

ANNOTATION

In this diploma thesis a tool is introduced that can reduce the time a penetration tester needs by automating the process of identifying potential security flaws in PHP source code by using static source code analysis. The finds can then be easily reviewed by the penetration tester in its context without reviewing the whole source code again. Given the limitations of static source code analysis a vulnerability needs to be confirmed by the code reviewer.