SURE TRUST

MINI PROJECT -1

XSS GAME

DOCUMENTATION

Guided by : PRESENTED BY

Mr.Himaneesh sir K.SAI JAYANTH

Sure Trust Organisation

Cyber Security

Objective:

To understand and exploit XSS vulnerabilities.

Background:

XSS (Cross-Site Scripting) is a type of web security vulnerability that allows an attacker to inject malicious code into a web page. This code can then be executed by the victim when they view the page. XSS vulnerabilities can be used to steal sensitive data, deface websites, and even take control of user accounts.

Procedure:

Identify potential XSS vulnerabilities:

a. Review the application's code: Look for instances where user-supplied data is directly inserted into the HTML output without proper sanitization.

b. Use web scanners: There are many automated tools that can help you identify potential XSS vulnerabilities. These tools can scan your website and report any instances of user-supplied data that is not properly sanitized.

Verify XSS vulnerabilities:

a. Manual testing: Manually test potential XSS vulnerabilities by submitting different types of user-supplied data and observing the response. If the user-supplied data is reflected back in the HTML output without being escaped, then there is likely an XSS vulnerability.

b. Use web fuzzers: Web fuzzers can be used to automate the process of testing for XSS vulnerabilities. These tools can generate random input data and submit it to the application, looking for any signs of XSS vulnerabilities.

Exploit XSS vulnerabilities:

a. Once a XSS vulnerability has been verified, determine the extent of the vulnerability: This may involve trying to inject different types of malicious code to see what is possible.

b. Use the vulnerability to steal sensitive data, deface websites, or even take control of user accounts: The specific type of exploit will depend on the nature of the vulnerability.

Example:

Scenario:

A web application allows users to submit comments on a blog post. The application uses the following code to display the comments:

HTML

<div id="comments">

<?php

foreach ($comments as $comment) {

echo "<p>" . $comment . "</p>";

}

?>

</div>

Use code with caution. Learn more

This code is vulnerable to XSS because the user-supplied comment data is not properly sanitized before being inserted into the HTML output. This means that an attacker could inject malicious code into a comment, which would then be executed by any user who views the blog post.

Step 1: Identify potential XSS vulnerabilities:

The user-supplied comment data is not properly sanitized before being inserted into the HTML output. This is a potential XSS vulnerability.

Step 2: Verify XSS vulnerabilities:

Submit the following comment:

<script>alert('XSS');</script>

This comment contains JavaScript code that will display an alert box when the blog post is viewed. If the alert box is displayed, then the application is vulnerable to XSS.

Step 3: Exploit XSS vulnerabilities:

The attacker could inject malicious code into a comment to steal sensitive data, deface the website, or even take control of user accounts. For example, the attacker could inject code that would redirect users to a phishing website, or that would submit a form with the user's login credentials.

Mitigation:

To prevent XSS vulnerabilities, it is important to properly sanitize user-supplied data before inserting it into the HTML output. This can be done using a variety of methods, such as:

Escaping HTML characters: This involves replacing special characters, such as <, >, and &, with their HTML entity equivalents.

Using a Content Security Policy (CSP): A CSP is a security feature that allows you to specify which sources are allowed to load scripts on your website. This can help to prevent XSS attacks by blocking malicious scripts from being loaded.

Conclusion:

XSS is a serious vulnerability that can have a significant impact on the security of web applications. By understanding and exploiting XSS vulnerabilities, security professionals can better identify and mitigate these risks.