Practice Website

Vulnerability Report

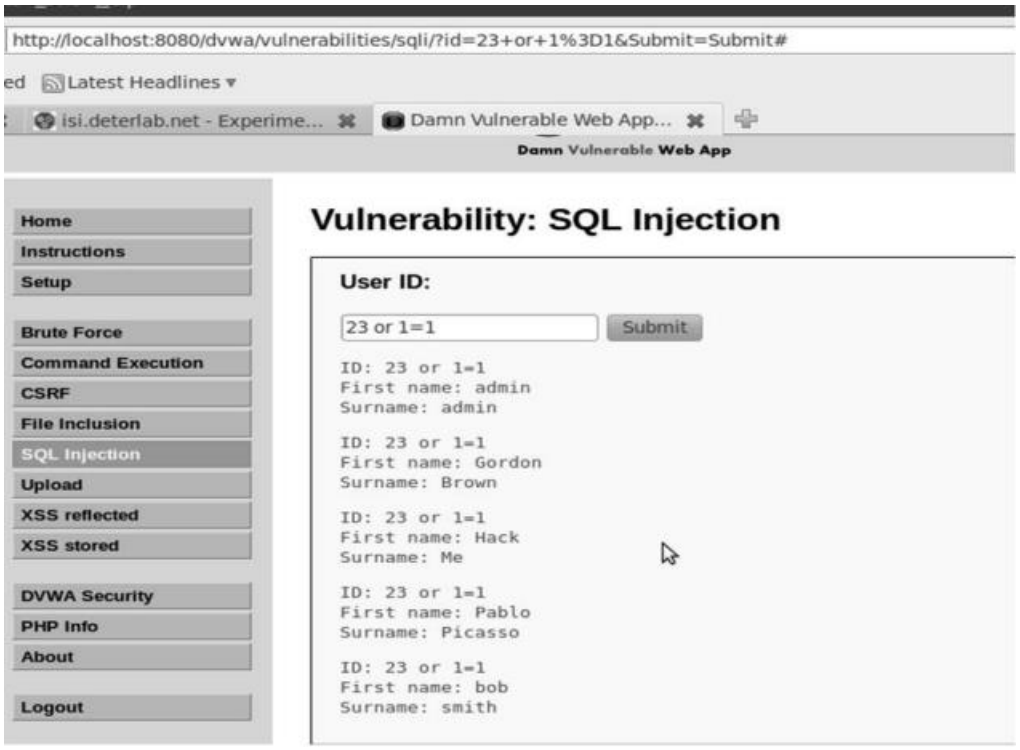
Team: 9.1

Date: 22/10/23

List of Vulnerabilities:

SQL Injection:

We attack the SQL Injection page by inserting the command 23 or 1=1 into the submission field. This give us all users and passwords in the data base, since the field is left vulnerable on the page. After we log the keystrokes using Lynx we make a script and repeat the process 30 more times and have Shark record the traffic. This last step is followed for all three vulnerabilities.

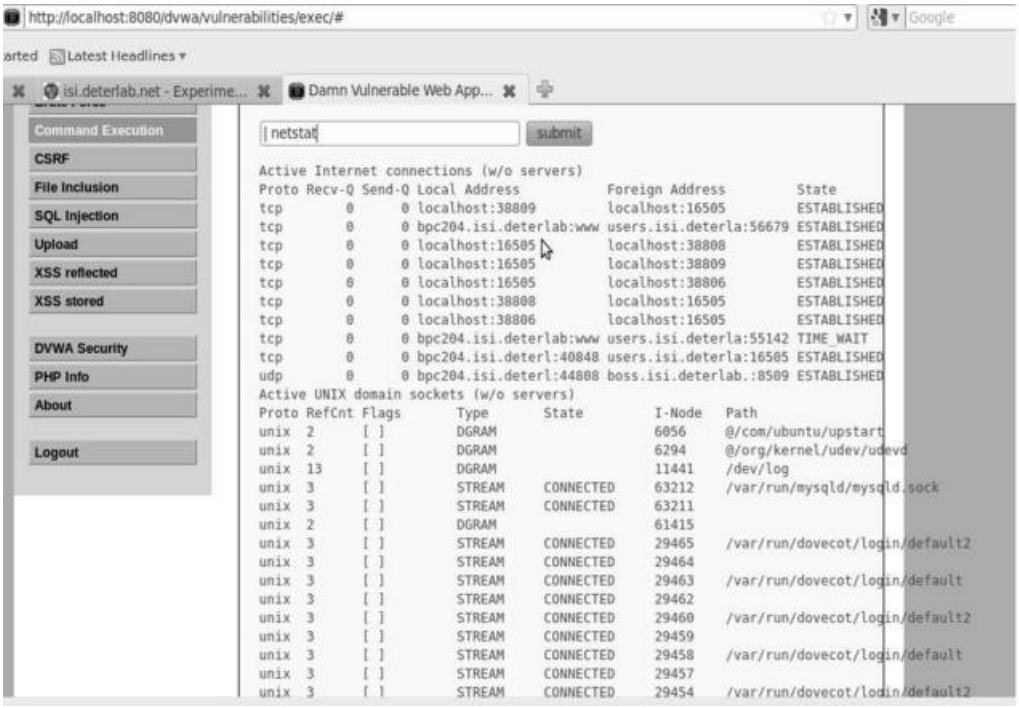


SQL Injection

Command Execution:

We look at the source file for Command Execution and see that this page has been made secure against the command and the &&; however,

pipelining is still available. We insert — netstat into the submission page hit enter and discover this vulnerability is exploitable and we can use Linux commands through this submission file.



Command Execution

File Inclusion:

We attack the File Inclusion page by inserting the tag "../../../../../../../../etc/passwd" at the end of the URL. Because of the insecurity of the php on this page, we are able to view the passwd file stored on LAMP.

File Inclusion

Thank You!