SQL Injection

Begin by using docker to launch the mutillidae exploitable framework:

```
docker run -p 1337:80 szsecurity/mutillidae
```

The objective is to dump the `accounts` table from the `nowasp` database using sql injections. You should use the `burp` program in Kali as demonstrated in class, then use the `sqlmap` program. There is an instructional video back on the schedule page that shows how I did this with DVWA.

If I was using the browser and burpsuite on Kali, I first had to modify a browser setting so that all my traffic would go to the Burp proxy. Go to `about:config` and change `network.proxy.allow_hijacking_localhost` to `true`. Make sure you set your proxy settings to `127.0.0.1` and port `8080`.

Hint: Don’t have burpsuite intercept anything until you are ready to load the form. The form you are looking for is under owasp 2013->A1->SQL1->user info.

**To pass off**

Upload your screenshot of your dumped table and a timestamp.