Internship Task 1

Deadline : 3 september 2025

Penetration testing on Vulnerable site (testphp.vulnweb.com)

The goal is to identify and exploit vulnerabilities in the application to assess its security posture. This exercise will help students understand real-world vulnerabilities and their implications

Tools and Techniques

Both **Manual** and **automated testing** is mandatory

Automated Testing

OWASP ZAP

Nmap

Nikto

Hydra

Sqlmap etc

Manual testing (Compulsory)

Manual testing is the process of manually examining a web application or software to identify vulnerabilities, bugs, or unexpected behaviors without using automated scripts

Use Burp suite or other proxy tools

Internship Task 1

Reporting Guidelines

Table of content

List of figures

Finding severity rating : When reporting vulnerabilities, categorize them based on **CVSS v3 scores** to indicate risk level and impact. Use the cve table as reference

Executive Summary: Overview of the engagement, objectives, and scope.

Methodology: Detailed explanation of the testing approach, including both manual and automated techniques.

Findings: For each identified vulnerability, provide:

Description: Brief explanation of the vulnerability.

Risk Level: Categorize as Low, Medium, or High.

Proof of Concept (PoC): Screenshots demonstrating the exploitation of the vulnerability (**Compulsory**)

Remediation: Suggested fixes or mitigations.

Conclusion: Summary of the overall security posture of the application and recommendations for improvement

Best regard

Jafar Ali

Lead - Black Byt3