MAT JOURNALS

Journal of Web Development and Web Designing
Volume 4 Issue 2

Testing Tool: Offensive Server Side Security Analyser

Sahil A. Bhat[1], Vitthal N. Pankar[1*], Namrata Kumari[1], Vrushali Desale[2]
[1]UG Students, [2]Professor
[1,2]Department of Computer Engineering, D. Y. Patil College of Engineering, Pune, Maharashtra, India
E-mail: *vitthalpankar888@gmail.com*
DOI:

Abstract

The main purpose of making this tool is that administrators are not aware of many recent attacks like Symlink attack, obfuscated back dooring etc. So, our tool will effectively help them in finding the vulnerabilities.We have planned to design a server side penetration application that will effectively analyse all loopholes and help the server side administrator to secure his server. Ideally, this tool will work on local host and will operate through web browser. This tool will be able to test vulnerabilities in any server hosted on windows or any flavour of Linux.

Keywords: *Analyser, attack, goal, testing tool*

INTRODUCTION

For the people who are facing problem in real-time sector for securely developing software which cannot be hacked or destroy by the outsiders. In this work, we have discussed the design and implementation of testing tool which will conclude all the problem in a short, as by developing this tool tester we come to know that from where system can be destroyed or hacked, thus later they can be fixed by listing the information like from where or how system is getting leak. So, this tool will give a brief abouthow system and command is being used. This will help the risk management team.

PURPOSE AND SCOPE OF DOCUMENT

- This project having speciality to detect bugs, different vulnerability, misconfiguration, etc.,in server side to protect from outside environment.
- The purpose of the toolis to helpteam to get rid ofdifferentsoftware's errors or bugs.
- This project is better in the field of risk management.

Problem Statement

- Any form of errors occur from outside environment is get solved to make the software error free.
- The real time bugs, vulnerabilities or errors can be retrieved by user.

Goals and Objectives

- The main goal of our system is to design and implement a testing tool that will detect bugs different vurnabilites or errors.
- The primary role is to help the testing team to detect and solve the problems occurred.

CONCLUSION

The main objective of our project is to detect vulnerabilities, bugs, misconfigurations, etc., in the server-side and report, so that the administrator can patch the detected bugs, misconfiguration, etc., at the server end.

ACKNOWLEDGEMENT

It gives us great pleasure in presenting the preliminary project report on "Testing Tool: Offensive Server-Side Security Analyser".

REFERENCES

1. Brute Force attack : https://www.cloudways.com/blog/what-is-brute-force-attack/
2. SQL Injection attack : https://www.acunetix.com/websitesecurity/sql-injection/
3. IEEETransaction: https://www.ieeexplore.com/administrator/offensiveserversidesecurity/

Cite this article as: