Internship Studio EH Internship

TASK 3 REPORT

Title: Cross Site Scipting (XSS)

Domain : vulnweb.com

Subdomain: testphp.vulnweb.com

Steps to reproduce:

1. Visit testphp.vulnweb.com/search.php?test=query

2. Enter XSS payload - <script>alert(1)</script> into search field ('searchFor' container

3. Alert '1' pops up

Impact: Cross-Site Scripting (XSS) attacks allow attackers to inject malicious scripts into trusted websites viewed by other users. By exploiting XSS vulnerabilities, attackers can steal sensitive information such as cookies, session tokens, and personal data, impersonate users, and execute unauthorized actions on their behalf. Additionally, they can spread malware, manipulate website content, and perform phishing attacks, compromising both the security of the website and the privacy of its users. This can lead to identity theft, financial loss, and damage to the website's reputation.

Mitigation:

1. Input Validation and Sanitization: Ensure all user inputs are validated and sanitized. Reject or properly encode any inputs that could be interpreted as code.

2. Output Encoding: Encode data before rendering it to the user, especially data that originates from untrusted sources. Use context-specific encoding to prevent scripts from being executed.

3. Content Security Policy (CSP): Implement CSP to restrict the sources from which scripts can be loaded and executed. This can prevent the execution of malicious scripts even if they are injected.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated