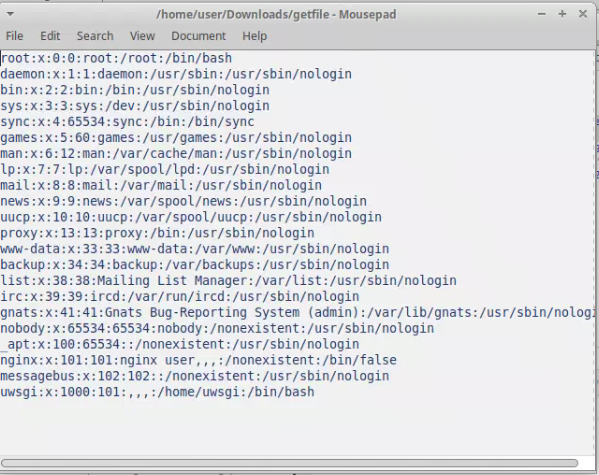
Assignment 8: Injection Attacks

[40 points]Complete all of the following challenges. For each, provide a brief explanation of what you did and screenshot of the result.

Part 1: Path Traversal [10 points]

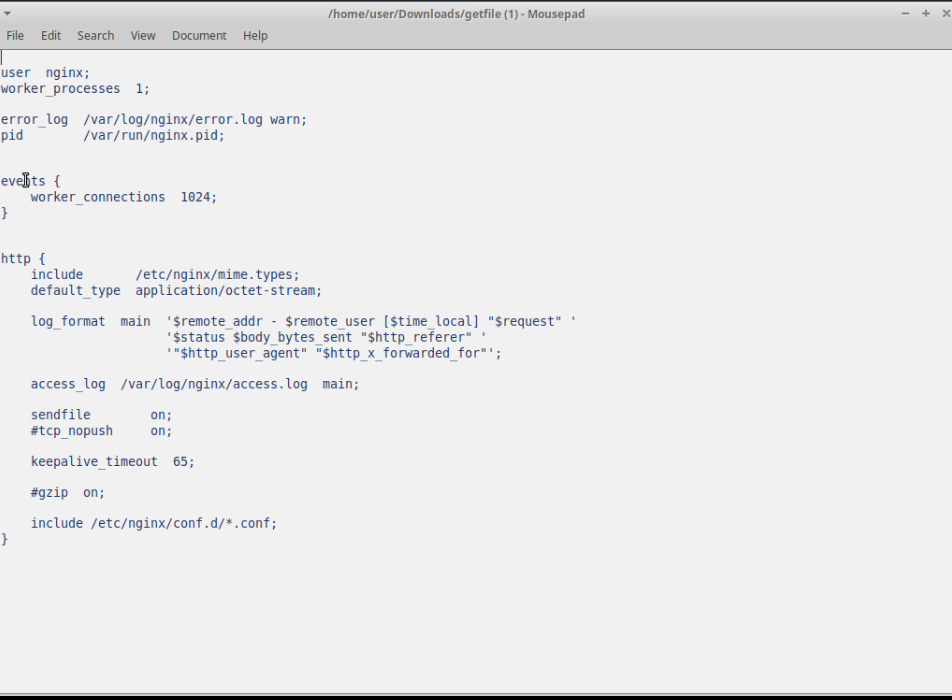
There is an application providing lecture notes at http://server.cs491:5000/. Exploit the application to download the /etc/passwd file.

I changed the file key value in the url to ../../../../../../../etc/passwed

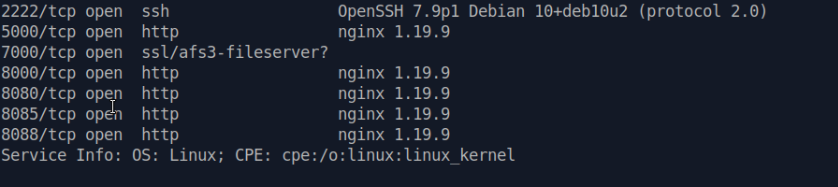


Extra Credit [2 points]: download the webserver configuration file (it will be in the /etc directory).

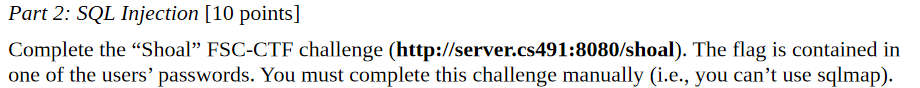
I changed the file key value in the url to ../../../../../../../etc/nginx/nginx.conf



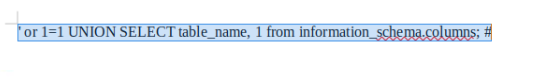
I found the type of the server through nmap:



Through a Google search, I found that nginx config files are stored in /etc/nginx/nginx.conf



Initially, I did a Union SELECT to get the table names:



There was a table called fish.

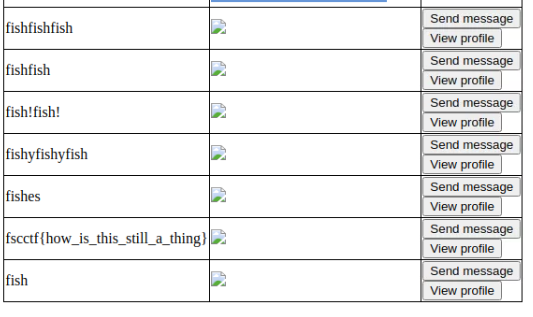
I did another UNION SELECT to get the column names:

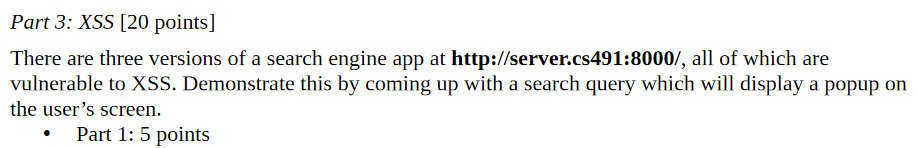


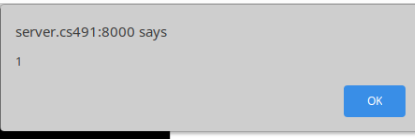
I found a column name for password.

I did a union select to select all the passwords from fish:



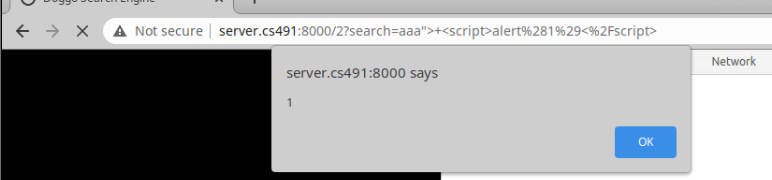






User Input : 





The same input works: 

Part 3: 10 points

