International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 29th June 2021.
Link: https://ijiemr.org/downloads/Volume-10/Issue-06

DOI: 10.48047/IJIEMR/V10/I06/40

Title: **OPEN WEB APPLICATION SECURITY PROJECT (OWASP)**

Volume 10, Issue 06, Pages: 199-204

Paper Authors: **Oripov Rustamjon Xoldorali o'g'li[1], AxmedovYusufxonAlisher o'g'li[2], Radjabova Madina Shavkatovna[3], Sofoyeva Fotima Davlatyorovna[4]**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

Oripov Rustamjon Xoldorali o'g'li[1], AxmedovYusufxonAlisher o'g'li[2], Radjabova Madina Shavkatovna[3], Sofoyeva Fotima Davlatyorovna[4]
[1,2,3,4]Tashkent University of Information technology named after Muhammad Al-Kharazmiy masters degree's 1-cource students

Abstract: Using widely of web vulnerability testing applications and their differences in effectiveness make them common and effective these scanners. The OWASP ZAP application, which is belong to the Open Web Application Security Project (OWASP), a common non-profit web security organization. The goal of research paper is identifying the primary quality characteristics of functionality OWASP ZAP application from app user's perspective and what type of organizations actually interested in to use it. Furthermore, it is presented the outcome based on a task-based evaluation that involved over 31.000 users of different level of experience from diverse organizations conducted by IT Central station center (specialized to gathering and comparing feedbacks and application users result). Apart from that how the usability evaluation of penetration testing application also addressed.

Keywords: penetration testing, owasp zap, web resources, vulnerabilities, penetration testers.

Introduction

Today we are living more developed Information technology world, we have much systems that are transmitted on online regime. It means that information is more vulnerable than ever before; and every technological system grows new security threat that requires new security solutions. According to the Internet Security Threat Reports by Symantec, web-based attacks are increased 56% growth in the past few years. Average 30 to 40 million attacks are detected per month[1]. In the recent years web application exploitation has been used excessively against internet-based applications.Thus, conducting security audit and controlling probability of risks is growing day by day as the cyber threat is increasing.The penetrating testing is used regularly to conduct identify risks and manage them to achieve higher security standards. The penetration test is a controlled process of penetrating into the network or web application environment in order to identify the vulnerabilities [1]. Along with this growing need there is also a growing need of standardization/benchmarking in the processes followed and tools used by penetration testers[2]. There is a tool that developed by OWASP ZAP is a free, open-source penetration testing application that is developed by the number of global volunteers and maintained under Open Web Application Security Project (OWASP). Especially, it is specialized for both automated as well as manual security testing, the project ZAP is cross platform tool, it can be used on Windows, Unix/Linux and Macintosh operation system. It stands as a "middle-man proxy" between a tester's browser and the web application and is used to intercept and manipulate the transmitted requests. Its key features are traditional and AJAX spiders, Fuzzer, Web socket support and a REST based API.

Methods and Solutions

System Requirements

OWASP ZAP[1] provides cross-platform i.e. it works across all OS (Linux, Mac, Windows).The OWASP ZAP require a

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

computer with the official Java Runtime Environment (64-bit edition, version 1.7 or later) installed. JREs are available for various popular operating systems, including Windows, Linux and Mac OS X. For the best experience with OWASP ZAP Professional, it is recommend using a machine with at least 8 GB of memory and 2 CPU cores. If clients want to performing large amounts of work, or testing large or complex applications, it needs more memory than this.

[1] Symantec Internet Security Threat Report

https://www.symantec.com/content/dam/symantec/docs

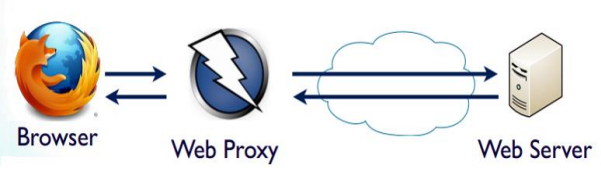


Fig. 1. Logic position of tool

ZAP creates a proxy server and makes the website traffic to pass through the server. The use of auto scanners in ZAP helps to intercept the vulnerabilities on the website. Refer to this flow chart for a better understanding:

1.1. Obtain performance data

WASP ZAP software is intercepting proxies that sets between the client browser and the webserver to captured and manipulate requests exchange. It has some components also to use gathering and analyzing data:

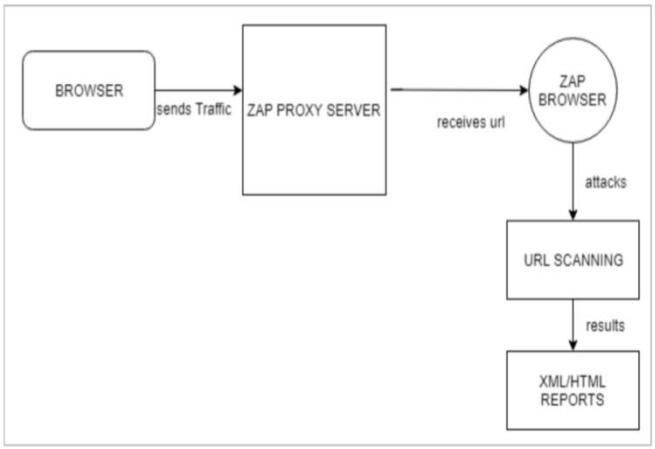
a) The Spider, user will be able to crawl through a website. The software to

Fig. 2 ZAP Proxy server event proccesing

attempt retrieve every link and page that it could find within the scope that specified.

b) The Fuzzer, this mode plan to perform a big number of requests by changing one or more parameter each time

c) The Active Scanner, Penetration testers will perform various attack and it will show



how vulnerable is the application

[1]**https://www.zaproxy.org/**

2. Requirement Analysis for Performance Testing

2.1. System Business Requirements

The OWASP ZAP tool is cross-platform, it can run on all OS (Linux, Mac, Windows), and performance testing web application under test by scanning or manipulating requests between server and client.

2.2. Functional Requirements Analysis:

It is free and open-source project actively maintained by volunteers for finding vulnerabilities in web applications.The priority of using automated vulnerability scanners to unveil flaws in web applications before they are deployed has been realized by many organizations today [3]. Due to the ever-growing cybercrime, this study has examined some scanners that can be used to detect vulnerabilities that can be easily be missed by manual testing

Design and architecture

2.3. Analyzing User Interface

The user interface can be a little disappointing when you see it first time. It gets intuitive and includes all the primary info you need to know. It has 6 simple items on primary interface.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Fig. 3. OWASP ZAP 2.8.0 Main window

1. Menu Bar – Provides access to many of the automated and manual tools.
2. Toolbar – Includes buttons that provide easy access to most commonly used features.
3. Tree Window – Displays the Sites tree and the Scripts tree.
4. Workspace Window – Displays requests, responses, and scripts and allows you to edit them.
5. Information Window – Displays details of the automated and manual tools.
6. Footer – Displays a summary of the alerts found and the status of the main automated tools.

OWASP Zap has functionality but needs to be upgraded with plugins. There is a straightforward learning curve for it. OWASP Zap has one fuzzer window, which makes it harder to look for in fuzzer results, particularly once you run different fuzzers.

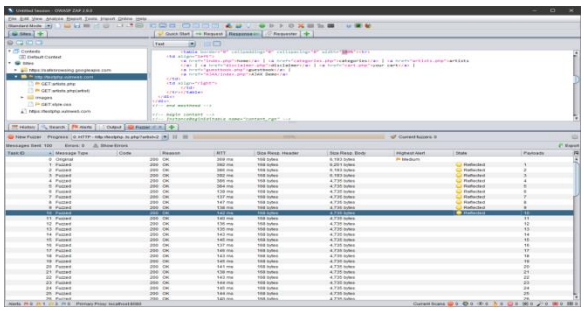


Fig. 4.ZAP 2.8.0 Fuzzer window

1.1. Extending usage and Integration analyze Another important point of OWASP ZAP, which is a special thing that is made Zap is common its API, that makes for integrate easily or contribute works automatically. There is an access to the API from the web browser or other user agents like curl or SDKs/libraries.

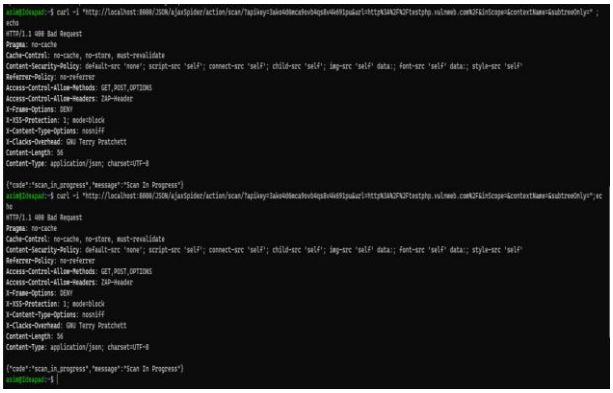


Fig. 5. An example is using the API to spider a host and getting the results, e.g. crawling testphp.vulnweb.com from the console.

The tool can be used on DevOps and/or DevSecOps pipelines [4]. It was introduced in 2018, and this opportunity makes easier to integrate the software with other tools and workflows. OWASP ZAP the easiest to integrate into DevSecOps pipelines by this feature no matter how big or small is your environment[1].

Testing Results

4.1 Performing test.The easiest way to start using ZAP is via the Quick Start tab. Quick Start is a ZAP add-on that is included automatically when you installed ZAP. To run it, start ZAP and click the Quick Start tab of the Workspace which can see in Fig. 3. Click the large Automated Scan button. In the URL to attack text box, enter the full URL of the web application proposed to test. At the end click the Attack option. Another option for the Active scan is that we can access the URL in the ZAP proxy browser as Zap will automatically detect it. Upon right-click on the URL -> Active scan will launch. Once the crawl is complete, the active scan will start. Attack progress will be displayed in the Active Scan Tab. and the Spider tab will show the list URL with attack scenarios. Once the Active scan is complete, results will be displayed in the Alerts tab.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

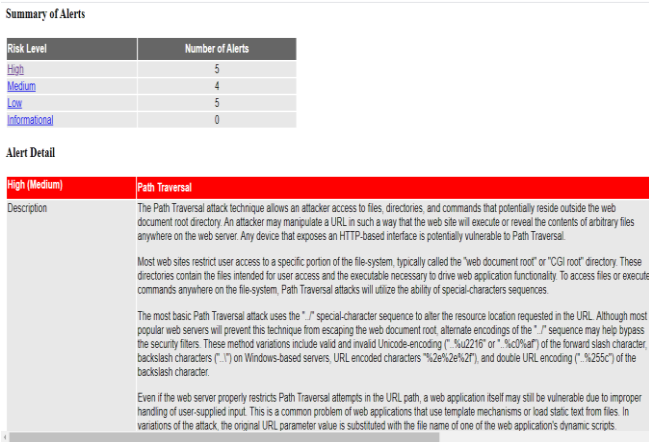
4.2. View Alerts and Alert Details

Main part

The left-hand side of the Footer contains a count of the Alerts found during the test, broken out into risk categories. These risk categories areHigh, Medium, and Low severity risks based on categorizing of ZAP.

The OWASP ZAP can scan through the web application and detect issues related to:

- SQL injection
- Broken Authentication
- Sensitive data exposure
- Broken Access control
- Security misconfiguration
- Cross Site Scripting (XSS)
- Insecure Deserialization
- Components with known vulnerabilities
- Missing security headers


Summary of Alerts

Risk Level	Number of Alerts
High	5
Medium	4
Low	5
Informational	0

Alert Detail

High (Medium)	Path Traversal
Description	The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP-based interface is potentially vulnerable to Path Traversal. Most web sites restrict user access to a specific portion of the file-system, typically called the "web document root" or "CGI root" directory. These directories contain the files intended for user access and the executable necessary to drive web application functionality. To access files or execute commands anywhere on the file-system, Path Traversal attacks will utilize the ability of special-characters sequences. The most basic Path Traversal attack uses the " ../" special-character sequence to alter the resource location requested in the URL. Although most popular web servers will prevent this technique from escaping the web document root, alternate encodings of the " ../" sequence may help bypass the security filters. These method variations include valid and invalid Unicode-encoding (" %u2216" or " %c0%af") of the forward slash character, backslash characters (" \") on Windows-based servers, URL encoded characters "%2e%2e%2f"), and double URL encoding (" %255c") of the backslash character. Even if the web server properly restricts Path Traversal attempts in the URL path, a web application itself may still be vulnerable due to improper handling of user-supplied input. This is a common problem of web applications that use template mechanisms or load static text from files. In variations of the attack, the original URL parameter value is substituted with the file name of one of the web application's dynamic scripts.

Fig. 7. An example for getting report of OWASP ZAP tool

4.3. Verification of conducting test.

High-profile security breaches have been dominating the cybersecurity world. Therefore, to understand how methodologies and tools for security testing have evolved is an important task. It is considered by experts today the giant penetration testing conducted by OWASP ZAP, Burp suite, Acunetix Vulnerability Scanner and Veracode [5]. During the research we used user review sentences from IT Central station center review results. It includes 31.194 (OWASP ZAP) reviews from experienced users and customers from some governmental and private sector. In the table below will introduce which companies are on the top to use OWASP ZAP software.

	Category company	OWASP ZAP
	Aerospace/Defense Firm	13%
	Energy/Utilities Company	13%
	Manufacturing Company	13%
	Computer Software Company	25%

Tab. 1.Top industries title who chosen OWASP ZAP.

It can be clearly seen that, mainly Computer Software Companies picked OWASP ZAP software dominantly with about 60 percentages.

	Category company	OWASP ZAP
	1-200 Employees	18%
	201-1000 Employees	24%
	1001+ Employees	59%

Tab. 2. Company size who chosen OWASP ZAP.

Moreover, the report addresses quality characteristics, and further classified these reviews based on the system view and the behavior theory and compared the difference on the distributions of various functional requirements between user reviews and industrial requirements specifications.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

According to IT Central station center (Top Application Security Testing (AST) Vendors 2021).

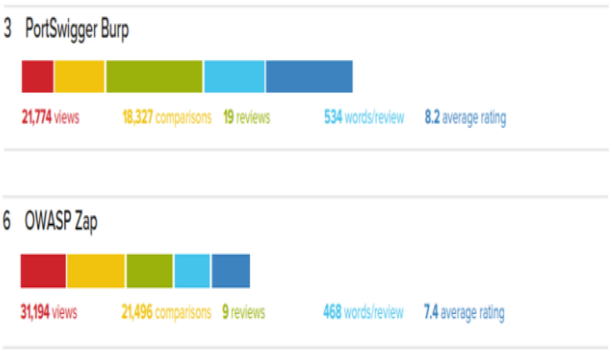


Fig. 8. Comparing OWASP ZAP and Portswigger Burp User's perspective

It is also shown onthe Google trends. OWASP ZAP has been chosen nearly on every top 10 instruments of the year. We can see since they emerged to the market, they are gaining more and more momentum and users as we see in google trends for the past 5 years (2015-2020)[1].

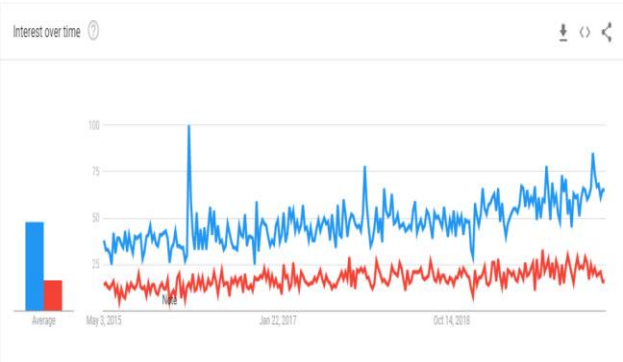


Fig. 9. Google Trends showing Burp suite in blue and OWASP ZAP in Red

We can see from the line graph Burp is more popular than OWASP ZAP according to Google trends data. Interested in Burp has been grown slightly during over 5 years (with 30). While OWASP ZAP has experienced fluctuation via 25 per day.

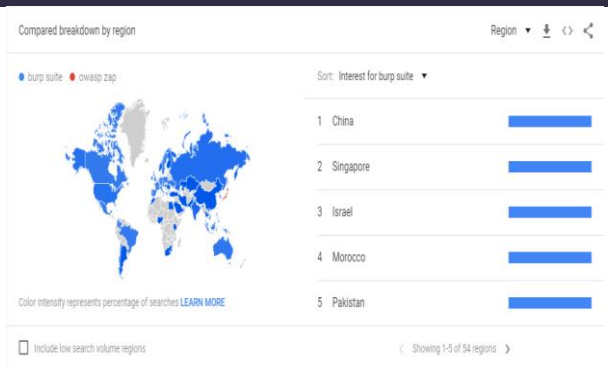


Fig. 10. Google Trends showing Burp suite in blue and OWASP ZAP in Red

Burp suite is used dominantly over the first three countries China, Singapore and Israel.

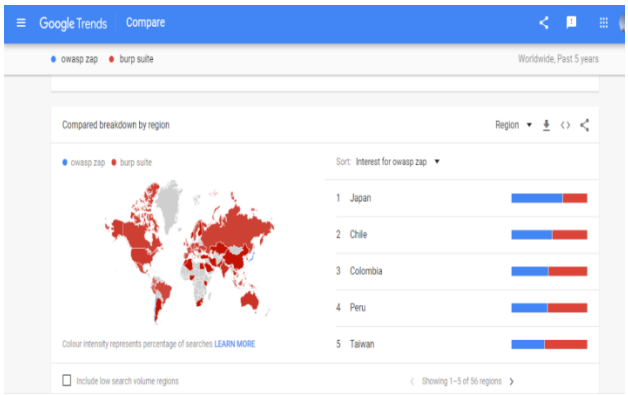


Fig. 11. Google Trends showing Burp suite in blue and OWASP ZAP in Red

The graph is informed about interested in OWASP ZAP tool is popular in Asian and Southern America countries.

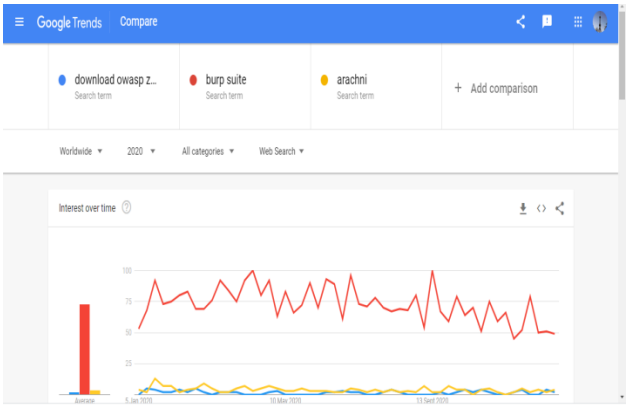


Fig. 12. Google Trends showing Burp suite in blue, OWASP ZAP in Red and Arachni is yellow

Conclusion

In this paper we analyzed for identifying key components of quality characteristics of functionality OWASP ZAP application from app user's perspective. Furthermore, task-based evaluation that involved over 31.000 users of different level of experience from diverse organizations conducted by IT Central station center (specialized to gathering and comparing feedbacks and application users result) are reviewed. It is clear that, which is not possible to consider any scanner comprehensively when scanning web vulnerabilities. However, by combining the performance of these two scanners on both criteria, we concluded that ZAP performed better than Arachni in the SQLI, XSS, and CMDI categories. Arachni, on the other hand, had much better results in the LDAP category. In the further researches it is planning to make a detailed comparative evaluation of the scanners which is worked differently in different categories.

References

1. Comparative Analysis of the Automated Penetration Testing Tools Mandar Prashant Shah. School of Computing National College of Ireland
2. Open Source Web Vulnerability Scanners: The Cost Effective Choice?
3. Kinnaird McQuade. Information Technology Department Marymount University Arlington
4. N. I. Daud, K. A. A. Bakar, and M. S. M. Hasan, "A case study on web application vulnerability scanning tools," in 2014 Science and Information Conference, 2014, pp. 595-600.
5. Performance of DevOps compared to DevSecOps – DevSecOps pipelines benchmarked! Jimmy Björnholm Tutor, Rita Kovordanyi Examinator, Jalal Maleki Linköpings Universitet
6. Evaluation of Web Vulnerability Scanners Based on OWASP Benchmark Balume Mburano. Western Sydney University Sydney, Australia