Owasp Zed Attack Proxy

Jobin T.J
Department Of Computer Applications,
Amal Jyothi College Of Engineering
Kanjirapally,Kottayam
tjjobin@amaljyothi.ac.in

Karthika Suresh Babu
PG Scholar,
Amal Jyothi College Of Engineering
Kanjirapally,Kottayam
karthikasureshbabu@mca.ajce.in

***Abstract*—Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool.It is kept up to date under the auspices of the Open Web Application Security Project (OWASP). ZAP is a web application testing framework that is both flexible and extendable. ZAP is a so-called "man-in-the-middle proxy" at its core. It runs between the tester's browser and the web application, intercepting and inspecting messages transmitted between the two, modifying the contents if necessary, and then forwarding those packets on to their intended destination. It can be performed as a daemon process or as a stand-alone application.**

Keywords—security measures, penetration testing, web vulnerability scanner, Zed Attack Proxy

I. INTRODUCTION

Web apps have become integrated in our ordinary routine, but many of them are installed with crucial vulnerabilities that can be fatally exploited. The attackers' tactics are becoming more complex as the technology used to build these applications becomes more advanced. As a result, network vulnerability scanners have been widely used to evaluate web application protection. Benchmarking is one of the methods for doing so. The effectiveness of web vulnerability scanners has been measured using a variety of benchmarks. These include the Web Input Vector Extractor Teaser)benchmark, IBM Application Security Insider benchmark, Web Application Vulnerability Scanner Evaluation Project)benchmark, and OWASP benchmark.

To fill in the gaps in our knowledge, we first utilise the OWASP benchmark to analyse and evaluate two popular web scanners, Arachni and OWASP ZAP, in their most recent versions (v1.5.1 and v2.7, respectively).

The OWASP Zed Attack Proxy (ZAP) is a user-friendly open source scanner for detecting vulnerabilities in online applications.

It is one of the OWASP flagship projects for web application vulnerability checking, and it is recommended by OWASP[2]. For automated security checks that can be integrated into the continuous development environment, ZAP is commonly used by security practitioners, developers, and functional testers[2]. ZAP is also a free Open Source cross-platform scanner that is gaining traction as a tool for advanced web application vulnerability testing. [1].

Hackers typically use Client-side or Server-side attacks to gain access to networks and look for weaknesses. It can be accessed through HTTP methods such as the get method (through URL), post method (message content), put and delete method, or web cookies (Home Page), and the threats are detected using automated or manual testing[1].

These days, data security is of the utmost importance, thus finding security weaknesses in networks and web applications is a top concern[2]. The major purpose of this study is to figure out how hackers uncover network infrastructure flaws and use them to target web applications[1].

To obtain information and cyber threat-related information, vulnerability analysis and online assessment techniques are utilised[3]. This study will aid in the future security of web applications.

The OWASP ZAP web application security scanner is free and open-source. It's designed to be utilised by both newcomers to application security and experienced penetration testers[3]. It has been designated as a Flagship project and is one of the most active Open Web Application Security Project initiatives.

II. LITERATURE SURVEY

In web application security development, the OWASP ZAP analysis tool is used to assess the vulnerability level. It's used for both automated and human web application testing. The manual testing was carried out with the help of the Vulnerability Assessment and Penetration Testing (VAPT) tool, and the results were 100 percent accurate, indicating that manual testing outperformed automation testing[1].

Ransomware and spear-phishing are examples of cybercrime attacks against websites, and test results were examined using Vulscan and the OWASP ZAP online vulnerability scanner. SQL injection and cross-site scripting (XSS) vulnerabilities would be detected.[1].

There are a variety of web vulnerability scanners available. Previous research has also revealed that the results reported by different scanners can differ[1]. The performance of these scanners varies depending on the vulnerability categories and crawler coverage[1]. This necessitates a more thorough assessment of the scanners' effectiveness. Because of its regular updates, large number of authors, and widespread appeal, ZAP is the best[1].

The OWASP Zed Attack Proxy (ZAP) is an open source scanner for detecting vulnerabilities in web applications that is simple to use. It is one of the OWASP flagship projects for web application vulnerability testing, and it is endorsed by OWASP[4].

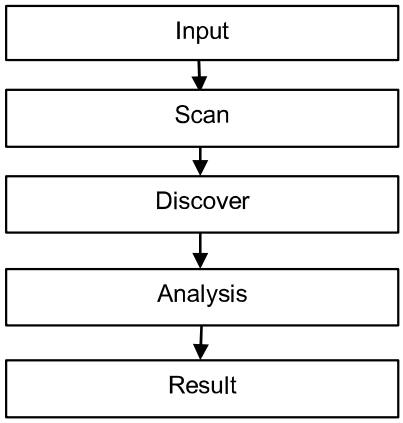
ZAP is often used by security specialists, developers, and functional testers for automated security testing that can be included in the continuous development environment. ZAP is also a free, cross-platform Open Source scanner that's gaining interest as a framework for advanced web application vulnerability testing [2].

10.5281/zenodo.5101067
ISBN:978-93-5426-386-6@2021 *MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam*

III. METHODOLOGY

The OWASP ZAP security scanner is used to check web applications for vulnerabilities. It features a number of modules, including a proxy for capturing, a fuzzer for identifying vulnerabilities, a spider for detecting web applications, a scanner for active and passive attacks, and a dictionary approach for gaining access to files[1].

There are five steps in the testing phase. Just like the previous, the Host Name/ Host ID should be given as an input to attack. The scanning process is then carried out to find the network infrastructure's flaws. A risk analysis method is carried out when such problems have been detected. Risk is divided into four categories: low, high, informative, and medium. As the final step, the result is concluded[2].



ZAP discovers medium and low-level hazards following the scanning procedure, and the vulnerabilities are described below:

OWASP ZAP detects hazards at the medium (high) level, such as

- Third-party URL rewriting can be linked to the session ID
- Application error disclosure—Sensitive data may be exposed in the hands of attackers, perhaps leading to a ransomware assault
- The header for X Frame Options (XFO) is not set. The attacker will be able to control the computer's actions without the user's knowledge (clickjacking attack)
- SQL injection is a technique for attacking an application's database layer weaknesses and changing information using DELETE, INSERT, and ALTER queries to delete, add, and modify database data.

Risks at a low (medium) level, such as

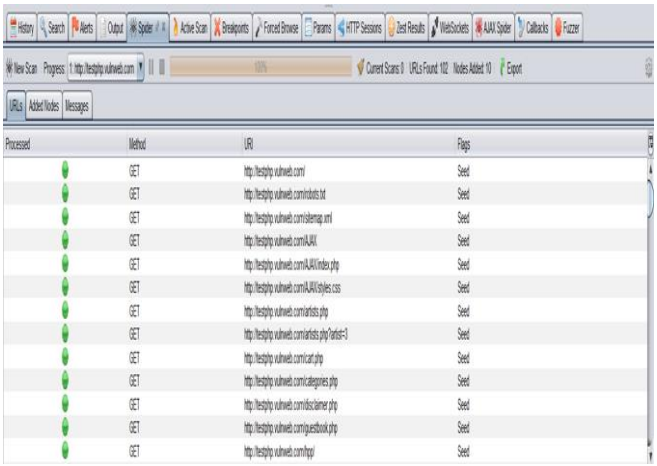
- Cross-Site Request Forgery(CSRF) The malicious file can be inserted into many links linked to the original files using JavaScript code, doing undesirable behaviours.
- Cookie without secure flag and HTTP only flag- A man-in-the-middle attack occurs, resulting in a loss of authentication, data, security, honesty, integrity, and confidentiality.
- Threats of media type sniffing attacks generate a security vulnerability since the X-Content model is missing.
- Cross-site scripting (XSS) attack: XSS security was disabled in the web browser. It's a system of web software security weaknesses.
- Mixed content is present on secure pages. The papers become swamped with video files, pictures, and style sheets due to an insecure HTTP connection.
- Pragma HTTP and cache control does not correctly implement HTTP headers.

The scanning method was used to detect vulnerabilities and flaws in the testing environment, and medium and low-level attacks were uncovered in the 10 domains. Not only has a security flaw been discovered in one domain, but all domain vulnerabilities have been discovered as well. The ZAP result is given.

A. Finding vulnerability using ZAP – Automated Scan

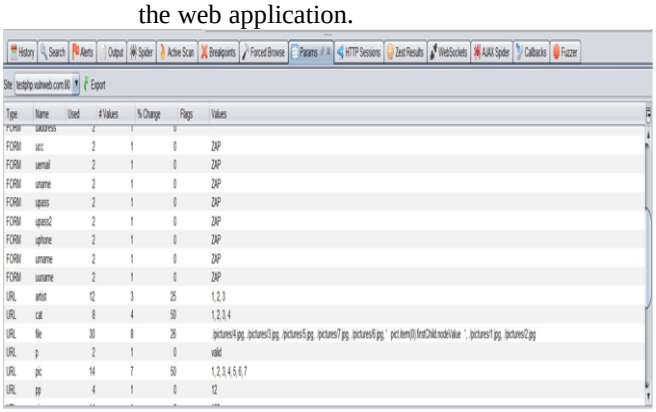
- Inserting URL

- Different types of links available inside the web application are getting listed in the spider tab.

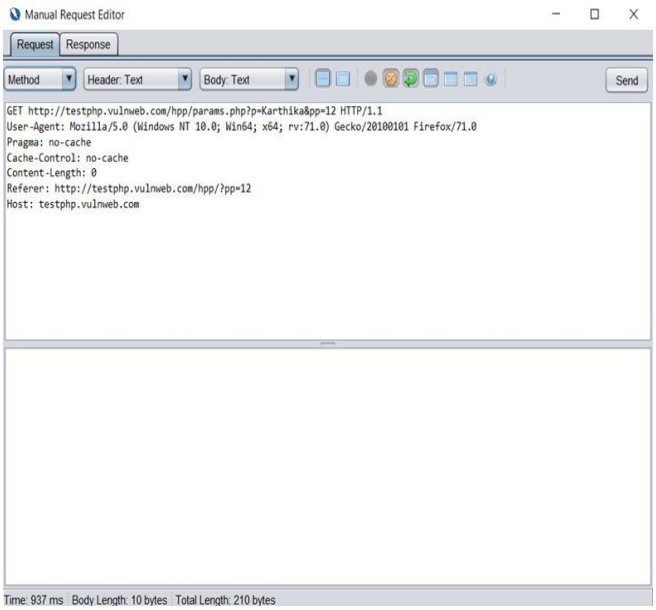


10.5281/zenodo.5101067
ISBN:978-93-5426-386-6@2021 *MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam*

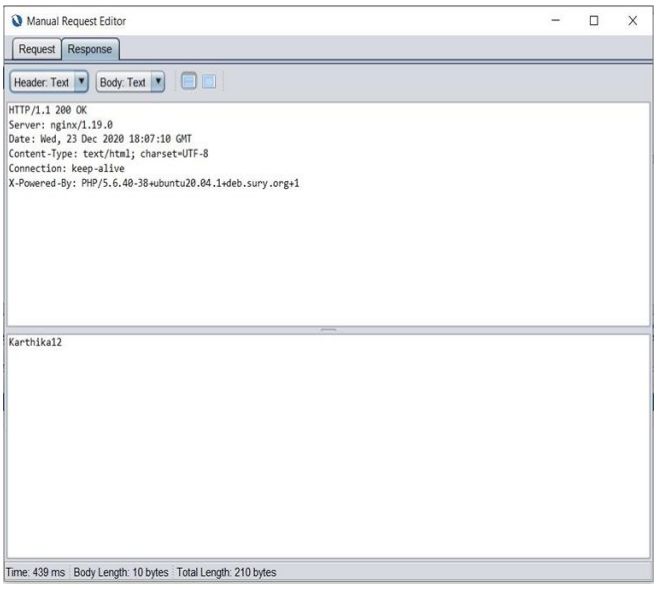
- Params tab lists all the parameters found inside the web application.



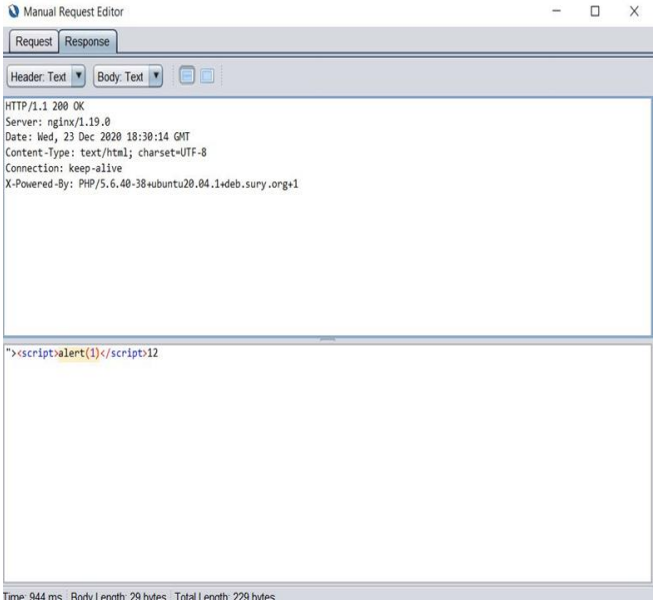
- Injecting payload inside the parameter



- Inserted payload is reflecting in the response tab.



- Inserting script



- Getting request on browser

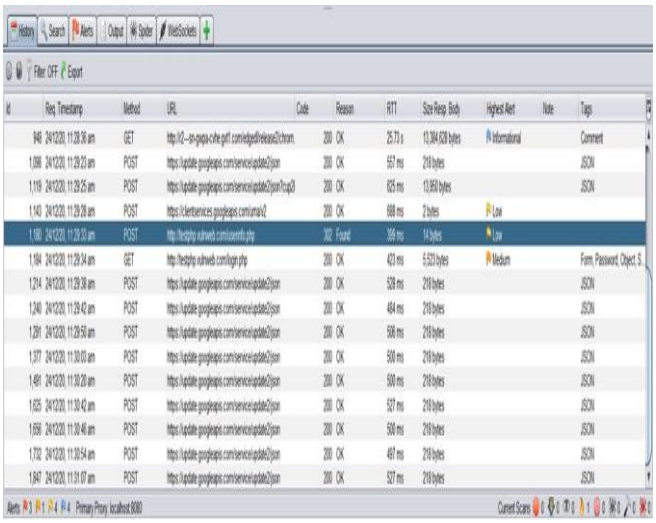
B. Dictionary Attack

A dictionary attack is a way of breaking into a password-protected computer or server by typing every word in a dictionary as a password in a methodical manner.

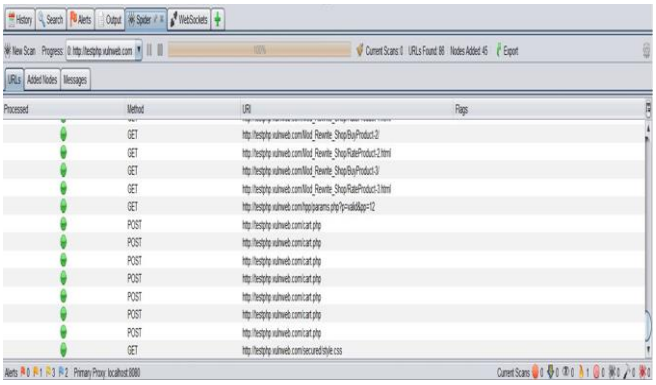
- ZAP will then use its spider to crawl the web application and passively scan each page it discovers.

10.5281/zenodo.5101067
ISBN:978-93-5426-386-6@2021 *MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam*

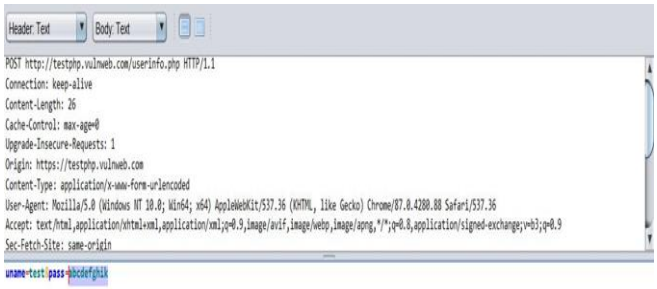
- Spider Crawl result



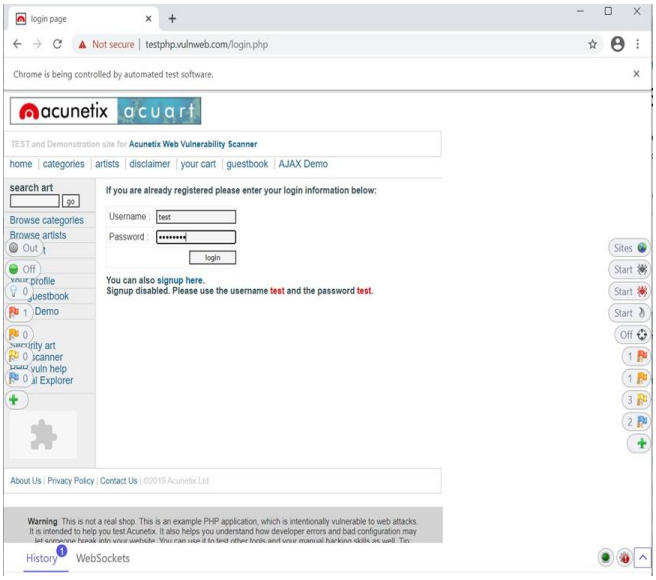
- Request tab showing the sample value entered by the attacker



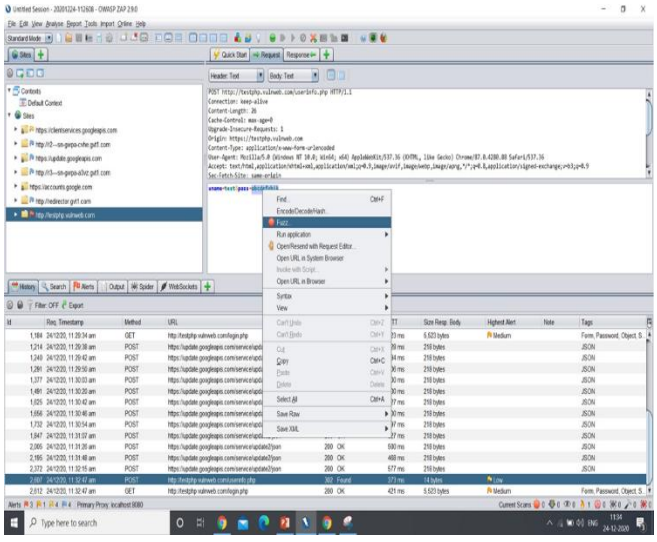
- Inserting sample value to test site



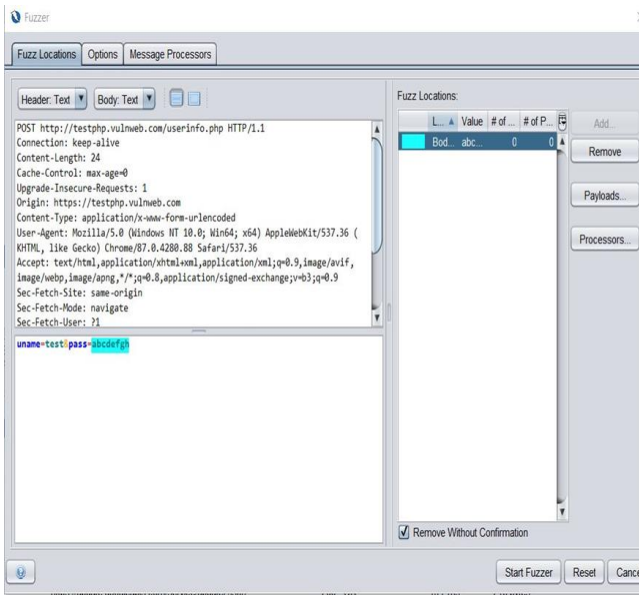
- Using Fuzzer on password field by keeping username same

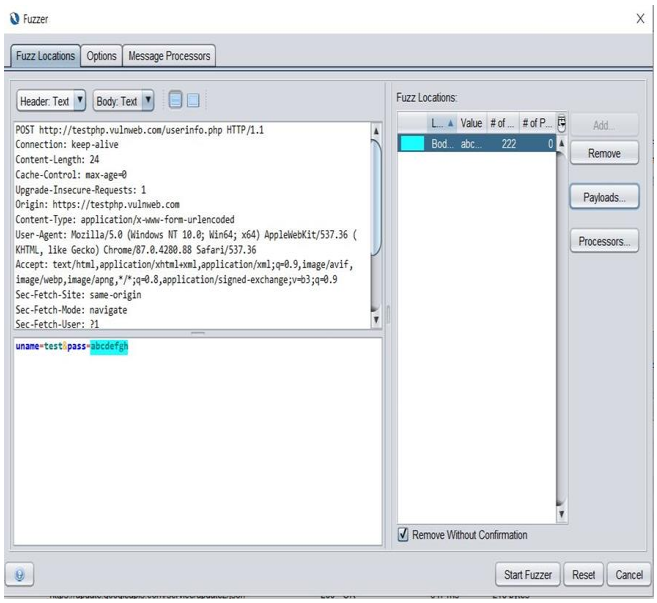


- POST method which sends data to the website

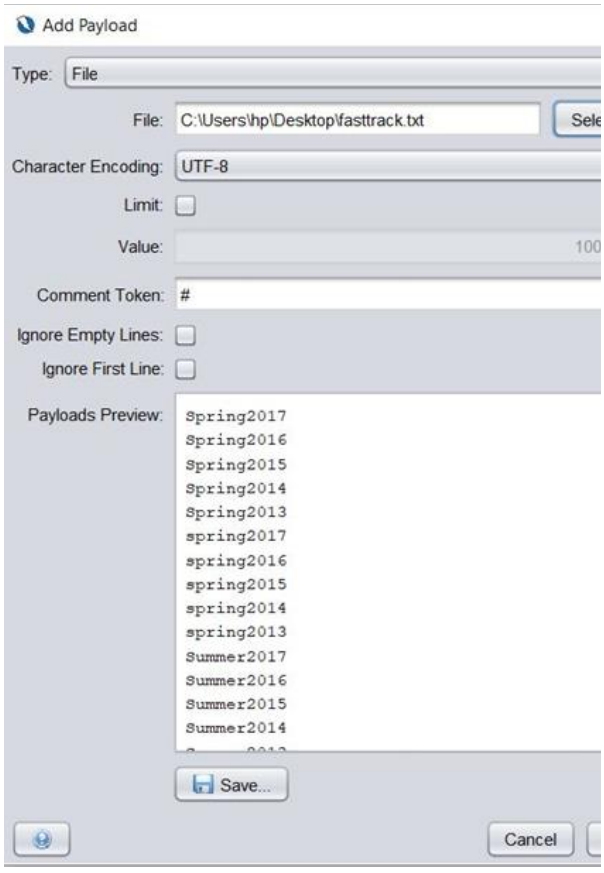


- Adding a text file as payload to do the dictionary attack





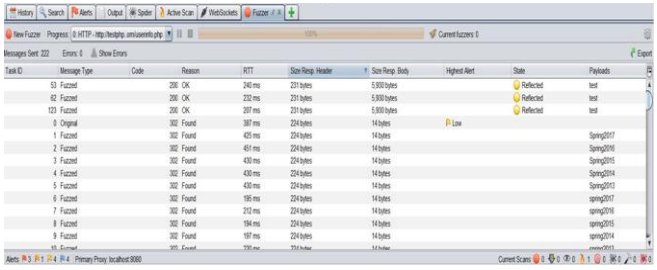
- FPayload file preview which contains the passwords to be tested



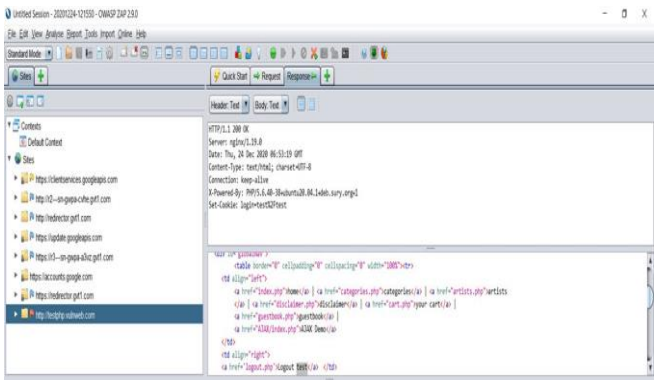
- Click start fuzzer button

  Starting fuzzer will start the dictionary attack(Will check all the passwords in the file attached as payload)

- Result obtained after the dictionary attack. Reflected state payloads gives you more winning probability.



- Password found from the reflected payload list[3]



IV. RESULTING STEPS

A. Running an automated scan

- Start ZAP and go to the Workspace Window's Quick Start tab.

10.5281/zenodo.5101067
ISBN:978-93-5426-386-6@2021 *MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam*

- Select Automated Scan from the drop-down menu.
- In the URL to attack text box, type the complete URL of the online application you want to attack.
- Select the Attack option.

B. Exploring an application manually

- Start ZAP and go to the Workspace Window's Quick Start tab.
- The Manual Explore button should be clicked.
- Enter the full URL of the web application you want to investigate in the URL to explore text box.
- Choose the browser you want to use.
- Select the Launch Browser option[3].

V. CONCLUSION

ZAP is a free, open-source community-developed platform that aims to make the internet a safer place. Using penetration testing, security flaws were discovered in all areas of domains, with the OWASP ZAP tool detecting medium and low-level warnings. More vulnerabilities were discovered as a result of our research and experimentation with automated testing, including The X-XSS-Protection header is not specified, Uncommon header identified, SSL and the strict transport-security HTTP header is not defined, and more. The server leaks inodes using ETag, which is collected using a header from the Nikto tool rather than the OWASP ZAP. Various vulnerabilities such as cookie without secure flag, cross-site request forgery (CSRF), URL rewriting, and application error disclosure warnings were discovered using both tools in web application testing.It is important to protect web applications and networks from cyber-attacks[5].

VI. FUTURE WORK

It's possible that any updates might be made to make it more user-friendly. The reporting format has little production, is cluttered, and takes a long time to complete. If they could have a marketplace to add extra features to the tool, that would be great. The application's automated risk tests must be streamlined and varied

VII. REFERENCE

[1] Testing for Security Weakness of Web Applications using Ethical Hacking,R.Sri Devi,Research Scholar,Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, India. Proceedings of the Fourth International Conference on Trends in Electronics and Informatics (ICOEI 2020) IEEE Xplore Part Number: CFP20J32-ART; ISBN: 978-1-7281-5518-0.

[2] UKEssays. (November 2018). Evaluation of Web Vulnerability Scanners Based on OWASP Benchmark. Retrieved from https://www.ukessays.com/essays/computer-science/evaluation-of-web-vulnerability-scanners-based-on-owasp-benchmark.php?vref=1

[3] https://owasp.org/www-project-zap/

[4] https://en.wikipedia.org/wiki/OWASP_ZAP

[5] https://resources.infosecinstitute.com/topic/introduction-owasp-zap-web-application-security-assessments/