**Unit 15 Homework-Brenda Schecher**

**Web Application 1: Your Wish is My Command Injection**

**Ping 8.8.8.8**

**A picture containing text

Description automatically generated**

**8.8.8.8 && pwd**

**A picture containing text

Description automatically generated**

**8.8.8.8 && cat ../../../../../etc/passwd**

**Text

Description automatically generated**

**8.8.8.8 && cat ../../../../../etc/hosts**

**Text

Description automatically generated**

**Mitigation Strategy-**

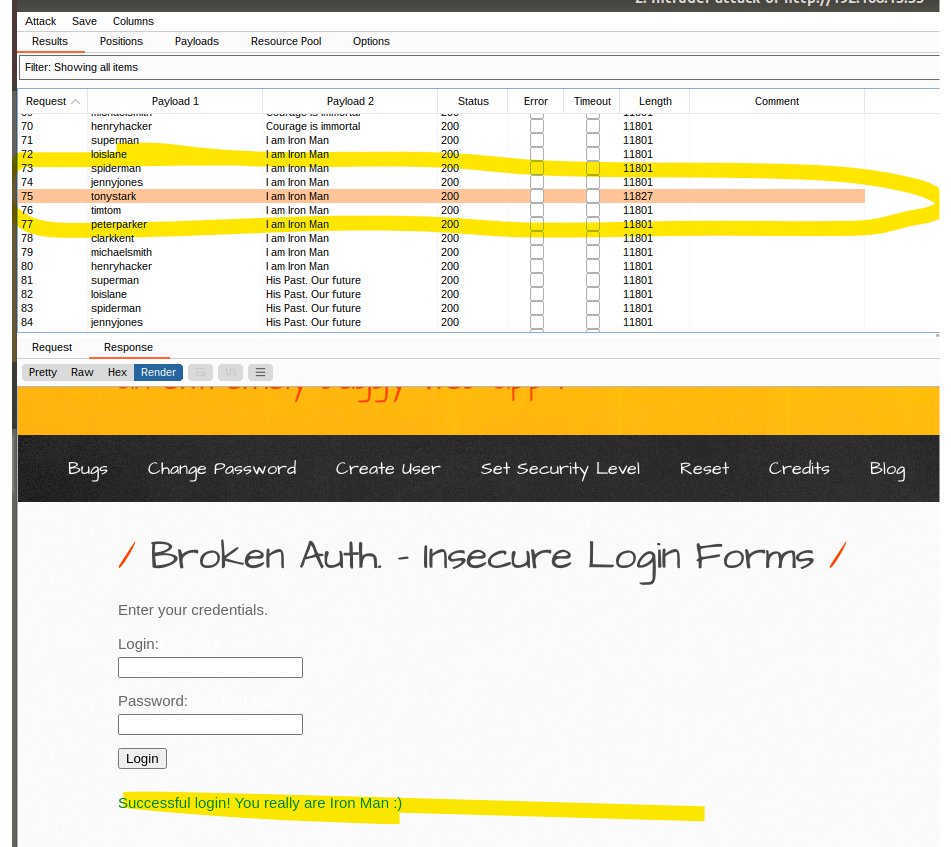
There are many strategies, but a few mentioned in our module is to limit user input when calling for files from the web application. Using input validation to limit the user’s ability to modify the file that is being accessed will help mitigate risk. Web servers should run under a special service user account where that user only has access to that folder.

Use the principle of least privilege, where an application has the minimal authority to perform a task. Another strategy could be making the root user unable to access via remote connection.

According to Portswigger, the way to prevent a directory traversal attack is to avoid passing user-supplied input to filesystem Aps altogether. If that that cant happen, then adding two layers of defense should help prevent attacks. <https://portswigger.net/web-security/file-path-traversal>

**Web Application 2: A Brute Force to Be Reckoned With**

After entering in the admin user name and passwords, I went through payload 1 and payload 2 results. Tonystark and I am Iron Man credentials are vulnerable to a brute force attack.

****

**Mitigation strategy-** It would be good to add complexity to usernames and passwords. Upper/lower case and numbers will help mitigate unauthorized users’ accessing applications.

Another strategy would be to add a certain number of failed attempts before the user’s account gets locked. Using multi-factor authentication methods will help as well because only the user can accept the generated token.

**Web Application 3: Where’s the BeEF?**

**Google log in**

**Graphical user interface, text, application, email

Description automatically generated**

**Graphical user interface, text, application

Description automatically generated**

**Graphical user interface, text, application

Description automatically generated**

**Social Engineering >> Pretty TheftGraphical user interface, text, application

Description automatically generated**

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

**Social Engineering >> Fake Notification Bar**

Graphical user interface, text, application

Description automatically generated

**Host >> Get Geolocation (Third Party)**

Graphical user interface, text, application, website

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

**Mitigation Stategy-**one strategy would be to train employees on these types of cross scripting attacks. Make sure to have them research before adding credentials into websites. Make sure they are secure and are the correct website address. Ensure the browser is up to date as they will have the latest security tools installed. Properly santizing data.Adding no-script plubins to the browser to help block malicoius scrips would help as well.