ZAP Proxy and OWASP Top 10

Author: MCS Eduard Ramos Flores

Advisor: PhD Jeff Duffany

Graduate School, Polytechnic University of PR

Electrical & Computer Engineering and Computer Science Department

Abstract

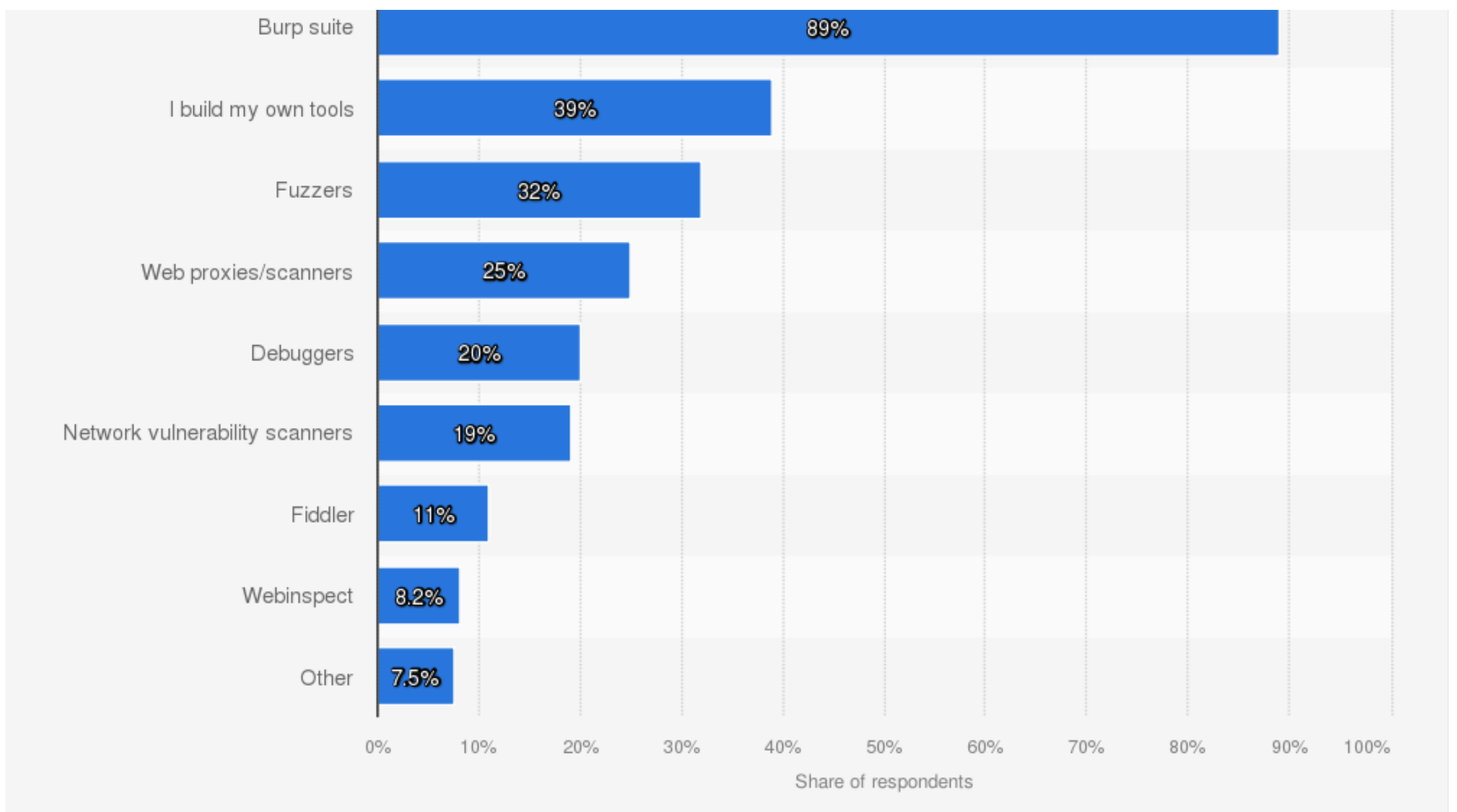
The Zed Attack Proxy is a well-known and popular assessment tool in the cybersecurity community. The Open Web Application Security Project community offers, develops, and maintains the Zed Attack Proxy. The Open Web Application Security Project community also publishes the top ten security risks faced by web applications. Paired with the Zed Attack Proxy, The Open Web Application Security Project's top 10 security risks publication, serves as a baseline for security professionals assessing the security compliance of web applications. This study aims to evaluate the effectiveness and efficiency of the Open Web Application Security Project's Zed Attack Proxy tool against real world production web applications and vulnerable by design penetration labs web applications.

Introduction

Open Web Application Security Project provides the Zed Attack Proxy tool. To assess Zed Attack Proxy's capabilities, various scans of web applications were performed to demonstrate Zed Attack Proxy's functionality and capability assessing the Open Web Application Security Project's top ten security risks.

Background

A survey published in 2020 states that in 120 countries and territories 69% of the participants chose Burpsuite as a security assessment tool, leaving Zed Attack Proxy in fourth place with 25% popularity. This study aims to assess the usability, efficiency and effectiveness of Zed Attack Proxy as a security assessment tool. And to find the reason for the 64% difference in popularity for the tools.

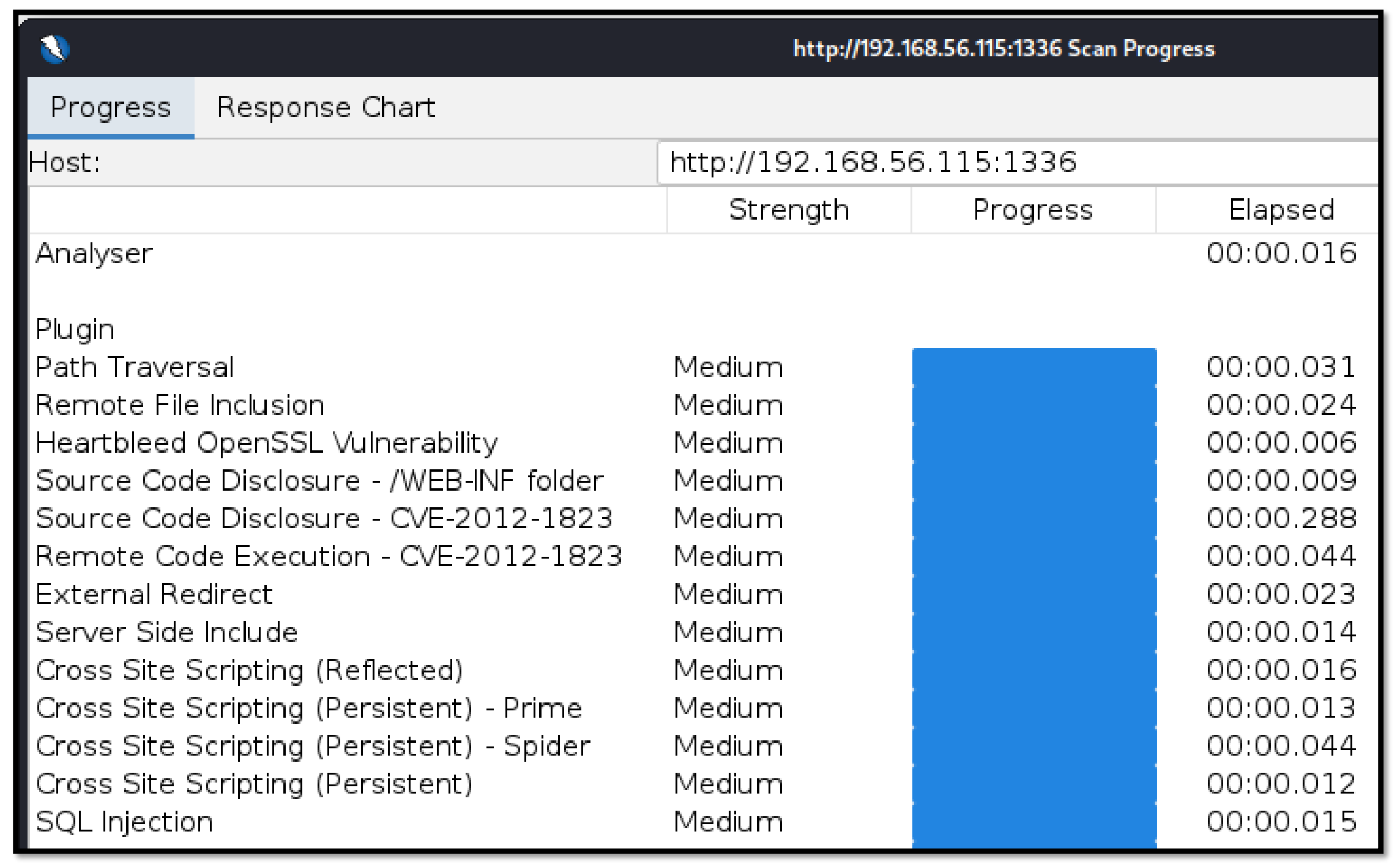


Problem

For profit security assessment tools for web applications aim to provide ease of use, effective functionality, and accurate reporting. If a paid for tool is mature, it can even go as far as to provide the ability to perform advanced assessments using functions like automation for example. Security assessment software, still requires knowledge and skillset considered intermediate to advanced. Is Zed Attack Proxy capable of successfully meeting the needs of a security practitioner? Is there a handicap in Zed Attack Proxy that justifies monetary investment in a proprietary tool?

Methodology

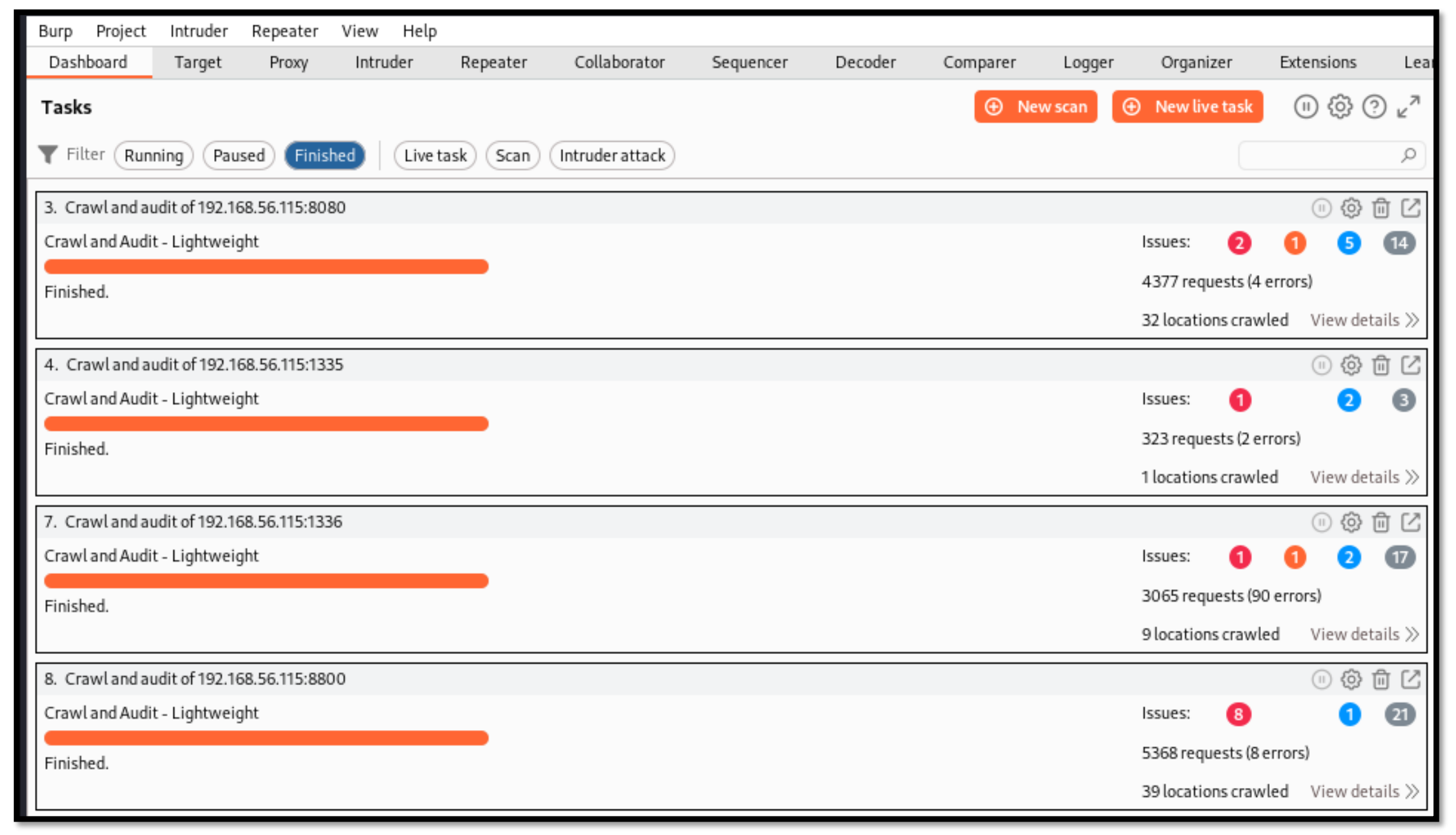
To evaluate the capabilities of the assessment tools, pentesting vulnerable web applications were scanned. These web applications are purposedly designed to present flaws like SQL Injection, Broken Authentication, Cross Site Scripting (XSS) among others. Resources like PortSwigger's Web Security Academy, Zed Attack Proxy in Ten, and Open Web Application Security Project Web Security Testing Guide 4.2 were used as validation reference.



```
http://192.168.56.115:1336 Scan Progress

Host:                                          http://192.168.56.115:1336
                                              Strength   Progress   Elapsed
Analyser                                                            00:00.016

Plugin
Path Traversal                                 Medium               00:00.031
Remote File Inclusion                          Medium               00:00.024
Heartbleed OpenSSL Vulnerability               Medium               00:00.006
Source Code Disclosure - /WEB-INF folder       Medium               00:00.009
Source Code Disclosure - CVE-2012-1823         Medium               00:00.288
Remote Code Execution - CVE-2012-1823          Medium               00:00.044
External Redirect                              Medium               00:00.023
Server Side Include                            Medium               00:00.014
Cross Site Scripting (Reflected)               Medium               00:00.016
Cross Site Scripting (Persistent) - Prime      Medium               00:00.013
Cross Site Scripting (Persistent) - Spider     Medium               00:00.044
Cross Site Scripting (Persistent)              Medium               00:00.012
SQL Injection                                  Medium               00:00.015
```



```
Tasks

3. Crawl and audit of 192.168.56.115:8080
Crawl and Audit - Lightweight                  Issues: 2 1 5 14
Finished.                                      4377 requests (4 errors)
                                               32 locations crawled

4. Crawl and audit of 192.168.56.115:1335
Crawl and Audit - Lightweight                  Issues: 1 2 3
Finished.                                      323 requests (2 errors)
                                               1 locations crawled

7. Crawl and audit of 192.168.56.115:1336
Crawl and Audit - Lightweight                  Issues: 1 1 2 17
Finished.                                      3065 requests (90 errors)
                                               9 locations crawled

8. Crawl and audit of 192.168.56.115:8800
Crawl and Audit - Lightweight                  Issues: 8 1 21
Finished.                                      5368 requests (8 errors)
                                               39 locations crawled
```

Results

The following tables show results by website name, vulnerability and Common Weakness and Enumeration category. The CWE code can be used to obtain details of the discovery. For Table 1, only the results that matched from scans performed by both tools are listed. The results shown by vulnerable by design bWApp, DVWApp, Mutillidae II and WebGoat were expected.

TABLE 1
VULNERABILITIES FOUND BY BOTH BURP SUITE AND ZED ATTACK PROXY

Site	Vulnerability	Category
bWApp	Clear Text Password Submission	CWE-319 CAPEC-117
DVWApp	None	
OWASP Mutillidae II	Cross Site Scripting	CWE-1021
WebGoat	None	
Amazon	HTTP Strict Transport Security (HSTS)	CWE-523
Facebook	Cross Site Scripting	CWE-1021
NmapWeb	Missing Anti-clickjacking Header	CWE-693 CWE-1021 CAPEC-103
Microsoft	None	

Table 1 Shared Findings

Scans performed with Zed Attack Proxy (Table 2) show individual results that were not discovered by BurpSuite.

TABLE 2
VULNERABILITIES FOUND BY ZED ATTACK PROXY BUT NOT FOUND BY BURP SUITE

Site	Vulnerability	Category
bWApp	Hidden Sensitive File Found phpinfo.php	OWASP_2021_A05 WSTG-v42-CONF-05 OWASP_2017_A06
DVWApp	None	
OWASP Mutilidae II	Directory Browsing, SQL Injection, Source Code Disclosure	CVE-2012-1823
WebGoat	None	
Amazon	None	
Facebook	Cookie No HttpOnly Flag	CWE-16 CAPEC-31
NmapWeb	Server Leaks Version Information via "Server" HTTP Response Header Field	CWE-200
Microsoft	Vulnerable JS Library	CVE-2020-11023 CVE-2020-11022 CVE-2019-11358

Table 2 Zed Attack Proxy Findings

BurpSuite reported vulnerabilities (Table 3) that were not discovered by Zed Attack Proxy during scans.

TABLE 3
VULNERABILITIES FOUND BY BURP SUITE BUT NOT FOUND BY ZED ATTACK PROXY

Site	Vulnerability	Category
bWApp	Cookie No HttpOnly Flag	CWE-16 CAPEC-31
DVWApp	Clear Text Password Submission	CWE-319 CAPEC-117
OWASP Mutilidae II	XPath injection	CWE-94 CWE-116 CWE-159 CWE-643 CAPEC-83
WebGoat	Clear Text Password Submission	CWE-319 CAPEC-117
Amazon	TLS certificate	CWE-295 CWE-326 CWE-327
Facebook	Password field with autocomplete enabled	CWE-200
NmapWeb	Unencrypted communications	CWE-326
Microsoft	TLS certificate	CWE-295 CWE-326 CWE-327

Table 3 Burp Suite Findings

Conclusion

Burp Suite may enjoy more popularity among seasoned cybersecurity professionals for its advanced tools and granularity, but it comes at a cost. Two of the most useful tools required by every security practitioner, an automated scanner and reporting capabilities are only available on Burp Suite Professional and Enterprise which require an annual paid subscription from the user. BurpSuite's user interface requires understanding of PortSwigger's view of how a security assessment of a web application should be performed. The analysis of Zed Attack Proxy show that the tool is very well suited as an everyday tool for novice to advanced security practitioners. The tool bundles all the functionality and reporting needed out of the box allowing for a thorough assessment of a web application's security scorecard. The support from the open-source developers community provides some guarantee that the tool will be continuously updated. For comprehensive web application security testing, and based on the study findings, it is recommended to use both Zed Attack Proxy and Burp Suite as each tool uncovers unique vulnerabilities the other might miss.

Future Work

How efficient is the automation feature offered by Zed Attack Proxy. Is Zed Attack Proxy as effective through automation as it is in standalone use. How does performance scale through the leverage of container technologies used by the automation feature. In terms of cloud computing, could it possible to scale out or up through automation. If true, why this capability does not add to Zed Attack Proxy's popularity?

References

1. OWASP, "OWASP foundation, the open source foundation for application security," owasp.org, Dec. 01, 2001. https://owasp.org/
2. OWASP, "OWASP ZAP," Zaproxy.org, 2020. https://www.zaproxy.org/
3. Open Web Application Security Project Foundation, "OWASP Top Ten Web Application Security Risks | OWASP," owasp.org, Dec. 01, 2001. https://owasp.org/www-project-top-ten
4. L. Sujay Vailshery, "Best Tools for Hacking 2020," Statista, Mar. 23, 2020. https://www.statista.com/statistics/800916/worldwide-useful-software-hacking (accessed May 20, 2023).
5. Open Web Application Security Project Foundation, "WSTG - v4.2 | OWASP," owasp.org, Dec. 03, 2020. https://owasp.org/www-project-web-security-testing-guide/v42/

Acknowledgements

I would like to thank PUPR and the National Science Foundation Cybercorps program for my SFS scholarship. Ph.D. Jeff Duffany for his great insight and incredibly engaging teaching methods. And the Graduate School remarkable staff for their help throughout this process.