Module 6

Assignment : Client Side Attacks

Project Title: Web Application Security Assessment and Remediation

Project Description:

In this project, students will perform a comprehensive web application security assessment on a test web application (e.g., DVWA) to identify vulnerabilities related to client-side attacks, XSS, CSRF, and other web security issues. The project will include assessment, exploitation, and remediation steps.

Project Components:

Select a Vulnerable Web Application:

Choose a vulnerable web application like DVWA or another test environment where students can practice and assess security vulnerabilities.

Initial Assessment:

Start with an initial assessment of the web application to understand its functionality and potential security vulnerabilities.

XSS Assessment:

Perform a series of XSS assessments on the web application, including reflected, stored, and DOM-based XSS attacks.
Document the vulnerabilities found, their potential impact, and possible attack scenarios.

CSRF Assessment:

Explore CSRF vulnerabilities in the web application by crafting CSRF attack scenarios.
Identify potential risks and consequences of successful CSRF attacks.
Response Headers and Security Headers Analysis:

Analyze response headers, including security headers (e.g., Content Security Policy, X-XSS-Protection, X-Content-Type-Options).
Discuss the importance of security headers and how they mitigate certain vulnerabilities.

Brute Force Attacks Assessment:

Conduct dictionary-based and logical brute force attacks on the web application.
Document findings and discuss the significance of protecting against brute force attacks.

PII Assessment:

Identify personally identifiable information (PII) that may be exposed through vulnerabilities.
Discuss the legal and ethical implications of mishandling PII.

Remediation Steps:

Develop a plan for remediating the vulnerabilities identified during the assessment.
Include strategies for mitigating XSS, CSRF, and other security issues.

Emphasize the importance of secure coding practices and input validation.

Security Awareness Campaign:

Create materials or presentations to educate users and developers about the identified vulnerabilities and the importance of secure web application development.

Reporting:

Create a detailed security assessment report summarizing findings, risks, and remediation recommendations. Include steps for responsible disclosure if applicable.

Presentation:

Present the security assessment findings and remediation plan to the class or instructor.
Discuss the significance of web application security and the role of responsible disclosure.

Project Benefits:

- Provides practical experience in assessing and remediating web application vulnerabilities.
- Reinforces knowledge of client-side attacks, XSS, CSRF, and security headers.
- Encourages secure coding practices and responsible disclosure.
- Highlights the importance of protecting personally identifiable information (PII).
- This project allows students to apply their knowledge of web application security concepts in a hands-on manner, improving their skills in identifying, exploiting, and remediating vulnerabilities. It also emphasizes the critical role of security awareness and responsible disclosure in the field of cybersecurity.