**Unit 15 Homework**

**Web Application 1**

* /etc/passwd

Text

Description automatically generated

* /etc/hosts

Text

Description automatically generated

This exploit is happening because it is abusing the fact that the script is pinging an IP by inputting what’s being typed into the command line. Since the website is only meant to ping IP addresses, a few ways to mitigate this is to prevent anything besides numbers and decimal points to be input into the text fields, whitelist only allowed characters, or max out the text limit to a lower amount.

**Web Application 2**

* Burp results

Graphical user interface, table

Description automatically generated

* Confirmation that it works

Text

Description automatically generated

This exploit happened because users were suspected of using previously leaked passwords from a previous event. To help mitigate this, it would be best to create a better password policy that includes forced password changes and prevents the reuse of passwords.

**Web Application 3**

* Proof that the exploit worked using Pretty Theft

Graphical user interface, application

Description automatically generated

This exploit happens because users can manipulate html code while still being able to submit to the server. One of the best ways to mitigate this is to have client-side validation while also verifying it on the server-side. Another way to mitigate it is to have certain combinations of characters or words that are automatically removed from the input fields.