CMP020X305S: BSc Cyber Security

Portfolio Lab 06 (of 06): OWASP Juice Shop Challenge

###

Set Date:	**24th March 2023**
Requirement A	Document an OWASP Juice Shop Exploit
Milestone Deadline:	21st April 2023 13:00
Coursework Deadline:	21st April 2023 13:00
Submission Format:	Requirement A: Upload a single document to Moodle
Feedback and Marks:	Via Moodle
Marking Scale (Lab):	Maximum 10.0 marks for completion of Requirement A
Marking Scale (Wow Factor):	Maximum 6.2 marks for Wow Factor
Learning Outcome LO2:	Investigate measures that can be taken by both individuals and organizations including governments to prevent or mitigate the undesirable effects of computer crimes and identity theft.
Learning Outcome LO4:	Evaluate risks to privacy and anonymity in commonly used applications.

IMPORTANT: This is a living document and will be subject to changes and updates during the life cycle of the lab portfolio. Therefore, it is imperative that you check this document regularly!!

ACADEMIC MISCONDUCT

Your submission for this coursework will be scrutinised for plagiarism, collusion, and other forms of academic misconduct. Please ensure that the work that you submit is your own, and that you have cited and referenced appropriately, to avoid having to attend an academic misconduct hearing.

About this portfolio lab

This portfolio lab is problem-centred. Therefore, you will need to research and take responsibility for solving any technical challenges that you encounter. You are encouraged to work collaboratively with other students in your cohort. However, the work that you submit must be your own and any sources of assistance etc, must be acknowledged through referencing or where appropriate, code comments.

For this portfolio, you will:

1. research OWASP Juice Shop.
2. add an OWASP Juice Shop virtual machine to your sanitised network.
3. conduct an exploit of OWASP Juice Shop.

Resources Required for this Portfolio Lab

This lab requires resources from Portfolio 01:

- Kali Linux
- Ubuntu Server Gateway
- OWASP Juice Shop

Marking Criteria

This portfolio will be marked in accordance with the following rubrics:

Portfolio Requirement A: Document an OWASP Juice Shop Exploit	**Maximum Mark**
Not attempted	0
Evidence of a very limited level of completion in accordance with the requirement description.	1.0 - 4.1
Evidence of a limited level of completion in accordance with the requirement description.	4.1 - 4.5
Evidence of an adequate level of completion in accordance with the requirement description.	4.6 - 6.0

Portfolio Requirement A: Document an OWASP Juice Shop Exploit	**Maximum Mark**
Evidence of a good level of completion in accordance with the requirement description.	6.1 - 6.5
Evidence of full completion in accordance with the requirement description.	6.6 - 10.0

Portfolio (Optional): Wow factor!!	**Maximum Mark**
Not attempted	0
Evidence of a very limited attempt that is not directly relevant to the portfolio.	1.0 - 2.6
Evidence of a limited attempt that is somewhat relevant to the portfolio.	2.7 - 3.2
Evidence of an adequate attempt that is mostly relevant to the portfolio.	3.3 - 3.9
Evidence of a good attempt that is relevant to the portfolio.	4.0 - 4.6
Evidence of a very good attempt that is relevant to the portfolio.	4.7 - 5.2
Evidence of an excellent attempt that is relevant to the portfolio.	5.3 - 6.6

The **maximum mark for completing Requirements A and B for this lab portfolio is 10**. An **additional maximum mark of 6.6** can be awarded for "**Wow Factor**" that evidences appropriate, relevant and additional learning. Typically, wow factor demonstrates a self study contribution that extends or advances the core technical requirements of a lab portfolio.

Late Portfolio Submissions

For each week that a portfolio is late, two marks will be deducted from the portfolio score that is awarded at the time of assessment.

Requirement A: Document a SINGLE Juice Shop Exploit

Getting started

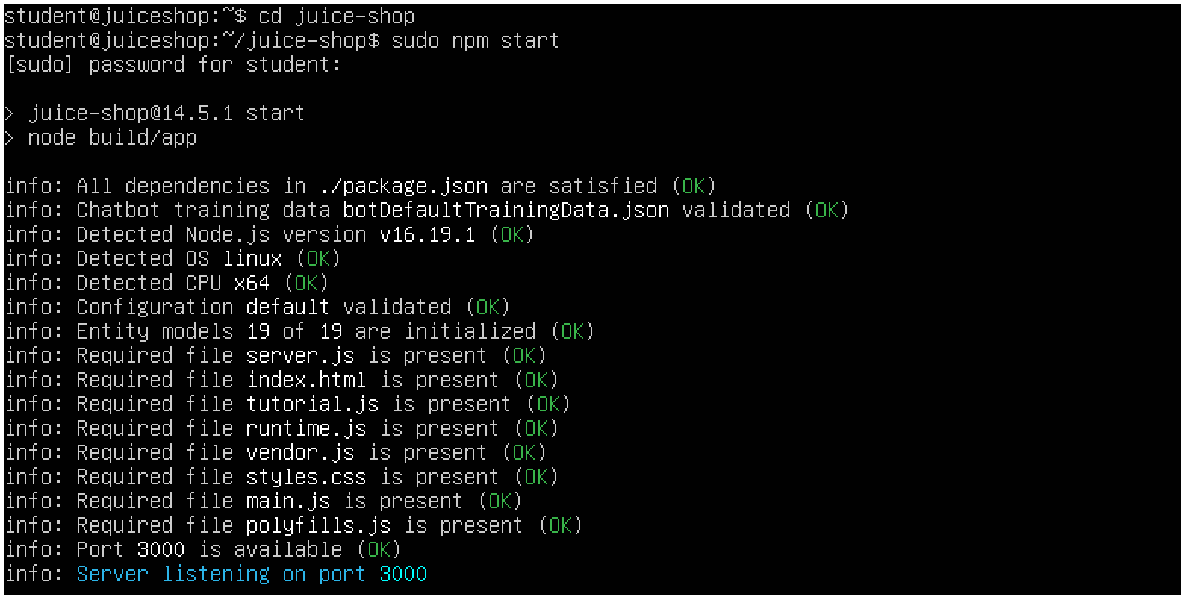
1. Add the Juice Shop virtual machine to your sanitised network (ask your instructor for Juice Shop USB key).
2. Login to the OWASP Juice Shop virtual machine with a username of `student` and a password of `Student1`.
3. Change directory to the `juice-shop` folder by typing...

   ```
   cd juice-shop
   ```

4. Start the webserver by typing...

```
sudo npm start
```

The server should start, displaying the following status...

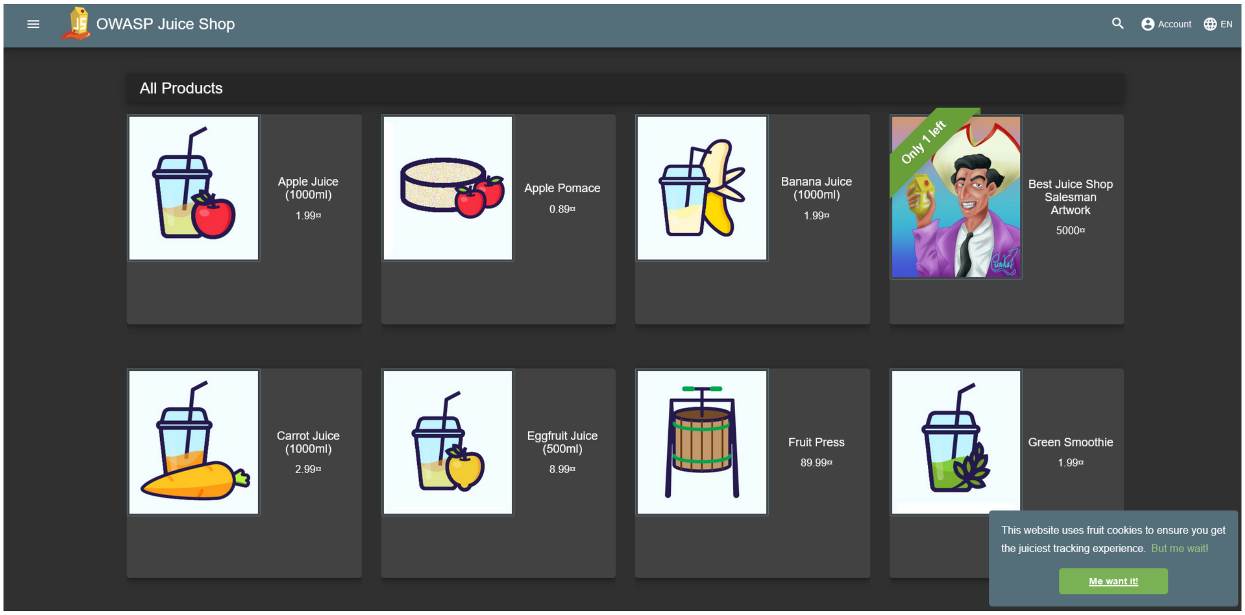


```
student@juiceshop:~$ cd juice-shop
student@juiceshop:~/juice-shop$ sudo npm start
[sudo] password for student:

> juice-shop@14.5.1 start
> node build/app

info: All dependencies in ./package.json are satisfied (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Detected Node.js version v16.19.1 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 19 of 19 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file main.js is present (OK)
info: Required file polyfills.js is present (OK)
info: Port 3000 is available (OK)
info: Server listening on port 3000
```

5. From your Kali virtual machine, open a browser and visit...

```
192.168.123.111:3000
```

The following page should load:



This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!

Your challenge!

Carefully read, review and explore information about OWASP Juice Shop. Feel free to use any resources that you like. Here are a few links to get you started:

- https://owasp.org/www-project-juice-shop/
- https://pwning.owasp-juice.shop/
- https://pwning.owasp-juice.shop/appendix/solutions.html
- https://pwning.owasp-juice.shop/part1/challenges.html
- https://pwning.owasp-juice.shop/part2/
- https://akash-pawar.github.io/owasp-juice-shop/

OWASP Juice Shop has many vulnerabilities. Having read and research OWASP Juice Shop, your challenge is to:

1. Decide on a single vulnerability of your choice. This can be a 1, 2 or 3 star vulnerability (they will be awarded the same maximum mark).
2. Exploit your chosen vulnerability.
3. Document the exploit in your own words and screenshots and upload the document to Moodle.

Wow factor suggestions!

It is feasible to pass this portfolio without completing any "wow factor". However, if you decide to take on this additional learning opportunity, the choice of what contribute is yours. Here are some examples to consider:

- Explore and document an additional 1 star OWASP Juice Shop Vulnerability OR
- Explore and document an additional 2 star OWASP Juice Shop Vulnerability OR
- Explore and document an additional 3 star OWASP Juice Shop Vulnerability.

NOTE: You only need to complete 1 additional vulnerability for WOW factor. The greater the number of stars, the higher the WOW factor mark.

End of Portfolio Lab :-)