**Session 3 Worksheet – Juice Shop Revisited**

First of all, if you didn’t come to the Give it a Go where we first covered Juice Shop, take a look at that week’s worksheet! You can view all the worksheets at [1]

1) Can you use Burp Suite’s Intruder module [2] to discover the contents of every user’s basket?

Hint: One part of the URL represents the user ID – you can change this to be a ‘payload’ in the Intruder, and configure it to discover each basket

2) Can you get the hashes for all the registered users and crack them with John the Ripper? [3]

Hint: Look up how to use John to crack a list of hashes, rather than doing it one by one!

3) Edit the review of another user using Burp suite!

4) Can you use the SQL query we crafted in the session to extract the following:

4.1) Usernames and passwords for all users?

4.2) Full names, addresses, and mobile numbers of customers?

4.3) All the possible captcha questions and answers?

4.4) Security questions and answers for all users?

Hint for 4.4: this one isn’t as simple as selecting from one extra table – you might need to ‘join’ something…

General hint: to make your results a bit easier to read, you can look at changing the names of the columns that are outputted as part of the query.

5.1) Can you use XSS to do the following:

5.1) Stop the admins using the administration panel by redirecting them each time they visit the page?

5.2) Make a request to add an item to a user’s basket every time they visit the ‘About Us’ page?

5.3) iframes are pretty conspicuous when they appear on the page – can you edit your payloads to make them more difficult to see?

5.4) Hard: Redirect unsuspecting users to download a ‘malicious’ file hosted on a server you own?

5.5) Extra hard: Steal the token cookie and post it to a server you control?

Hint: For 5.4 and 5.5 you will need to setup a server – if you’ve never done this before, I’ve written a simple server in Python that runs on localhost (your computer) and will print POST requests to your screen, which you can download here [4]. To run it, you’ll need to have Python installed, which you can get here [5]. For the cookie stealing you can use the document.cookie method discussed in the session, but you’ll need to look up how to make a POST request in Javascript too!

6) If you’ve managed all that, you’re well set up to become an expert in web application hacking! We’ve covered most of the key methodologies and tools that you’ll need, from the first steps in exploring a site using developer tools and gobuster, to manipulating requests with Burp Suite, to some more advanced exploits with SQL Injection and XSS. With all this knowledge, you should be able to complete the rest of the challenges on the Juice Shop scoreboard!

**Appendix**

[1] – <https://www.shefesh.com/wiki/worksheets>

[2] – <https://portswigger.net/burp/documentation/desktop/tools/intruder>

[3] – <https://www.openwall.com/john/>

[4] – <https://gist.github.com/Twigonometry/a619bc5234d39296737e8d00899f23af>

[5] – <https://www.python.org/downloads/>