**Session 1 Worksheet – An Introduction to Web Hacking**

1) We found the URLs using a Javascript beautifier [1] – can you think of a different way to discover all the possible paths on a website? Note: we do not recommend the use of an automated tool against the Heroku instance at [2] – please only run brute-force tools against a TryHackMe or local instance, as they are more stable and better contained.

Hint: Search ‘directory traversal tools’

2) We found the scoreboard (the list of challenges) via our previously discovered list of paths. In some versions of Juice Shop, the scoreboard button is hidden from the navbar initially – can you reveal it another way?

Hint: Is there an attribute in the HTML/CSS that stops you from seeing the link to the page?

3) We used basic SQL Injection to login as an admin user – but is there an easier way?

Hint: Not everyone is as aware of cybersecurity as you are!

4) You don’t have to use Burp Suite to do a lot of the things we did in session – can you use your browser’s Developer Tools (press F12 to activate them) to do the following?

4.1) Extract the user token

4.2) Register an admin user

5) As you saw, Burp Suite is a very powerful tool for editing requests, that we can use to register admin users amongst other things. Can you use it to do the following?

5.1) Submit a 0-star review in Customer Feedback

5.2) Submit a review as another user

6) Can you perform a persisted XSS attack via the Customer Feedback page that copies the current user’s token and displays it on the page?

Hint: Make use of the ‘recursive sanitisation’ flaw we discussed in the session today. You might need to look up the syntax for reading browser cookies with Javascript!

**Appendix**

[1] - <https://beautifier.io/>

[2] - https://juice-shop.herokuapp.com