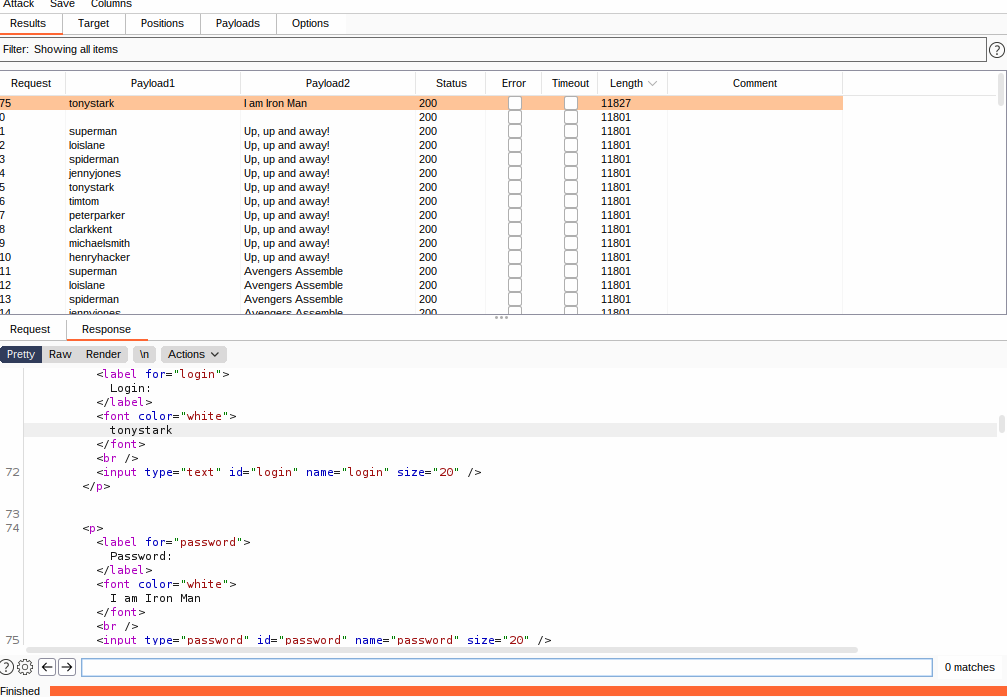
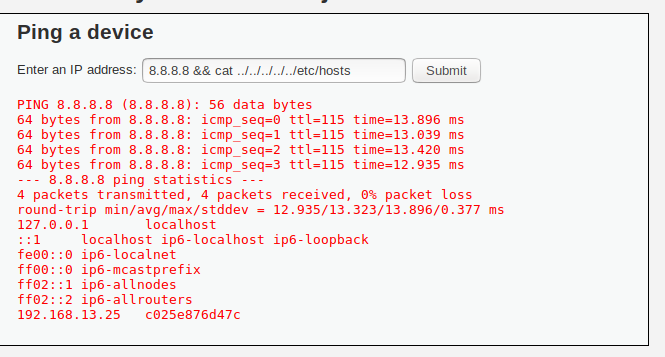
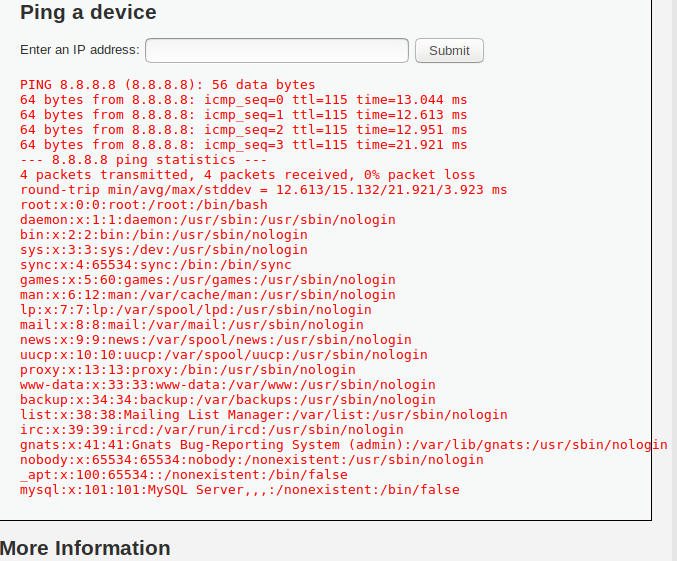
1. Brute Force Attack



The best way to mitigate a brute force attack on a web server is to put a minimum character length on password and usernames. The other way to make it a bit harder for an attacker to perform a brute force attack is to make the password have a special character requirement as well.

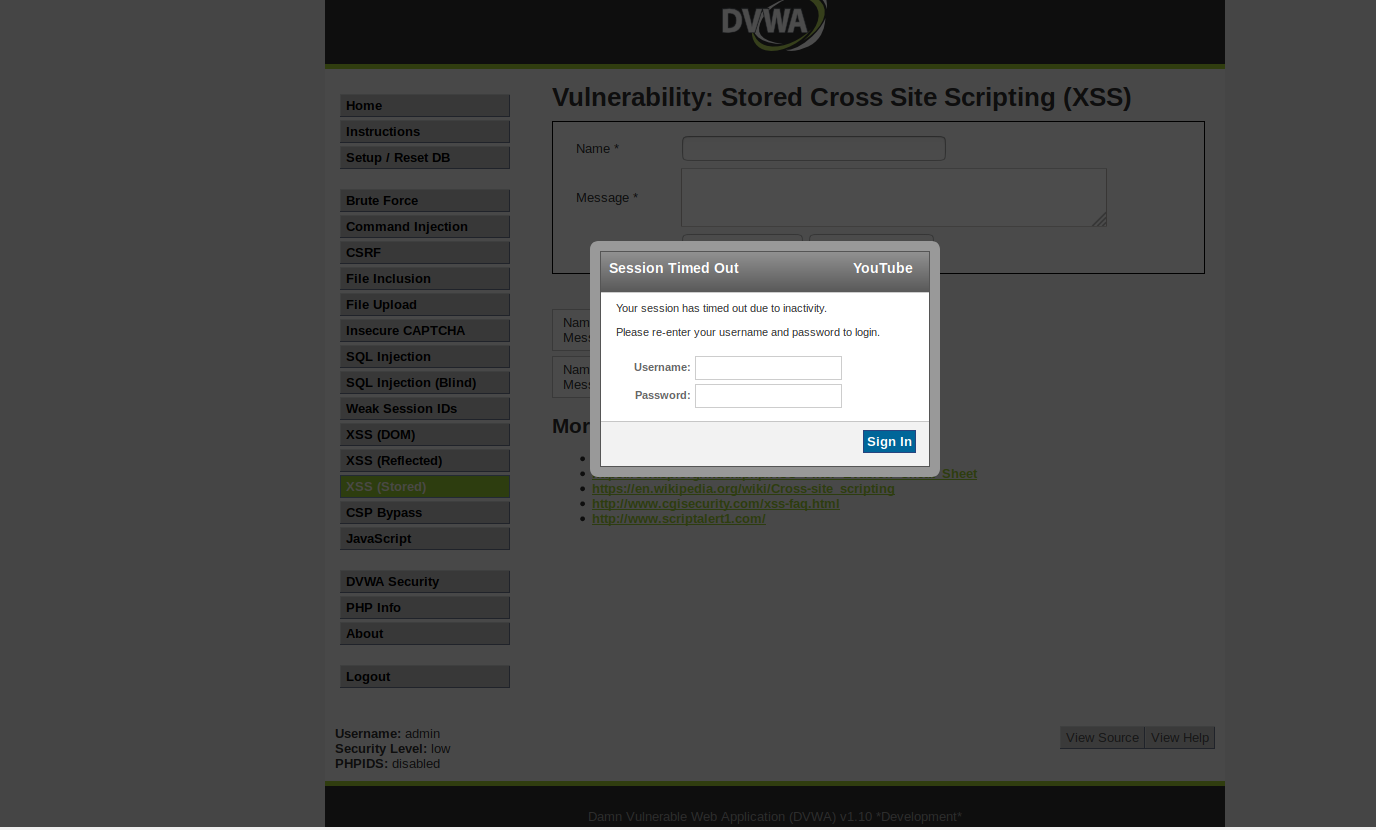
2. Code Inection





1.The best way to make sure that the website is not vulnerable to code injection is to make sure that there is a character limitation to what is able to be entered into the box. Another good way to mitigate this is to make sure that you put a system in place to make sure that the only command able to be run from the data entry field is the one set as the original parameter.

3. XSS



1. The best way to mitigate the risks of XSS is to make sure that the webserver only communicates in HTTPS. Another good way to mitigate XSS is to make sure there is nothing that states script when being sent.