|  |  |
| --- | --- |
| **Student Number:** | **Seat Number:** |
| **Student Name:** | **Module Group:** |



**Web Application Pen-Testing**

Year 2 (2021/22), Semester 4

## School of InfoComm Technology

Diploma in Cybersecurity & Digital Forensics

**COMMON TEST**

Date: 16 December 2021 (Thursday)

Time: 4:00 PM – 5:30 PM

INSTRUCTIONS TO CANDIDATES:

1. Write your Student Number, Name, Module Group and Seat Number CLEARLY in the boxes provided above.
2. This paper consists of **11** pages including this cover page. Check carefully to make sure your set is complete.
3. Answer **ALL** questions.
4. Type your answers in **BLUE** below each question in this paper.
5. **All screenshots must show the Host OS (Windows 10) Current Date & Time. This would prove the screenshots are taken during this test and not prior to this test. Use “Print Screen” key on your keyboard to capture the entire screen.**

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

**QUESTION 1 (30 marks)**

***The screenshots must show the Host OS (Windows 10) Current Date & Time. Use “Print Screen” key on your keyboard to capture the entire screen.***

1. Use *Zap* tool to intercept a HTTP Get Request Header, a HTTP Post Request Header, and a HTTP Response Header for any of the broken web applications of your choice (owaspbwap / bWAPP).
2. Provide a screenshot for each of the intercepted HTTP Get Request Header, HTTP Post Request Header, and HTTP Response Header.

(9 marks)

|  |
| --- |
|  |
|  |
|  |

**QUESTION 1 (Contd.,) (30 marks)**

***The screenshots must show the Host OS (Windows 10) Current Date & Time. Use “Print Screen” key on your keyboard to capture the entire screen.***

1. Based on your screenshots for Q1(a)(i), identify, and describe TWO major differences (in terms of their content) between a HTTP Request Header and a HTTP Response Header.

(6 marks)

|  |
| --- |
| 1. Request shows the web browsers info while Response shows the server info 2. Request had no date but response does |

1. Use the ***curl*** tool to list all the various HTTP methods supported by the web server that is running the OWASP Broken Web Apps (owaspbwa). Provide a screenshot highlighting the ***curl*** tool command and its output.

(3 marks)

|  |
| --- |
|  |

**QUESTION 1 (Contd.,) (30 marks)**

1. Use appropriate tools to perform any type of Credential Brute Forcing attack on any of the vulnerable web applications running inside the owaspbwap / bWAPP virtual. Provide important step by step screenshots highlighting the tool’s commands and their respective outputs.

(12 marks)

|  |
| --- |
| After failing multiple attempts, we realize that there is no lockout for this website making it susceptible to brute forcing attacks.    The above highlighted are the parameters that we will be bruteforcing    Here, both parameters have been configured with common usernames and passwords as payloads.    We see that admin admin is a valid set of credentials |
|  |

**QUESTION 2 (30 marks)**

***The screenshots must show the Host OS (Windows 10) Current Date & Time. Use “Print Screen” key on your keyboard to capture the entire screen.***

1. Use an appropriate tool targeting the web server that is running the OWASP Broken Web Apps (owaspbwa), to detect its Server OS, Open Ports, and Running Services/Software Versions. Provide screenshots highlighting the tool’s commands and their respective outputs.

(8 marks)

|  |
| --- |
|  |

1. Use an appropriate tool targeting the web server that is running the OWASP Broken Web Apps (owaspbwa) to detect the Web Server OS. Provide screenshots highlighting the tool’s command and its output.

(3 marks)

|  |
| --- |
|  |

**QUESTION 2 (Contd.,) (30 marks)**

***The screenshots must show the Host OS (Windows 10) Current Date & Time. Use “Print Screen” key on your keyboard to capture the entire screen.***

1. Use an appropriate tool to Spider the bWAPP website running in the bee-box v1.6 VM.
2. Provide screenshots highlighting the tool’s input parameters and its spidering output. [You may stop the scan halfway in case it is taking longer than usual time to complete].

(3 marks)

|  |
| --- |
|  |

1. How does this task of Spidering help in web application pen-testing?

(3 marks)

|  |
| --- |
| In web application pen-testing, a crawler or spider is a tool that automatically goes through a website following all links in it and sometimes filling in and sending forms; this allows us to get a complete map of all the referenced pages within the site and record the requests made to get them and their responses. |

1. Looking at the Spidering output, list and justify at least ONE interesting file/page that may be used by the hackers to attempt hacking, finding, and exploiting vulnerabilities.

(4 marks)

|  |
| --- |
| User\_new.php. This file page has a form submission seeing that there is a post request of the page. Hackers may use this to find vulnerabilities such as SQL injection, brute-force attack, and XSS. |

**QUESTION 2 (Contd.,) (30 marks)**

***The screenshots must show the Host OS (Windows 10) Current Date & Time. Use “Print Screen” key on your keyboard to capture the entire screen.***

1. Use any appropriate tool to brute force and find the directories and files of any ONE website of your choice running under the OWASP Broken Web Apps (owaspbwa). Provide screenshots highlighting the tool’s command and its output. [You may stop the scan halfway in case it is taking longer than usual time to complete].

(3 marks)

|  |
| --- |
|  |

1. Use any automated vulnerability scanning tool of your choice to either scan for Vulnerabilities in Server OS or Vulnerabilities in Web Application targeting the web server running in the bee-box v1.6 VM. Provide screenshots highlighting the tool’s input parameters and its top vulnerabilities (critical or high or medium) that have been detected. [You may stop the scan halfway in case it is taking longer than usual time to complete].

(6 marks)

|  |
| --- |
|  |

**QUESTION 3 (40 marks)**

***The screenshots must show the Host OS (Windows 10) Current Date & Time. Use “Print Screen” key on your keyboard to capture the entire screen.***

1. Answer the following questions based on the screenshot shown below.



Figure 3(a): Screenshot of a discovered vulnerability

1. Based on Figure 3(a) above, identify which vulnerability the web app pentester discovered.

(2 marks)

|  |
| --- |
|  |

1. Justify your answer for Q3(a)(i) by providing explanation, specifically pertaining to the pentester’s input, how this input was handled by the webpage and the output displayed on the webpage.

**QUESTION 3 (Contd.,) (40 marks)**

***The screenshots must show the Host OS (Windows 10) Current Date & Time. Use “Print Screen” key on your keyboard to capture the entire screen.***

1. Use Kali Linux to perform an attack on the Hostname/IP field shown in Figure 3(a) to spawn a reverse shell on the operating system running the website identified shown in Figure Q3(a). Provide screenshots highlighting the command used to start a listener, webpage where the injection code is submitted, and the output showing a successful functioning reverse shell.

(10 marks)

|  |
| --- |
|  |
|  |
|  |

**QUESTION 3 (Contd.,) (40 marks)**

***The screenshots must show the Host OS (Windows 10) Current Date & Time. Use “Print Screen” key on your keyboard to capture the entire screen.***

1. Use *BeEF* tool to exploit XSS vulnerability in the DVWA website running under the OWASP Broken Web Apps (owaspbwa).
2. Provide screenshots highlighting the specific DVWA webpage where the XXS vulnerability could be exploited, the BeEF XSS hook code that needs to be submitted, and the output showing a successfully hooked browser inside the BeEF user interface / dashboard.

(5 marks)

|  |
| --- |
|  |

1. Use the BeEF interface / dashboard to mount any ONE of the post-exploitation attacks on the hooked browser. Provide screenshot highlighting the attack setup in the BeEF interface / dashboard and the successful attack output on the hooked browser.

(5 marks)

|  |
| --- |
|  |

**QUESTION 3 (Contd.,) (40 marks)**

***The screenshots must show the Host OS (Windows 10) Current Date & Time. Use “Print Screen” key on your keyboard to capture the entire screen.***

1. Use sqlmap tool to carryout SQL Injection attack on mutillidae à user-info.php page under the OWASP Broken Web Apps (owaspbwa).
2. Provide screenshot displaying the list of all the databases supported by the database server hosted in the OWASP Broken Web Apps VM v1.2. **You may use the results generated previously in class, no need to run sqlmap scanning from scratch.**

(3 marks)

|  |
| --- |
|  |

(3 marks)

1. Use sqlmap to extract the Column Names in the Table “users” in the dvwa database. Provide screenshot highlighting the sqlmap command used and its output.

(3 marks)

|  |
| --- |
|  |

1. Use sqlmap to dump records in the Table “users” in the dvwa database. Provide screenshot highlighting the sqlmap command used and its output.

(3 marks)

|  |
| --- |
|  |

-- END OF PAPER--