**Session 5 Worksheet – Automation in Python**

1) Can you write a bash script to deploy Juice Shop on your local computer? You should first install Node JS [1] and Git [2] and then run the appropriate commands specified on the Juice Shop deployment page [3] (under ‘From Sources’).

2) Write a bash script that launches a Simple Python HTTP Server (use python3 -m SimpleHTTPServer) in a given directory, with the option to move a file to the directory ready to be served.

3) Try out some of the challenges on Scraping Club. The paginated scraping challenge [4] is a good place to start.

4) Adapt the Repeater [5] and the Customer Feedback Script [6] to better simulate human behaviour (think about how long a human might take to do these things, and what other requests they might make along the way to get to the form…)

Note: You can fork the repositories to do this if you wish, or just download and edit the code

5) Use the Password Cracker [7] to crack the passwords for some of the Juice Shop accounts – you might want to add the full RockYou list [8] to the wordlists folder, as the ones currently in the repo don’t contain all the passwords you need!

**Appendix**

[1] – <https://nodejs.org/en/download/>

[2] – <https://git-scm.com/downloads>

[3] – <https://bkimminich.gitbooks.io/pwning-owasp-juice-shop/content/part1/running.html>

[4] – <https://scrapingclub.com/exercise/list_basic/>

[5] – <https://github.com/Twigonometry/CTF-Tools/tree/master/repeater>

[6] – <https://github.com/Twigonometry/sesh-automation/blob/master/capture-captcha.py>

[7] – <https://github.com/Twigonometry/CTF-Tools/tree/master/password_cracker>

[8] – <https://github.com/brannondorsey/naive-hashcat/releases>