RIT | Golisano College of Computing and Information Sciences
Department of Computing Security

Evaluating the Effectiveness of Modern Protection Techniques against Cross-Site Scripting

Sumayyah Alahmadi, Graduate Capstone Advisors: Prof. Rob Olson, Prof. Sumita Mishra

Introduction

- Cross-site scripting (XSS) is a client-side code injection attack and one of the most common vulnerabilities in web applications. XSS is when the attacker injects Java Script in a victim's browser which can lead to session hijacking or malicious redirection to steal sensitive information.
- This project aims to evaluate the effectiveness of modern protection solutions against XSS vulnerabilities on top used browsers.
- We also discuss some related work of best practices against XSS, such as Encoding HTML, and using specific defense tools such as Xbuster browser extension.

Methodology

- Testing begins by identifying and deploying five vulnerable web applications.
- Next, we test the vulnerable parameter to verify which browsers the XSS attack works on.
- Based on the results, for each vulnerable web application, we implement and test three common solutions to XSS with different browsers.
- The following steps are followed with each vulnerable web application:
  - Identify vulnerability
  - Deploy vulnerable web application
  - Test the vulnerable parameter
  - Implement modern solutions against XSS
  - Analyze the results

Implementation

- Web applications are vulnerable to XSS if they aren't using sanitized user input.
- The five recent vulnerable web applications that were tested in the project are as follows:
  1) WordPress Plugin Quizlord 2.0
  2) Joomla Core 3.9.1
  3) Gila CMS 1.9.1
  4) Rukovoditel ERP CRM 2.4.1
  5) InoERP 0.6.
- These vulnerable web applications were tested on different operating systems: Linux, Windows and Mac OS, and on the following browsers: Chrome, Safari, Firefox, Opera, Internet Explorer, and Microsoft Edge.
- Three main common solutions against XSS were implemented : mod security web application firewall, content security policy and X-XSS- protection headers.

Results

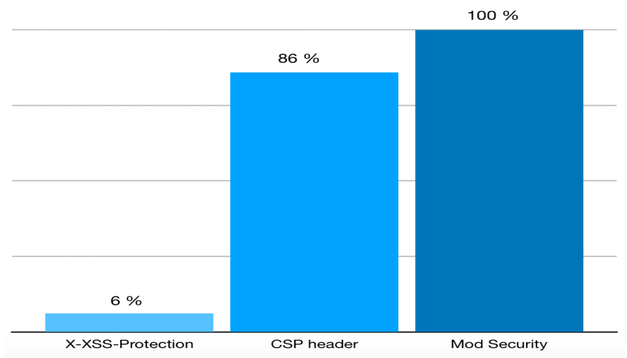

Chart 1: Success rate of each protection technique when tested against vulnerable web applications

Results Cont.

- While implementing mod security firewall, web application and content security policy header defense against XSS, other security header such as XSS protection header were found to be ineffective. The result of the project proves that not all XSS protection techniques worked as expected.

Table 1: Results of testing XSS techniques on different browsers

Browsers	Web application firewall Mod-Security	Content Security Policy headers	X-XSS-protection headers
Chrome	✓	✓	✗
Firefox	✓	✓	✗
Opera	✓	✓	✗
Safari	✓	✗	✗
Internet Explorer	✓	✗	✗
Microsoft Edge	✓	✓	✗

Conclusion and Future Work

- Testing the modern defense techniques against XSS on most common browsers to validate and ensure their capability to protect the users from cross site script attacks is the main focus of this project.
- We also give the developers and security researchers more insight on these solutions.
- Defense in depth by using multiple tools and techniques to protect against XSS is always recommended.