Project outline

Group: Ming Dai, Amitoz Brar

For the project, we will implement an attack called ***Cross-Site Scripting Attack Lab (Elgg)*** in the SEED project.

The lab primarily revolves around exploring and understanding Cross-Site Scripting (XSS) attacks and countermeasures. Participants will delve into how XSS attacks exploit web applications by injecting malicious scripts, potentially affecting other users of that application.

One key focus is on the self-propagating XSS worm, which is a malicious JavaScript program that can propagate itself. The Samy Worm, a real-world example from 2005, managed to affect over a million users in just 20 hours. The lab details two methods for a worm to propagate itself: the Link Approach and the DOM Approach.

The next section examines the countermeasures used by Elgg, a popular open-source social networking engine, to defend against the XSS attack. Two main techniques are highlighted: HTMLawed, a security plugin, and PHP's built-in method htmlspecialchars().

The final part of the lab introduces the Content Security Policy (CSP), a mechanism designed to defeat XSS attacks. Participants will experiment with CSP by setting it up on different websites and observing its effects. The CSP configurations can be done either by the web server (like Apache) or by the web application itself.

Introduction to XSS

Explanation of Cross-Site Scripting (XSS) attacks.
How they affect web applications.

Self-Propagating XSS Worm

Understanding how a worm can propagate itself.
Studying the notorious Samy Worm.
Learning the Link Approach for self-propagation.
Learning the DOM Approach for self-propagation.

Elgg's Countermeasures against XSS

Introduction to Elgg and its security measures.
Understanding how Elgg uses the HTMLawed plugin.
Familiarizing with PHP's built-in method htmlspecialchars().

Defeating XSS Attacks Using CSP

Introduction to Content Security Policy (CSP).
Understanding inline vs. link approaches for JavaScript inclusion.
Setting up CSP Policies:
- Configuration by Apache.
- Configuration by web applications.

Lab experiments using different CSP configurations.

By the end of the lab, we should have a solid understanding of XSS vulnerabilities, how they can be exploited, and how to effectively protect against them using modern techniques like CSP.