School of Computing and Information Systems

COMP90074: Web Security

Assignment 2 - Project Hermes

Due date: No later than 11:59pm on Sunday 9th May 2021
Weight: 12.5% Marked out of 100
Note: All challenges have a flag in the format: FLAG{something_here}
Note: None of the challenges are related to each other. They are entirely independent.

Submission format

All students must submit a zip file with all their code. A PDF version of their report should be submitted separately. The PDF must be named <username>-assignment2.pdf (e.g. testuser1-assignment2.pdf). The zip must be named <username>-assignment2.zip (e.g. testuser1-assignment2.zip).

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 Ashley.

Mandatory deliverable:

1. PDF report
2. Zip containing all code used

Report Writing (40%)

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, overall risk, and the remediation (making sure to tailor it to the application). The vulnerabilities must be listed in order of remediation priority, based on the risk posed. We expect an overall assessment of the risk posture for the application, using the findings from your penetration test. **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 (60%)

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

PleaseHold (PleaseHold Pty. Ltd.) is an inbound call centre servicing multiple organisations including banks and telecommunication companies. Its owners have recently kicked off an initiative to migrate from a filing cabinet to an electronic HR system. They have selected HRHub, a startup in the HR management solutions industry.

Due to the rapid need to quickly migrate to a digital system due to COVID restrictions and the need to work from home, PleaseHold has rapidly begun the implementation of HRHub into a production environment. Before cutting over to the new system, PleaseHold would like to ensure that the system is penetration tested and secure.

PleaseHold 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 the aforementioned COVID restrictions, the organisation has a limited budget, limited time, 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:

Vulnerability	Flag Format	Marks Weighting
SQL Injection	FLAG{}	25
XSS	FLAG{}	15
SSRF	FLAG{}	15
SQL Wildcard Attack	FLAG{}	5

Note: For the SSRF and SQLi vulnerabilities, we recommend using a scripting language like Python to process things quickly. This allows you to define the parameters of your automation easily!

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-hermes.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

Use your Melbourne University usernames as the username and password, for logging into the application.