Computer Security
Tutorial 7

Margus Lind
School of Informatics
University of Edinburgh

1   Web Security

For this tutorial you will be learning web security and solving relevant challenges using the Security Shepherd platform - an online web security tool developed by OWASP (if you don't know them look it up).

- Visit `https://shepherd.modulo.ee`

- Register an account for yourself

- You only have to choose a username and password

- Submitting your email or any other personal details is strictly voluntary

- Similarly, your username can be freely chosen (let's stay decent, please), and does not have to reflect your UUN.

- Finally, log on, and select Field Training from the left hand side menu.

Work through the tasks under this section from top to bottom - they are arranged in a logical order. Most tasks will also provide you with some instructions or links to materials online.

If you get stuck, don't hesitate to ask your tutor or fellow students. However, when giving advice, please try to not give straight answers and instead provide hints or guidance - this is a learning opportunity.

2   Web Proxy

It may be helpful to use an intercepting web proxy, however, the built in developer tools are sufficient for the initial section.

Burp Suite is a popular web proxy used by security testers. You can download the free version from `https://portswigger.net/burp/freedownload`. Make sure you get the JAR file

You can launch it from the terminal by typing `java -jar burpsuite_free_v1.7.27.jar` (or whatever you saved the jar file as). This will launch a proxy server on your machine at `127.0.0.1:8080`.

To configure your browser to use:

- Open the menu from the top right corner

- Choose Preferecnes

- Choose Advanced from the left hand side menu

- Choose Network tab within the page

- Select Connection Settings

- Configure Firefox to use a manual proxy configuration

- Set the HTTP proxy and SSL proxy to point at `127.0.0.1:8080`

- Don't forget to undo these setting when you want to use Firefox without Burp intercepting your traffic.

You have now successfully mounted a man-in-the-middle attack against yourself. Thus don't be alarmed when the browser tries to warn you of this. Some websites will not work, including Google. This is due to a protection mechanism called HSTS (see: `https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security`). You can use Chrome to browse the web while Firefox is configured to use Burp.

Good luck!