**Bug Hunting Through Web Application Penetration Testing**

By

**MURARI AKHILA**

**Abstract**

Security has become a key component in every industry and there are many fields in security which we can explore and one among many components is web application one of the core components which needs more IT Security than ever. My project is to demonstrate the ways which we use for finding bugs on web applications and exploring the vulnerable spots by doing Web Application Penetration Testing (W.A.P.T) and submitting report to the respective web application owner. It contains different stages and different exploits and tool are used to demonstrate the vulnerabilities in a website. The major take away for any web application is securing it from theft and the conclusion of my project is how to protect web application from various attacks.

**1. Introduction**

The internet became a crucial part in every aspect of our daily lives. From E-Commerce shopping to online grocery everything is available within a click in the World Wide Web. According to the statistics it is said that there are thousands of websites available online and this figure is set to rise by 2020.

Every website is unique in its own way from coding to execution but the common part in every website is bugs. These bugs help the hackers to gain unauthorized access.

The aim of this project is to perform penetration testing on website using different security tools.

This will help the web developers in building a robust and secured web application. This project “Bug Hunting through Web Application Penetration Testing” is a real time project. The main aim of the project is securing an existing Web Application Platform from bugs.

This is very crucial for any website as the bugs give an advantage for the hackers to further exploit the web application.

1. **PURPOSE, Scope and Applicability**

* The purpose of this project is to secure a web application from bugs.
* The scope of this project weighs from small enterprises to large applications.
* This project can be applied from the developer level to the Penetration Tester.

**Tools**

**Nmap**

Network Mapper (Nmap) is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.

**Burp suite**

Burp or Burp Suite is a graphical tool for testing Web application security. The tool is written in Java and developed by PortSwigger Web Security. The tool has three editions. A Community Edition that can be downloaded free of charge, a Professional Edition and an Enterprise edition can be purchased and The Community edition has significantly reduced functionality. Bur Suite was developed to provide a comprehensive solution for web application security checks. In addition to basic functionality, such as proxy server, scanner and intruder, the tool also contains more advanced options such as a spider, a repeater, a decoder, a comparer, an extender and a sequencer.

**Vulnerabilities**

# Cross Site Scripting (XSS)

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

**SQL Injection**

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

# Conclusion

The project entitle “Bug Hunting through Web Application Penetration Testing” will be useful for the web developers and students to secure a web application using the different tools and techniques. This will help to build a robust and dynamic application.