Website Security Research Project

Final Report

CS 467 - Summer 2021

Team Members:

Cody Medaris

Ray Franklin

Emanuel Ramirez

Website Security Research Project
CS 467 - Summer 2021

Team Members:
Cody Medaris
Ray Franklin
Emanuel Ramirez

Introduction:

The purpose of this project is to demonstrate common web based vulnerabilities and to teach defenses against those vulnerabilities. The website is hosted locally and should be restricted from being hosted on the internet due to the many vulnerabilities.

A description of what your software does from the user's perspective:

This project attempts to demonstrate the OWASP top ten most common vulnerabilities in web applications[1]. It shows the user the vulnerabilities through the lens of an attacker and guides them through the attack process.

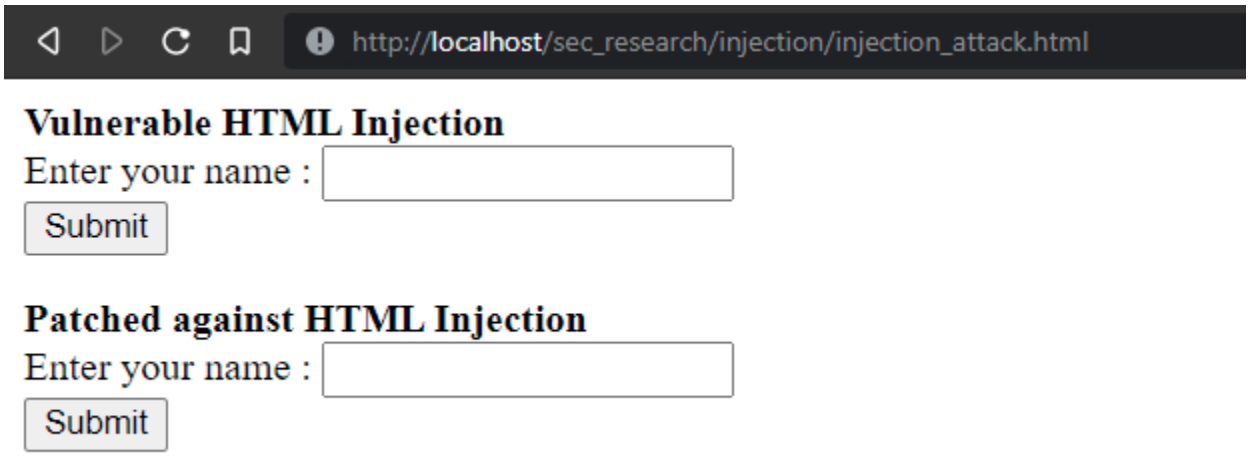

Figure 1. Example attack page.

A description of your development efforts compared and contrasted with the project plan. If there were major deviations, be sure to talk about why and what changed:

Our project kept to our original plan with little to no deviation. Our only change was to combine the write-up document with the submission for the midpoint document. This let us add all our detailed explanations and defenses coupled with the how-to use our project documentation. This document was to supplement our project's website so you could not only experience the vulnerabilities but also learn about them and how to prevent them.

A listing of the major software libraries, languages, APIs, development tools, servers, and other systems you used to create the software or system setup, and deeper discussions of any of those you want to talk more about:

- XAMPP

Team Members:
Cody Medaris
Ray Franklin
Emanuel Ramirez

    - MySQL
    - Apache
    - PHP
    - phpMyAdmin
- Javascript & HTML

We used XAMPP which we found easy to use and portable to multiple platforms[2]. It's an effective way to create a development environment that includes the packages you could need to build and host a site locally. It would not work well for an internet facing site, but given the vulnerabilities we've included purposefully, keeping the project local became an ideal method.

The languages we used, HTML, Javascript, and PHP are some of the most common and easy to use languages for building applications. These were chosen because of accessibility and lended themselves to easy development.

The conclusion should sum up the above and discuss future directions (Research Projects):

In summary, we've found that building a purposefully made vulnerable application is an effective method to both learn the vulnerabilities and to create a safe environment to teach others about said vulnerabilities. Furthermore, the site is functional and provides the necessary teaching methods to help others, but it is better designed for developers to understand and could be difficult for people who have not had experience with web development. The project could be simplified and transitioned to target a more mainstream audience in hopes to raise awareness to these vulnerabilities and help secure the industry as a whole.

References:

1. "OWASP top ten," *OWASP*. [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed: 06-Aug-2021].
2. "Apache friends," *Apache Friends RSS*. [Online]. Available: https://www.apachefriends.org/index.html. [Accessed: 06-Aug-2021].