

Security Recommendation Report – Reflected XSS

This document contains flowcharts explaining how Reflected Cross-Site Scripting (XSS) works, the remediation steps, and the full professional security recommendation report.

Flowchart: How Reflected XSS Works

User Input → Application Accepts Input Without Validation →
Application Reflects Input in Response Page →
Browser Executes Malicious Script →
Attacker Gains Control (Cookie Theft, Redirects, Account Hijack)

Flowchart: XSS Remediation Steps

Identify Input Fields →
Apply Input Validation →
Apply Output Encoding →
Add Content Security Policy (CSP) →
Retest for XSS →
Deploy Fix

Security Recommendation Summary

Risk Rating: Medium

Description:

A reflected XSS vulnerability exists due to improper output encoding and lack of input validation.

Impact:

Possible session hijacking, user impersonation, data theft, and redirection to malicious websites.

Remediation:

1. Implement input validation.
2. Apply output encoding using `htmlspecialchars()`, encoding libraries, or framework sanitizers.
3. Disallow inline scripts.
4. Add a strict Content Security Policy (CSP).
5. Review and retest.

Conclusion:

The vulnerability can be fully mitigated by applying the above controls and following secure coding practices.