Zaproxy

OWASP Zap is a security testing framework much like Burp Suite. It acts as a very robust enumeration tool. It's used to test web applications.

Why wouldn't I use Burp Suite?

That's a GOOD question! Most people in the Info-sec community DO just use Burp Suite. But OWASP ZAP has a few benefits and features that the Burp Suite does not and it's my preferred program of the two.

What are the benefits to OWASP ZAP?

It's completely open source and free. There is no premium version, no features are locked behind a paywall, and there is no proprietary code.

There's a couple of feature benefits too with using OWASP ZAP over Burp Suite:

- Automated Web Application Scan: This will automatically passively and actively scan a web application, build a sitemap, and discover vulnerabilities. This is a paid feature in Burp.
- Web Spidering: You can passively build a website map with Spidering. This is a paid feature in Burp.
- Unthrottled Intruder: You can bruteforce login pages within OWASP as fast as your machine and the web-server can handle. This is a paid feature in Burp.
- No need to forward individual requests through Burp: When doing manual attacks, having to change windows to send a request through the browser, and then forward in burp, can be tedious. OWASP handles both and you can just browse the site and OWASP will intercept automatically. This is NOT a feature in Burp.

This guide will teach you how to do the following in ZAP:

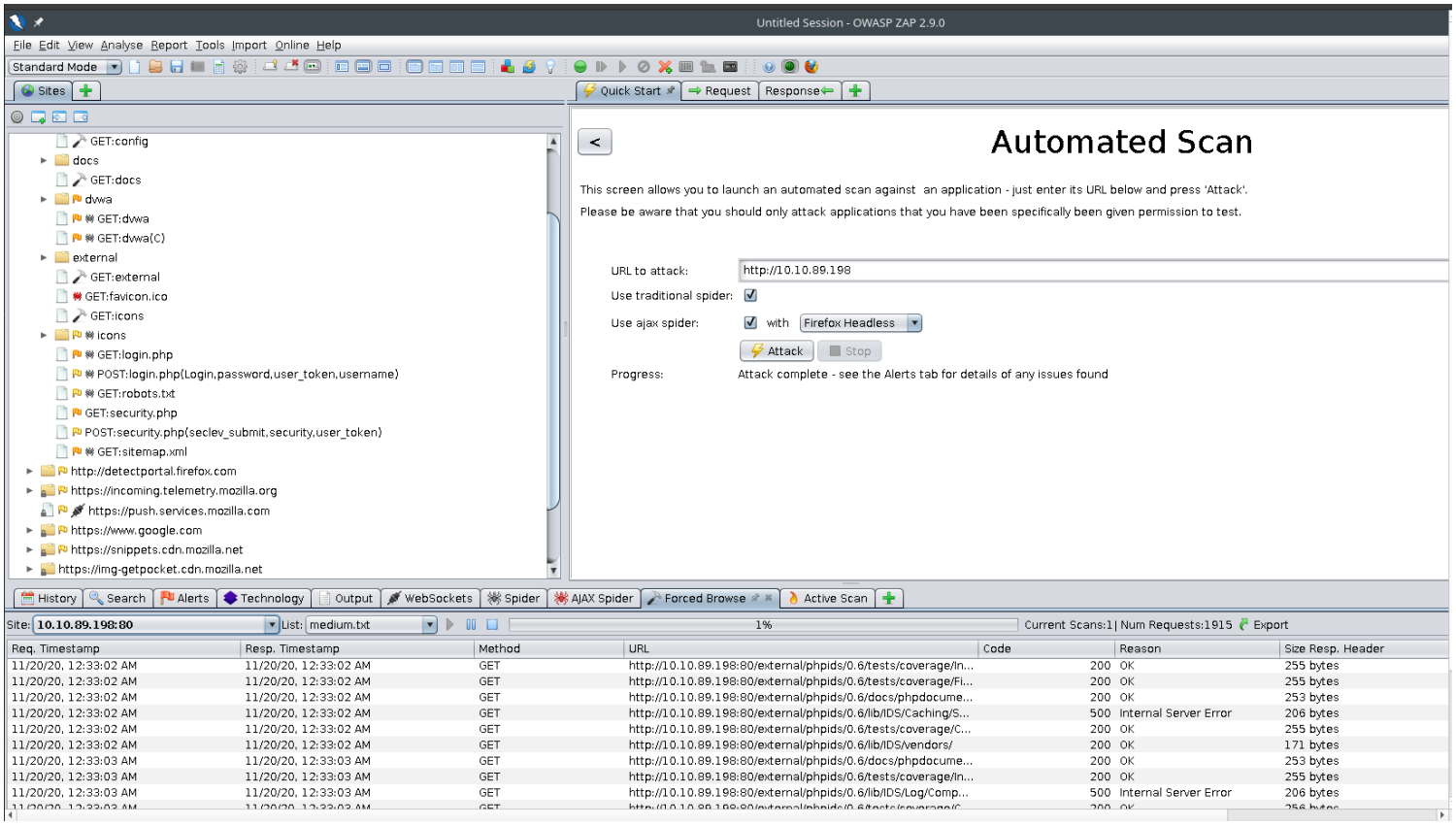
- Automated Scan
- Directory Bruteforce
- Authenticated Scan
- Login Page Bruteforce
- Install ZAP Extensions

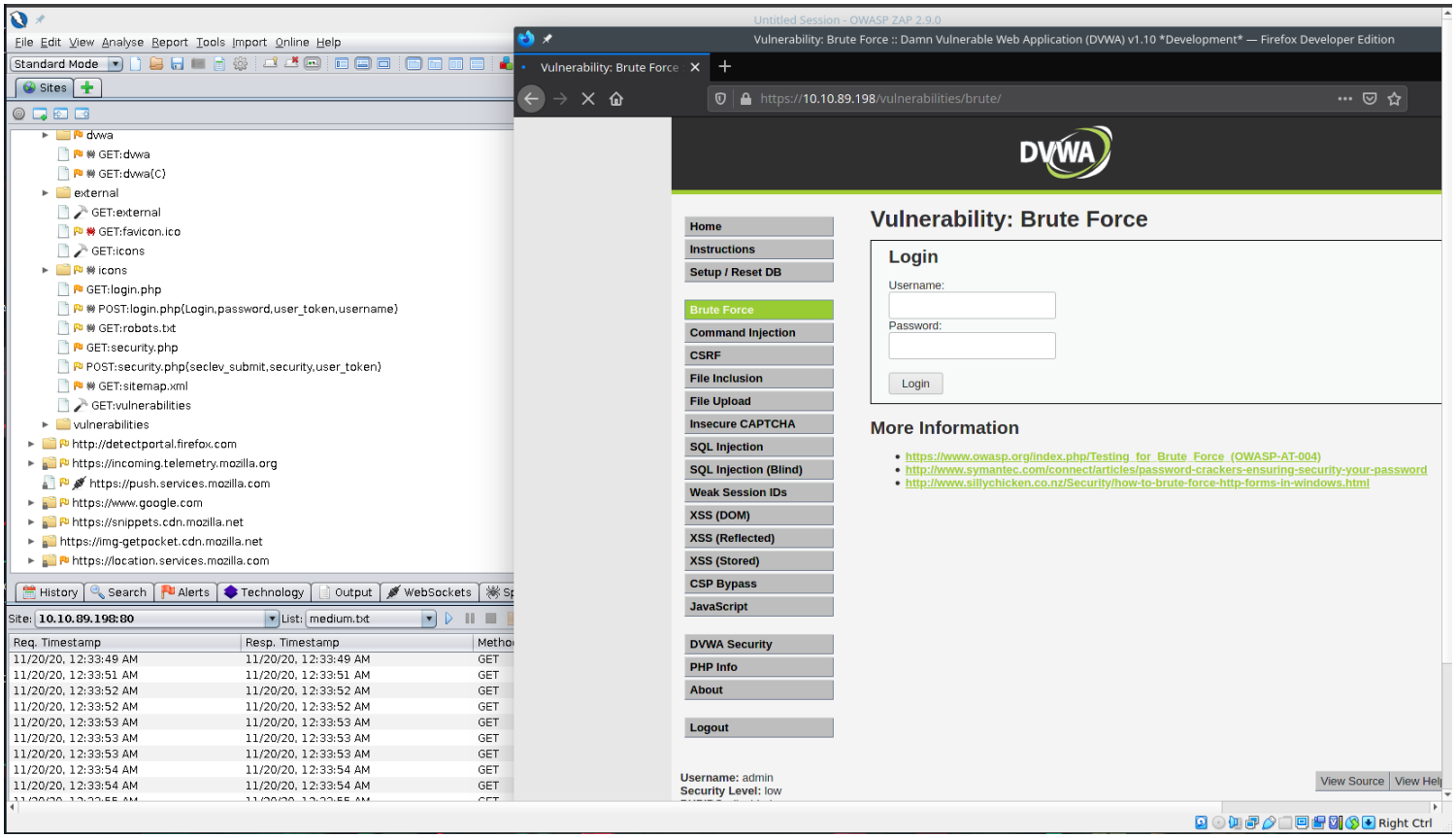
The automated scan performs both passive and automated scans to build a sitemap and detect vulnerabilities.

On the next page you may see the options to select either to use "traditional spider" or "Ajax spider".

A traditional spider scan is a passive scan that enumerates links and directories of the website. It builds a website index without brute-forcing. This is much quieter than a brute-force attack and can still net a login page or other juicy details, but is not as comprehensive as a bruteforce.

The Ajax Spider is an add-on that integrates in ZAP a crawler of AJAX rich sites called Crawljax. You can use it in conjunction with the traditional spider for better results. It uses your web browser and proxy.


Untitled Session - OWASP ZAP 2.9.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://10.10.89.198
Use traditional spider:
Use ajax spider:
with
Firefox Headless
Attack
Stop
Progress:
Attack complete - see the Alerts tab for details of any issues found
History
Search
Alerts
Technology
Output
WebSockets
Spider
AJAX Spider
Forced Browse
Active Scan
Site: 10.10.89.198:80
List: medium.txt
1%
Current Scans:1 | Num Requests:1915
Export
Req. Timestamp
Resp. Timestamp
Method
URL
Code
Reason
Size Resp. Header


Vulnerability: Brute Force :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* — Firefox Developer Edition
https://10.10.89.198/vulnerabilities/brute/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout
Vulnerability: Brute Force
Login
Username:
Password:
Login
More Information
https://www.owasp.org/index.php/Testing_for_Brute_Force_(OWASP-AT-004)
http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html
Username: admin
Security Level: low
View Source
Right Ctrl