What Is Web Application scanning ?

Web Application Scanning is a critical process that helps ensure reliability, Security and usability of web based applications. Employing Web application scanning is a way to identify potential issues with applications before launch.

Why Web Application ?

Web Application is a necessary component when it comes to Red Teaming. It's important to understand the vulnerabilities in which any of your web application may have. In terms of why you should Test your web applications. It’s important to remember that when releasing anything that users will interact with it’s required to make sure your applications meets the necessary needs of that of the users and to provide and safe and secure web application users can interact with.

Types of Web Applications Testing Methods

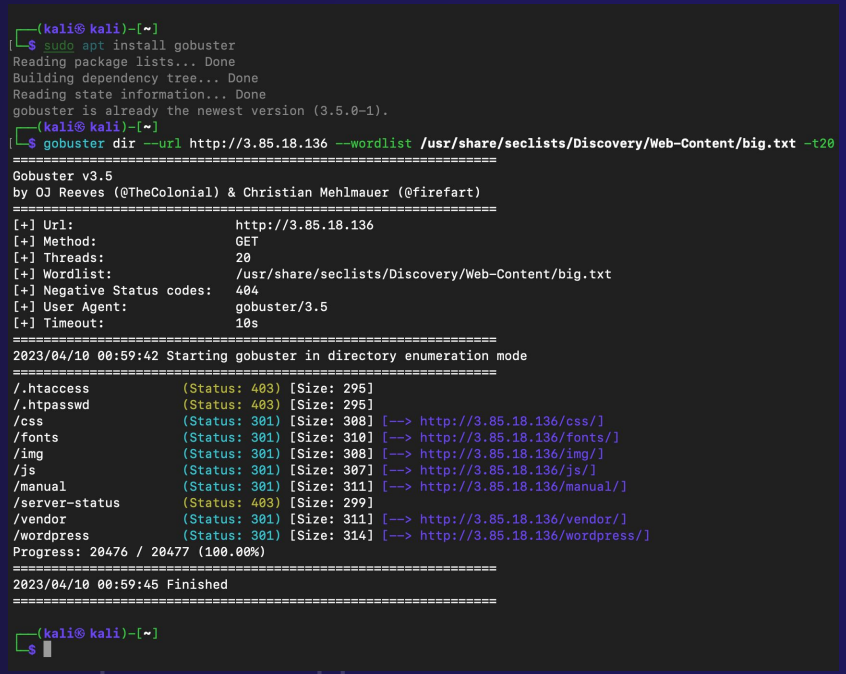
- **Automated testing** is a popular testing methodology that leverages automated tools and scripts to reduce testing time and effort and improve test coverage. Automated testing involves using software tools to execute test cases automatically, which helps save time and reduce manual errors.

- **manual testing** involves testers performing various tests on the web application. Manual testing is often used for exploratory testing, where testers perform ad-hoc testing to identify defects that might not have been identified during automated testing.

- **Security testing** ensures that the application is secure from various security threats. Analyzing which ports are open and what is allowed inbound and outbound.

- **Compatibility testing** aims to ensure that the application works seamlessly across various devices, browsers, and platforms, To ensure all users have a good experience with the application.

How to perform a directory Brute force using Gobuster



First you install gobuster.

Secondly You run the gobuster command.

Technical Documentation needed.

What is APPTRANA ?

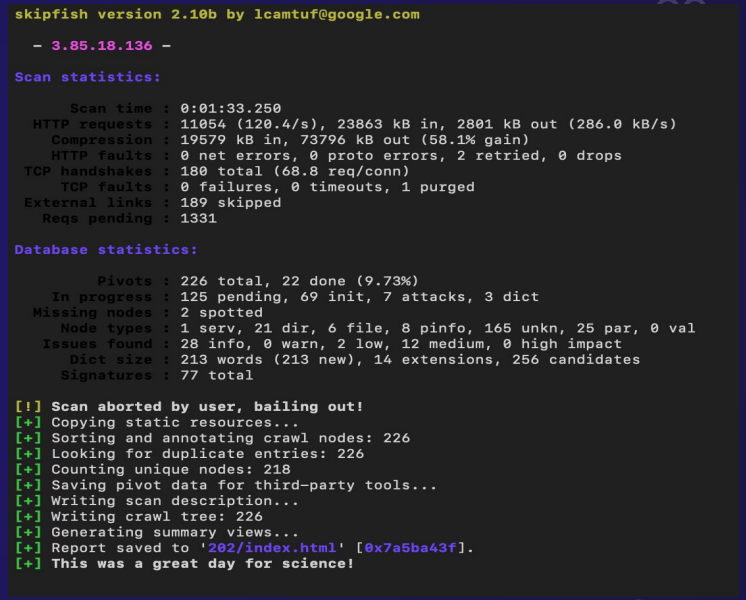
APPTRANA is a website and application tool. Designed to help businesses to manage and maintain cloud security using scanning, Pen testing, Risk detection. Also provides a dashboard to give more a visual to see what's going on with you web application security.

What is skipfish? How does it work?

SkipFish is a free open source automated penetration testing tool available on Github made for security researchers. Skipfish is used for Information Gathering and testing the security of websites and web servers. Skipfish is also known as an active web application security reconnaissance tool

Example of skipfish

In the screenshot you are seeing skipfish in action i'm using it to scan a vulnerable wordpress website. As you can see it does a typical network scan but also does a database scan as seen in the second row.



What is WAPITI?

- Wapiti is a command line tool to automate the audit of a web application.
- List of commands and different options used when running WAPITI Below.
- https://owasp.org/www-community/Automated_Audit_using_WAPITI