

Homework 2

Demonstrating Insecure Interaction between Components

Overview

In this homework you use AWS Cloud 9 to create two unique examples of insecure interaction between components such as SQL Injection, Command Line Injection, Cross-Site Scripting, Unrestricted Upload of File with Dangerous Type, Cross-Site Request Forgery (CSRF), and URL Redirection to Untrusted Site ('Open Redirect'). You will provide unique code that contains the vulnerability and then provide an updated version of the code that fixes the vulnerability. You should also describe why the original code was vulnerable and discuss specific attack methods a user could try to exploit the vulnerability. Finally discuss how the new code fixes the vulnerability.

Assignment Hints:

1. Be sure you have carefully read and understand the materials in week 1 and 2 as well as successfully configured your environment.
2. Select 2 CWE/SANS Top 25 vulnerabilities under the category of **Insecure Interaction between Components**. Review and try the existing examples in links in the classroom. You can use AWS Cloud-9 to experiment as appropriate. Work in multiple languages where possible.
3. Your code examples do not need to large or fully functional from an application standpoint. However; they need to include all of the code such that the vulnerability can be fully explained and corrected.
4. Use the information in the CWE/SANS Top 25 vulnerabilities to understand and experiment.
5. Be sure your documentation and descriptions are detailed and completed.
6. You may need to conduct additional research to better understand the vulnerability or the features associated with a specific language.

Deliverables

Provide all of your source files for this assignment along with your well-organized documentation (word or PDF file) supporting the files. Be sure to provide all documentation in one word or PDF document. You can compress the source files and documentation into a zip application for easier upload.

Grading Rubric:

Attribute	Meets
Vulnerabilities	50 points Selects 2 CWE/SANS Top 25 vulnerabilities under the category of Insecure Interaction between Components. (10 points) Creates unique example for each of the 2 vulnerabilities in this category. (20 points)

	Demonstrates for each application, they are vulnerable to an attack. (20 points)
Mitigation	25 points Fixes the issues in each of the two examples you created. (25 points)
Documentation and submissions	25 points Provides all source files (those with vulnerabilities and those fixed. (15 points) Within a word or PDF file, documents vulnerabilities and describe specifically how the issues were corrected. (10 points)