|  |  |
| --- | --- |
| **Student Number: S10222894** | **Seat Number:301** |
| **Student Name: Dominic** | **Module Group:p02** |



**Web Application Pen-Testing**

Year 2 (2022/23), Semester 4

## School of InfoComm Technology

Diploma in Cybersecurity & Digital Forensics

**COMMON TEST**

Date: 15 December 2022 (Thursday)

Time: 8:30 AM – 10:00 AM

INSTRUCTIONS TO CANDIDATES:

1. Type your Student Number, Name, Module Group and Seat Number CLEARLY in the boxes provided above.
2. This paper consists of **10** pages including this cover page. Check carefully to make sure your set is complete.
3. Make sure to answer ALL questions. If you face any errors or have been unsuccessful with any of the tools, do not hesitate to include screenshots of it as well, we want to see your effort and attempts towards answering these questions. And if you don’t know how to use a particular tool but know the procedure you can describe it in words too. Don’t leave any question unanswered. Manage your time and don’t get stuck for too long at any question, you can always come back and have a go at it again.
4. Type your answers inside the answer boxes provided. Feel free to extend these answer boxes if needed.
5. The screenshots must show the Host OS (e.g., Windows 10/11) Current Date & Time. Use “Snipping Tool” to capture the entire screen and its “Highlighter” and “Copy” features. Marks would be deducted for not following this instruction.

|  |  |
| --- | --- |
| **GRADE** |  |

**QUESTION 1 (30 marks)**

You are tasked to pen-test “Peruggia” website provided under the “OWASP Broken Web Apps VM v1.2 (OWASPBWA)”: http://OWASPBWA\_IP/peruggia/

Graphical user interface, application

Description automatically generated

Graphical user interface

Description automatically generated

**QUESTION 1 (60 marks)**

**The screenshots must show the Host OS (e.g., Windows 10/11) Current Date & Time. Use “Snipping Tool” to capture the entire screen and its “Highlighter” and “Copy” features.**

1. Use OWASP ZAP or Burp Suite and provide below screenshots depicting a HTTP Get Request Header, a HTTP Response Header, and a HTTP Post Request Header with POST Parameters, for the Peruggia website. Use the Highlighter to highlight the key differences you noticed in the screenshots of these 3 Headers (no explanation is required).

(10 marks)

|  |
| --- |
|  |

**QUESTION 1 (Contd.,) (60 marks)**

**The screenshots must show the Host OS (e.g., Windows 10/11) Current Date & Time. Use “Snipping Tool” to capture the entire screen and its “Highlighter” and “Copy” features.**

1. Use an appropriate tool targeting the server that is running the Peruggia website, to detect its Server OS, Open Ports, and Running Services/Software Versions. Provide screenshots highlighting the tool’s commands and their respective outputs.

(6 marks)

|  |
| --- |
|  |

1. Use an appropriate tool targeting the webserver that is running Peruggia website to detect the Web Server OS and X-Powered-By details. Provide screenshots highlighting the tool’s command and its output.

(4 marks)

|  |
| --- |
|  |

**QUESTION 1 (Contd.,) (60 marks)**

**The screenshots must show the Host OS (e.g., Windows 10/11) Current Date & Time. Use “Snipping Tool” to capture the entire screen and its “Highlighter” and “Copy” features.**

1. Type in the Username: user and Password: user, to login to the Peruggia website. On the top menu bar, click Upload/Delete. On this page perform Unrestricted File Upload vulnerability exploitation and post-exploitation.

**Use**: php/reverse\_php as the payload for both msfvenom and metasploit.   
[**Do not use**: php/metrepreter/inverse\_tcp]

Provide important screenshots such as:

* msfvenom command
* metasploit’s multi/handler options (show options)
* Successful file upload via the Peruggia’s Upload/Delete page
* Exploitation: Command shell session opened
* Post-Exploitation: run commands: pwd, whoami, and cat /etc/passwd

(15 marks)

|  |
| --- |
|  |

**QUESTION 1 (Contd.,) (60 marks)**

**The screenshots must show the Host OS (e.g., Windows 10/11) Current Date & Time. Use “Snipping Tool” to capture the entire screen and its “Highlighter” and “Copy” features.**

1. Peruggia website provides “Comment on this picture” feature. Use BeEF tool to perform Stored XSS vulnerability exploitation and post-exploitation on this feature.

Provide important screenshots such as:

* Highlight the BeEF XSS hook script that needs to be submitted to the Peruggia website.
* Exploitation: Show that you have successfully hooked a browser that is running on your Host OS (e.g., Windows 10/11).
* Post-Exploitation: Execute Command: Pretty Theft (Under Social Engineering) from the BeEF UI Panel to the hooked browser and show the captured details that were entered by the victim who is using the hooked browser.

(15 marks)

|  |
| --- |
|  |

**QUESTION 1 (Contd.,) (60 marks)**

**The screenshots must show the Host OS (e.g., Windows 10/11) Current Date & Time. Use “Snipping Tool” to capture the entire screen and its “Highlighter” and “Copy” features.**

1. Use dirb tool to brute force and find the directories and files of Peruggia website and perform Directory Listing vulnerability exploitation.

Provide important screenshots such as:

* Highlight the dirb tool’s command.
* Highlight dirb tool’s output that are vulnerable to Directory Listing.
* Exploitation: Output of Peruggia webpages that are vulnerable to Directory Listing.

(10 marks)

|  |
| --- |
|  |

**QUESTION 2 (40 marks)**

**The screenshots must show the Host OS (e.g., Windows 10/11) Current Date & Time. Use “Snipping Tool” to capture the entire screen and its “Highlighter” and “Copy” features.**

1. Use sqlmap tool to perform SQL Injection exploitation and post-exploitation on bWAPP à SQL Injection (GET/Search) page under the bee-box v1.6 VM.

URL: http://bWAPP\_IP/sqli\_1.php

A picture containing timeline

Description automatically generated

Provide important screenshots such as:

* Highlight the sqlmap tool’s command.
* Exploitation: List of available databases
* Exploitation: List of tables inside the “bWAPP” database
* Exploitation: List of columns inside the “users” table in the “bWAPP” database
* Post-Exploitation: Dump the “Users” table along with any cracked passwords

(15 marks)

|  |
| --- |
|  |
|  |

**QUESTION 2 (Contd.,) (40 marks)**

**The screenshots must show the Host OS (e.g., Windows 10/11) Current Date & Time. Use “Snipping Tool” to capture the entire screen and its “Highlighter” and “Copy” features.**

1. Use OWASP ZAP to perform Credential Brute Forcing attack on Damn Vulnerable Web Application website: http://OWASPBWA\_IP/dvwa/login.php

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Provide important screenshots such as:

* The Fuzzer window after configuring it with the 2 payloads.
* Add Message Processor window with Tag Creator details.
* Exploitation: Successful identification of correct Username & Password pair after the completion of Brute Forcing.

(15 marks)

|  |
| --- |
| Username payload = http\_default\_users Password payload = http\_default\_pass      Admin, admin |

**QUESTION 2 (Contd.,) (40 marks)**

**The screenshots must show the Host OS (e.g., Windows 10/11) Current Date & Time. Use “Snipping Tool” to capture the entire screen and its “Highlighter” and “Copy” features.**

1. Identify a bWAPP webpage that is vulnerable to OS command Injection. Use Commix tool on that webpage to perform OS Command Injection Exploitation and Post-Exploitation.

Provide important screenshots such as:

* Highlight the commix tool’s command.
* Exploitation: Successful Pseudo-Terminal Prompt
* Post-Exploitation: Successful execution of any two OS commands via the Pseudo-Terminal

(10 marks)

|  |
| --- |
|  |

END OF PAPER

OPTIONAL

If you have reached here earlier than expected Good Job 😊

Since you think you have time at hand go ahead please try other vulnerabilities inside Peruggia website. You may paste your screenshots here. These can add to your CA 10% marks. 😊