Stage 2

Overview of Nessus Tool:

Nessus is a remote security scanning tool developed by Tenable, Inc. It is one of the most popular vulnerability scanners in the world, used by organizations of all sizes to identify and remediate security vulnerabilities in their networks.

Nessus checks operating systems, software applications, and network devices for vulnerabilities. It may be configured to scan both internal and external networks and to look for specific vulnerabilities or classes of vulnerabilities.

When Nessus discovers a vulnerability, it creates a report with details about the issue, such as its severity, exploitability, and how to fix it. Nessus reports may be utilized to prioritize vulnerability mitigation activities and track progress over time.

Nessus is a great tool for increasing network security in enterprises. It can assist companies in identifying and correcting vulnerabilities before they are exploited by attackers.

Benefits of using Nessus:

- It can scan for a wide range of vulnerabilities. Nessus includes a library of over 100,000 vulnerability checks, covering a wide range of operating systems, software applications, and network devices.
- It is easy to use and customize. Nessus has a user-friendly interface, and it can be customized to scan for specific vulnerabilities or types of vulnerabilities.
- It is scalable. Nessus can be used to scan networks of all sizes, from small businesses to large enterprises.

- It is updated regularly. Tenable regularly updates Nessus with new vulnerability checks and security patches.
- If you are looking for a way to improve the security of your organization's network, Nessus is a great option to consider.

Target websites:

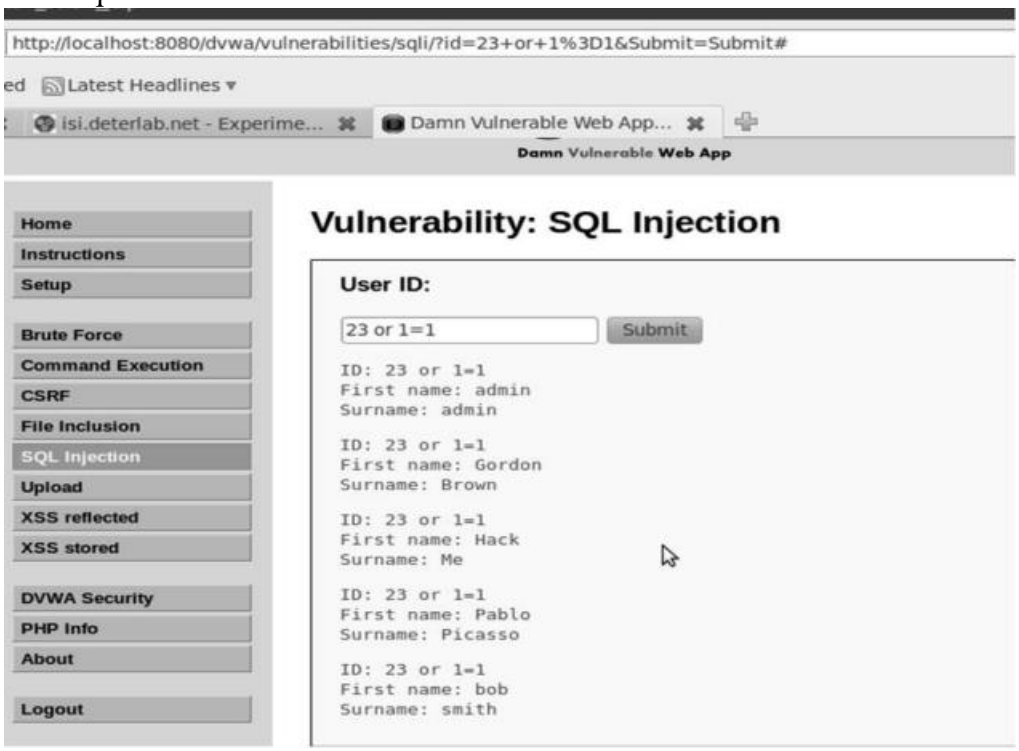
Practice Website – https://www.isi.deterlab.net/index.php3

Main website – https://anix.to/

List of Vulnerabilities:

SQL Injection:

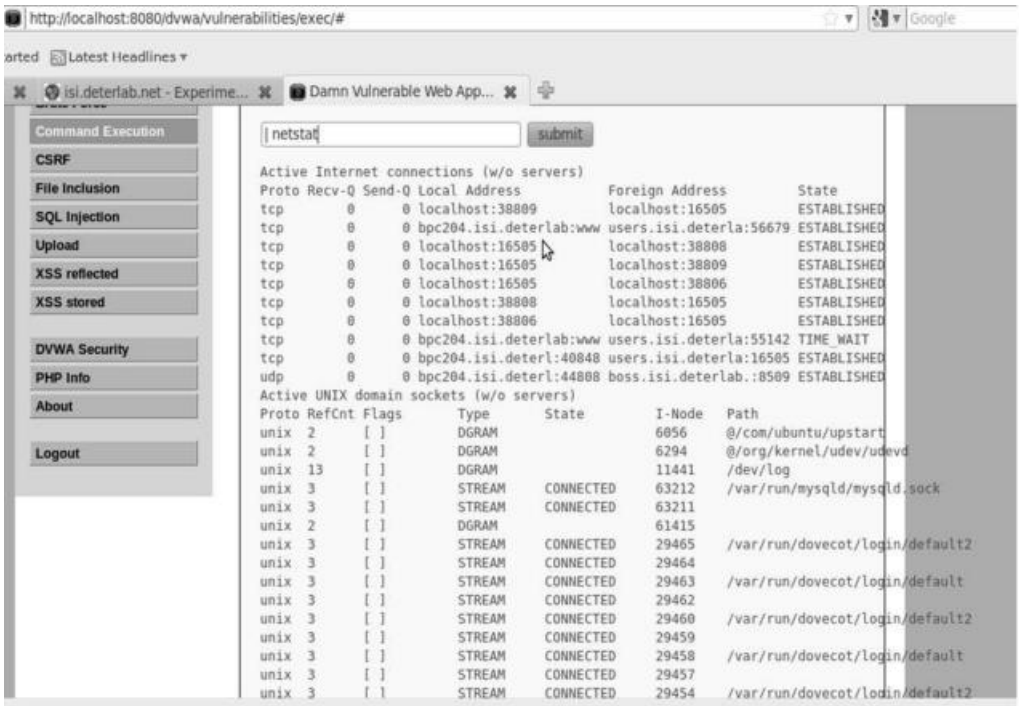
We attack the SQL Injection page by inserting the command 23 or 1=1 into the submission field. This give us all users and passwords in the data base, since the field is left vulnerable on the page. After we log the keystrokes using Lynx we make a script and repeat the process 30 more times and have Shark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