International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Web Application Security Testing

Reiffel R

Dr. M.G.R. Educational and Research Institute, Maduravoyal, Chennai 600095, India

ABSTRACT

Fundamentally, our society is more technologically reliant than ever before and there is no sign that this trend will slow down. As this trend increases, the crimes happening in the cyber world also increases.So it is necessary to ensure safety and security while depending on cyber space. Like the modern technology, the cyber criminals are also becoming more sophisticated in their attack. The lack of adequate security and knowledge leads to be victim of many attacks. While thinking aboutescaping all these attacks, Web Application Security Testing tool comes into picture. Web Application Security Testing tool is a best defensive mechanism to avoid to be a victim of such attacks and ensure security.Web Application Security Testing is an automated open source tool built to check the security of a web application and web pages. It conducts security assessment by performingdifferent attacks in real time so as to detect any vulnerability present and report it to the user. As a result, the user will get to know about the vulnerabilities present in the web page and web application and patch it before any attacker tries exploits it.

Keywords: Web Security, Cyber Security, Vulnerability Assessment, Penetration Testing

1. Introduction

Web Application Security Testing tool is a command line tool in Linux which is used to test the security of web pages using different techniques. It is an open source tool,which means using anyone can use this tool at free of costs.It has an interactive user interface thatintegrates more than seven different types of techniques/methods to test the security of web pages.Web Application Security Testing is an initiative to learn more about web application penetration testing and how it works in real-time.

1.1. Overview of the project

Web Application Security Testing is used in performing several security assessments and vulnerability checks on any website or web-based application. According to the security policy, it allows to select the type of security assessment. This assessment contains nine techniques and methods. They are Directory Brute forcing; Subdomain Brute forcing; Send Requests and View Responses; Takes Screenshot of Web pages; CORS Misconfiguration Scanner; Get URL in a Web page; Path Traversal Attack Scanner;Open Redirection Attack Scanner; Banner Grabber.

2. System Study

2.1. Problem Definition

Web application penetration tools available now are very costly so it is not accessible for many beginners. Moreover, web application penetration tools need prior knowledge about protocols, web based terminology and vulnerabilities. So they are very hard to use for people who are not related to the cyber security field because they don't have any knowledge about those. Web applications security tools available now do not have a combination of recon techniques, scanning techniques and attacking techniques they are only focused on one of them. So we need to use different tools in order to conduct

* *Reiffel R*
E-mail address: reiffelr@karunya.edu.in

different vulnerability scan on a single unit. As a result, it costs a hefty amount of money and time. Also, managing all these tools needs enormous efforts and patience. This may lead to misconfiguration of security setup which keeps integrity of the organization at stake.

2.2. Existing System Demerits:

- Higher costs of tools.
- Users should pay for each tool if they want to perform batch assessment (multiple vulnerability checks).
- Complicated user interface that makes difficult for a layman to handle.
- Validity expiration of the purchased tools.
- Manual intervention required in each and every step of the security assessment.
- Managing lot of tools requires a lot of human effort and manpower and might be confusing as well.

2.3. Project Perspective

The aim to develop this project is to enable security measures in an IT environment over web applications at ultimately free of costs.It will help beginners who just started their security testing career because it is free and easily accessible. It has an interactive user interface; due to this tester doesn't need to study how the tool works nor any prior knowledge to operate the tool. It works by'select the option' algorithm, so you are just expected to click on the desired assessment criteria you want to perform and the tool will execute it for you. It also have nine different techniques combined together in this tool which includes recon techniques, scanning techniques and attacking techniques. So for these techniques should only use one tool. It will be hosted in the free hosting services available in the market as paid services will costs a lot of money. Users can make use of this tool to enhance their security requirement and knowledge.

2.4. Proposed System

Web Application Security Testing tool is an open source tool. It will be uploaded to GitHub and can be used by anyone, be it a developer or student, for free. Instead of using several security tools, security professionals can identify the flaws by using this single security tool. It allows the user to choose the desired tool according to their need. This makes the implementation of security measures fast and enables us to perform several security tests all at once as it allows for batch processing (multiple checks in one go). It also allowsuser to generate reports based on the results of the assessment for clearer picture.

2.5. Advantages of Proposed System

- Combination of security tools– Users can perform several vulnerability and security check by using this single platform for multiple assessment without relying on different tools (paid or unpaid) for different assessment.
- Batch Processing –It allows to execute all the nine modules all at once or select the desired modules (multiple) to perform certain security checks.
- Entirely free of costs – No need to spend money for purchasing tools (single or multiple).
- Flexibility and scalability – According to our needs we can customize the assessment. It allows to execute single process or batch process.
- Deployment and ease of use – Even a layman can use the tool because of its simpleruser interface.Tool management will be minimal.
- Generate Reports – Have the ability to generate report based on scanned result and provide detailed description how to fix the vulnerability.
- No need of manpower as it is completely an automated process.

3. Working

To use Web Application Security Testing, type WAST –h you will get the help page of the tool. Basically WAST take to options –h and –u.-h gives the help page and –u with URL gives the URL of the website to test. It takes the URL and check if it exists. If it does not exist the tool exits. Otherwise it provides the tools available. Select the tool you want to use then it executes the code and returns the output. If the user wants to perform batch scanning, he/she can select multiple options desired. After execution, the results of the assessment is displayed. The user can click on 'generate report' button to generate a report on the findings which can be used to create a log of the assessment.

3.1. Design and Implementation Constraints

Even though it is an open source online tool, it has limitations in its working environment. It doesn't work on a fully automated platform. The user has to manually choose what operation to be executed at a particular time. The user should have an active internet connection for accessing this tool.

3.2. Assumptions and Dependencies

- Limited to only few scanning modules.
- It needs an active internet connection to execute the scan as it an online web-based tool.
- Active and non-automated scanning methodology.

4. Intended Audience and Reading Suggestions

All personnel who are responsible for the implementation of security measures and users of cyber space. Different types of users can use this document as listed below:

- Vulnerability testers
- Penetration testers
- Information security analysts
- System administrators

5. Conclusion

Web Application Security Testing tool was an attempt to create a web application security assessment tool that is available for everyone, can be used even by people with no prior knowledge of cyber security and can be used as a tool for multiple vulnerability assessment and securitytesting of webpages and web applications. In future, this tool can be further developed to add more modules to enhance the efficiency of the tool to suit the requirements of future technologies.

References

[1] Prokhorenko, K.-K. R. Choo, and H. Ashman, Web application protection techniques: a taxonomy, Journal of Network and Computer Applications, vol. 60, pp. 95–112, 2016

[2] S. E. Idrissi, N. Berbiche, F. G. and, and M. Sbihi, Performance Evaluation of Web Application Security Scanners for Prevention and Protection against Vulnerabilities.pdf, International Journal of Applied Engineering Research, vol. 12, pp. 11068-11076, 2017.

[3] M. Cova, V. Felmetsger, and G. Vigna, Vulnerability Analysis of Web Applications, in Testing and Analysis of Web Services, L. Baresi and E. Dinitto, Eds. Springer, 2007.

[4] D. Stuttard, M. Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Second edition, Wiley Publishing Inc.

[5] Z. Shaw, Learn Python the Hard Way: A Very Simple Introduction to the Terrifyingly Beautiful World of Computers and Code, 3rd Edition