|  |  |
| --- | --- |
| **Student Number: S10222894G** | **Seat Number:** |
| **Student Name: Dominic Lee** | **Module Group: P02** |



**Web Application Pen-Testing**

Year 2 (2022/23), Semester 4

## School of InfoComm Technology

Diploma in Cybersecurity & Digital Forensics

**PRACTICAL TEST**

Date: 16 February 2023 (Thursday)

Time: 4:00 PM – 5:30 PM

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 **5** pages including this cover page. Check carefully to make sure your set is complete.
3. Make sure to answer ALL the **4** questions totaling **50 Marks**. 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 on 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 (10 marks)**

You are tasked to execute a proof-of-concept that is related to “A06:2021-Vulnerable and Outdated Components” on the server hosting the bWAPP (Bee Box) an extremely buggy web app!

**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.**

Provide important screenshots such as:

* Commands and the output of the tool used to discover the vulnerability that is related to “A06:2021-Vulnerable and Outdated Components”.
* Critical steps and/or commands used to exploit this vulnerability.
* Commands and/or output showing/highlighting successful post-exploitation.

(10 marks)

|  |
| --- |
|  |
| Here we see that the serer is vulnerable to heartbleed attacks.and we have succesffuly exploited the vulnerability. |

**QUESTION 2 (15 marks)**

You are tasked to solve the challenge “Deluxe Fraud” inside the OWASP Juice Shop website, that is related to “A08:2021 - Software and Data Integrity Failures”. Deluxe Fraud Challenge is to obtain a Deluxe Membership without paying for it.

Graphical user interface

Description automatically generated

**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.**

Provide important screenshots such as:

* Successful registration of any new user account on the OWASP Juice Shop website.
* Critical steps and/or commands used to exploit this challenge / vulnerability.
  + Must Include the relevant HTTP Requests and Responses screenshots.
* Commands and/or output showing successful completion of this challenge.

(15 marks)

|  |
| --- |
| **Delete disabled=”true” and “mat-button disabled”** |

**QUESTION 3 (15 marks)**

You are tasked to solve the challenge “Premium Paywall” inside the OWASP Juice Shop website, that is related to “A02:2021- Cryptographic Failures”. Premium Paywall challenge is to Unlock Premium Challenge to access exclusive content. This challenge can be found listed at the http:// Ubuntu 64-bit-WAPT-VVM\_IP:3000/#/score-board.



**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.**

Provide important screenshots such as:

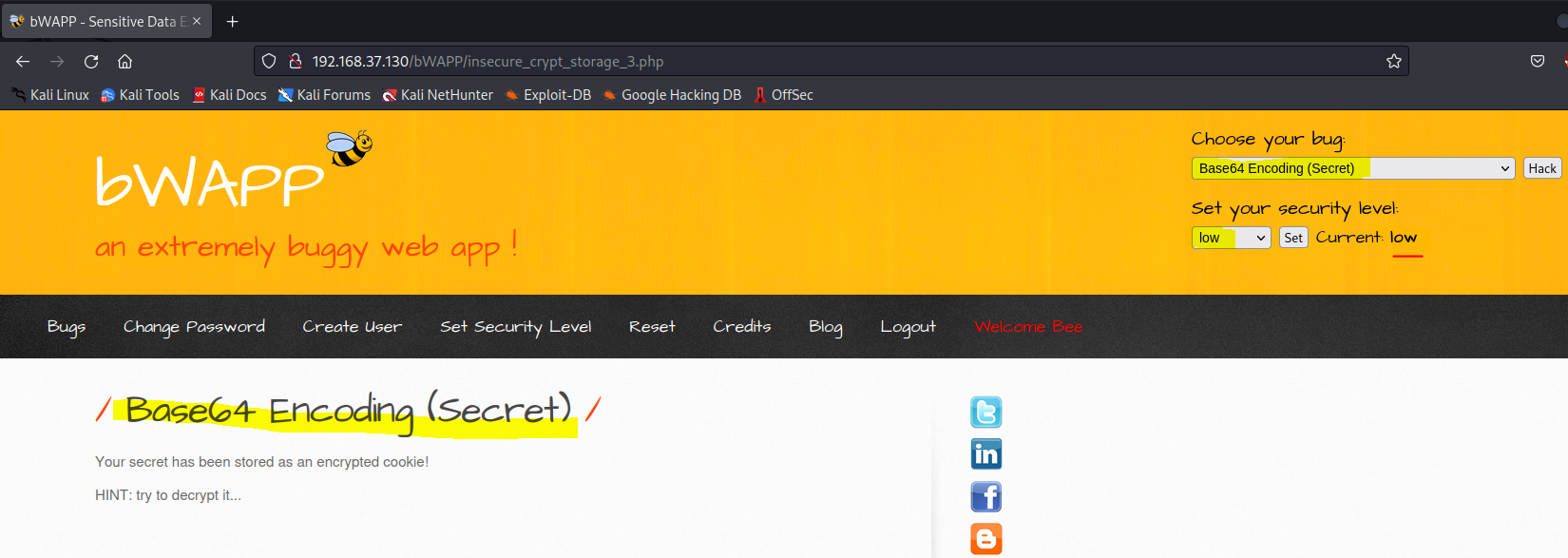
* Location of the encrypted comment.
* Command and the output of any tool that you have used to discover a directory containing relevant details required to decrypt the comment.
* Command and the output of the tool used to decrypt the comment.
* Successful display of the “exclusive content” and successful completion of this challenge.

(15 marks)

|  |
| --- |
| **Challenge Solved** |

**QUESTION 4 (10 marks)**

You are tasked to solve a challenge “Base64 Encoding (Secret)” inside the bWAPP (Bee Box) an extremely buggy web app, that is related to “A06:2017 – Sensitive Data Exposure / A02:2021- Cryptographic Failures”.



Use the hints provided on the page:

Base64 Encoding (Secret)

Your secret has been stored as an encrypted cookie!

HINT: try to decrypt it...

**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.**

Provide important screenshots such as:

* Command and/or tool used to capture the cookie.
* Critical steps taken to decrypt the secret in the cookie.
  + Use the decoder already available in the tool you are using to capture the cookie or any decoder available in the Kali Linux, Internet access is NOT required for this.
* Output of the successfully decrypted secret in the cookie.

(10 marks)

|  |
| --- |
| We used the decode button and the cookie decoded into the value above in the screenshot. The next step is to then convert it from Base 64 into text.    Thus, the decrpyted value is “test”. |

END OF PAPER