CMP020X305S - Cyber-Security:

Portfolio 6 Submission Template

|  |  |
| --- | --- |
| First Name | Antonio |
| Last Name | R Oliver |
| Student ID | YIT19488399 |

Requirement A

What vulnerability have you exploited for Requirement A?

|  |
| --- |
| Access the administration section of the store |

What difficulty level is the vulnerability (i.e., number of stars)?

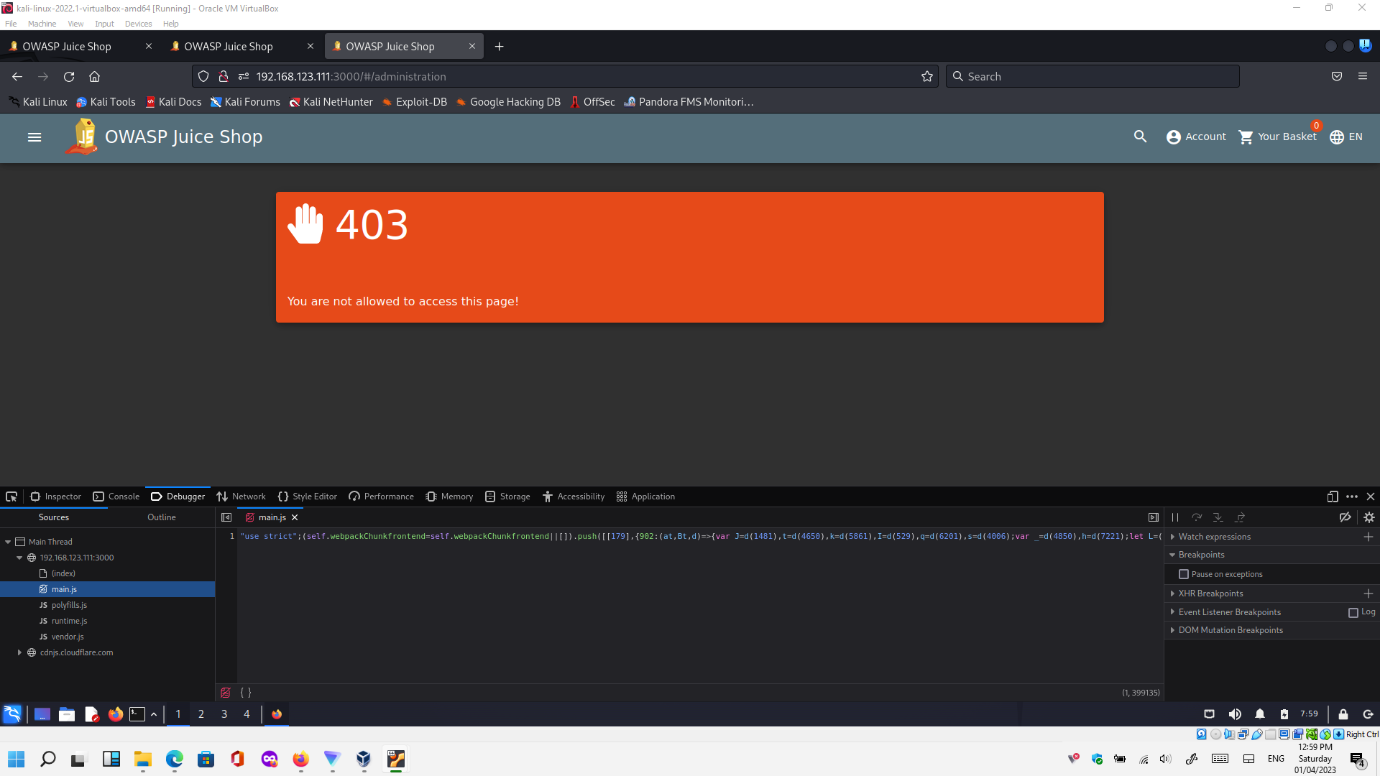
|  |
| --- |
| TWO (\* \*) |

What tutorial did you use to complete the vulnerability (enter web address(es))?

|  |
| --- |
| <https://youtu.be/rsj2MEZcRA8>  <https://youtu.be/TomSqm79JoA>  <https://youtu.be/S-KF_YC-Gfc> |

What tools did you use as part of the exploit process?

|  |
| --- |
| Injection first to login as admin (admin’ or 1=1;), and after broken access control to administration dashboard website (www…. /administration). |



A screenshot of a computer

Description automatically generated

This challenge discovered without intention while accessing to the administration section of the sore.

Graphical user interface, website

Description automatically generated

To solve the initial vulnerability about accessing to the administration section of the store, it is necessary to login as admin to the store, and this is done by injection in the login section of the website.

Graphical user interface, website

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Simply add /administration in the URL of the website address while logged as admin (previous step).

If you try see the /administration or /admin/ or /administrator before logging as admin; error will appear (please, see first screenshot).

Clearly describe the steps that you took to complete the vulnerability in your own words and include annotated screenshots where appropriate.

Wow Factor

What vulnerability have you exploited for Requirement A?

|  |
| --- |
| Previous vulnerability has associated two star level vulnerability and accidentally I exploit “Error handling”, 1 star level vulnerability. |

What difficulty level is the vulnerability (i.e., number of stars)?

|  |
| --- |
| Two and one |

What tutorial did you use to complete the vulnerability (enter web address(es))?

|  |
| --- |
| Same as Requirement A because it is a prerequisite, and accidentally discovered while performing the desired vulnerability. |

What tools did you use as part of the exploit process?

|  |
| --- |
| Described in previous part of the portfolio. |

Clearly describe the steps that you took to complete the vulnerability in your own words and include annotated screenshots where appropriate.

Please have a look at all vulnerabilities done before updating requirements:



Graphical user interface, website

Description automatically generated

Graphical user interface

Description automatically generated

A screenshot of a computer

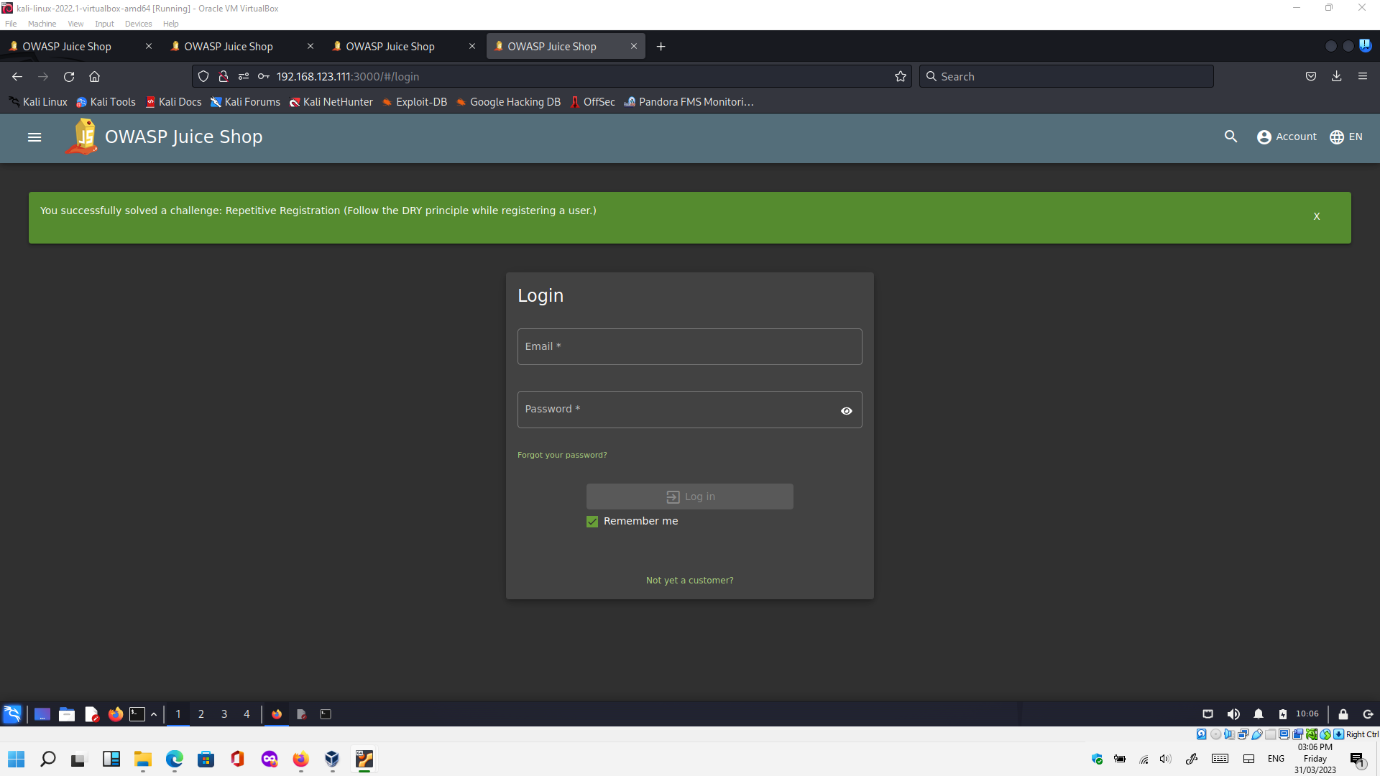
Description automatically generated

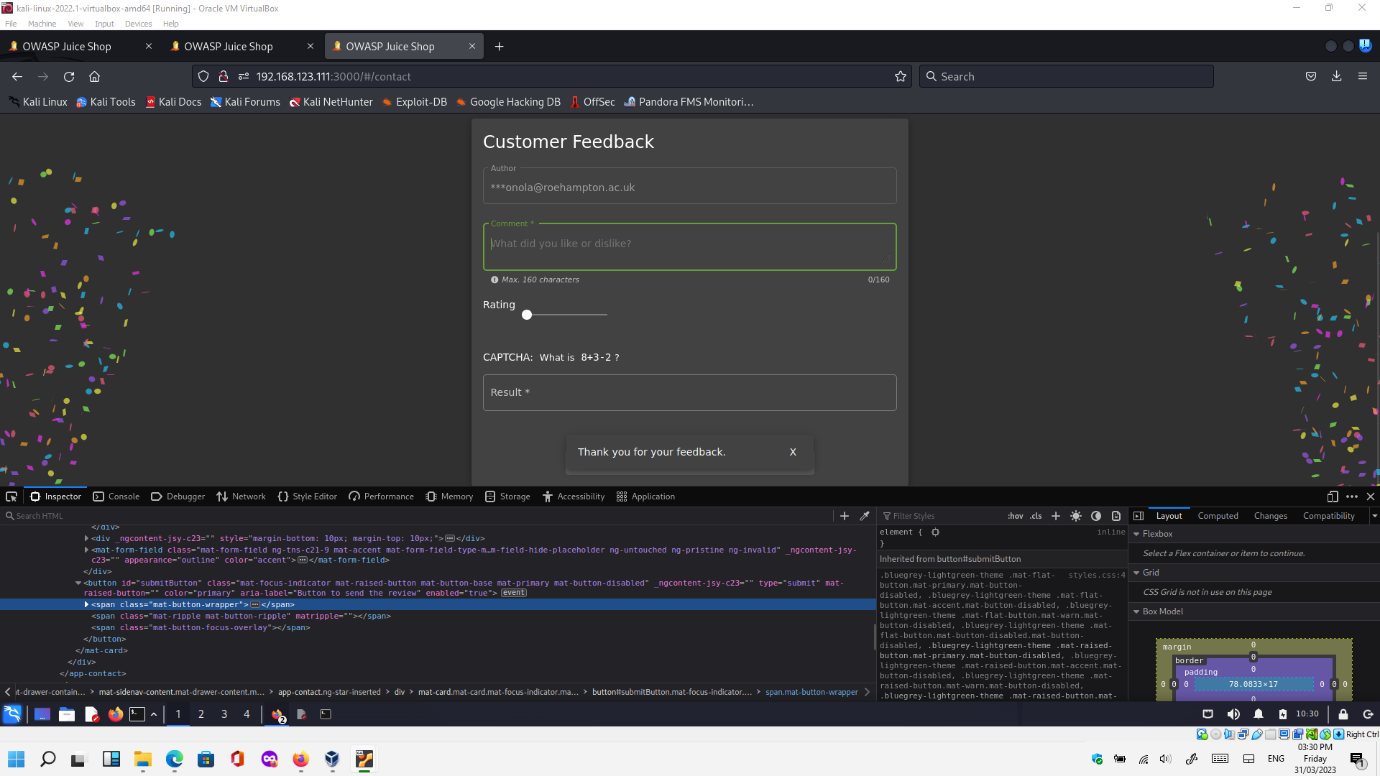
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated





Graphical user interface

Description automatically generated



A screenshot of a computer

Description automatically generated



[This Photo](https://citizentruth.org/has-the-us-already-declared-a-cyber-war-on-iran/) by Unknown Author is licensed under [CC BY-ND](https://creativecommons.org/licenses/by-nd/3.0/)



[This Photo](https://tekhdecoded.com/cyberwars-battles-are-now-raging-on-the-internet/) by Unknown Author is licensed under [CC BY-SA-NC](https://creativecommons.org/licenses/by-nc-sa/3.0/)