Module 4

Assignment : VAPT

Project Title: Vulnerability Assessment and Penetration Testing of "testphp.vulnweb.com"

Project Description:

In this project, students will conduct a hands-on vulnerability assessment and penetration test on the "testphp.vulnweb.com" website. This website is intentionally vulnerable, making it an ideal target for learning and practicing cybersecurity skills. The project will allow students to apply their knowledge in vulnerability assessment, OWASP, CVE, CWE, and the use of tools like Nmap, Nikto, and Burpsuite.

Project Components:

Preparation:

Obtain authorization from the website owner or administrator to perform the assessment and penetration test.

Set up a controlled testing environment, including a dedicated network or virtual machines.

Vulnerability Assessment:

Use Nmap to perform a network scan and identify open ports and services on the target website.

Run Nikto to conduct an automated vulnerability scan and gather information about the web application.

Web Application Assessment:

Utilize Burpsuite to perform a manual web application assessment.

Identify common web vulnerabilities such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).

OWASP Top 10 Analysis:

Analyze the target website against the OWASP Top 10 vulnerabilities.

Identify and document instances of OWASP Top 10 vulnerabilities found on the website.

CVE and CWE Analysis:

Research and identify specific CVEs (Common Vulnerabilities and Exposures) and CWEs (Common Weakness Enumeration) associated with any vulnerabilities discovered.

Document the details and potential impact of each vulnerability.

Reporting:

Create a comprehensive vulnerability assessment and penetration test report.

Include an executive summary, methodology, findings, risk assessment, and recommendations for mitigating vulnerabilities.

Remediation Recommendations:

Provide detailed recommendations and steps to remediate the vulnerabilities found during the assessment.

Prioritize the recommendations based on severity.

Presentation:

Present the findings and recommendations to the class or instructor, simulating a real-world scenario where you report to a client or management.

Discussion and Reflection:

The students are encouraged to discuss the challenges they faced during the project and the lessons they learned.

Reflect on the importance of ethical hacking and responsible disclosure.

Project Benefits:

- Offers practical experience in conducting vulnerability assessments and penetration testing.
- Allows students to apply their knowledge of OWASP, CVE, CWE, and security tools.
- Highlights the importance of ethical hacking and responsible disclosure.
- Enhances critical thinking and problem-solving skills in the context of real-world web application security.
- This project provides a hands-on opportunity for students to apply their cybersecurity skills to identify and mitigate vulnerabilities in a controlled environment.
- This project will align well with the course content covered earlier and will help the learners gain practical experience in the field of cybersecurity.