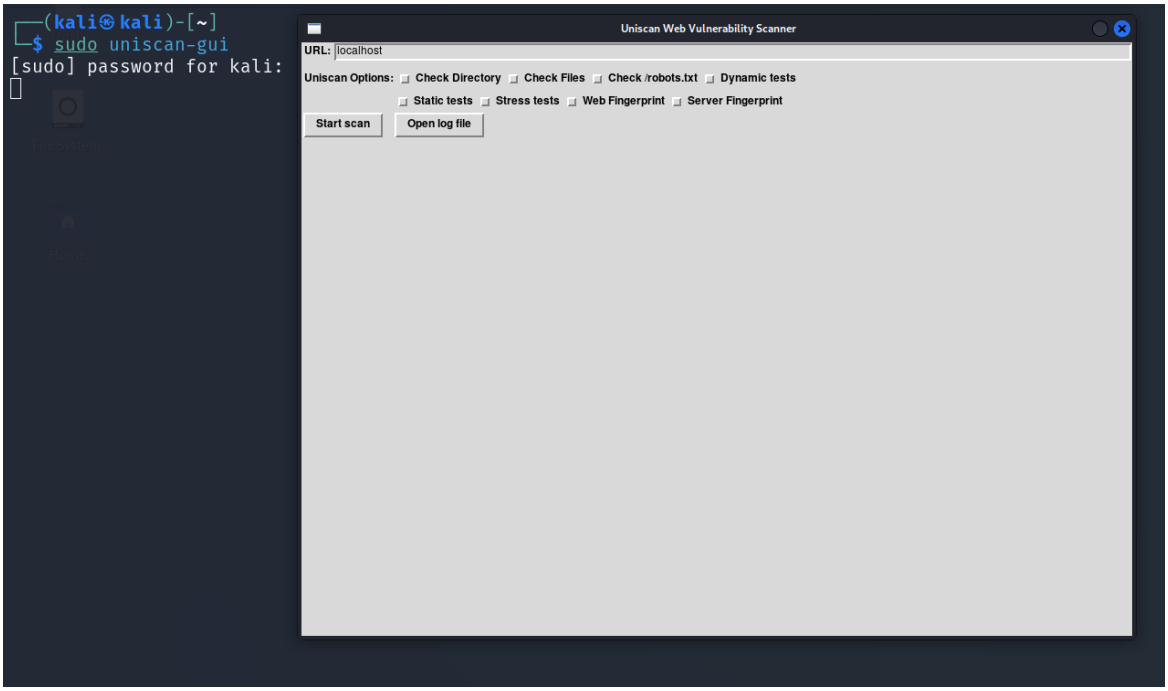
Uniscan

Uniscan is a comprehensive web vulnerability scanner designed to identify security issues in web applications. It supports a range of scanning techniques, including static and dynamic analysis, and can detect common vulnerabilities such as SQL injection, cross-site scripting (XSS), and file inclusion exploits. Uniscan is available in both command-line and graphical user interface (GUI) versions, making it accessible to both advanced users and those who prefer a more user-friendly interface. By automating the detection of web application vulnerabilities, Uniscan helps security professionals and developers enhance the security posture of their web applications and mitigate potential threats effectively.

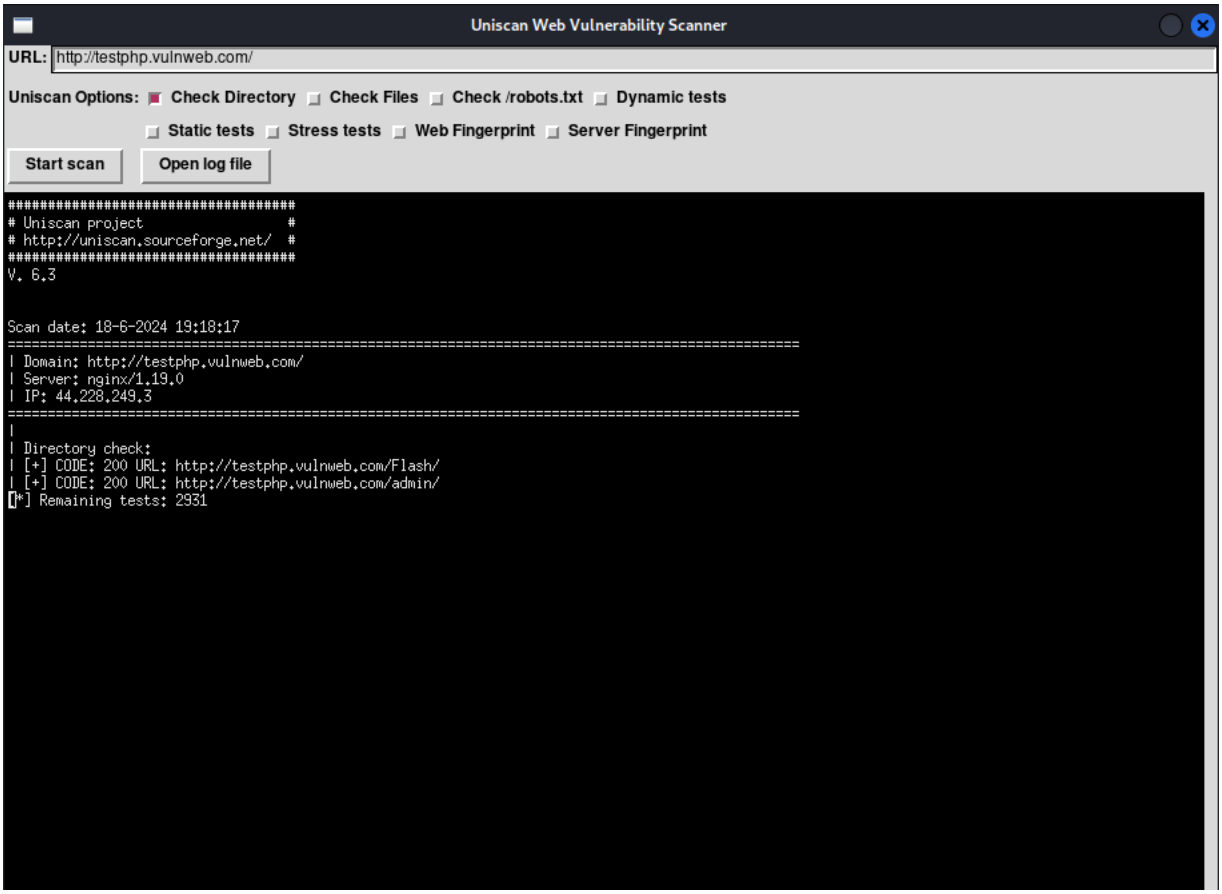
Vulnerability Scanners are game-changing tools that detect a vulnerability on the target domain. Uniscan tool is an automated tool developed in the Perl Language used for Fingerprinting and Vulnerability Testing. Uniscan tool is available on GitHub. Uniscan tool is an open-source and free-to-use tool. Its GUI Version is too powerful and easy to use as all the results are shown in the GUI Window itself.

Examples: -

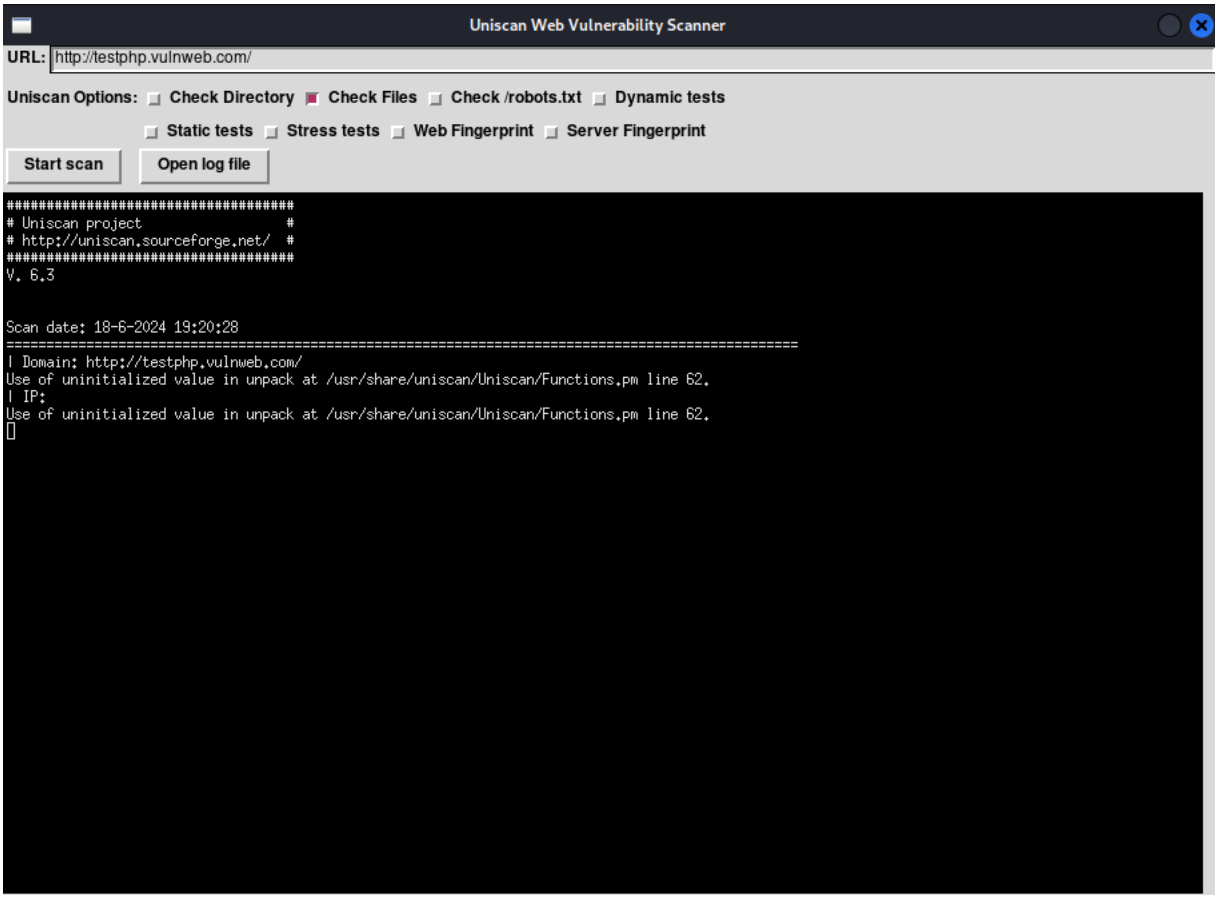
1. To run the uniscan use uniscan-gui command inside terminal and inside URL section enter the target URL.



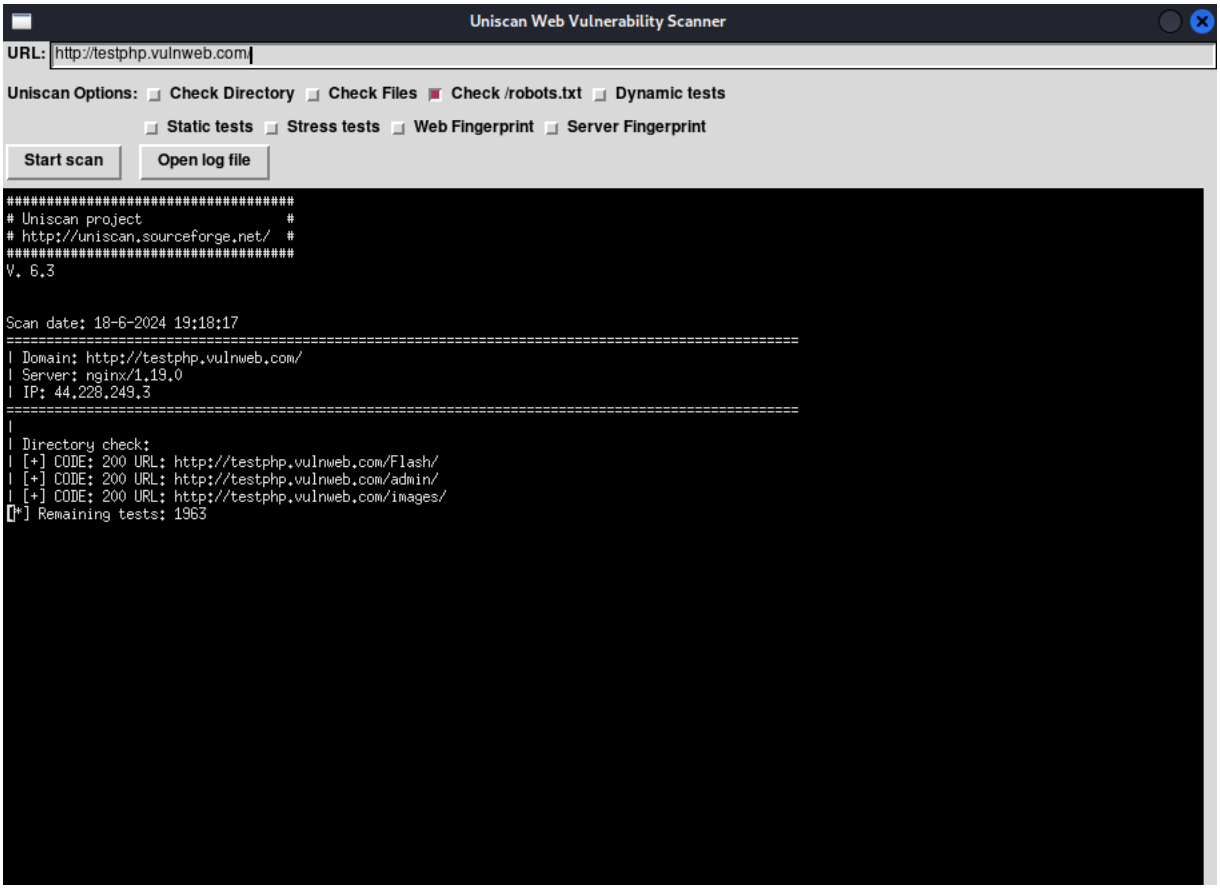
2. This scan for exposed directories on the web server. This includes directories that should not be publicly accessible, such as administrative interfaces, temporary directories, and directory.



3. It involves scanning for common and sensitive files on the web server that may be accessible publicly.



4. This is used to find hidden or sensitive directories and files that might be disallowed for legitimate crawlers.



5. The Dynamic checks involve active interaction with the web application to identify vulnerabilities that require execution, such as SQL injection, cross-site scripting (XSS), and other injection flaws.