School of Computing and Information Systems

COMP90074: Web Security

Assignment 1 - Project Dusty Rose

Due date: No later than 11:59pm on Sunday 2nd April 2023
Weight: 12.5% Marked out of 100
Note: All challenges have a flag in the format: FLAG{something_here}

Submission Format

All students must submit a single zip file with all their code and a separate PDF version of their report (PDF not in the zip). The zip must be named <username>-assignment1.zip (e.g. testuser1-assignment1.zip). **Failure to follow these guidelines will lead to marks being deducted.**

All code for each challenge must be clearly labelled and stored in a separate file, so it is not confused with the code for other challenges.

Finally, all code must be referenced within the report. This implies that there will be code in both the report and the separate code file for each task.

If you have any questions or queries, please feel free to reach out via the discussion board, or by contacting Sajeeb, or Maleehah.

First Blood

Penetration testing and hacking depends heavily on the skills of the hacker, however efficiency and swiftness plays a very large part in all individual's careers. To help motivate students to train the efficiency and swiftness aspect of their technical skills, we will be awarding 1 bonus mark to the first student to message Sajeeb the flag for the challenges with a quick list of bullet point steps stating how they found it. This implies a total of 4 bonus marks are up for grabs.

Report Writing (25%)

For this assignment, we expect a professionally written report, provided to the client (teaching staff), explaining and specifying each vulnerability you identified by discussing the vulnerability, the process of exploitation (steps to reproduce the exploits), the potential impact to the organisation, and the remediation (making sure to tailor it to the application). **Also, please ensure that the flag is displayed in a screenshot at the end**

of each challenge's writeup. We will not be accepting any flags that are not displayed in a screenshot.

Please use the sample report template provided. There will be marks deducted for anyone who does not use this template.

Testing Scenario (75%)

You have recently graduated from your cyber security degree and have formed "We Test Pens Incorporated".

InHR is a startup that is about to launch an HR portal and has hired you to perform an exhaustive penetration test of its web application prior to go-live. The organisation has strict timelines and would like to publically launch the product on the Monday following your delivery of the penetration testing report.

InHR has selected you for this task due to the high reputation of your cyber security degree, and a belief that you will perform with a very high degree of skill. Due to being a startup, the organisation has a limited budget and was not able to set up a full testing environment. You will be performing all your testing in a production environment and therefore must use great care and skill, performing only manual penetration testing, while being acutely aware of your behaviour in the organisation's environment to prevent potential denial of service attacks **(this means no automated scanning)**.

As you are now a professional, your goal is to present your findings in a high quality report for delivery at the end of this engagement. The quality of your work and the effort that you put in cannot be judged without a quality report detailing all your findings, potential consequences, and recommended remediations. Please see the "Submission format" section for a further explanation on what you must submit for this assignment to be marked.

Lastly, as a tip, you will be testing the full web application specified in the "Scope" section, and are expected to find the following vulnerabilities:

- LFI -> FLAG{} is available
- SQL Injection -> FLAG{} is available
- XSS -> FLAG{} is available
- Information Disclosure -> FLAG{} is available

Please ensure you write up these findings in a suitable format in your report as you find them. **Also make sure to add in your own mitigation recommendations! The practicality of the remediation is very important (tailor the recommendations to the application).**

BONUS MARKS: If you are able to identify vulnerabilities that have not been listed, please report them for a chance at bonus marks. Bonus marks will be provided at the discretion of the lecturer based on complexity of the finding and quality of the writeup.

Scope

Testing must only be performed on http://assignment-dusty-rose.unimelb.life/
Testing must be manual only. Manual tools may be used (Burp, Zap, etc), *however you may not use the automated scanning capabilities of these tools*.
No automated scanning or automated tools can be used.
No load testing, denial of service (DOS) or distributed denial of service (DDOS) attacks.
You may use Burp's Intruder, but use less than 30 payloads per minute.

User Credentials

Each of these users are identical, however feel free to use whichever you please.

Username	Password
user1	Randompassword123
user2	SecurePass654
user3	TotallyLegit357