COMPX519-23B

Assignment 3

Total Marks: 20
Due: 27 October 2023, 5.00 PM
Submission: Online (Submit through Moodle)

Note: In part 1, random string passed as part of the attack string/payload could be anything, e.g., your student ID. This random string should be same for all attacks to be tested.

!!!Important!!!

The website is designed to be tested and contains vulnerabilities. Please do not upload the website to any hosting provider's public html folder or internet facing servers. You must use a Virtual Machine (VM). Required tools to complete the assignment's tasks and setting up the website can be installed in VM. Please handle the provided files carefully.

This assignment has two parts.

For this assignment you will deploy a given website, perform penetration testing on it to discover vulnerabilities and secure the website to be resilient against those vulnerabilities. To deploy the website, you will need a webserver and MySQL database on the deployment machine.

Your target for pen-testing is the website 'testsite' on moodle. Inside testsite.zip you will find three versions of the website, built using PHP, Python **2** and ASP.NET/C#. The eventual functionality of all the three versions is same and they all use MySQL as the database. You can choose any one of these three to deploy the website locally on your machine. 'test.sql' contains SQL statements that will create the required tables and insert data in those tables. It just needs to be imported to MySQL.

Part1: Testing (Marks: 15)

You will test the website for possible Injection and XSS vulnerabilities and record every **successful and unsuccessful** attempt. Clearly identify if an attack was successful or unsuccessful.

Attacks to test the website for:

1. Command injection
2. Code injection
3. Database identification through string concatenation
4. Database name and version information through SQL injection
5. Enumeration of tables using UNION
6. Enumeration of columns in the above tables using UNION
7. Execution of multiple statements (Stacked queries)
8. Conditional statement exploit
9. Reflected XSS
10. Stored XSS

Report

For each attack, you must provide a screenshot and description of:

1. attack string/payload
2. a random string passed as part of the attack string/payload
3. explain how you designed the attack string/payload
4. what will be expected from a successful attack
5. whether the attack was successful

Part2: Injection and XSS Defense (Marks: 5)

Modify the website using client side, server side and database controls to defend against the vulnerabilities that have been identified. Your website will be tested for Injection and XSS vulnerabilities listed above and will be marked based on which existing vulnerabilities have been patched.

Report

Provide brief details of the controls that you have applied.

Assignment submission

You will need to submit:

1- A report (part 1 and part 2).

2- The zipped website code (after applying defense mechanisms) with the same flat directory structure as the one provided to you.

3- Additionally, if you have used database controls, submit them as a separate .sql file.

Extensions

No extensions will be given unless approved by the Department of Computer Science (https://www.cs.waikato.ac.nz/student-resources/application-for-an-extension-of-deadline)
You can submit late. However, late submissions will be deducted **1 mark/ day.**

Plagiarism

Please credit all sources you refer to. Students found plagiarising will be reported to the disciplinary committee. You are expected to follow the University's guidelines here:

https://www.waikato.ac.nz/students/academic-integrity/student-information/plagiarism

Assignments will be checked against anti-plagiarism checkers.