Task 1:

A computer screen shot of a computer

Description automatically generated

What: An alert pops up because the javascript in Alice’s profile was executed by the browser.

Why: The script in Alice’s brief description was accessed on this page, and the browser executed it because it was valid HTML.

Task 2:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Cookies: cookies are small bits of text data that websites store on the user machine for various purposes. The specific type of cookie that we’ll care about for this lab are cookies which store authentication data (designed so that we don’t have to repeatedly sign in).

Task 3:

Log in as another user. Look at Samy’s profile. What happens? Samy is added as a friend

A screenshot of a computer

Description automatically generated

Task 4:

A screenshot of a computer

Description automatically generated

Task 5:

A screenshot of a computer

Description automatically generated

Regex is used to look for specific patterns, and code is definitely a specific pattern. So, regex can be used to see if any malicious code has been injected into the loaded webpage in order to stop its execution. Or more specifically it can be used to look for common patterns in malicious code.

Task 6:

A screen shot of a computer program

Description automatically generated

It’s likely that encoding is general can do a lot more than what is shown here, but this is a good example of “mangling” inputs. The main effect is that these inputs are no longer valid code and are unable to be executed in this state.

Task 7:

The main thing I learned is how shockingly insecure the combination of web browsers and JavaScript is and how easy it is to execute malicious code when safeguards are lacking. It was also very useful to see the safeguards against XSS in action. The ability to use regex to identify malicious code patterns was very insightful and not something that I had considered as an option. And finally, it was good to learn about the effectiveness and ease of use of encoding.