде қолданылған сканерлердің әрқайсысының жұмыс нәтижелері әртүрлі болатыны белгілі. Сканердің жұмыс нәтижесінде есептер құрылатынын жоғарыда айтып кеттік. Олардың есепті қорытындыдағы көрсеткіштеріне толық талдау жасамай, қысқаша ғана бірнеше кесте түрінде көрсетіп кетсек жеткілікті (Сурет 27, 28).

Уязвимости	Риск	CVE	XSpider	IS	Retina	Nessus	Реально
EhloCheck: SMTP daemon supports EHLO	низкий	CAN-1999-0531	-1	1	-1	-1	1
iquery: DNS server inverse queries	средний		-1	1	-1	-1	1
zonexfer: DNS honors zone transfer requests requests	средний	CAN-1999-0532	-1	1	-1	-1	1

Сурет 27 – 2.host2.test түйін осалдығы

Уязвимости	Риск	CVE	XSpider	IS	Retina	Nessus	Реально
Рекурсия	средний	CVE-1999-0024	1	-1	-1	-1	1
Итого			**1**	**3**	**0**	**0**	
Найдено уязвимостей			1	3	0	0	
False Positives (ложное обнаружение)			0	0	0	0	
False Negatives (пропуск)			0	0	2	2	
False Negatives (отсутствие в базе)			3	1	2	2	

Сурет 28 – 2.host2.test түйін осалдығы

Бұл түйінде (host1. test) түйін үшін табылған осалдықтан айырмашылығы, SMTP қызметін қолдау (EHLO командасы) мүмкіндігі табылды. Берілген түйін бойынша қысқаша деректер:

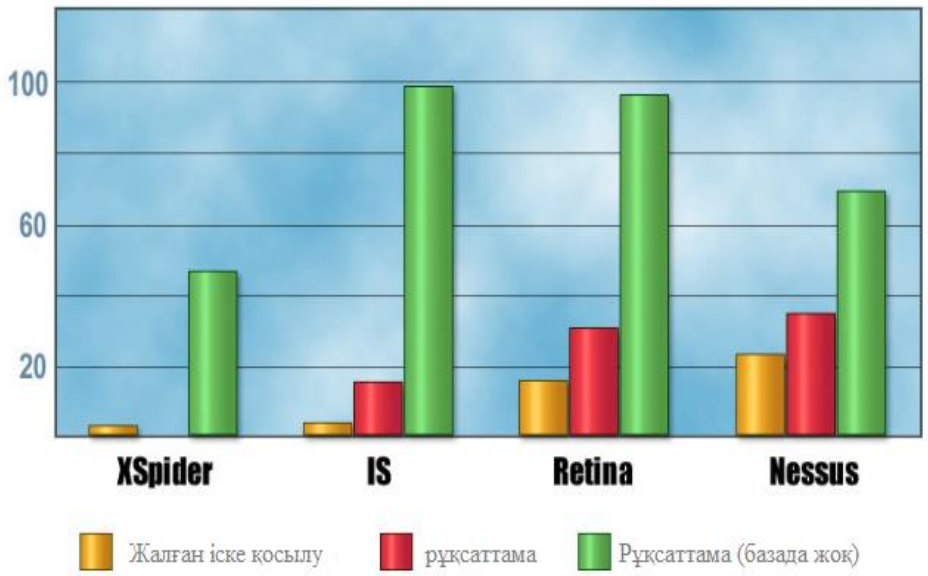
- XSpider төрт мүмкін болатыннан бір осалдық тапты;
- Internet Scanner – 3;
- Retina – 0;
- Nessus – 0;

Жалған осалдық табу аңғарылған жоқ (Сурет 29).

Уязвимости	Риск	CVE	XSpider	IS	Retina	Nessus	Реально
Доступен метод TRACE	низкий		1	1	1	1	1
Apache cookie: Apache cookies buffer overflow	высокий		0	-1	0	0	0
Apache-SSL Client Certificate Forging	низкий	CVE-2004-0009	0	0	-1	0	0
Итого			**1**	**0**	**0**	**1**	

Сурет 29 – (host3. test) тексеру

Бұл жағдайда жалған осалдық табу аңғарылды, бұл әрекет сары түспен боялған (Сурет 30).



Сурет 30 – сканерлер жұмысының нәтижелік көрсеткіштерінің диаграммасы.

Осы диаграмма арқылы сынақтан өткен 4 сканердің жұмысына толық көз жеткізуге болады. [8]

2.3.3 Қауіпсіздік сканерлерін салыстыру көрсеткіштері, тиімдісін таңдау

Жалпы зерттеулер және талдаулардың нәтижесінде бірнеше сканерлердің жиі қолданылатынын байқауға болады. Сканерлердің бағасы, қолдайтын жүйелері, интерфейсі, сканерлеу мүмкіндігі, сервистер мен қосымшаларды сәйкестендіру, сканерлеу нәтижесі бойынша есеп құрастыру,

жаңарту тиімділігі, техникалық қолдау сияқты бөлімдер бойынша жиі қолданылатын бірнеше сканерлер таңдалады (Кесте 2.1).

Кесте 2.1 – Осалдықтар сканерлерін салыстыру

Сканер	Nessus	Retina	XSpider	IS
Бағасы	131400 р/жыл	72000 р/жыл	Хосттардың санына байланысты, 14000-млн р-ға дейін	Құны IP мекенжайларының санына байланысты өзгереді (номинал — 6000 р)
Қолдайтын жүйелері	Кроссп латфор малық ПҚ	Cisco, Linux, UNIX, Windows	Windows XP/Server 2003/Vista/2008/2008 R2/7 және т.б.	Windows, AIX, HP-UX, Linux и Solaris
Интерфейстің достығы	Қарапайым және түсінікті интерфейс	Түсінікті интерфейс	Достық және түсінікті интерфейс	Түсінікті интерфейс
Сканерлеу мүмкіндігі	Сканерлеудің мүмкін нұсқалары: SYN scan, FIN scan –таза FINзапрос; Xmas Tree-сұранымға FIN, URG, PUSH; Null scan, FTP bounce scan, Ident scan, UDP scan және т.б. кіреді.	Осалдықтарды анықтау ену сынағының көмегімен, ал тәуекелдерді бағалау және оларды азайту басымдығын анықтау — пайдалану мүмкіндігін бағалау негізінде жүргізіледі. Осалдықтар (Core Impact, Metasploit, Exploit-db), CVSS және басқа да факторлардан).	**XSpider** веб-бағдарламашылар құрған кодты тексере алады, пошта, веб-серверлер, операциялық жүйелер, деректер қорының серверлері және желіде жұмыс істейтін басқа да сервистер осалдықтардың, қарапайым немесе бос парольдердің, баптаудағы қателердің және т.б. болуын тексере алады. Қауіпсіздікті талдау барысында хост шексіз санын жүздеген тексеру орындалуы мүмкін	FTP, LDAP және SNMP тексеру; электрондық поштаны тексеру; RPC, NFS, NIS және DNS тексеру; "Қызмет көрсетуден бас тарту" түріндегі шабуылдарды жүзеге асыру мүмкіндігін тексеру»; "парольді таңдау" (Brute Force) түріндегі шабуылдардың болуын тексеру; web-серверлер мен CGI-скрипттерді, web-браузерлерді және X-терминалдарды тексеру; желіаралық экрандар мен proxy-серверлерді тексеру; қашықтан қол жеткізу сервистерін тексеру; және т.б.
Сервистер мен қосымшаларды сәйкестендіру	Сервистер мен қосымшаларды сәйкестендіру процедурасын сапалы жүзеге асыру.	ОЖ, қосымшалар, ДҚ, веб қосымшаларды анықтау.	ОЖ, қосымшалар, ДҚ, веб қосымшаларды, порттарды, веб-серерлерді, қолданбалы ПҚ-ды анықтау.	Желілік сервистердің, ОЖ, маршрутизаторлардың, пошта және Web-серверлердің, желіаралық экрандардың және қолданбалы БҚ осалдығын сәйкестендіреді.
Есеп генерациясы	+	+	+	+
Еркін есепті жасау мүмкіндігі	+	-	+	+

Жаңарту жиілігі	Жүйелі, бірақ қолданушылар триал-версияны ала алмайды.	+	Жүйелі жаңарту	Жүйелі жаңарту

2.1 кестенің жалғасы

Техникалық қолдау	+	+	+ орыс тілінде	+

Нәтижесінде қарапайым қолданушыға ыңғайлы сканерлердің бірнеше серияларын интернет-ресурстардан алып, жұмысын салыстыруға мүмкіндік бар екендігіне көз жеткізілді. Nessus сканерін тегін алуға болады, оның да қойылған мақсатқа байланысты қолданылатынына көз жеткізілді. Дегенмен, қорытынды есепті құрастырғанда оның толыққанды мәлімет бере алмайтынына көз жеткізілді. Ол – Ақпараттық жүйелерді қорғауда белгілі кемшіліктерді автоматты түрде іздеу бағдарламасы. Ол осалдықтардың ең жиі кездесетін түрлерін анықтауға қабілетті, мысалы:

- қызметтердің осал нұсқаларының немесе домендердің болуы;
- конфигурациядағы қателер (мысалы, smtp серверінде авторлаудың қажеті жоқ);
- әдепкі парольдер, бос немесе әлсіз парольдер болуы сияқты мүмкіндіктерді жүзеге асырады.

Зерттеу барысында бұл сканерге қарағанда Xspider сканерінің мүмкіндіктерінің кеңдігі, оның жиі қолданылатындығы анықталып, осы сканердің жұмысын кеңірек қарау мақсат етіп қойылды. [9]

Web Application Security Consortium деректеріне сәйкес, осалдықтарды анықтау бойынша XSpider мүмкіндіктерін қамтыған жинақ кестесі берілген (Кесте 2.2) (http://www.webappsec.org/projects/threat/).

Кесте 2.2 – Оалдықтытарды анықтау бойынша XSpider мүмкіндіктерін қамтитын жинақ кесте

Осалдық типі	XSpider қолдауы
Аутентификация	
Іріктеу	Иа (Basic)
Жеткіліксіз аутентификация	Иа
Парольді қалыпқа келтіру қауіпсіз емес	Жоқ, іске асыру тәсілдерінің айырмашылығына байланысты
Авторландыру	
Сессия идентификаторының болжамды мәні	Иә, стандартты қосымшаларда
Жеткіліксіз авторизация	Иә, қолжетімділікті шектеу жүйесіне байланысты
Сессия таймаутының жоқтығы	Жоқ, формализация қиындығына байланысты

Клиенттерге шабуыл	
Құрамын алмастырып жіберу	Иә
Сценарийлерді сайтаралық орындау	Иә, сүзгілерді айналып өту әдістерін қоса алғанда

2.2-кестенің жалғасы

HTTP-жауапты жіктеу	Иә, сүзгілерді айналып өту әдістерін қоса алғанда
Кодты орындау	
Буфердің аса толуы	Иә, стандартты қосымшаларда
Қатарларды форматтау функциясына шабуыл	Иә, стандартты қосымшаларда
LDAP операторларын ендіру	Иә
ОЖ командаларын орындау	Иә
SQL операторларын ендіру	Иә, "соқыр" опцияны қоса алғанда
Серверлік кеңейтілулерді ендіру	Иә
XPath операторларын ендіру	Иә, "соқыр" әдісті қоса алғанда
Ақпаратты жария ету	
Директорияны индекстеу	Иә
Қосымшаны идентификациялау	Иә
Ақпараттың шығуы	Иә, нәтижелерді қолмен талдаумен бірге
Директориядағы кері жол	Иә
Ресурстардың болжамды орналасуы	Иә
Логикалық шабуылдар	
Функционалдық мүмкіндіктерді теріс пайдалану	Жоқ, формализация қиындығына байланысты
Қызмет көрсетуден бас тарту	Иә, стандартты қосымшаларда
Автоматтандыруға қарсы жеткіліксіз әрекет	Иә, кейбір жағдайларда
Процесті жеткіліксіз тексеру	Жоқ, формализация қиындығына байланысты

Осылайша Xspider сканерін желіні, веб-қосымшаларды осалдыққа тексерген кезде еркін қолдануға болатындығын көрсетуге болады.

2.4 Неге XSpider таңдалды?

XSpider сканері дегеніміз не? Бұл жүйені тексеру және ақпаратты жинау құралы, процестерді барынша автоматтандыру құралы бар. Бағдарламаны әзірлеу кезінде сарапшылар желіге енудің нақты тәсілдеріне барынша жақын болатын осалдықтарды іздеу алгоритмдері мен тетіктерін жобалады. Mspider әртүрлі деңгейде осалдықтармен жұмыс істейді-жүйеден бастап қолданбалы деңгейге дейін. Атап айтқанда, XSpider қуатты және терең веб-серверлер мен веб-қосымшаларды қорғау анализаторын қамтиды. Егер соңғы уақытқа дейін осы өнімді пайдалану үшін оны сатып алу және өз компьютеріңізге немесе жергілікті желіге орналастыру қажет болса, кейінгі уақытта бағдарламаның

соңғы нұсқасын пайдалануға негізделген Mspider online – сайттарын тексеруге арналған онлайн сервис пайда болды. [9]

Осы сервистің көмегімен веб-қолданбалар мен веб-серверлердің қорғалуын тексеру жергілікті орнатылған бағдарлама арқылы ортануға ұқсас тексеруге болады. Әрине, шектеулер бар. Мысалы, жергілікті желіде орналасқан және одан тыс шығу мүмкіндігі жоқ (яғни жаһандық IP-мекенжайы жоқ) ресурстарды тексеру мүмкін емес. Мұндай ресурстарды осы желі ішінде ғана тексеруге болады (Сурет 31).

Сурет 31 – Орындалатын тапсырмалар тізімін баптау

Ресурстарды сканерлеу кезінде алуға болатын нәтижелер туралы айтпас бұрын, сервисті пайдаланудың артықшылықтары мен кемшіліктеріне тоқталған жөн. Артықшылықтарға осы қызметтер үшін төлемнен кейін сервисті пайдалану мүмкіндігі сияқты сәттерді жатқызуға болады (компьютерді бөлу, бағдарламаны орнату және баптау қажет емес). Осалдықтар деректер қорын жаңарту қажеттілігі болмайды – жаңартулар сервисте автоматты түрде орындалады және оның мүмкіндіктерін пайдаланатын барлық адамдарға қол жетімді. Бағдарламаның өзін жаңартуға қатысты: әзірлеушілер жаңартуды өз бетінше орындайды.

Нәтиже алу үшін пайдаланушыларға ең аз параметрлерді орындау қажет

Сонымен қатар, бағдарламаны анықтау қажет емес – нәтиже алу үшін ең аз баптаулар жеткілікті. XSpider online қызметі жергілікті желіден тыс, сондықтан сіздің желіге сырттан кіруден қорғауды тексеру үшін өз компьютеріңізді одан тыс жерде орнатудың қажеті жоқ. Ал бұл, өз кезегінде, сканерлеу жүргізуге жұмсалатын трафиктің төмендеуіне әкеледі. Бірнеше ресурстарды сканерлеу, кез келген желі нүктесінен міндеттерді басқаруға және кез келген уақытта және кез келген компьютерден нәтижелер алуға болады.

Бұл плюс. Бірақ сервис мүмкіндіктеріне тікелей қатысы жоқ кемшіліктер бар. Веб-ресурстарыңызды сканерлеу, ұйым үшін осалдығын анықтау не ену, не оның жұмыс істеуін бұзу үшін осы сервисті

қолданбайтынына ешқандай кепілдік жоқ. Сонымен қатар, алынған нәтижелер таныстарымен ғана таратылып қана қоймай, ашық қол жетімді болуы мүмкін. Егер бұл нәтижелерді бірінші болып сканерленген сервис иелері көрсе, ал жоқ болса? Әрине, мұндай сканерлеу XSpider бағдарламасының көмегімен де орындауға болады, бірақ бұл жағдайда сканерлеу жүргізілген компьютердің IP – мекенжайы "іздері" қалады. Сервисті пайдалану кезінде барлық іздер соған апарады, ал оның пайдаланушылары қандай да бір ресурсты сканерлеуді кім орындағаны туралы ақпарат беруге сервис иелері міндетті емес.

Ал енді сервис мүмкіндіктеріне және оның көмегімен алуға болатын нәтижелерге жүгінеміз. Сервис өз желілік ресурстарының қауіпсіздігін тұрақты негізде тексергісі келетін пайдаланушыларға бағытталған. Сервистің негізгі мүмкіндіктері мен қасиеттері жұмыстың осындай сценарийімен жобаланған. Сервистің типтік пайдаланушысы болып аптасына 1-2 рет 1-20 хостқа аудит жүргізетін пайдаланушы саналады. (Тексеруді кез келген күнге жоспарлауға болады, ортадан басқа – бұл сервистің техникалық қызмет көрсету күні.) Бірақ осы күні есептерді қарауға, өз міндеттерін реттеуге болады (Сурет 32).

Сурет 32 – Тапсырмаларды
редакциялау

Жұмысты орындау үшін негіз тапсырма болып табылады. Тапсырма – бір сканерлеу профилін пайдалана отырып, бірыңғай кесте бойынша сканерленетін желілік адрестер тізімі. Шектеу: бір тапсырмада 64 хосттан артық болуы мүмкін емес, бірақ есептер саны шектелмейді. Әрбір пайдаланушының кем дегенде бір тапсырмасы бар, оны түзете алады, бірақ жою мүмкін емес. (Ал тапсырмаға ең болмағанда бір хост енгізілгеннен кейін сканерлеуді орындау уақытын толық қалдыруға болмайды.)

Профильді таңдау хостты сканерлеу кезінде шешетін міндеттерге байланысты

Программамен жұмыс істегенде пайдаланушы өз бетінше тексеру параметрлерін баптай алады, таңдалған Хоста тексерілуі тиіс мәселелерді анықтай алады. Сервисті пайдаланушылардың жұмысын жеңілдету үшін әзірлеушілер профильдер деп аталатын үш стандартты баптауларды

дайындады. Осылайша, профиль – бұл белгілі бір жағдайда оңтайлы нәтиже алуға арналған параметрлер жиынтығы. Профильдер барлығы үшін бірдей және оларды редакциялау мүмкіндіктері пайдаланушыларда жоқ.

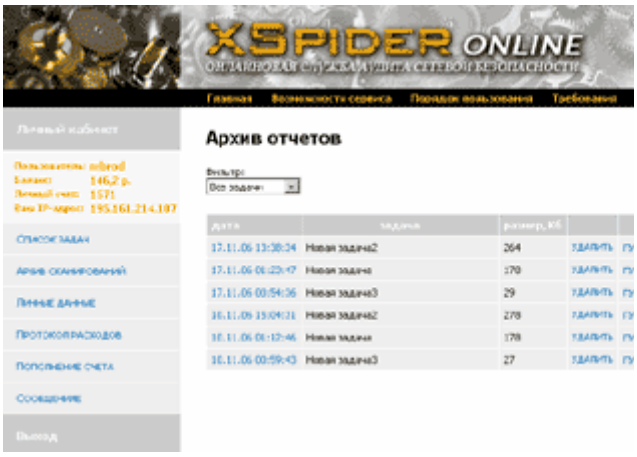
Пайдаланушыда рұқсат етілген үш профильдердің бірін таңдау мүмкіндігі бар:

- экспресс-барлық ықтимал қызметтерге толық талдау жасалады. стандартты емес dos-шабуылдарға тексеру жүргізілмейді. веб-қосымшаларды тексеру шектеулі көлемде – ең типтік қауіп-қатерлер бойынша жүргізіледі;

- веб-қосымша-веб-скрипттердің барлығын терең талдауды қамтамасыз етеді. басқа сервистер мен веб-қосымшаның жүйелік бөлігін талдауды қамтымайды;

- максималды-барлық интеллектуалды алгоритмдерді пайдалана отырып, барлық сервистерді толық тексеру, соның ішінде веб-қосымшаларды терең талдау.

Тіркелгеннен кейін пайдаланушының міндетіне төрт мекенжайды тегін қосу мүмкіндігі бар. Мұндай мүмкіндік тек бір рет беріледі – барлық келесі қосылулар, тіпті егер бірден екі мекен-жай қосылған болса да, ақылы негізде жүргізіледі. Сервисті пайдалану-ақылы, Абоненттік төлем негізінде. Бұдан басқа, сканерлеу нәтижелері бойынша базаға орналастырылған әрбір есеп үшін төлем алынады. Есеп құны таңдалған профильге және есептегі хост санына байланысты. "Экспресс" профиліндегі әрбір хост үшін сканерлеудің ең аз құны, ең көбі – "максимал"профилінде (Сурет 33).



Сурет 33 – Есептер мұрағатының көрінісі

Тапсырманы баптау кезінде сізге тек профильді таңдау керек, сканерлеу орындалатын күн (немесе күндер) мен уақытты таңдау керек, есептер жіберілуі мүмкін пошта мекенжайын анықтау керек. Бұл мүмкіндік-қосымша, өйткені кез келген жағдайда есептер базада сақталады және оларға кез келген уақытта қол жеткізуге болады. Базаға орналастырылған әрбір есеп жүйеге кірмей, оны сырттан көру мүмкіндігі үшін сілтеме алады, сондықтан сіз есепті

қызметкерлерге немесе достарға жібермеуге, оларға қарау үшін сілтеме беруге болады.

Сканерлеу тереңірек болған сайын, оған уақыт қажет. Бірақ сервис жұмысы сіздің қатысуыңызды талап етпейді

Әрбір міндет бойынша сервис тапсырмаға қосылған барлық хостар бойынша сканерлеу кезінде табылуы мүмкін барлық осалдықтар туралы толық есеп береді. Сканерлеу орындалатын уақыт жеткізушілермен реттелмейді, ол тексерудің тереңдігі мен егжей-тегжейіне байланысты. Қалыптасқан есептің басында сканерлеудің жиынтық деректері – осалдықтар саны және олардың қауіптілік дәрежесі, әртүрлі деңгейдегі осалдықтар саны және анықталған қауіптілік деңгейі бойынша хостыларды бөлу ұсынылады.

Бұдан әрі есепте анықталған осалдықтар тізбесі және олардың толық ашылуы (осалдықтың сипаттамасы, осындай осалдықтың анықталған БҚ нұсқасы, осалдықты пайдалану мүмкіндігі, осалдықты жою бойынша шешім және қосымша ақпарат көздеріне сілтеме) келтіріледі. Кейбір жағдайларда зиянкестердің табылған осалдығын пайдалану мысалы да келтірілуі мүмкін. (Әдетте, ашық ақпарат бар жағдайларда.) Осылайша, пайдаланушыға өз сервисінің сенімділігін бағалау және кемшіліктерді жою жөнінде шешім қабылдау мүмкіндігі беріледі (Сурет 34, 35).

Сурет 34 – Түрлі деңгейлі қауіпсіздіктер осалдықтары

Сурет 35 – Түрлі дәрежелі қауіпсіздіктер осалдықтары

Мысалы, көптеген осалдықтар PHP-да әзірленген қозғалғыштарды пайдаланумен байланысты. Төменде -алынған есептің мысалы берілген. Анықталған осалдықтар жоғары қауіптілік деңгейіне жатқызылған - буфердің толып кетуі(PHP) деген атпен белгілі.

Қысқаша сипаттамасы

Осалдық қашықтағы пайдаланушыға қызмет көрсетуден бас тартуға немесе мақсатты жүйеде еркін кодты орындауға мүмкіндік береді.

Толық сипаттамасы

Осалдық "htmlentities()" және "htmlspecialchars ()"функцияларындағы деректер шекараларын тексеру қателігінен орын алады. Қаскүнем арнайы құрылған PHP деректерін осал функцияларды пайдаланатын қолданбаға бере алады, буфердің толып кетуіне және мақсатты жүйеде еркін кодты орындай алады.

Осал нұсқалар

PHP 5.1.6 және алдыңғы

PHP 4.4.4 және алдыңғы

Осалдықты пайдалану

Осалдықты қашықтан пайдалану: иә

Осалдықты Жергілікті пайдалану: иә

Жалған іске қосу (False Positives)

Осалдықтың болуы туралы қорытынды сканерленетін тораптағы сервистер мен қосымшаларды сәйкестендіру нәтижелері бойынша нұсқа негізінде жасалған. Егер жаңартуды орнату кезінде нұсқа нөмірі өзгермесе, осалдықты жалған анықтау мүмкін.

Шешім

http://www.php.net/downloads.php,

CVE (CVE-2006-5465): http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5465;

Bugtraq (Bid 20879): http://www.securityfocus.com/bid/20879 Securitylab: http://www.securitylab.ru/vulnerability/276352.php

Мұнда барлығы бар - сипаттама, және бұл сервис жұмысындағы осалдықты және осалдықты жою жолдарын сипаттайтын мәліметтерді қамтиды. Мұндай ақпаратты алғаннан кейін осы қауіпті жою үшін шаралар қабылдау және өзінің қызметін қайтадан қорғауға тексеру ғана қалады. Бірнеше тексеру циклдары сенімділіктің жоғары дәрежесімен қамтамасыз етеді.

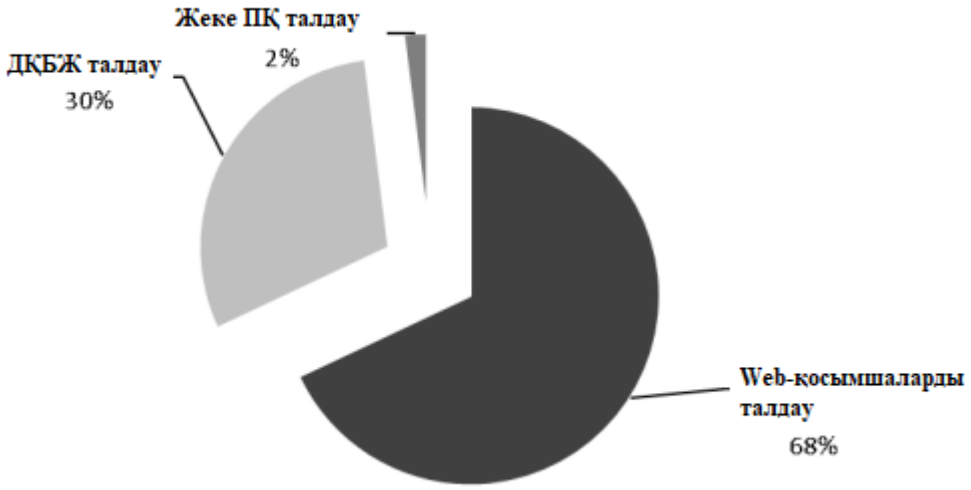
Артықшылықтары:

- ыңғайлы да көрнекі көптерезелі интерфейс;
- қауіпсіздік мониторингі процесін тиімді басқару үшін «тапсырмалар» және «профильдер» концепциясын қолдану;
- жұмысты автоматтандыру үшін тапсырмаларды ыңғайлы жоспарлаушы;
- бір мезгілде компьютерлердің үлкен санын сканерлеу;
- TCP байланыс сапасының нашарлығына қарамастан, стандартты пк-дың конфигурацияларына тәуелсіз жұмыс істеуі;
- есептер қалыптастыру (түрлі деңгейді, нақты тәтпіштелген);
- контекстік анықтама мен оқу материалдарын қамтитын құжаттама;
- ОЖ платформаларына бейімділігі;
- аппараттық талаптардың төмендігі;
- лицензиялаудың ыңғайлы сұлбасы, қолданушылардың хосттарды лицензияға өз беттерінше қоса алуы.

2.5 Қауіпсіздік сканерінің бүгінгі таңдағы ахуалы

Бүгінгі АҚ нарығы қауіпсіздік сканерлеріне жататын түрлі өнімдерден тұрады. Олардың көпшілігі белгілі бір технологиялық саладағы осалдықтарды іздеуге бағытталған. Негізінен бұл келесі салалар: - Web-қосымшалар (HP WebInspect, Acunetix Web Vulerability Scanner, Open Source w3af және т.б.); - ДҚБЖ қауіпсіздігі (AppSecInc AppDetective, NGSS, Safety-Lab Shadow Database Scanner және т.б.); - ОЖ және желілік қосымшалар қауіпсіздігі (GFI LANguard Network Security Scanner, Microsoft Baseline Security Analyzer және т.б. Сондай-ақ жоғарыда аталған барлық технологиялық салалардың қорғалуын талдау мүмкіндігін біріктіретін өнімдер бар (Positive Technologies XSpider, TENABLE Nessus, IBM Internet Scanner және т.б.). Осы секілді өнімдерді қолдану (All-in-One) ұйымға салынған инвестициялардан максимальді қайтарым алуға мүмкіндік береді (Return on investment, ROI), оған себеп: - барлық негізгі технологиялық салаларды қамтиды; - Лицензия құны тек бір өніммен шектелген. Сонымен қатар қауіпсіздіктің кешендік сканері қолданысқа көптеп ендірілуде, ол көбінесе сканерлеу жүргізілетін ақпараттық жүйелердегі барлық осалдықтарды дұрыс анықтау қабілетіне байланысты. Мұнда вирусқа қарсы шешімдермен параллель жұмыстар жүргізуге болады. Жалпы ақпарат қауіпсіздігін қамтамасыз етуде қолданылатын сканерлерге талдау жасай келе, Xspider технологиясының кең қолданысқа ие екендігіне, оның қолданылу саласының кең екендігіне назар еріксіз назар аударуға болады. Бұл сканерді кез келген қолданушы өз компьютеріне орнатып, сол ортадағы осал жерлерді анықтауға мүмкіндік ала алады.

Төмендегі диаграммада (33-сурет) ұсынылған статистикаға сәйкес, сауалнамаға қатысқан ұйымдардың көпшілігі осалдықтар сканерін Web-қосымшалардың қорғалуын талдаудың қосымша құралы ретінде (68%) пайдаланады. Компаниялардың үштен бірі деректер қорын басқару жүйелерін сканерлеу үшін (30%) XSpider пайдаланды. Тек бірнеше ұйым (2 %) жұмыс алгоритмінде кемшіліктердің бар-жоғына өз утилиталарын тексеру үшін бағдарламаны пайдаланады (Сурет 36).



Сурет 36 – Xspider-ді қолдану мақсаты

Кез келген ақпаратты қорғау бағдарламасы сияқты, XSpider шетелдік аналогтары бар. Мысалы, желі тораптарының белгілі осалдығын іздеу үшін әзірленген Nessus бағдарламасын ерекше атап өтуге болады. Бұл өнімнің клиент-серверлік сәулеті бар, бұл сканерлеу мүмкіндігін кеңейтуге мүмкіндік береді. Xspider секілді, Nessus та порттарды сканерлеу және порттар пайдаланылатын сервистерді анықтау үшін пайдаланылады. Осалдықты тестілеу NASL (NessusAttackScriptingLanguage) тілінде жазылған плагиндердің көмегімен орындалады. Алайда, ол зияткерлік осалдықтарды іздейді, тек қана Xspider сияқты мерзімділікпен жаңартылып отыратын базалармен салыстырылады. Төмендегі диаграммада (Сурет 37) компаниялардың түрлі сканерлерді пайдалану статистикасы ұсынылған:

Сурет 37 – Осалдықтар сканерлерін пайдалану диаграммасы

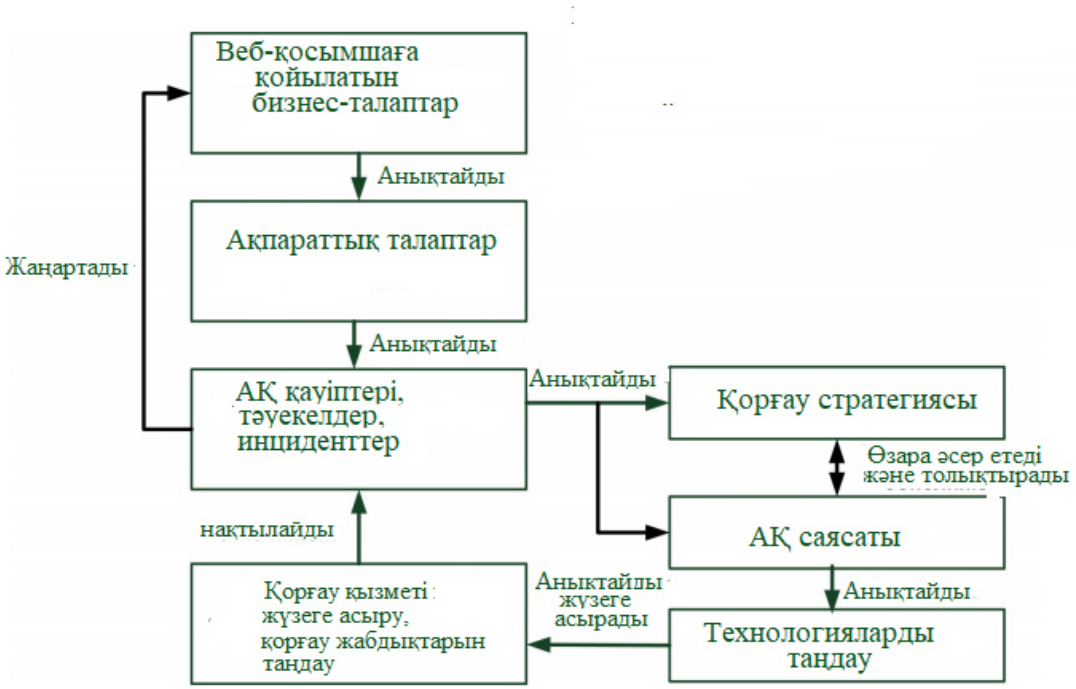
Диаграммада көрсетілгендей, XSpider Ресей нарығында танымал осалдық сканері болып табылады. Бұл ұзақ уақыт бойы жасалып, нарықта өзін көрсете білді. Сондай-ақ, XSpider 7.8.24 нұсқасындағы желілік қауіпсіздік сканері Ресейдің техникалық және Экспорттық бақылау жөніндегі

Федералдық қызметінің 2014 жылғы 24 қазандағы № 3247 сәйкестік сертификатын алды. Сертификат 2017 жылдың 24 қазанына дейін жарамды. Сертификаттау «ақпаратқа рұқсатсыз қол жеткізуден қорғау. 1-бөлім. Ақпаратты қорғау құралдарын бағдарламалық қамтамасыз ету. Декларацияланбаған мүмкіндіктер болмауын бақылау деңгейі бойынша жіктеу» (Ресей Мемтехкомиссиясы, 1999 жыл) — декларацияланбаған мүмкіндіктер мен техникалық жағдайлардың болмауын бақылаудың 4 деңгейі бойынша», сондықтан ол мемлекеттік және муниципалдық мекемелерде қолданылуы мүмкін. [10]

Бүгінгі күні осалдықтардың сканерлері түрлі ақпараттық жүйелердің қорғалуын бақылаудың тиімді құралы болып қалады және Кәсіпорынның корпоративтік желісінде қорғауды құру кезінде, сондай-ақ жұмыс станцияларында жұмыс істеу кезінде пайдалы. Өзекті сканерлердің тұрақты жаңартулары бар осалдықтарды анықтау үшін олардың мүмкіндіктерін тиімді пайдалануға мүмкіндік береді, бұл ақпараттық жүйенің жалпы қорғалуына оң әсерін тигізеді.

3 Қосымшаны қорғау механизмі

Веб-қосымшаға төнетін қауіптерді талдау, қауіптердің алдын алу, болдырмау, олардың пайда болу жолдарын анықтау туралы алдыңғы бөлімдерде айтылғандарды талдай отырып, сол қорғауды бір кешен түрінде ұйымдастырғанның тиімді екенін білуге болады. Сол кешен құрамына кіретін қорғау әдістерін, жабдықтарын және механизмдерін таңдау аса маңызды кезеңдердің бірі ретінде веб-қосымшаны қорғаудың өмірлік циклінде қамтылады. Олардың құрамындар осалдықты анықтау сканерлерінің алатын орны зор (Сурет 38).



Сурет 38 – Қорғалған web-қосымшаны әзірлеудің және сүйемелдеудің өмірлік циклі

Әдетте, веб-қосымшалардың қорғалуын талдау кезінде қауіпсіздік сканерлері келесі міндеттерді шешуге мүмкіндік береді:

- іске асыру немесе конфигурация кезеңдерінде жіберілген дөрекі кемшіліктерді іздеу;
- жақсы белгілі осалдықтарды іздеу;
- қауіпсіздік стандарттарының талаптарына сәйкестігін тексеру.

Қолмен тестілеу барысында жіберілген осалдықтардың жоқтығын тексеру керек. [11]

XSpider жалпы мақсаттағы қауіпсіздік сканері мысалында веб-қосымшалардың осалдығын іздеу әдістері мен механизмдерін қарастырайық.

Веб-қосымшалардың қорғалуын талдау шеңберінде сканер қауіпсіздік XSpider келесі негізгі мүмкіндіктері бар:

- ерікті түрде веб-қосымшаларды автоматты түрде анықтау порттар;

- SSL/TLS отбасы хаттамаларымен жұмыс;
- процесс функциясы бар веб-серверді автоматты түрде индекстеу;
- жасырын директорияларды және файлдардың сақтық көшірмелерін іздеу;
- http-basic аутентификациясын және стандартты емес схемаларды қолдау;
- аутентификация;
- сессияларды автоматты бақылау;
- мазмұны бойынша осал және зиянды сценарийлерді іздеу;
- веб-құжат;
- веб-қосымшалардың негізгі осалдықтарын эвристикалық іздеу.

3.1 XSPIDER-ді қолдану нұсқалары

Егер ашық порттар мен қызметтерді идентификациялау барысында сканирленетін желіде веб-сервер анықталса, сканер оның түріне (мысалы, Apache, IIS, Nginx және т.б.), сондай-ақ орнатылған кеңейтімдерге (ASP, FrontPage және т. б.) сәйкес осалдықтарды іздеуді орындайды.

Келесі кезең веб-қосымшалардың белгілі осалдықтарын аутентификациялау, авторландыру және тексеру болып табылады. Қазіргі уақытта XSpider сканер ядросы үш аутентификация механизмін қолдайды:

- basic;
- NTLM;
- жеке аутентификация схемалары (мысалы, аутентификация-веб-қосымша формасы арқылы беру).

Егер сервер жеке аутентификация механизмдерін пайдаланса, онда екі нұсқаның бірін пайдалануға болады.

Олардың біріншісі-жеке бастапқы сұранысты пайдалану. Бұл жағдайда сканер сайтқа алғаш рет жүгінген кезде қолданылатын HTTP-сұрау салуды көрсетуі қажет. Екінші әдіс әр HTTP-сұраныста жіберілетін аутентификациялық деректері бар (Cookie, X-Auth-Token және т.б. тақырыптары) HTTP тақырыптарын конфигурациялауды және пайдалануды білдіреді. Сұраудың мазмұнын Wireshark, Httpwatch) немесе прокси сервері (Burp Suite сияқты) сияқты кез келген желілік талдаушы арқылы алуға болады.

Содан кейін жасырын директорияларды іздеу және мазмұнды индекстеу механизмі қосылады. Мазмұнды жинау барысында XSpider сканер ядросы веб-беттің гиперсілтемелерінің болуын, сондай-ақ сервердегі түрлі қызметтік және ақпараттық файлдарды (мысалы, robots.txt немесе readme.txt) талдау жасайды. Сайт картасын құрастырғаннан кейін сканер бағдарлама консолінде табылған осалдықтарды іздеу режиміне өтеді.

1-қадам. Сынақ қауіпсіз веб-қосымшаны ашу. XSpider сканерін іске қосу. "Web scan"сканерлеу профилін жасау немесе ашу. Сканерленетін порттар тізімі 80/tcp және 443/tcp мәндерімен шектеледі. UDP порттарын сканерлеу, сервистер идентификациясын қосу. [12]

2-қадам. HTTP бөлімінде барлық опцияларды қосу. "Мазмұн Анализаторы" бөлімінде сөздіктерді пайдалану, ескі файлдарды іздеу және зиянды кодты іздеу опцияларын қосыңыз. Қажет болса, қосымша Сілтемелер қосу.

3-қадам. "Осалдықтар түрлері" бөлімінде тек "SQL-инъекциялар", "командаларды қашықтан орындау", "ерікті файлдарды қарау" және "Сайттағы скриптинг (XSS)"қалдыру керек.

Тіркеу жазбаларын өшіру. Профильді сақтау. Жасалған профильді пайдаланып веб-бағдарламаны сканерлеуді бастау. Нәтижелерді қарау. Осалдықтардың болуына тексеру жүргізу кезінде сканер жіберген сұраныстарды талдау.

4-қадам. Веб-қосымшада аутентификация. Сұраныстарға талдау жасау көмегімен аутентификациялық деректерді (Cookie, тақырыптар және т.б.) қамтитын HTTP сұрауларын сақтау қажет. "Web scan" профилін ашу, "қосымша сұрау өрістері" бөлімінде аутентификациялық деректерді қосу. Профильді сақтау.

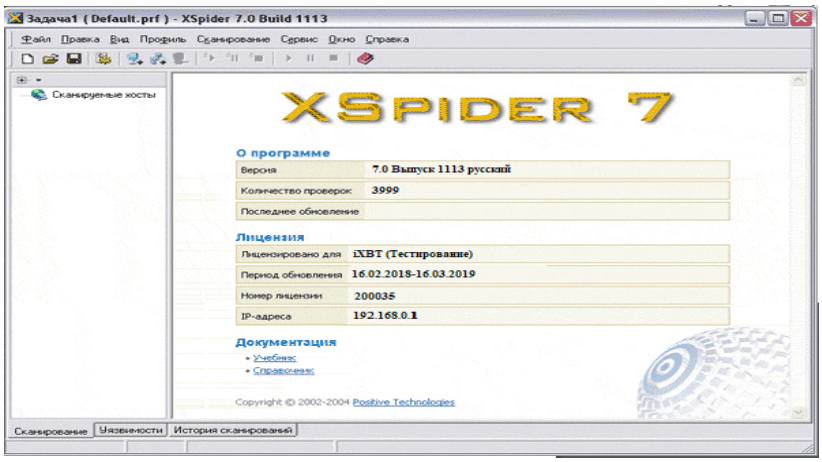
Қайта сканерлеу. Нәтижелерді салыстыру.

XSpider-ді орнату

Mspider Windows кез келген ОЖ орнатуға болады. Ол желілердің бағдарламалық және аппараттық платформаларына қарамастан барлық ықтимал осалдықтарды тексереді: Windows ұяластықты жұмыс станцияларынан бастап және Cisco желілік құрылғыларымен, соның ішінде *nix, Solaris, Novell, AS400 және т. б. аяқтайды. XSpider орнату процесі толық автоматтандырылған. Инсталлятор іске қосылғаннан кейін лицензиялық келісімнің шарттарымен келісіліп, бағдарлама орнатылған папканы таңдап, Бастау мәзіріне папканың атауын енгізу қажет. Осыдан кейін XSpider файлдары көшіріліп, көшіру аяқталғаннан кейін компьютерді қайта жүктеусіз бірден іске қосылуы мүмкін.

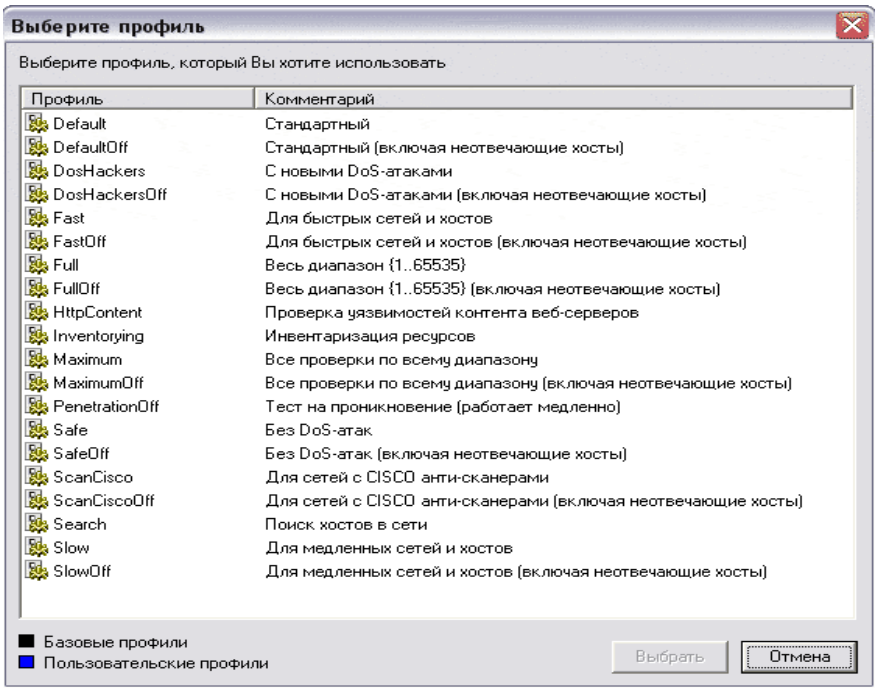
Интерфейс

XSpider Орнату және іске қосқаннан кейін экранда төмендегі 39 суретте көрсетілген бағдарламаның басты терезесі көрсетіледі:



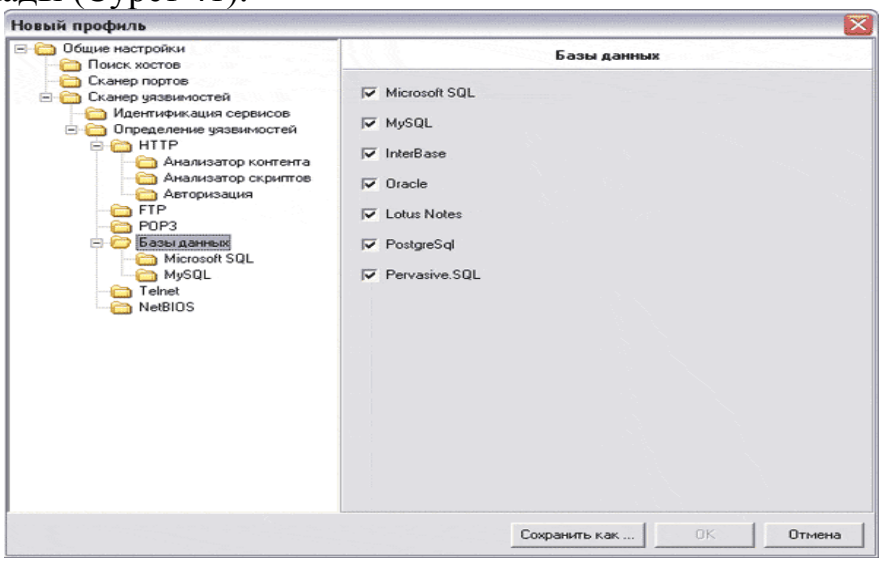
Сурет 39 – XSpider Орнату және іске қосқаннан кейінгі көрініс

Сканерленген хосттар тізіміне сканерлеу үшін адрестерді қосу керек. Адрес ауқымын бірден қосуға болады. Хостер тізімі құрылған соң, тексеру профилін таңдау керек, не бар, немесе өз қалаулары бойынша жаңа профильді жасау. Бар профильдер 40 суретте көрсетілген:



Сурет 40 – Профиль таңдау

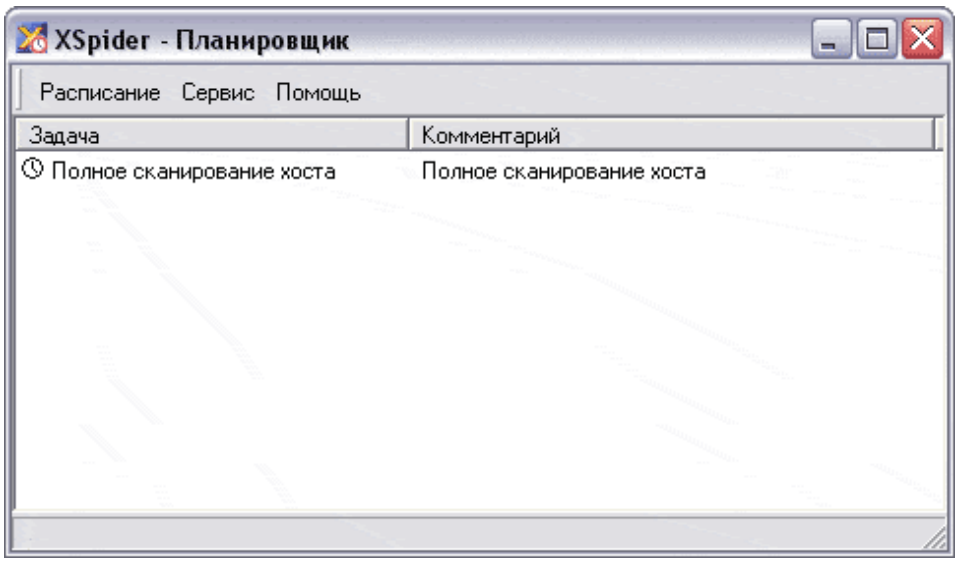
Бар профильдердің кез келгенін баптауға немесе жаңа профильді жасауға болады (Сурет 41).



Сурет 41 – Профиль таңдауда қолданушының өзі қосатын профильдер

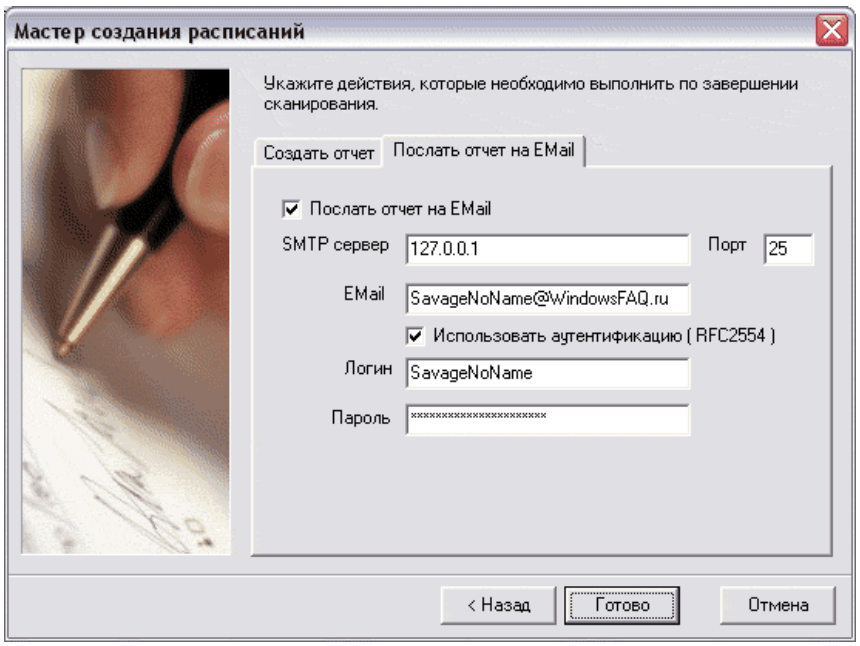
Тапсырма бапталғаннан кейін оны сақтап қалуға болады.

Жоспарлаушы баптау арқылы жасалған және сақталған тапсырмаларды іске қосуды жоспарлауға болады (Сурет 42).



Сурет 42 – Жоспардаушы терезесі

XSpider жоспарлаушысы Windows жоспарлаушысына ұқсас қарапайым. Төменде көрсетілген тапсырманы орнатудың соңғы кезеңі назар аударуға лайық (Сурет 43).



Сурет 43 – Есепті почталық мекенжайға жіберуді дайындау

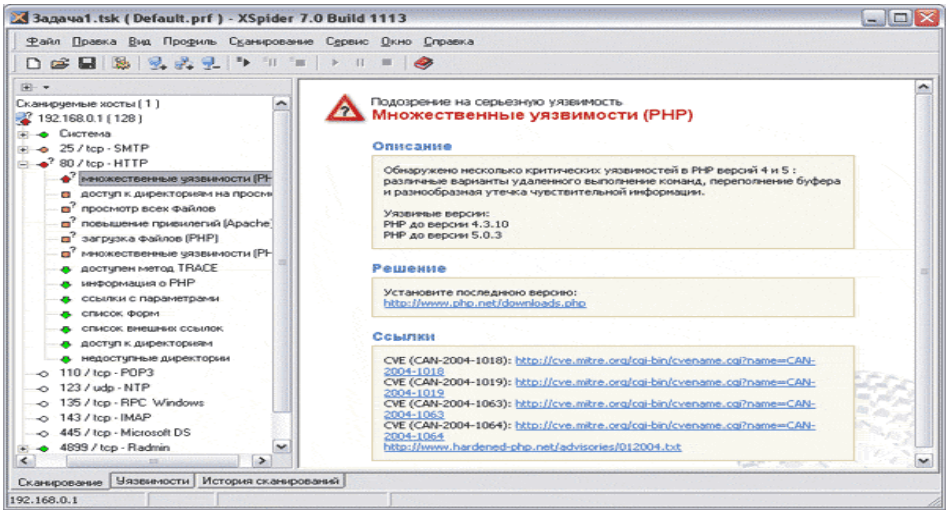
XSpider жоспарлаушысының жаңа тапсырма құру шебері салымында есепті почталық адреске жіберуге немесе белгілі бір папкада сақтауға болады

3.2 Web, Mail серверлермен жұмыс істейтін хосттарды қашықтан әкімшілендіру жүйесі арқылы тексеру нәтижелері

Әрбір бапталған тапсырма файлда сақталады. Егер жоспарлаушы бойынша тапсырманы іске қосу жоспарланған болса, оның орындалу нәтижесі .tsk файлда сақталады. Ол XSpider арқылы кез келген уақытта ашылуы

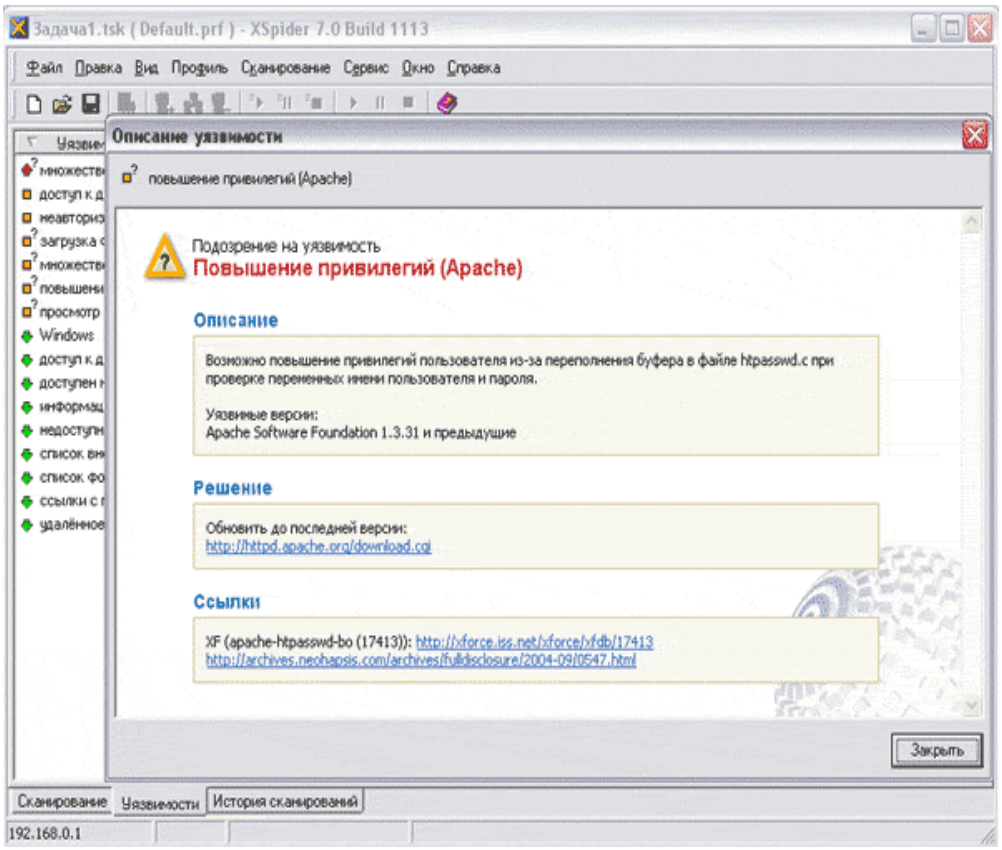
мүмкін. Файлда тек соңғы хост немесе хост тексеру нәтижесі ғана емес, барлық тексеру тарихы сақталады. Осылайша, бұрын анықталған осалдықтарды жойғаннан және операциялық жүйелер мен сервистерді жаңартқаннан кейін қауіпсіздік деңгейінің өзгеруін бақылауға болады. [13]

Жүктелген тапсырманың мысалы 44 суретте көрсетілген.



Сурет 44 – Осалдықтар көрінісі

Баптауда Windows 2007-де файрвол қосылып, Apache, PHP, mySQL, жаңалықтарға жазылу үшін тегін скрипт, MERAK Mail Server почталық сервердің демоверсиясы орнатылған (Сурет 45).

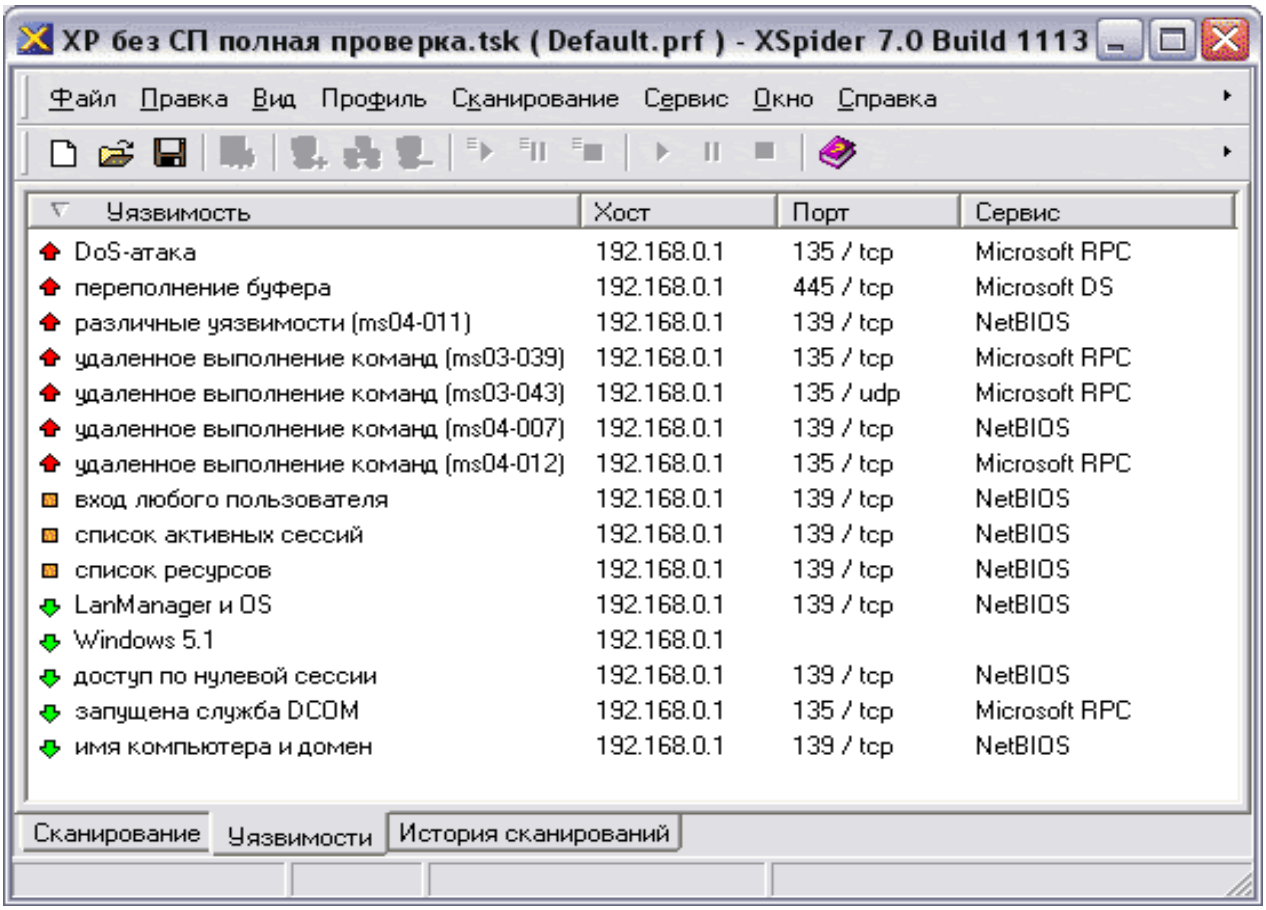


Сурет 45 – Маманданған сайттардағы осалдықты сипаттауға сілтемелер

Тексеру нәтижелерінде анықталған осалдықтар туралы ақпараттан басқа, қауіпсіздікке маманданған сайттардағы осалдықты сипаттауға сілтемелер келтірілген және бағдарламалық қамтамасыз етудің жаңартылған нұсқаларын жүктеуге сілтемелер берілген.

3.3 Операциялық жүйеден хостты брандмауэрсіз тексеру нәтижелері

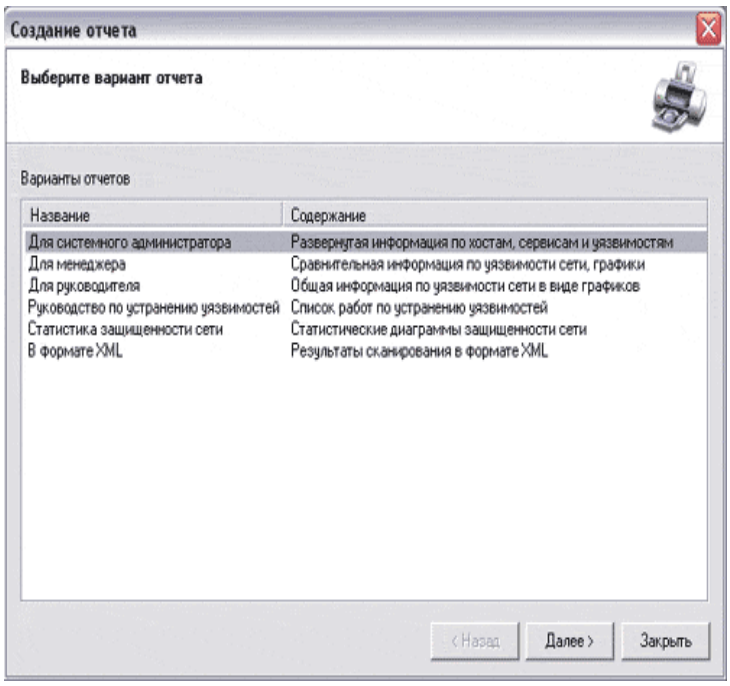
Жалпы сканердің жұмысын екі нұсқада іске қосу көзделген болатын. Бірінші нұсқада брандмауэрді қосып, сканерлеу процесі жүзеге асырылса, екінші нұсқада брандмауэрді ажыратып, сканерлеу жүзеге асырылады. Кез келген операциялық жүйеде (Windows ұяластықты) сканер жұмысқа жүктеледі. Қажетті профильді орнатқаннан кейін сканерлеу процесі басталады. Бұл аудит процесі 46 суретте көрсетілген.



Сурет 46 – XSpider бас терезесіндегі Осалдық салымы

Сканерлеу барысында бірнеше сыни осалдықтар анықталды. Жұмыс нәтижелерінде анықталған осалдықты және осы осалдықтарды жоятын түзетулерді жүктеу үшін сілтемелерді сипаттайтын Microsoft білім базасындағы мақалалардың сілтемелері берілді.

Xspider тексеру нәтижелері туралы есептердің бірнеше стандартты түрлерін таңдауға ұсынады (Сурет 47). [13]

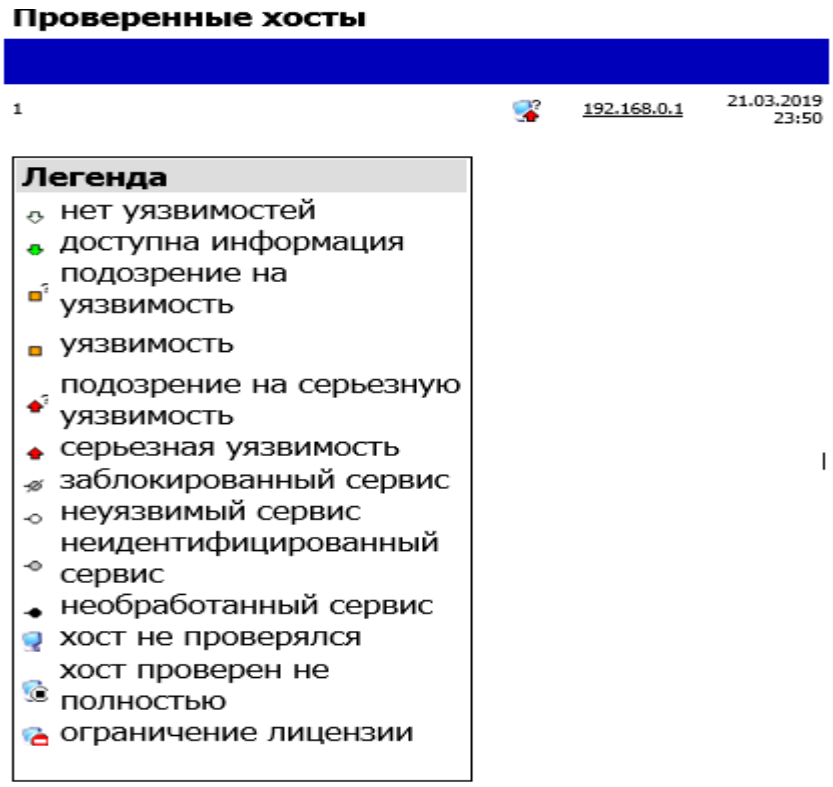


Сурет 47 – Есеп құрастыру нұсқасын таңдау

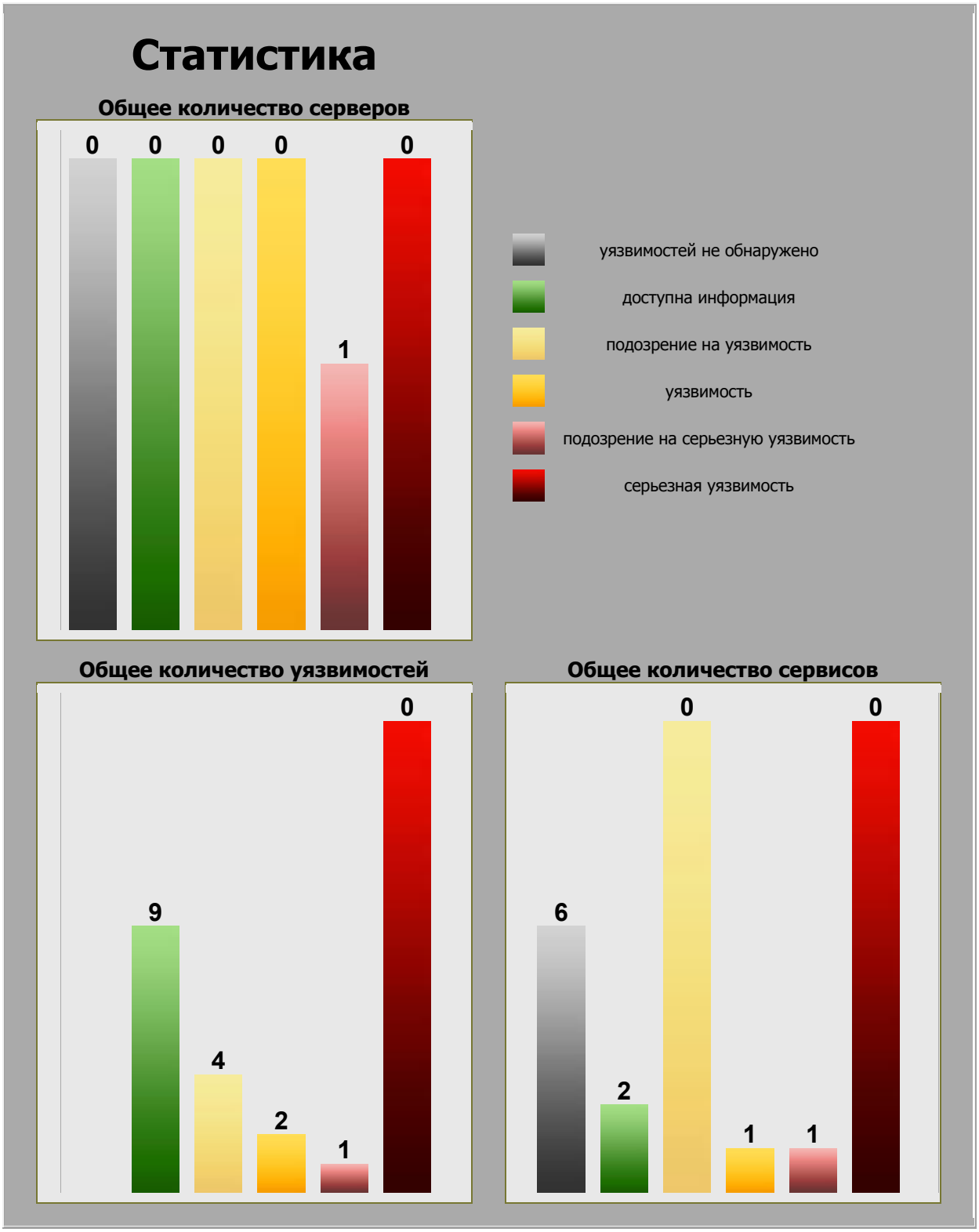
3.4 Есептер қалыптастыру

3.4.1 Бірінші тестілеу нәтижелері туралы есептер мысалдары

Жүйелік әкімшіге арналған есеп: хостар, сервистер, осалдықтар бойынша толық ақпарат (Сурет 48, 49). [14]



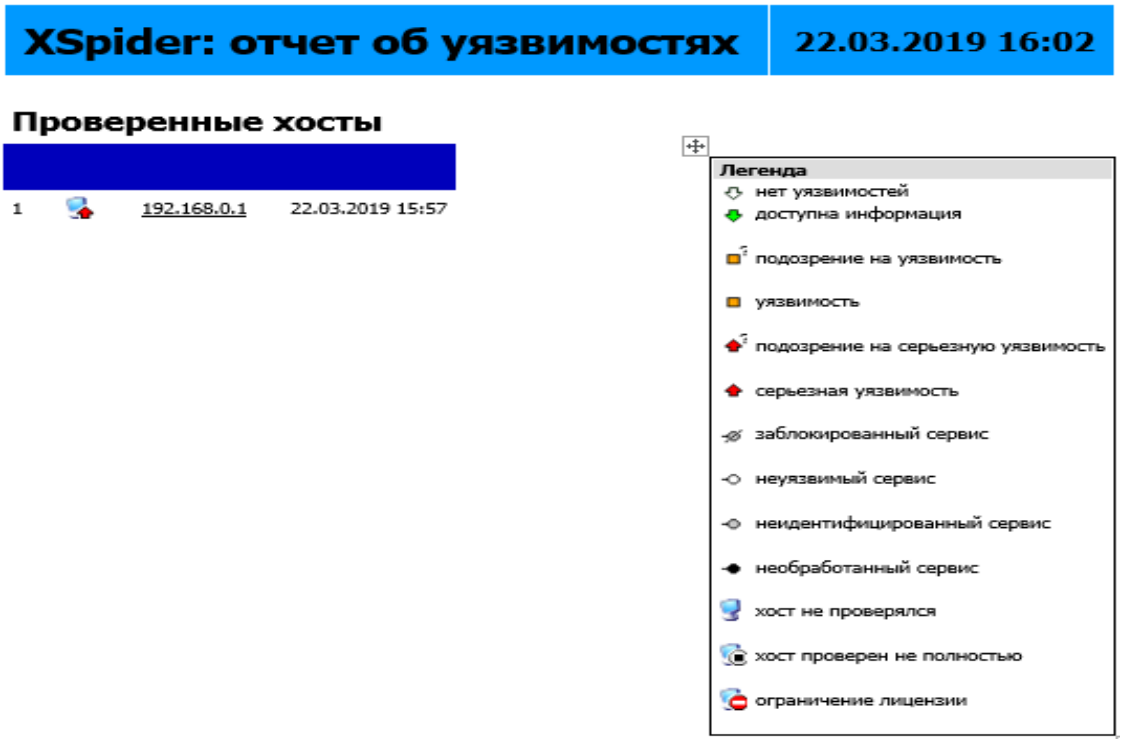
Сурет 48 – Тексерілген хосттар



Сурет 49 – Бірінші тестілеу нәтижесінің диаграммасы

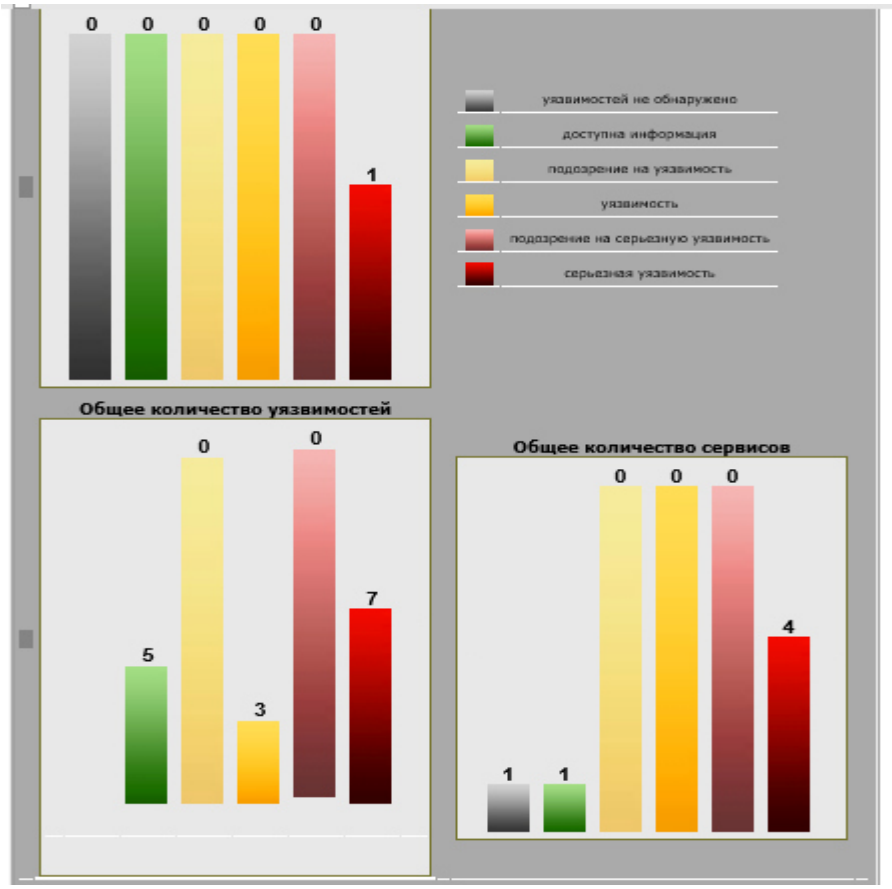
3.4.2 Екінші тестілеу нәтижелері туралы есептер мысалдары

Жүйелік әкімшіге арналған есеп: хостар, сервистер, осалдықтар бойынша толық ақпарат (Сурет 50, 51). [15]



Сурет 50 – Осалдылықтар

Статистика



Сурет 51 – Екінші тестілеу нәтижесінің диаграммасы

4 Өмір тіршілік қауіпсіздігі

4.1 Компьютерден бөлінетін сәулелердің адамға әсері

Қазіргі әлемде компьютерсіз өмірді елестету қиын. Бұл құрылғылар жақында ғана адамның өміріне кіріп, барлық қызмет салаларында орын алып, таптырмас көмекшілерге айналды. Компьютер көптеген технологиялық процестерді жылдамдатып, адамдар арасындағы әлеуметтік қарым-қатынасты жеңілдетті. Компьютер – ақпараттық процестерді жүзеге асыратын негізгі ақпараттық құрылғы, ал ақпараттық процестер дегеніміз ақпаратты алу, есту, көру, өңдеу, тарату болып табылады. Тоқсан ауыз сөзді түйіндер болсақ «компьютер – уақыт талабы». Компьютер көп жұмысымызды оңайлататыны анық .

Сонымен компьютердің адам ағзасына залалын тигізетін факторлары мынадай:

- көздің көру қабілетін төмендетеді:
- омыртқалардың қисаюына әкеледі;
- жүйкеге салмақ түсіреді;
- шаршағыштық, әлсіздік басады.

Бірақ компьютер қандай жақсы көмекші болсын, ол адамның денсаулығына зиян келтіретінін ұмытпаңыз! Компьютермен ұзақ жұмыс көру ағзасының, бұлшықеттердің, буындардың, ішкі ағзалардың және ағза жүйелерінің әртүрлі ауруларының даму қаупін арттыруға қабілетті. Біріншіден, компьютер мониторының жұмысына байланысты адамның көзі зардап шегеді. Көп жағдайда компьютермен ұзақ уақыт жұмыс істегенде көз бұлшық еттері тартылып, көзде ауыр сезімдер пайда болады немесе көру айқындығы нашарлайды. Осындай құбылыспен компьютерден күніне бірнеше сағаттан үзіліссіз өткізетін барлық адамдар таныс. Екіншіден, компьютермен жұмыс істеу кезінде дене босаңсығандай болады, бірақ бұл олай емес. Компьютер алдында отырған адам белгілі бір қашықтықтан экранға қарап, қолдарын пернетақтада немесе басқару органдарында ұстап тұруы тиіс. Бұл оның денесін белгілі бір жағдайды қабылдауға және оны жұмыс соңына дейін өзгертуге мәжбүрлейді. Компьютермен жұмыс істегенде адамның қолы көптеген ұсақ қозғалыстар жасауға мәжбүр болады, қатты шаршайды, ал ұзақ уақыт жұмыс істегенде созылмалы аурулар дамиды. Компьютерлік техниканы пайдаланушылардың денсаулық жағдайын нашарлататын факторлар қатарына электромагниттік және электростатикалық өріс, акустикалық шу, ауаның иондық құрамының және үй-жайдағы микроклимат параметрлерінің өзгеруі жатады. Компьютердің жұмысы ультрадыбысты қоса алғанда, акустикалық шуылдармен сүйемелденеді, ультрадыбыстың оқыту және жад процестеріне кері әсер ететіні белгілі. Шу барабанды тесікке, ал одан әрі мидың дің және қабық құрылымдарына әсер етеді. Қан тамырларының тонусы жоғарылайды, соның салдарынан артериялық қысым, ақыр соңында, балалар жасында гипертониялық аурудың дамуына алып келеді. Әсер етудің бастапқы кезеңінде тітіркендіргіш, ұйқының бұзылуы, эмоциялық тұрақсыздықпен

көрінетін жүйке жүйесінің қоздырғыштығы жоғарылауы мүмкін. Кейіннен астениялық жағдай, яғни физикалық және жүйке-психикалық әлсіздік дамиды. Көрсетілген симптомдар әртүрлі дәрежеде көрінуі мүмкін. Физикалық зиянды және қауіпті факторлар: электромагниттік, рентгендік, ультракүлгін және инфрақызыл сәулеленудің жоғары деңгейі; статикалық электрдің және жұмыс аймағы ауасының тозаңдануының жоғары деңгейі; оң аэрондардың жоғары құрамы және жұмыс аймағы ауасындағы теріс аэрондардың төмен құрамы; электр тізбегіндегі кернеудің жоғары мәні, оның тұйықталуы адам денесі арқылы болуы мүмкін [16].

Компьютермен жұмыс істеу кезінде оның зиянды әсерлерінің алдын алу үшін келесідегідей ережелерді сақтаған жөн:

- компьютердің мониторы мен көзіңіздің арақашықтығы кемінде 50 см болуы қажет; компьютер тұрған бөлменің ауасы жиі тазартылуы керек;
- күн сайын бөлмеде ылғалды тазалық жұмыстарын жүргізгеніңіз дұрыс;
- компьютермен жұмыс істеп болғаннан кейін қолыңызды салқын сумен жуыңыз;
- ересек адамдар үшін әрбір екі сағат сайын 15 минут үзіліс жасау керек;
- көзге жасалатын жаттығуларды жасап отыру керек;
- оқуға тиісті құжаттарды принтерден басып шығарып алып оқу керек, көзіңіздің саулығына үлкен пайдасы тиеді.

Мәліметтерді қорытындылай келе, компьютермен жұмыс жасауға отырмас бұрын мына кеңестерді басшылыққа алып жүруді ұсынамын. Компьютерде жұмыс істеу үшін 7 кеңес:

1) өзіңізге қолайлы жұмыс орнын жасаңыз;

2) егер сіз компьютерде 2 сағаттан артық отыратын болсаңыз, ноутбукке арналған арнайы тығыршықты қолданыңыз;

3) монитор мен сіздің көздеріңіздің арасындағы қашықтық 50 см-ден кем болмауы керек;

4) жоғарғы бөлігі сіздің көзіңіздің деңгейінде орналасатындай биіктік бойынша монитор күйін келтіріңіз;

5) әлсін-әлсін креслодан тұрыңыз және арқаның бұлшық етін асықпай тартыңыз;

6) сіздің жұмыс орныңыз көңілді, жақсы болса, деңеңіз бір қалыпты болып, шаршамайсыз. сондықтан мониторды , пернетақтаны, креслоны мерзімінде түзетіңіз.

4.2 Электр магниттік өрісінің адамға әсері және олардан қорғану шаралары

Электр магнитік өрістің әсері – электр заряды не магниттік моменті бар бөлшектер арасындағы электромагнитік өріс арқылы берілетін белгілі. Адам өмірге келгеннен бастап, электромагнит сәулесінің әсерінде болады. Адамға, жануарларға, өсімдіктерге, микроорганизмдерге жер қыртысынан бөлінетін гамма сәулелер және ғарыш сәулелері сырттан,организмде болатын

радиоактивті элементтер сәуелері іштен әсер етеді. Егер бұл сәулелер тірі организмге артық мөлшерде өтсе, клеткалардың, органдардың тіршілігіне қауіпті ауру жабысады. [17]

Радиожиілікті қондырғылар шығаратын электромагниттік сәулелерді мөлшерден көп қабылдаған жағдайда ол адамда мамандық ауруға әкеліп соғады. Нәтижесінде нерв жүйесі жүрек қан тамырлары эндокриналды жүйе және де басқа да ағзаларға әсер етуі мумкін. Электромагниттік өріс әсерінде ұзақ уакыт болған жағдайда адамдар тез шаршайды, ұйқышылдық пайда болады, жиі-жиі басы ауырады, нерв жүйесі бұзылады және тағы да басқа ауруларға тап болады. Системетикалық сәулелену болған жағдайда психикалық ауру, қан қысымының өзгеруі, жүрек соғысының баяулауы және шашының түсуі байқалады.

Электромагинттік өрістен қорғану әдістері:

1) сәуле шығару көзіндегі сәулелену азайту;

2) өте жоғары жиілікті және ультра жиілікті қондырғыларды дұрыс орнату;

3) экрандалған бөлмелердегі қондырғыны алыстан бақылау;

4) жұмыс істеу орнын және сәуленің шығу көзін экрандау немесе мыстан жасалатын жоғары өткізгіштік қасиеті бар тор металдар шағылдырғыш жерлету;

5) экран ретінде пайдалану шаралар «электромагниттік сәулелену дозиметр көмегімен кемінде айына бір рет тексеру;

6) жылына медициналық тексеруден бір рет өткізу.

Ағзаға әсер ететін факторлардың тобына:

- табиғи иондаушы емес электромагниттік сәулеленулер мен өрістер;
- статикалық электрлік өрістер;
- тұрақты магниттік өрістер;
- электромагниттік сәулелену мен өнеркәсіптік жиіліктегі және радиожиілікті диапазонындағы өрістер;
- лазерлік сәулелену жатады.

Өндіріс жағдайында адамға аталған өрістер мен сәулеленулердің соңғы төрт түрі әсер етеді [18].

Өнеркәсіптік жиіліктегі электрмагниттік өрістердің әсеріне өндіріс жағдайында ұшыраған жұмысшылардың денсаулық жағдайында өзгерістер байқалады. Олар негізінен ағзаның неврологиялық статусындағы өзгерістерді (бас ауруы, жоғары ашушаңдық , тез қажығыштық, салғырлық, ұйқышылдық), сонымен қатар жүрек-тамыр қызметінің бұзылыстарын (тахикардия және брадикардия, артериалық гипертензия немесе гипотония, тамыр тұрақсыздығы, гипергидроз) және асқазан-ішек жолдарындағы өзгерістерді білдіретін шағымдар түрінде болады. Шеткі қан құрамында өзгерістер-орташа дәрежеде тромбоцитопения, нейтрофильді лейкоцитоз, моноцитоз, ретикулопенияға бетбұрыс болуы мүмкін.

Өнеркәсіптік жиіліктегі электрлік өрістердің ШРЕД-і толық жұмыс күні үшін 5 кВ/м деңгейінде орнатылады, ал 10 минуттан аспайтын әсеріне

арналған максималды ШРЕД-і 25 кВ/м құрайды, қарқындылығы 5-20 кВ/м аралығындағы рұқсат етілген болу уақыты келесі өрнек бойынша анықталады:

$$T = E /50 - 2 \quad (4.1)$$

Мұндағы, Т – электрлік өрістің әсерінде болатын рұқсат етілген уақыты, сағатпен[5].

Е – кВ/м берілген бақыланатын зонадағы электрлік өрістің әсер ететін кернеулілігі.

Магниттік өрістердің шектік рұқсат етілген деңгейлері жалпы (барлық денеге) және жергілікті (аяқ-қолға) әсер ету жағдайлары үшін жұмысшының болу уақытына байланысты өрістің кернеулілігі (Н) немесе магнитті индукция (В) бойынша орнатылады.

4.3 Операторлық бөлменің желдету жүйесін есептеу

Желдету - әртүрлі жүйелер мен құрылғылар көмегімен жүзеге асырылатын үй-жай жағдайындағы ауа алмасу.

Адам бөлмеде тұрғанда, ауа сапасы нашарлайды. Экзальді көміртегі диоксидімен қатар басқа метаболизм өнімдері, шаң, зиянды өндірістік заттар ауада жиналады. Сонымен қатар, температура мен ылғалдылық артады. Сондықтан ауа алмасуды қамтамасыз ететін бөлмені желдету, ластанған ауаны кетіру және оны таза ауамен ауыстыру қажеттілігі туындайды.

Ауа алмасу терезе мен транскастер арқылы табиғи жолмен жүзеге асырылуы мүмкін.

Ауа алмасудың ең жақсы тәсілі жасанды желдету болып табылады, онда ауаны тазарту және ластанған ауаны жою механикалық түрде желдеткіштер мен басқа құрылғылардың көмегімен жүзеге асырылады.

Жасанды желдетудің ең озық нысаны - ауаны баптау. Технологиялық процестерді, жабдықтарды және құралдарды қамтамасыз ету, мәдени және көркемдік құндылықтарды сақтау үшін ең қолайлы (ыңғайлы) техникалық құралдарды пайдалану арқылы ғимарат пен көлік құрастыру ауасын баптайды.

Кондиционер ауа ортасының оңтайлы параметрлерін, оның температурасын, салыстырмалы ылғалдылығын, газ құрамын, қозғалыс жылдамдығын және ауа қысымын құру арқылы қол жеткізіледі.

Кондициялау қондырғылары шаңнан ауаны тазарту, жылыту, салқындату, ылғалдандыру және ылғалдандыруға арналған құрылғылармен, сондай-ақ автоматты басқару, бақылау және басқару үшін жабдықталған. Кейбір жағдайларда ауаны көмірқышқыл газын, оттекті байытуды және ауаны бактериологиялық тазартуды жоюды (ауаны хош иісті заттармен қанықтыру), дезодорацияны (жағымсыз иістерді бейтараптандыру), ион құрамын реттеуді (иондалуды), әуедегі инфекциямен ауыратындар) ауаны кондициялау жүйелері арқылы жүйеге асады. [19]

Әдетте, барлық құрылымдарда және жергілікті бөлмелерде орталық бөлмеде қызмет көрсететін орталықтандырылған кондиционер бар.

Кондиционерлеу әртүрлі типтегі кондиционерлермен жүзеге асырылады, олардың дизайны мен құрылысы олардың мақсатына байланысты. Ауа баптау үшін әртүрлі жабдықтар пайдаланылады: желдеткіштер, ылғалдандырғыштар, ауа ионизаторлары. Үй ішіндегі оңтайлы температура қысқы ауа температурасы + 19-дан +21 С дейін, жазда - +22-ден +25-ке дейін салыстырмалы ылғалдылықта 60-дан 40% -ға дейін, ал әуе жылдамдығы 30 см/с-тан аспайды.

Ауа алмасуын есептеу келесі жағдайларда жүргізіледі: артық ыстықты кетіруді есептеу, ластанудан тазалау және басқалар. Бірақ олар тек кәсіби деңгейде жинақталады және міндетті емес, тұрмыстық желдету үшін барлығы қарапайым:

- едендік кеңістік;
- көпше;
- санитарлық-гигиеналық нормалар.

Желдету - бұл үй-жайдан зиянды газдар мен шаңмен ластанған ауаны кетіруді қамтамасыз ететін ұйымдастырылған және реттелетін ауа алмасу, сондай-ақ өндірістік үй-жайларда микроклиматтық жағдайларды жақсарту.

Желдетуді келесідей жіктеуге болады:

1. ауа алмасуды ұйымдастыру әдісіне сәйкес – жалпы алмасу, ауаның ауысуы үй-жайдың толық көлемінде жүзеге асырылған кезде; жергілікті алмасу, онда бөлмедегі белгілі бір жерде әуе беріледі немесе жойылады;

2. қозғалыс күштерінің табиғаты бойынша – табиғи, табиғи күштердің арқасында ауа қозғалысы болғанда; жасанды (механикалық), ауа желдеткіштің көмегімен қозғалғанда;

3. әрекет принципі бойынша – сырттан ауа үрлеу (ауаны беру) немесе ештегі ауаны шығару (ауаны кетіру).

Табиғи желдету ол сыртқы ауаның салмағы және бөлмедегі ауа салмағының айырмашылығы есебінен (гравитациялық қысым), сондай-ақ жел күші (желдің қысымы) әсерінен туындаған ауа алмасу.

Газ көлемі 1 ° С температура көбейгенде 1/273 есе артады. Демек, ауа температурасы оның массасының азаюына әкеледі. Жылы және суық ауаның көлемдік массасындағы айырмашылық қысымның өзгеруін тудырады. Салқын ауа құрылыстық материалдардың тесіктері арқылы және бөлме ішіндегі кездейсоқ саңылауларға (инфильтрация) еніп, үстіңгі жақта орналасқан (жылу қысымына) қарағанда жеңіл, жылы ауа алмастырады. Әрине, термиялық қысым артқан сайын бөлмедегі және одан тыс жерлердегі температураның айырмашылығы артады, және же кіріс және шығыс тесіктері арасындағы биіктігі де артады. Жел өз жолындағы кедергілерге қысым жасайды (жел қысымы). Желдің қысымы желдің жылдамдығымен көтеріледі. Ғимараттың қабырғаларында тесіктер мен кездейсоқ саңылаулар арқылы, жел жағындағы терезе тесіктері арқылы жел қысымымен бөлме ішіне ауа кіреді, ал жел ығында тұрған қысымы төмен жақтан ауа шығады.

Табиғи желдету кезінде жылу мен жел қысымдары бір мезгілде әсер етеді.

Өндірістік ғимараттардың табиғи желдетудің ең тиімді және тиімді ұйымдастырылған желдету түрі - аэрация, желдету ғимарат қабырғаларында және төбесінде арнайы саңылаулар арқылы жүзеге асырылады; сыртқы температура, бағыт, жел жылдамдығы және т.б. факторларды ескере отырып, осы саңылауларды қолдануға болады.

Аэрация заманауи өндірістік кәсіпорындардың ірі өндірістік үй-жайларында қарқынды ауа алмасуды (20-40 есе) қамтамасыз етеді. Аэрацияны реттеу – оны дұрыс пайдаланудың маңызды шарттарының бірі. Бұл желдің күші мен бағытына, ауа температурасына және т.б. байланысты.

Жазда сыртқы ауа ғимараттың төменгі тесіктеріне шығуы керек. Желдің көлденең жағында орналасқан жел өткелі жабық болуы керек.

Қыста суық ауаны жұмыс аймағына кіргізбеуі үшін, ауа еденнен 4,5 метрден төмен емес орналасқан саңылаулар арқылы ағып кетуі керек.

Табиғи күштерге байланысты зиянды заттардың пайда болу орнынан ауаны кетіретін қолшатырлар, арнайы шахталарды ұйымдастыру арқылы жоюға болады.

Аэрация, әдетте, шаң мен зиянды заттардың концентрациясы тиімділіктің 30% -нан аспайтын шеберханаларда қолданылады.

Жел қысымын пайдалану үшін, пайдаланылған шахталар дефлекторометрлермен жабдықталады, бұл бөлмедегі ауаны соруға үлес қосады, себебі желдің беткі жағындағы дефлекторға вакуум пайда болады.

Механикалық желдету, әдетте, табиғи желдеткіштің гигиеналық талаптарға сай көрсеткіштерге жете алмаған кезде қолданылады.

Механикалық желдету жүзеге асыру жағынан күрделі болып табылады, табиғи желдетуге қарағанда бірқатар маңызды артықшылықтарға ие:

1) ауа температурасын, салыстырмалы ылғалдылықты қамтамасыз ету мүмкіндігі;

2) климаттық жағдайларға тәуелсіз, талап етілетін көлемде жыл бойына біркелкі пайдалану мүмкіндігі;

3) бөлменің кез келген нүктесінде ауаны жеткізу және ауа ағымынан бөлу мүмкіндігі;

4) құрылғының жергілікті сору қабілеті;

5) бөлмеден алынатын желдетілетін ауаны тазарту мүмкіндігі.

Арнайы бағыттау желдетуі кезінде желдету аумағы берілген аумақтан көлемдірек болуы мүмкін.

Төмендегі құрылғылар таза ауаны желдетудің элементтері болып табылады: қабылдау құрылғысы, жылу, ауаны ылғалдандыру, ауа қозғалысының күшейткіші, шеберханаға ауа беру үшін ауа өткізгіш жүйе. Сыртқы ауа қабылдайтын орын ғимараттың сыртқы қабырғасындағы тесік, ауа сорғыш білігі және т.б.

Формулаларға ауыстырудың барлық қажетті желдету стандарттары арнайы СНиП, ГОСТ және басқа нормативтік құжаттарда келтірілген.

Бөлменің аумағына негізделген желдету жүйесін есептеу

Бір сағат ішінде қанша рет бөлменің көлемі толығымен таза ауамен толтырылғанын және пайдаланылғандардан тазартылғандығын сипаттайтын мән, көпше деп аталады. Бөлмедегі ауаның айырбас бағамы, анықтамасынан анық болғандай, осы бөлме көлеміне байланысты. Яғни, егер бізде бір сағат ішінде үйдің бір бөлігінің таза ауасы болса, онда бұл жағдайда бірнеше есе көп, бұл іс жүзінде іс жүзінде үй жағдайында жүз пайызға тең.

Көптеген бөлмелерде желдетуді есептеу

Бұл есептеу үшін тек екі цифрды ескеру керек: нормалар 1 $м^2$ бөлме үшін 3 $м^3$ / сағ таза ауаны жеткізуді орнатады. Сонымен қатар, бөлмедегі адамдардың саны мүлдем маңызды емес. Бөлменің ұзындығын, биіктігі мен енін біле отырып, желдетудің өнімділігін есептейміз. [20]

Көптеген бөлмелерде желдетуді есептеу

Әр бөлме көлемін санау - біз осы бөлмелердің биіктігін, ұзындығын және енін көбейтеміз немесе үйді немесе пәтерді қабырғасы жоқ бөлме ретінде қараймыз - бұл жағдайда біз үйдің немесе пәтердің жалпы көлемін ғана қарастырамыз;

Формулаға сәйкес әрбір бөлме үшін қажетті ауа көлемін есептеу:

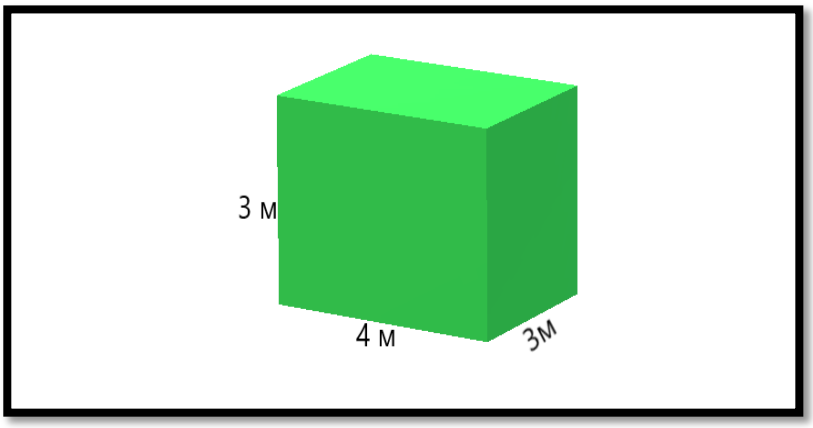
$$L = n \cdot V \qquad (4.2)$$

(мұнда L - талап етілетін ауа көлемі, n - ауа алмасу жылдамдығы (SNiP анықталады), V - бөлменің көлемі) [5].

Жеткізу және шығатын ауаның көлемі есептеу кезінде бірдей болуы керек екенін есте ұстаған жөн. Егер бірінші шамасы екіншіден асып кетсе, онда ол ең аз мөлшерде қабылданған бөлмелері үшін шығатын ауаның мәндерін ұлғайту қажет.

Санитарлық-гигиеналық нормаларды есептеу

Бұл есепте қайтадан екі суретті есте сақтау қажет: бір адамға 60 $м^3$ / сағ, ауада уақытша тұрып жатқан адамға 20 $м^3$ / сағ. Бұл сандар тұрғын үйлер мен әкімшілік орындардың санитарлық нормаларын белгілейді. Яғни, бір адам тұрақты және біреуі уақытша тұрып жатқан бөлмеде сағатына ауа көлемі 80 $м^3$ құрайды (Сурет 52).



Сурет 52 – Бөлме сұлбасы

Операторлық бөлме көлемі [5]:

$$V=4*3*3=36 \text{ м}^3 \quad (4.3)$$

Әкімшілік бөлме үшін адам 1 адамға керекті ауа алмасу жылдамдығы 20 $м^3$/сағ.

4.2-формулаға сәйкес:

n=20 $м^3$/сағ,
V=4*3*3=36 $м^3$,
L=n*V=20*36=720.

Ауаның кіру жылдамдығы 20 $м^3$/сағ, шығу жылдамдығы 20 $м^3$/сағ болуы тиіс.

5 Техникалық-экономикалық негіздемесі

Бұл дипломдық жобаның мақсаты – веб-қосымшаларды қорғау бойынша талдау және зерттеу үшін бағдарламалық өнімдерді (ақпараттық қауіпсіздік сканерді) әзірлеу.

Ақпараттық қауіпсіздік сканерлері (осалдылық сканерлері) компьютерлік желілерді, жеке компьютерлерді және қауіпсіздік проблемалары үшін орнатылған қолданбаларды тексеру үшін пайдаланылатын бақылау құралдары болып табылады.

Бағдарламалық өнімді мамандар тобы әзірлейді, олар мыналарды қамтиды: техникалық менеджер, программист-әзірлеуші. Техникалық менеджер бағдарламалық өнімді дамытуды бақылап, жобаны оңтайландыруға бағыт беруі керек. Программисттің жауапкершілігіне бағдарламаны әзірлеу, тестілеу, техникалық сипаттамаларды әзірлеу және дамыту кіреді.
Техникалық-экономикалық негіздемені мынадай бөлімдер қамтиды:

- БӨ дамуының күрделілігін анықтау;
- БӨ -ны дамыту шығындарын есептеу;
- негізгі құралдардың құнсыздануын есептеу және басқа да шығындар;
- БӨ -ның ықтимал (шарттық) бағасын анықтау;
- БӨ жұмысын бағалау.

5.1 ПП дамуының күрделілігін анықтау

Бағдарламалық өнімді әзірлеудің күрделілігін дәл анықтау үшін, бүкіл тапсырманы қарапайым кезеңдерге бөлу қажет. Бұл күрделі міндеттерді қарапайым қосалқы тапсырмаларға
бөлу арқылы бағдарламалық жасақтама дамуының барысын бақылайды. Бағдарламалық жасақтаманың күрделілігінің және даму сатысының үлестіру үлгісі 5.1-кестеде келтірілген.

Кесте 5.1 – Бағдарламаны әзірлеу сатылары

Бағдарламалық өнімнің даму кезеңдері	Жұмыс түрі	Күрделілік, адам/сағ
Кезең 1	Тапсырмаларды орнату	5
Кезең 2	Бағдарламалық өнімге ТҚ дамыту және бекіту	10
Кезең 3	Ұқсас бағдарламаларды іздеу және зерттеу	25
Кезең 4	Байланысты әдебиеттерді іздеу және зерттеу	20
Кезең 5	Бағдарламалық өнімге аналитикалық кестесін құру	5
Кезең 6	Бағдарламалық өнімнің теориялық бөлігін жасау	15

5.1-кестенің жалғасы

Кезең 7	Бағдарламалық өнімнің практикалық бөлігін жасау	25
Кезең 8	Жөндеу және ақаулықтарды жою	20
Кезең 9	Бағдарламалық өнімді тестілеу	10
Кезең 10	Жобаны қорытындылау және енгізу	55
Кезең 11	Есеп беруді ұйымдастыру, жұмыс нәтижелерін және бағдарламалық өнімдерді енгізу	30
Барлығы: жобаның күрделілігі		215

Жұмыс күнінің ұзақтығы – 8 сағат. Нәтижесінде бағдарлама өнімін енгізу үшін 27 (215: 8) жұмыс күні қажет.

5.2 Бағдарламалық өнімді әзірлеуге шығындарды есептеу

Бағдарламалық жасақтама өнімін дамыту үшін қажетті шығындарды анықтау мынадай элементтерді қамтитын қолда бар бағалау негізінде жүзеге асырылады:

- материалдық шығындар;
- еңбекке ақы төлеу;
- әлеуметтік салық;
- негізгі құралдардың амортизациясы;
- басқа шығындар

Материалдық шығындар материалды, энергияны және БӨ-ді дамытуға қажетті басқа да шығындардың негізгі және қосымша шығындарына бөлінеді. Материалдық шығындарды есептеу 5.2 кестеде көрсетілген нысан бойынша жүзеге асырылады.

Кесте 5.2 - материалдық ресурстардың құны

Материалдың атауы	Маркасы	Өлшем бірлігі	Саны	Бағасы бірлік теңгеде	Теңгедегі сома
Кеңсе қағазы	International Paper	Қаптама	1	1 000,00	1 000,00
Дәптер (96 бет)	Маяк Канц	Дана	2	190,00	380,00
Блокнот	КТС-ПРО	Дана	1	400,00	400,00
Қалам	Jotter	Дана	2	90,00	180,00
Компьютерлік тышқан	TECH	Дана	1	2 000,00	2 000,00
USB flash 32 Gb	Transcend	Дана	1	2600,00	2600,00
Барлығы:					6 560,00

Материалдық ресурстар үшін талап етілетін жалпы сома ($З_м$) келесі формула бойынша есептеледі:

$$З_м = \sum P_i * Ц_i, \quad (5.1)$$

мұндағы P_i - і-ші материалдық ресурстардың, табиғи бірліктердің тұтынуы;

$Ц_i$ - і-ші материалдық қордың бірлігіне баға;

і - материалдық ресурстардың түрі;

n - материалдық ресурстардың саны.

Қажетті жабдықтар мен бағдарламалық қамтамасыз етудің құнын есептеу 5.3-кестеде келтірілген түрде жасалады.

Кесте 5.3 – Жоба үшін қажетті жабдықтар мен бағдарламалық қамтамасыз етудің құнын есептеу

Материалдың атауы	Маркасы	Өлшем бірлігі	Саны	Бағасы бірлік теңгеде	Теңгедегі сома
Ноутбук	Acer E5-576G NX.GU2ER.011	Дана	1	280 000,00	280 000,00
Принтер	HP LaserJet Pro M15a	Дана	1	36 200,00	36 200,00
Модем	ID Net	Дана	1	4600,00	4600,00
Барлығы:					320 800,00

Зм = 6 560 + 320 800 = 327 360,00 (тг)

Бағдарламалық жасақтама өнімін енгізу үшін 327 360,00 теңге сомасында материалдар қажет.

5.3 Электр энергиясының құнын есептеу

Бағдарламалық жасақтама өнімі электр энергиясын тұтынусыз жасай алмайтындықтан, электр энергиясының құнын есептеу керек.

5.1 кестеге сәйкес, бағдарламалық өнімді әзірлеуге 215 сағат кетеді, енді 215 сағатта жұмсалатын электр энергиясының құнын есептеу қажет. Принтер үшін есептеулер 24 сағат бойы орындалады, өйткені принтерді үнемі пайдалану қажет емес.

$$Э = З_{эл.эн.ж.} + З_{қос.қаж}, \quad (5.2)$$

мұнда $З_{(эл.набор.)}$ – электр жабдықтардың құны;

$З_{(қосымша)}$ – қосымша қажеттіліктер үшін электр энергиясының құны.

Жабдықтарға қажетті электр энергиясын есептеу келесі формула бойынша анықталады:

$$З_{эл.эн.ж.} = \sum W * К \quad * S * T, \qquad (5.3)$$

Мұндағы, W – энергия тұтыну,

$к_п$ – пайдалану коэффициенті ($к_п$ = 0,7..0,9);

Т – жұмыс уақыты;

S – тариф (1 кВт / сағ = 23,85 Тг).

Тұтынылатын электр энергиясының құнын есептеу нәтижелері 5.4-кестеде келтірілген.

Кесте 5.4 – Электр энергияға шығындар

Құралдың атауы	Паспорттық күші, кВт	қуат Коэффициенті	Жабдықтың жұмыс уақыты, с	ЭЭ Бағасы тг/кВтч	Сомасы, тг.
Ноутбук	0,6	0,7	215	23,85	2 153,65
Модем	0,08	0,9	215	23,85	369,20
Принтер	0,5	0,9	30	23,85	321,97
Кондиционер	0,8	0,9	180	23,85	3 090,96
Жарықтандыру	0,3	0,7	215	23,85	1 076,83
Барлығы:					7012,61

$$З_{эл.эн.ж.} = 7012{,}61 \text{ (тенге)}$$

Қосымша қажеттілік үшін шығындар электр энергиясының өзіндік құнын 5% мөлшерінде ұлғайту индикаторы негізінде есептеледі:

$$З_{кос.каж} = 5\% * З_{эл.эн.ж.}, \qquad (5.4)$$

Формулаға сәйкес қосымша талаптардың құнын анықтаңыз (5.4):

$$З_{қос.каж} = 0.05 * 7012{,}61 = 350{,}63 \text{ (тенге)}$$

Барлық есептеулерге негізделген қосымша қажеттілікпен жалпы энергия шығыны:

$$Э = 350{,}63 + 7012{,}61 = 7363{,}24 \text{ (тенге)}$$

5.4 Еңбек шығындарын есептеу

Бұрын айтылғандай бағдарламалық өнімдерді әзірлеу үшін екі қызметкер қажет:

- жоба жетекшісі – жұмыс уақытын басқару, жұмыс процестерін түзету, үйлестіру, пәндік саланы зерттеу;

- әзірлеуші – бағдарламалық қамтамасыз етуді әзірлеу, тестілеу және техникалық қызмет көрсету.

Еңбекке ақы төлеу шығындарының мөлшері мынадай формула бойынша есептелуі мүмкін:

$$З_{тр} = \sum ЧС_i * T_i \quad (5.5)$$

Мұндағы, $ЧС_i$ – і-ші қызметкердің сағаттық ставкасы, тг;

T_i – модельді дамытудың күрделілігі, адамдар × сағ; і - қызметкер санаты;

n – БӨ-ді дамытумен айналысатын қызметкерлердің саны.

Жобаны іске асыру кезінде қатысушыларға жұмыс уақыты біркелкі емес, сондықтан әр қызметкердің сағаттық мөлшерлемесін және жалпы жалақыны белгілеу маңызды.

Қызметкердің сағаттық ставкасы келесі формула бойынша есептеледі:

$$ЧС_i = \frac{ЗП_i}{ФРВ_i} \quad (5.6)$$

мұнда $ЗП_i$ і-ші қызметкердің айлық жалақысы, мр;

$ФРВ_i$- і-ші қызметкердің жұмыс уақытының айлық қоры, сағ.

Менеджердің айлық жалақысы 270000 теңге, ал әзірлеушінің айлық жалақысы 170000 теңге. Әрбір қызметкердің (5.6) формуласына сәйкес сағаттық ставкасын есептеңіз:

$$ЧС_{жетекші} = \frac{270\,000{,}00}{22 * 8} = 1\,534 тг/ч$$

$$ЧС_{әзірлеуші} = \frac{170\,000{,}00}{22 * 8} = 966\ тг/ч$$

Менеджердің сағаттық ставкасы - 1534 (тг / сағ), дамудың күрделілігі - 100 сағат. Әзірлеушінің сағаттық жылдамдығы - 966 (тг / сағ), дамудың күрделілігі - 215 сағат. Формула бойынша (5.5) жұмысшылардың жалақысына жұмсалатын шығындардың мөлшерін есептеу мүмкін болады:

$$З_{тр} = 1\,534 * 100 + 966 * 215 = 153\,400 + 207\,690 = 361\,090{,}00$$

Еңбекке ақы төлеу бойынша есептеулер 5.5 кестеде көрсетілген.

Кесте 5.5 – Жалақы

Қызметкер санаты	Біліктілік	Дамудың күрделілігі ПП, сағат	сағаттық тариф, тг/сағ	Сомасы, тг.
Жетекші	Жобаның	100	1 534	153 400,00

	жетекшісі			

5.5-кестенің жалғасы

Әзірлеуші	Программист	215	966	207 690,00
Барлығы:				361 090,00

5.5 Әлеуметтік салықтық шығындарды есептеу

Қазақстан Республикасының Салық кодексіне сәйкес әлеуметтік салық жалақы жобасының 9,5% құрайды. Әлеуметтік салық келесі формула бойынша есептеледі:

$$С_н = (ФОТ - ПО) * 0,095 \quad (5.7)$$

онда ПО - зейнетақы қорына шегерім, олар жалақы қорының 10% құрайды.

$$ПО = 361\,090 * 0,1 = 36\,109,00 \text{ тенге}$$

$$С_н = (361\,090 - 36\,109) * 0,095 = 30\,873,20 \text{ тенге}$$

Есептеулердің нәтижелері кестеде келтірілген (5.6):

Кесте 5.6 – Әлеуметтік салықты есептеу

Қызметкер санаты	Адам саны	Еңбек ақы, тг	Зейнетақы аударымы, тг	Әлеуметтік салық, тг
Жетекші	1	153 400,00	15 340,00	13 115,70
Әзірлеуші	1	207 690,00	20 769,00	17 757,50
Барлығы:				30 873,20

5.6 Негізгі құралдардың тозуы және басқа да шығыстар

Негізгі құралдар бойынша амортизация нормалары Қазақстан Республикасының салық кодексіне сәйкес анықталуы тиіс. ОБ құнсыздануы мынадай формула бойынша анықталуы мүмкін:

$$A_г = \frac{С_{об} * Н_а}{100} \quad (5.8)$$

Мұндағы, $С_{об}$ - жабдықтың құны;

$Н_а$ - амортизация нормасы (амортизация нормасы = 25);

Формула (5.8) ноутбуктың бір жылдағы амортизациясы үшін қажетті соманы есептеуге мүмкіндік береді:

$$A_г = \frac{280\,000 * 25}{100} = 70\,000,00 \text{ тенге}$$

Енді даму кезеңіндегі амортизация нормасын есептеу қажет:

$$A_{\text{г}} = \frac{70\,000 * 27}{365} = 5\,178{,}08 \text{ тенге}$$

Сол сияқты барлық жабдықтар үшін амортизация нормасын есептеу қажет. Есептеулердің нәтижелері 5.7 кестеде келтірілген.

Кесте 5.7 – Құнсыздану

Жабдықтардың бағдарламалық өнімнің атауы	Жабдықтар мен бағдарламалық өнімнің құны, тг	Жылдық амортизация лық нормасы %	Жыл ішіндегі амортизация сомасы, тг	Даму уақытында амортизация сомасы, тг
Ноутбук	280 000,00	25	70 000,00	5 178,08
Принтер	36 200,00	25	9 050,00	669,45
Модем	4600,00	20	920,00	68,05
Барлығы:			79 970,00	5916,00

БӨ- дамытуға арналған шығындар.

Барлық ұсынылған есептердің негізінде 5.8 кестеде келтірілген нысан бойынша бағдарламалық жасақтама әзірлеудің өзіндік құнын бағалау қажет. Сурет 53 жұмыс шығындарының кестесін көрсетеді.

Кесте 5.8 – ҚБ-ны дамытудың болжамды құны

Шығын құны	Сомасы, тг	%
Жабдықтар мен материалдық ресурстардың құны	327 360,00	45%
Еңбекке ақы төлеу	361 090,00	49%
Әлеуметтік салық	30 873,20	4%
Энергия шығыны	7363,24	1%
Негізгі құралдардың амортизациясы	5916,00	1%
Жалпы бағалау:	732 602,44	100%

Сурет 53 – Шығындар Диаграммасы

5.7 БӨ-нің ықтимал (шарттық) бағасын анықтау

Бағдарламалық жасақтама өнімінің құны өндірілген өнімнің сапасына, оның даму мерзіміне және өнімнің сапасына қарай анықталады. Бағдарламалық жасақтама үшін $Ц_Д$ құны келесі формула бойынша есептеледі:

$$Ц_Д = З_{нир}\left(1 + \frac{P}{100}\right), \qquad (5.9)$$

Мұнда, $З_{нир}$ – бағдарламалық өнімді әзірлеу құны, тг;

Р – рентабельділігінің орташа деңгейі, (%). Бұл параметр 25% деп есептеледі.

$$С_{приб} = 732\ 602{,}44 * \frac{25}{100} = 183\ 150{,}61 \text{ тенге}$$

$$Ц_Д = 732\ 602{,}44 + 183\ 150{,}61 = 915\ 753{,}05 \text{ тенге}$$

Бұдан әрі, ҚҚС-ты қоса алғанда, сатудың өзіндік құнын анықтау қажет, ҚҚС ставкасы Қазақстан Республикасының заңнамасымен белгіленеді. 2019 жылға ҚҚС ставкасы 12% құрайды. Сатылымның құны, ҚҚС қоса есептегенде, келесі формула бойынша есептеледі:

$$Ц_р = Ц_д + Ц_д * ҚҚС, \qquad (5.10)$$

$$Ц_р = 915\ 753{,}05 + 915\ 753{,}05\ * 0{,}12 = 1\ 025\ 643{,}42 \text{ тенге}$$

Осылайша, бағдарламалық өнімді (өзіндік құны) құрастыру құны 732 602,44 теңгені құрады, ал кіріс (кірістілік) 183,150,61 теңгені құрады. Осы

негізде келісілген баға 915 753,05 теңгені құрайды. Сатылымның құны ҚҚС есебімен 1,025,643,42 теңгені құрады.

Қорытынды

Зерттеу нәтижелері айқын оң үрдістерге қарамастан, веб-қосымшалардың жалпы қорғалу деңгейі жеткілікті төмен болып қала береді. Веб-қосымшалардың жартысынан астамында қауіпті осалдықтар анықталған, бұл ретте қаскүнемде бастапқы кодқа қол жеткізу мүмкіндігі болған кезде бұл көрсеткіш күрт өседі. Анықталған осалдықтар бұзушыға көптеген сезімтал ақпаратты алуға мүмкіндік береді, мысалы, қосымшаның бастапқы коды немесе пайдаланушылардың жеке деректері, соның ішінде банктер мен мемлекеттік мекемелердің сайттарында. Қосымшалар және пайдаланушылардың өздері шабуылдардан қорғалмаған: іс жүзінде барлық қосымшалар зиянкестерге оларға шабуыл жасауға мүмкіндік береді. Сонымен қатар, веб-қосымшалардың осалдығы зиянкестерге қолжетімді компанияның ішкі желісіне ену векторларының бірі болып табылады, зерттелген жүйелердің арасында шамамен төрттен бір бөлігі ішкі ресурстарға рұқсатсыз қол жеткізуге себеп болуы мүмкін.

Ақпараттық жүйелерді, ақпараттық ресурстарды қорғауда көптеген жұмыстар жасалуда, көптеген жерлерде желілік қауіптерден қорғауда желіаралық экрандарды қолдану ұсынылып жатады. Шабуыл осал жерлерді анықтаудан басталады. Осыған байланысты дипломдық жұмыста ақпарат қауіпсіздігіне жасалатын шабуылдар зерттеледі. Шабуылдардың қандай салаға бағытталатыны, қандай осалдықтарды көздейтіні, сол шабуылдардың нәтижесінде кәсіпорынның қандай салалары зиын шегіп жатады, осыларға талдау жасалады. Осалдықтар тәуекелінің ең жоғары дәрежесіне байланысты осал сайттар үлесі, әртүрлі тәуекел дәрежесіндегі осалдықтары бар сайттар үлесі, ең көп таралған осалдықтар OWASP зерттеу компаниясының көрсеткіштерімен нақтыланады. Соның ішінде веб-қосымшалардың үлесіне ерекше көңіл бөлінеді. Веб-қосымшалардың осалдығы және оларға төнетін қауіптер жіктеліп, қауіп салдары анықталады. Әрі қарай осы айтылғандарды болдырмау, алдын алу және жою шаралары қарастырылып, осы мақсатта қолданылатын сканерлеу программаларына, олардың жұмыстарына зерттеу жасалады. Бірнеше сканерлерге талдау жасалып (Xspider, Internet Scanner, Retina, Nessus), ішіндегі тиімдісі анықталады. Қарастырылып отырған зерттеулер нәтижесі бойынша Xspider сканерінің артықшылықтары көрсетіліп, оны тәжірибе жүзінде қолдану мысалы келтіріледі де, нәтижелік есеп құрастырылады. Бұл сканердің соңғы версиялары алдыңғыларына қарағанда (6-шы версиямен салыстырғанда Xspider-дің 7-ші версиясы) ерекше функцияларға ие.

Енді сканер толық автоматты режимде жұмыс істей алады. Сканерлеу міндеттерін орындау үшін жасалған және жоспарланған сканер базалары мен модульдерін автоматты түрде жаңарту мүмакіндігі қамтылған, есептерді автоматты түрде жасауға да болады. Positive Technologies мамандары жаңа осалдықтарды зерттеп, олардың алдын алу мүмкіндіктерін осы сканердің функцияларына жүйелі түрде қосып отырады. Сканерлердің соңғы

версиялары ақылы болғандықтан, интернетте тегін алуға мүмкіндік беретін XSpider 770 Build 1113 версиясы тәжірибеде екі режимде қолданылып, есептік нәтиже алынды. XSpider веб-бағдарламашылар құрған кодты тексере алады, пошта, веб-серверлер, операциялық жүйелер, деректер қорының серверлері және желіде жұмыс істейтін басқа да сервистер осалдықтардың, қарапайым немесе бос парольдердің, баптаудағы қателердің және т.б. болуын тексере алады. Толық есептер анықталған осалдықтардың сипаттамасын іздеуге уақыт жоғалтпай, анықталған кемшіліктерді жедел жоюға көмектеседі. Тексерулердің тарихын сақтай отырып, жасалған жұмыстың көлемін бағалауға және желінің, программалық қамтамалардың ағымдағы қауіпсіздігі туралы хабардар болуға мүмкіндік береді. XSpider анықтамалық жүйесі қарапайым тілде жазылған және сканер жұмысының барлық параметрлері мен принциптерін толық түсінуге мүмкіндік береді. Мұның бәрі жоғары деңгейде желінің ақпараттық қауіпсіздігін қолдау үшін әмбебап құрал болып табылады. Оны ақпаратты қорғаудың басқа шараларымен бір кешенде қолдану қауіпсіздіктің қажетті дәрежесіне қол жеткізуге мүмкіндік береді.

Әдебиеттер тізімі

1. Геннадий Б. Защита информации ограниченного доступа от утечки по техническим каналам. -М.: Телеком 2014. -594с.
2. Генри С. У. Алгоритмические трюки для программистов. – М.: «ВИЛЬЯМС», 2014. - 512 с.
3. Джон Эриксон Хакинг. Искусство эксплойта. –М.: Символ-Плюс 2010. -512с.
4. Дмитрий Скляров Искусство защиты и взлома информации. – Спб.: БХВ-Петербург, 2004. -288с.
5. Жуков Ю. Основы веб-хакинга. Нападение и защита. – Спб.: Питер, 2010. - 176 с.
6. Долгин А.А., Хорев П.Б. Разработка сканера уязвимостей компью терных систем на основе защищенных версий ОС Windows. 2005.
7. Информационный портал о безопасности [Электрондық ресурс] URL: http://www.securitylab.ru/ (кіру уақыты 27.03.19).
8. Онлайн журнал Softkey.info [Электрондық ресурс] URL: http://www.softkey.info/ (кіру уақыты 27.03.19).
9. Ресми сайт «GFI Software». [Электрондық ресурс] URL: http://www.gfi.ru/ (кіру уақыты 27.03.19).
10. Ресми сайт «Beyond trust». [Электрондық ресурс] URL: http://www.beyondtrust.com/Products/RetinaNetworkSecurityScanner/ (кіру уақыты 27.03.15).
11. Ресми сайт IBM [Электронный ресурс] Режим доступа. URL: http://www.ibm.com/ (кіру уақыты 20.04.19).
12. Ресми сайт Tenable Network Security [Электронный ресурс] Режим доступа. URL: http://www.tenable.com/products/nessus-vulnerability-scanner/ (кіру уақыты 20.04.19).
13. Ресми сайт «safety-lab.» [Электрондық ресурс] URL: http://www.safety-lab.com/ (кіру уақыты 20.04.19).
14. Решения IBM для обеспечения информационной безопасности [Э лектрондық ресурс]URL: http://www.ibm.com/ru/services/iss/pdf/ISS_2009_DB_s10.pdf (кіру уақыты 20.04.19).
15. Хорев П.Б., Методы и средства защиты информации в компьюте рных системах, -М.: Издательский центр «Академия», 2005.
16. Сулеев Д.К., Исаханова А.Б., Суйесинова Г.И., Болатбаева Т., Утепова А.Б. Электромагнитные поля в учебных аудиториях. –Алматы: Вестник КазНТУ, 2007. -№ 1/1 (58). С.22-27.
17. Суйесинова Г.И., Болатбаева Г,А., Тусупова А.А.,Уразбахова А., Мединский А.И. Исследование характеристик электромагнитных полей компьютеров // - Алматы: Вестник КазНТУ, 2009. №3(73).
18. Утепов Е.Б., Исаханова А.Б., Суйесинова Г.И., Мединский А.И., Батыркулов Н.Т. Снижение уровней электромагнитного поля на производстве. Монография. –Алматы: КазНТУ, 2010. -144 с.

19. Суйесинова Г.И. Электрмагниттік сәулелерге ұшырайтын жұмысшылардың еңбек жағдайын жақсарту. // «Тіршілік қауіпсіздігі саласындағы жаналықтар» атты он бірінші ғылыми-техникалық конференция. 3 т. -Алматы: КазНТУ, 2009. С.109-111.

20. Суйесинова Г.И. Электромагниттік сәулелердің жұмысшы ағзасына әсерін бәсеңдету бойынша іс-шараларды жасау. // «Тіршілік қауіпсіздігі саласындағы жаналықтар» атты XI Халықаралық ғылыми-техникалық конференция. 3 т. -Алматы: КазНТУ, 2009. С.111-112.

Қосымша А

Примеры отчетов о результатах первого тестирования

XSpider: отчет об уязвимостях | 21.03.202019 01:12

Отчет для системного администратора: развернутая информация по хостам, сервисам, уязвимостям

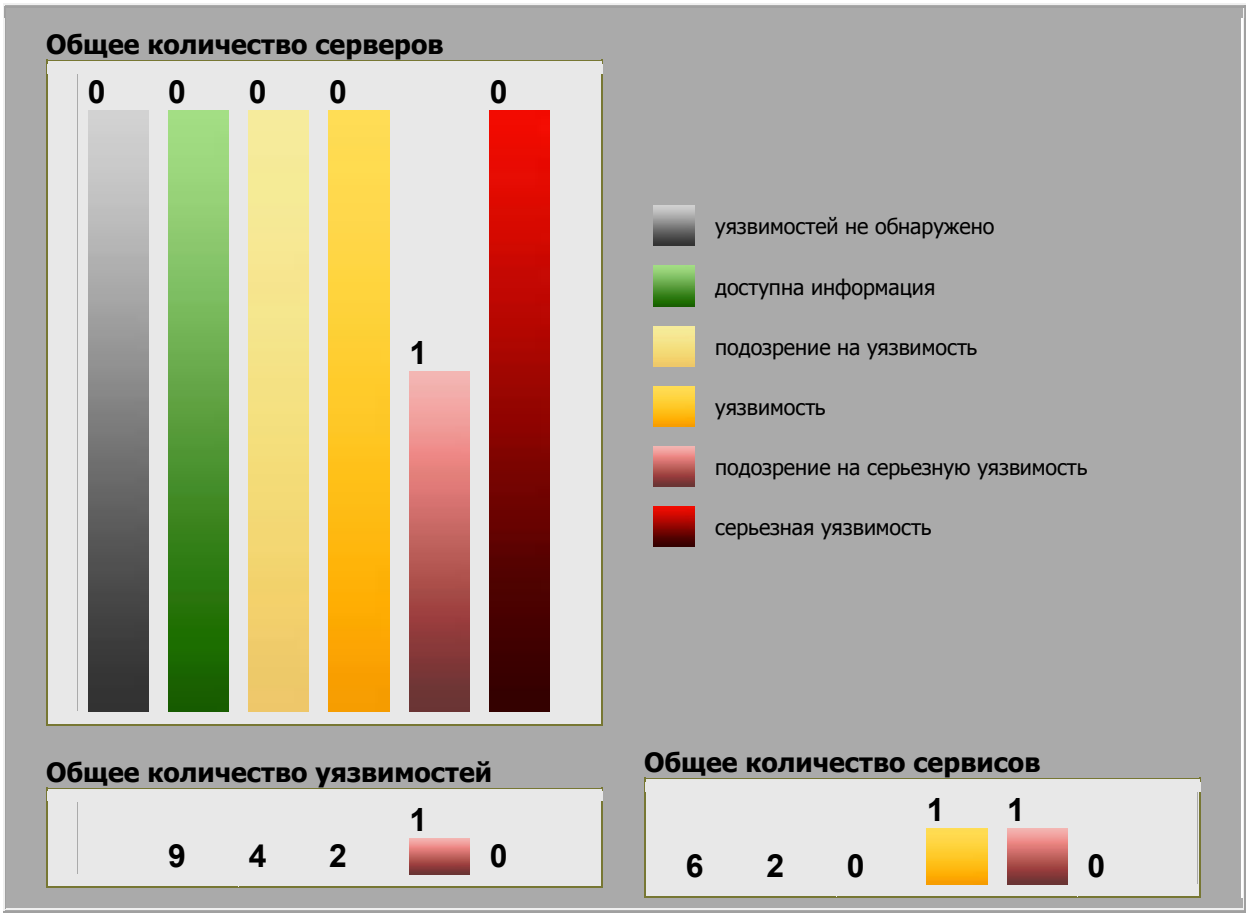
Проверенные хосты

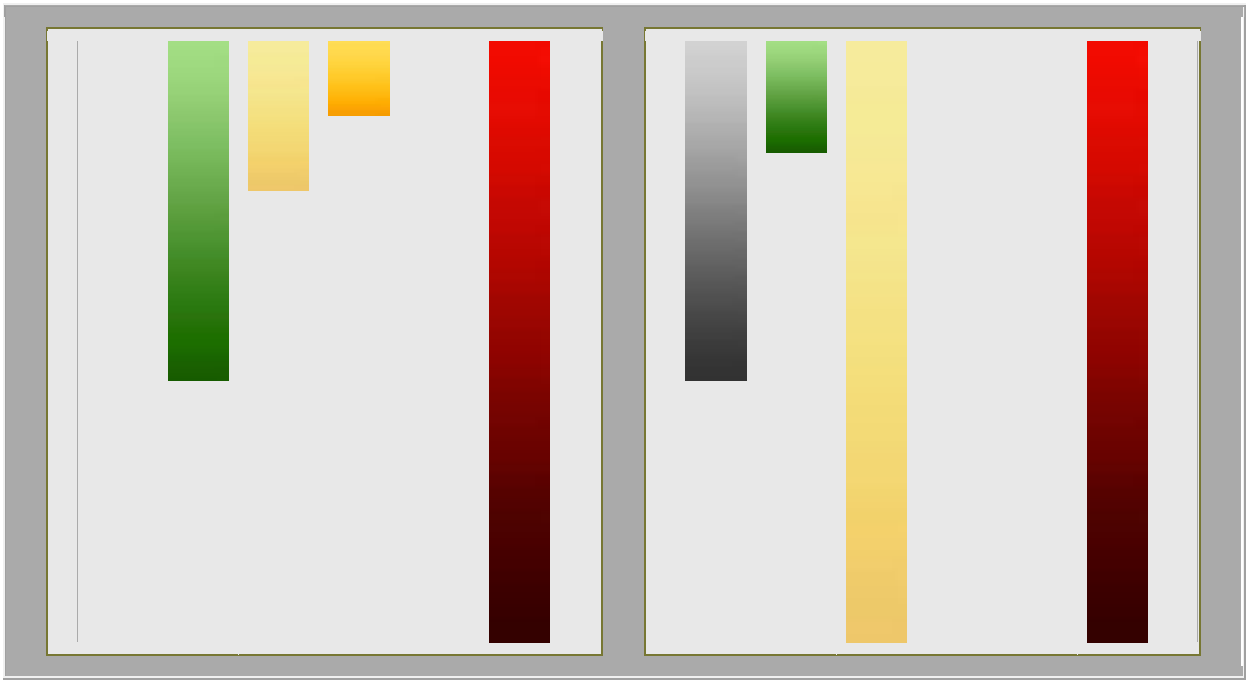
1		192.168.0.1	21.03.2019 23:50

Легенда

- нет уязвимостей
- доступна информация
- подозрение на уязвимость
- уязвимость
- подозрение на серьезную уязвимость
- серьезная уязвимость
- заблокированный сервис
- неуязвимый сервис
- неидентифицированный сервис
- необработанный сервис
- хост не проверялся
- хост проверен не полностью
- ограничение лицензии

Статистика





Информация о хостах

1 192.168.0.1 **21.03.2019 23:50 / XSpider 7.0 Build 1115**

- Система
- Windows

- 25 / tcp - SMTP
- неавторизованная отправка почты
- 80 / tcp - HTTP
- множественные уязвимости (PHP)
- доступ к директориям на просмотр
- просмотр всех файлов
- повышение привилегий (Apache)
- загрузка файлов (PHP)
- множественные уязвимости (PHP)
- доступен метод TRACE
- информация о PHP
- ссылки с параметрами
- список форм
- список внешних ссылок
- доступ к директориям
- недоступные директории
- 110 / tcp - POP3
- 123 / udp - NTP
- 135 / tcp - RPC Windows
- 143 / tcp - IMAP
- 445 / tcp - Microsoft DS
- 4899 / tcp - Radmin
- удалённое управление
- 32000 / tcp - HTTP

Сервисы и уязвимости

1.0 Система — **192.168.0.1 / TTL= 128**

1.0.1 Уязвимость системы — **192.168.0.1 / TTL= 128**

Windows

Описание

Вероятная версия операционной системы : Windows

1.1 Порт 25 / tcp - SMTP — **192.168.0.1 / TTL= 128**

Порт : **25** / tcp
Сервис : **SMTP**

220 mail.domain.com ESMTP MERAK 2.10.340; Tue, 21 03 2019 00:07:28 +0300

1.1.1 Уязвимость сервиса 25 / tcp - SMTP — **192.168.0.1 / TTL= 128**

неавторизованная отправка почты

Описание

Возможна неавторизованная отправка почты с адреса anybody@microsoft.com на адрес anybody@microsoft.com.

Решение

Закрыть неавторизованный релей.

Ссылки

CVE (CAN-1999-0512) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0512

1.2 Порт 80 / tcp - HTTP — **192.168.0.1 / TTL= 128**

Порт : **80** / tcp
Сервис : **HTTP**

Имя сервера : Apache/1.3.31 (Win32) PHP/4.3.6
состояние : 200 (OK)
текущие дата и время : Mon, 21.03.2019 21:08:11 GMT
формат содержимого : text/html
соединение : close

Информация об имени сервера подтверждена эвристическим методом
Apache HTTP Server (1.3.X)

Версия сервера полученная из файла ошибок : Apache HTTP Server (1.3.31)

1.2.1 Уязвимость сервиса 80 / tcp - HTTP — **192.168.0.1 / TTL= 128**

множественные уязвимости (PHP)

Описание

Обнаружено несколько критических уязвимостей в PHP версий 4 и 5 : различные варианты удаленного выполнение команд, переполнение буфера и разнообразная утечка чувствительной информации.

Уязвимые версии:
PHP до версии 4.3.10
PHP до версии 5.0.3

Решение

Установите последнюю версию: http://www.php.net/downloads.php

Ссылки

CVE (CAN-2004-1018): http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1018
CVE (CAN-2004-1019): http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1019
CVE (CAN-2004-1063): http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1063

CVE (CAN-2004-1064): http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1064
http://www.hardened-php.net/advisories/012004.txt

1.2.2 Уязвимость сервиса 80 / tcp - HTTP **192.168.0.1 / TTL= 128**

доступ к директориям на просмотр

Описание

Директории доступные для просмотра:
/documents/
/icons/

Решение

Закрыть доступ к директориям для просмотра, если он действительно не нужен.

1.2.3 Уязвимость сервиса 80 / tcp - HTTP **192.168.0.1 / TTL= 128**

просмотр всех файлов

Описание

Ссылка - http://192.168.0.1/config/connection.conf
Описание уязвимости : просмотр всех файлов

Уязвимость GetAccess может позволить злоумышленнику получить листинг любой директории на сервере, доступной для чтения веб-серверу.

Решение:

Установите последнюю версию:
http://www.entrust.com/getaccess/

Ссылки:

http://online.securityfocus.com/archive/1/224757

1.2.4 Уязвимость сервиса 80 / tcp - HTTP **192.168.0.1 / TTL= 128**

повышение привилегий (Apache)

Описание

Возможно повышение привилегий пользователя из-за переполнения буфера в файле htpasswd.c при проверке переменных имени пользователя и пароля.

Уязвимые версии:
Apache Software Foundation 1.3.31 и предыдущие

Решение

Обновить до последней версии:
http://httpd.apache.org/download.cgi

Ссылки

XF (apache-htpasswd-bo (17413)): http://xforce.iss.net/xforce/xfdb/17413
http://archives.neohapsis.com/archives/fulldisclosure/2018-19/0547.html

1.2.5 Уязвимость сервиса 80 / tcp - HTTP **192.168.0.1 / TTL= 128**

загрузка файлов (PHP)

Описание

Уязвимость обнаружена в PHP в обработке MIME данных. Уязвимость обнаружена в обработке массивов в SAPI_POST_HANDLER_FUNC() функции в 'rfc1867.c'. "$_FILES" определяет расположение загружаемых файлов. Удаленный пользователь может представить специально обработанный Content-Disposition заголовок в комбинации с уязвимостью обхода каталога, чтобы загрузить файлы в произвольное местоположение, чтобы затем выполнить произвольный код в этих файлах.

Пример:
Content-Disposition: form-data; name="userfile"; filename="../../../test.php"
Для успешной эксплуатации требуется PHP скрипт, который использует "$_FILES" массив для манипуляции с загружаемыми файлами.

Уязвимые версии:
PHP 4.3.8 и предыдущие
PHP 5.0.1 и предыдущие

Решение

Установите последнюю версию:
http://www.php.net/downloads.php

Ссылки
http://bugs.php.net/bug.php?id=28456
http://viewcvs.php.net/viewcvs.cgi/php-src/NEWS.diff?r1=1.1247.2.724&r2=1.1247.2.726
http://archives.neohapsis.com/archives/bugtraq/2018-19/0219.html

1.2.6 Уязвимость сервиса 80 / tcp - HTTP **192.168.0.1 / TTL= 128**

множественные уязвимости (PHP)

Описание
Уязвимость обнаружена в PHP, когда компилирован с включенным параметром 'memory_limit'. Удаленный пользователь может выполнить произвольный код на целевой системе. Атакующий может представить специально сформированный HTTP POST запрос, чтобы перехватить процесс выделения памяти пока Zend HashTables выделяется и инициализируется. Так-же он может представить специально обработанный HashTable destructor pointer и выполнить произвольный код на целевой системе.

Уязвимость обнаружена в PHP в функции strip_tags(). Удаленный пользователь может обойти фильтрацию функции и внедрить произвольные тэги в некоторые Web браузеры. Если отключено 'magic_quotes_gpc' и функция strip_tags() используется для удаления HTML тэгов из данных, представленных пользователем, атакующий может представить специально обработанные тэги, которые не будут должным образом отфильтрованы функцией. Пример: <\0script>

Уязвимость может эксплуатироваться в браузерах Microsoft Internet Explorer и Apple's Safari, которые игнорируют строку '\0' и интерпретируют тэги, приведенные выше, как правильные тэги.

Уязвимые версии:
PHP меньше 4.3.8
PHP меньше 5.0.0
Решение
Установите последнюю версию:
http://www.php.net/downloads.php
Ссылки
CVE (CAN-2004-0594): http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0594
http://security.e-matters.de/advisories/112004.html
http://securitytracker.com/id?1010698

1.2.7 Уязвимость сервиса 80 / tcp - HTTP **192.168.0.1 / TTL= 128**

доступен метод TRACE

Описание
С помощью использования метода TRACE в протоколе HTTP возможно выполнение атаки межсайтовый скриптинг.
Решение
Запретить выполнение этого метода.
Ссылки
Cert (VU#867593): http://www.kb.cert.org/vuls/id/867593
http://www.cgisecurity.com/articles/xss-faq.shtml

1.2.8 Уязвимость сервиса 80 / tcp - HTTP **192.168.0.1 / TTL= 128**

информация о PHP

Описание
Ссылка - http://192.168.0.1/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
Содержание : информация о PHP
(GET /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000 HTTP/1.0)

Решение:

Обновить или настроить программное обеспечение или закрыть доступ к этой ссылке.

1.2.9 Уязвимость сервиса 80 / tcp - HTTP **192.168.0.1 / TTL= 128**

ссылки с параметрами

Описание
Список ссылок найденных на веб-сервере, которые используют какие-либо параметры:

/index.php?caseid=home

1.2.10 Уязвимость сервиса 80 / tcp - HTTP **192.168.0.1 / TTL= 128**

список форм

Описание

Обнаружены формы (POST запрос), использующихся для передачи данных на сервер. В переменных HIDDEN может храниться специфическая или чувствительная информация. Переменные PASSWORD служат для ввода пароля.

Список форм:

POST /index.php HTTP/1.1
name=&mailpref=html&email=&form=new

1.2.11 Уязвимость сервиса 80 / tcp - HTTP **192.168.0.1 / TTL= 128**

список внешних ссылок

Описание

Список внешних ссылок найденных на веб-сервере:

http://www.triangle-solutions.com

http://www.tri7b

1.2.12 Уязвимость сервиса 80 / tcp - HTTP **192.168.0.1 / TTL= 128**

доступ к директориям

Описание

Доступные директории:
/admin/
/config/
/email/
/index/

1.2.13 Уязвимость сервиса 80 / tcp - HTTP **192.168.0.1 / TTL= 128**

недоступные директории

Описание

Существующие, но недоступные директории:
/cgi-bin/

1.3 Порт 110 / tcp - POP3 **192.168.0.1 / TTL= 128**

Порт : **110** / tcp
Сервис : **POP3**

+OK mail.domain.com MERAK 2.10.340 POP3 Tue, 21.03.2019 00:08:16 +0300 <20041221000816@mail.domain.com>

1.4 Порт 123 / udp - NTP **192.168.0.1 / TTL= 128**

Порт : **123** / udp
Сервис : **NTP**

Имя сервиса : Network Time Protocol

1.5 **Порт 135 / tcp - RPC Windows** **192.168.0.1 / TTL= 128**

Порт : **135** / tcp
Сервис : **RPC** **Windows**

Не удалось идентифицировать RPC сервис

1.6 **Порт 143 / tcp - IMAP** **192.168.0.1 / TTL= 128**

Порт : **143** / tcp
Сервис : **IMAP**

* OK MERAK 2.10.340 IMAP4rev1 Tue, 21.03.2019 00:09:02 +0300

1.7 **Порт 445 / tcp - Microsoft DS** **192.168.0.1 / TTL= 128**

Порт : **445** / tcp
Сервис : **Microsoft** **DS**

Имя сервиса : Microsoft Directory Service

1.8 **Порт 4899 / tcp - Radmin** **192.168.0.1 / TTL= 128**

Порт : **4899** / tcp
Сервис : **Radmin**

Имя сервиса : Remote Administrator Server
версия сервера : 2.1 - 2.2

1.8.1 **Уязвимость сервиса 4899 / tcp - Radmin** **192.168.0.1 / TTL= 128**

удалённое управление

Описание
Запущен сервис удалённого управления компьютером.

1.9 **Порт 32000 / tcp - HTTP** **192.168.0.1 / TTL= 128**

Порт : **32000** / tcp
Сервис : **HTTP**

Имя сервера : IceWarp Web Server
состояние : 401 (Access Denied)
аутентификация : Basic realm="MERAK"
текущие дата и время : Tue, 21.03.2019 00:09:26 +0300
формат содержимого : text/html

Подтверждение эвристическим методом не удалось

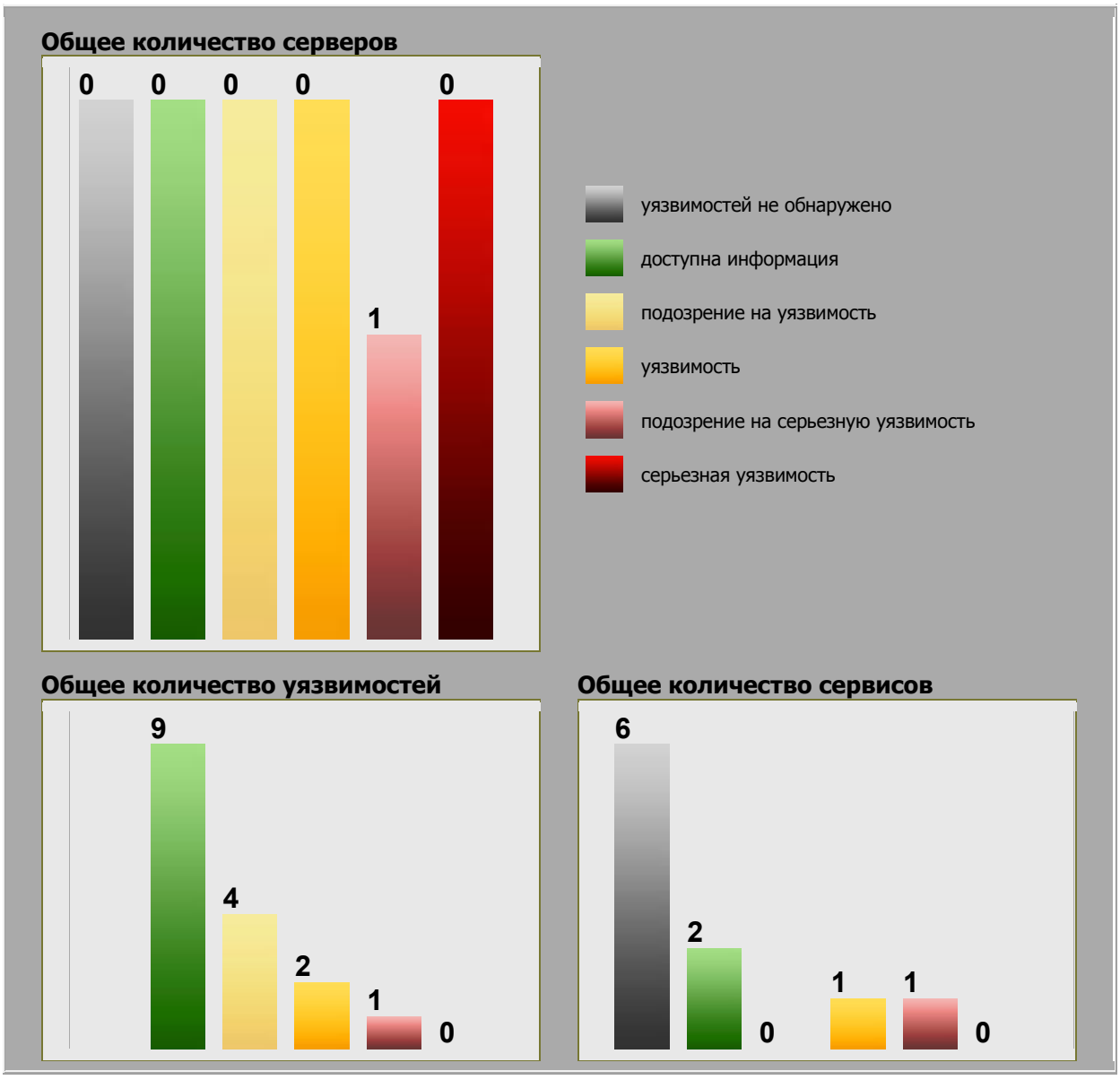
Проверенные хосты

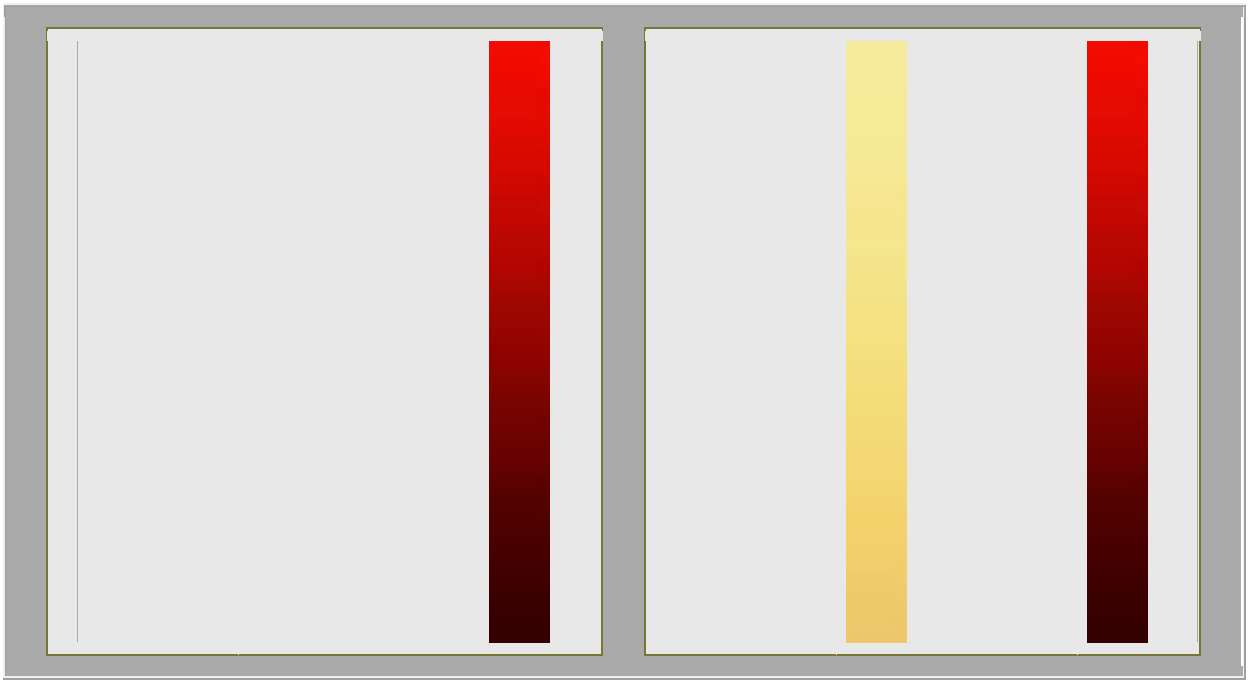
1		192.168.0.1	21.03.2019 23:50

Легенда

- нет уязвимостей
- доступна информация
- подозрение на уязвимость
- уязвимость
- подозрение на серьезную уязвимость
- серьезная уязвимость
- хост не проверялся
- хост проверен не полностью
- ограничение лицензии

Статистика





Примеры отчетов о результатах второго тестирования

XSpider: отчет об уязвимостях | 22.03.2019 16:02

Отчет для системного администратора: развернутая информация по хостам, сервисам, уязвимостям

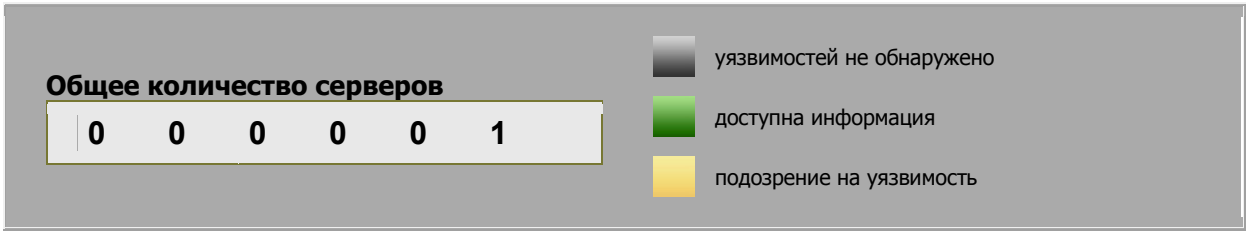
Проверенные хосты

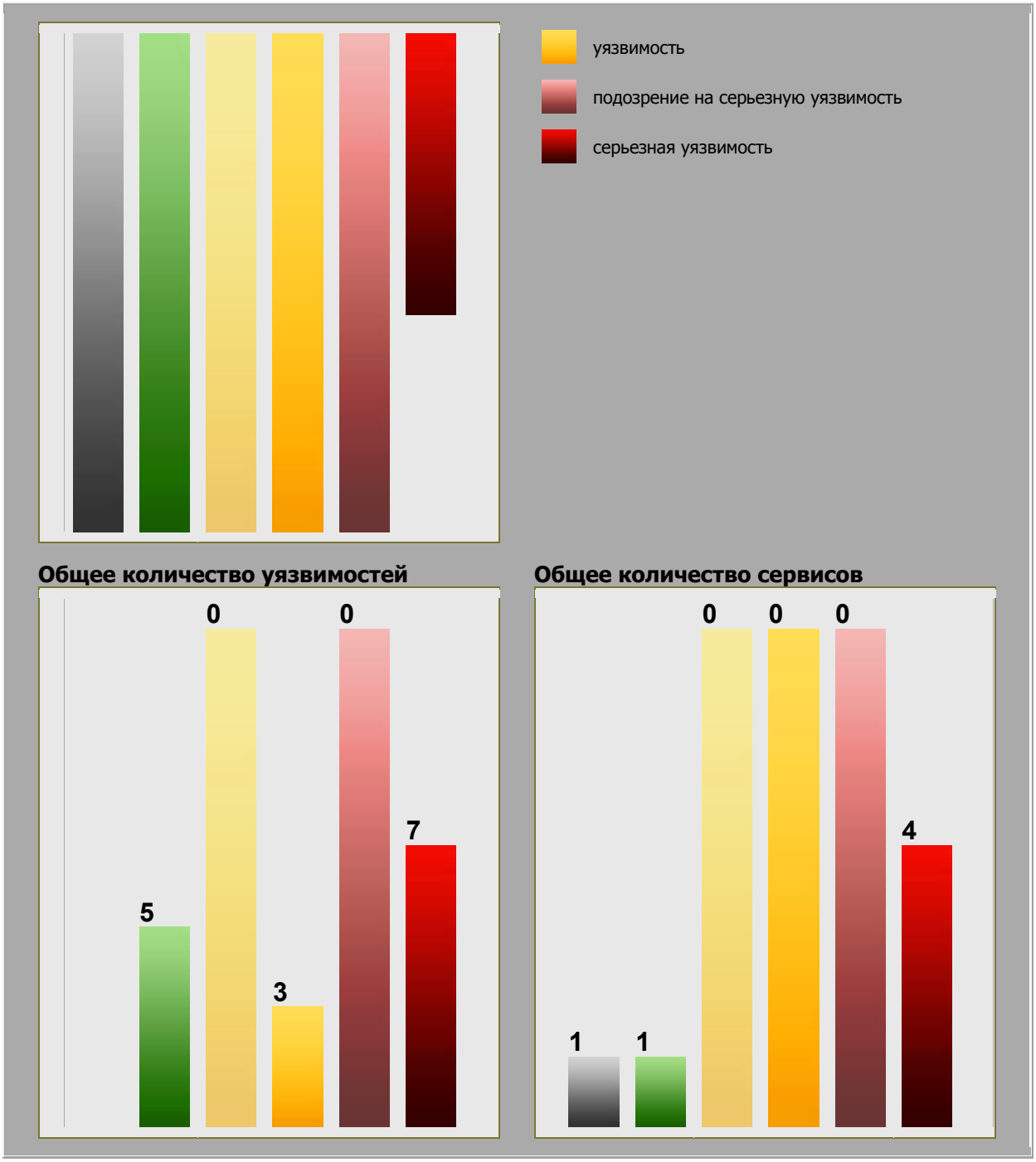
1 192.168.0.1 22.03.2019 15:57

Легенда

- нет уязвимостей
- доступна информация
- подозрение на уязвимость
- уязвимость
- подозрение на серьезную уязвимость
- серьезная уязвимость
- заблокированный сервис
- неуязвимый сервис
- неидентифицированный сервис
- необработанный сервис
- хост не проверялся
- хост проверен не полностью
- ограничение лицензии

Статистика





Информация о хостах

1 192.168.0.1	22.03.2019 15:57 / XSpider 7.0 Build 1115

Система
Windows 5.1

135 / tcp - Microsoft RPC
удаленное выполнение команд (ms03-039)
удаленное выполнение команд (ms04-012)
DoS-атака
запущена служба DCOM

- 135 / udp - Microsoft RPC
- удаленное выполнение команд (ms03-043)
- 137 / udp - NetBIOS-SSN
- 139 / tcp - NetBIOS
- удаленное выполнение команд (ms04-007)
- различные уязвимости (ms04-011)
- список ресурсов
- список активных сессий
- вход любого пользователя
- имя компьютера и домен
- доступ по нулевой сессии
- LanManager и OS
- 445 / tcp - Microsoft DS
- переполнение буфера

Сервисы и уязвимости

1.0 Система — **192.168.0.1 / TTL= 128**

1.0.1 Уязвимость системы — **192.168.0.1 / TTL= 128**

Windows 5.1

Описание

Вероятная версия операционной системы : Windows 5.1

1.1 Порт 135 / tcp - Microsoft RPC — **192.168.0.1 / TTL= 128**

Порт	: **135** /	tcp
Сервис	: **Microsoft**	**RPC**

Имя сервиса : Microsoft Remote Procedure Call

1.1.1 Уязвимость сервиса 135 / tcp - Microsoft RPC — **192.168.0.1 / TTL= 128**

удаленное выполнение команд (ms03-039)

Описание

Возможно получение удаленной командной строки с правами системы из-за переполнения буфера в DCOM RPC сервиса.

Решение

Установите обновление:
http://www.microsoft.com/technet/security/bulletin/MS04-012.mspx

Ссылки

CVE (CAN-2003-0715) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0715
CVE (CAN-2003-0528) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0528
CVE (CAN-2003-0605) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0605

1.1.2 Уязвимость сервиса 135 / tcp - Microsoft RPC — **192.168.0.1 / TTL= 128**

удаленное выполнение команд (ms04-012)

Описание

Возможно получение удаленной командной строки с правами системы из-за переполнения буфера в DCOM RPC сервиса.

Решение

Установите обновление:
http://www.microsoft.com/technet/security/bulletin/MS04-012.mspx

Ссылки

CVE (CAN-2003-0813) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0813

CVE (CAN-2004-0116) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0116
CVE (CAN-2003-0807) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0807
CVE (CAN-2004-0124) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0124

1.1.3 Уязвимость сервиса 135 / tcp - Microsoft RPC — 192.168.0.1 / TTL= 128

DoS-атака

Описание
Возможна DoS-атака на сервис RPC (Remote Procedure Call) с помощью некорректного запроса большой длины. Данная уязвимость приводит к нарушению работы сети компьютера или к его перезагрузке.
Решение
Установите обновление:
http://www.microsoft.com/technet/security/bulletin/ms03-010.asp
Ссылки
http://www.microsoft.com/technet/security/bulletin/ms03-010.asp

1.1.4 Уязвимость сервиса 135 / tcp - Microsoft RPC — 192.168.0.1 / TTL= 128

запущена служба DCOM

Описание
На компьютере запущена служба DCOM (Distributed Component Object Model).
Решение
Отключить службу DCOM, если она действительно не нужна.
Ссылки
CVE (CAN-1999-0658) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0658

1.2 Порт 135 / udp - Microsoft RPC — 192.168.0.1 / TTL= 128

Порт : **135** / udp
Сервис : **Microsoft RPC**

Имя сервиса : Microsoft Remote Procedure Call

1.2.1 Уязвимость сервиса 135 / udp - Microsoft RPC — 192.168.0.1 / TTL= 128

удаленное выполнение команд (ms03-043)

Описание
Переполнение буфера обнаружено в Messenger Service в Microsoft Windows. Удаленный атакующий может выполнить произвольный код на уязвимой системе. Проблема связанна с тем, что Messenger Service не проверяет длину сообщения. В результате злонамеренный пользователь может послать сообщение, которое переполнит буфер и выполнит произвольный код на уязвимой системе с привилегиями SYSTEM.
Решение
Установите обновление:
http://www.microsoft.com/technet/security/bulletin/MS03-043.asp
Ссылки
CVE (CAN-2008-0717) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2018-0717

1.3 Порт 137 / udp - NetBIOS-SSN — 192.168.0.1 / TTL= 128

Порт : **137** / udp
Сервис : **NetBIOS-SSN**

Имя сервиса : NetBIOS (Network Basic Input/Output System) Session Service Protocol

1.4 Порт 139 / tcp - NetBIOS — 192.168.0.1 / TTL= 128

Порт : **139** / tcp
Сервис : **NetBIOS**

Имя сервиса : Network Basic Input/Output System

1.4.1 **Уязвимость сервиса 139 / tcp - NetBIOS** **192.168.0.1 / TTL= 128**

удаленное выполнение команд (ms04-007)

Описание

Переполнение буфера обнаружено в Microsoft ASN.1 Library ("msasn1.dll") в процессе ASN.1 BER декодирования. Уязвимость может эксплуатироваться через различные службы (Kerberos, NTLMv2) и приложения, использующих сертификаты. Удаленный пользователь может послать специально обработанные ASN.1 данные к службе или приложению, чтобы выполнить произвольный код с SYSTEM привилегиями.

Решение

Установите обновление:
http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

Ссылки

CVE (CAN-2008-0818) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0818

1.4.2 **Уязвимость сервиса 139 / tcp - NetBIOS** **192.168.0.1 / TTL= 128**

различные уязвимости (ms04-011)

Описание

Найдено несколько уязвимостей, начиная от DoS-атаки и заканчивая удаленным выполнением команд.

Решение

Установите общее обновление:
http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

Ссылки

CVE (CAN-2003-0663) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0663
CVE (CAN-2003-0719) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0719
CVE (CAN-2003-0806) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0806
CVE (CAN-2003-0907) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0907
CVE (CAN-2003-0908) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0908
CVE (CAN-2003-0909) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0909
CVE (CAN-2004-0119) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0119
CVE (CAN-2004-0120) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0120
CVE (CAN-2004-0123) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0123
CVE (CAN-2003-0533) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0533
CVE (CAN-2003-0906) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0906
CVE (CAN-2003-0910) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0910
CVE (CAN-2004-0118) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0118

1.4.3 **Уязвимость сервиса 139 / tcp - NetBIOS** **192.168.0.1 / TTL= 128**

список ресурсов

Описание

Список ресурсов хоста :

E$ (Стандартный общий ресурс) - диск по умолчанию
IPC$ (Удаленный IPC) - pipe по умолчанию
print$ (Драйверы принтеров) - пользовательский
Z$ (Стандартный общий ресурс) - диск по умолчанию
ADMIN$ (Удаленный Admin) - диск по умолчанию
C$ (Стандартный общий ресурс) - диск по умолчанию

Всегда следует чётко следить за теми данными, которые пользователь предоставляет для общего доступа.

Решение

Windows:
Отключить доступ по нулевой сессии (см. уязвимость "доступ по нулевой сессии")

Samba:
Разрешить доступ к серверу только зарегестрированным пользователям: в файле smb.conf изменить ключ security= share на security= user (или security = server или security = domain).

1.4.4 **Уязвимость сервиса 139 / tcp - NetBIOS** **192.168.0.1 / TTL= 128**

список активных сессий

Описание

Список активных сессий:

хост : 192.168.0.100
пользователь : OFID45F345WDF
длительность подключения : 00:00:01

Получение списка активных сессий позволяет удалённому атакующему атаковать менее защищенные хосты, с которых осуществляются подключения к серверу, с целью получения привилегий на сервере.
Решение
Отключить доступ по нулевой сессии (см. уязвимость "доступ по нулевой сессии") и/или отключить гостевой логин на сервере.

1.4.5 **Уязвимость сервиса 139 / tcp - NetBIOS** **192.168.0.1 / TTL= 128**

вход любого пользователя

Описание
Возможен доступ на сервер для любого пользователя (произвольные логин и пароль).

Доступ к ресурсам :

print$ - только чтение
Решение
Отключить гостевой логин на сервере.

1.4.6 **Уязвимость сервиса 139 / tcp - NetBIOS** **192.168.0.1 / TTL= 128**

имя компьютера и домен

Описание
Имя компьютера : B52
Домен : TIVOLI

доступ по нулевой сессии

Описание
Эта уязвимость существует только в том случае, если Вы не являетесь Администратором на проверяемом хосте.

Доступ по нулевой сессии представляет собой возможность неавторизованного подключения к хосту с операционной системой основанной на Windows NT (или ОС семейства UNIX с установленным пакетом Samba) с пустым логином и паролем. При включенной нулевой сессии анонимный пользователь может получить большое количество информации о конфигурации системы (список расшаренных ресурсов, список пользователей, список рабочих групп и т.д.). Полученная информация в дальнейшем может быть использованна для попыток несанкционированного доступа.
Решение
Windows:
1. В разделе реестра HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA установить значение параметра RestrictAnonymous = 2 для Windows 2000/XP/2003/2007 (1 для Windows NT3.5/NT4.0) (тип параметра - REG_DWORD)

2. Для Windows 2000/XP/2003/2007: В разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver установить значение параметра RestrictNullSessionAccess = 1 (тип параметра - REG_DWORD)

Для Windows NT3.5/NT4.0: В разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer \Parameters
установить значение параметра RestrictNullSessAccess = 1 (тип параметра - REG_DWORD)

3. Перегрузить систему для вступления изменений в силу.

Samba:
Разрешить доступ к серверу только зарегестрированным пользователям:
в файле smb.conf изменить ключ security= share на security= user (или

1.4.7 **Уязвимость сервиса 139 / tcp - NetBIOS** **192.168.0.1 / TTL= 128**

security = server или security = domain).

Ссылки
CVE (CVE-2000-1200) : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1200
http://support.microsoft.com/support/kb/articles/q143/4/74.asp

LanManager и OS
Описание
LanManager: Windows 2000 LAN Manager
OS: Windows 5.1

1.4.8 Уязвимость сервиса 139 / tcp - NetBIOS 192.168.0.1 / TTL= 128

1.5 Порт 445 / tcp - Microsoft DS 192.168.0.1 / TTL= 128

Порт : **445** / tcp
Сервис : **Microsoft DS**

Имя сервиса : Microsoft Directory Service

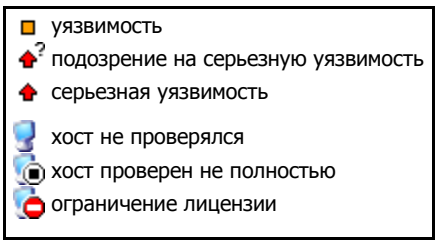
переполнение буфера
Описание
Возможна DoS-атака с помощью запроса большой длины. Размер буфера 10 Кб. Для определения этой уязвимости необходимо хорошее качество связи с проверяемым компьютером. Если вы уверены в качестве связи, то эта уязвимость действительно существует (для уверенности сделайте повторную проверку).
Решение
Обратиться к производителю программного обеспечения, в котором найдена эта уязвимость.

1.5.1 Уязвимость сервиса 445 / tcp - Microsoft DS 192.168.0.1 / TTL= 128

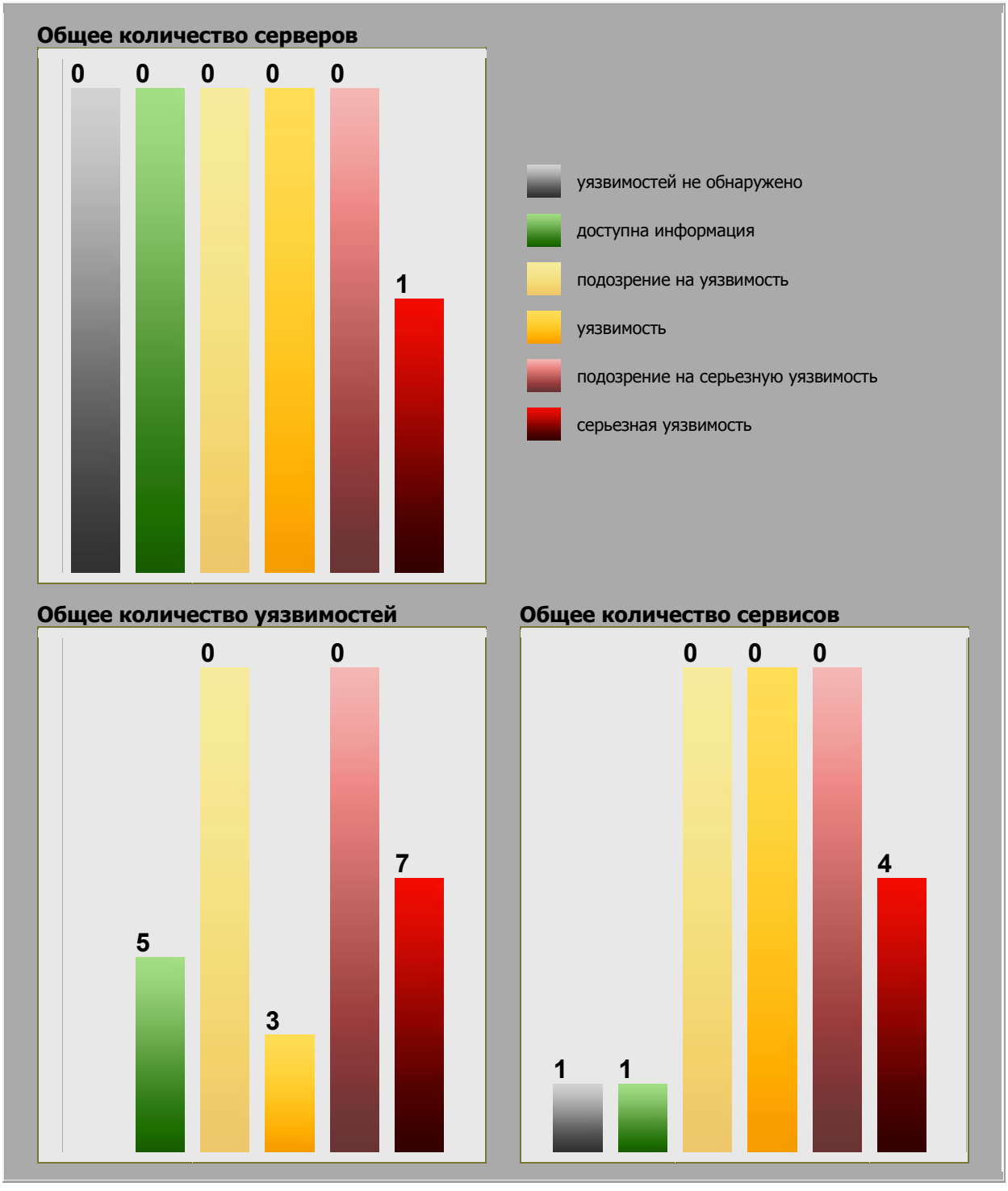
Проверенные хосты

1		192.168.0.1	22.03.2019 15:57

Легенда
- нет уязвимостей
- доступна информация
- подозрение на уязвимость


уязвимость
подозрение на серьезную уязвимость
серьезная уязвимость
хост не проверялся
хост проверен не полностью
ограничение лицензии

Статистика


Общее количество серверов
0
0
0
0
0
1
уязвимостей не обнаружено
доступна информация
подозрение на уязвимость
уязвимость
подозрение на серьезную уязвимость
серьезная уязвимость
Общее количество уязвимостей
5
0
3
0
7
Общее количество сервисов
1
1
0
0
0
4