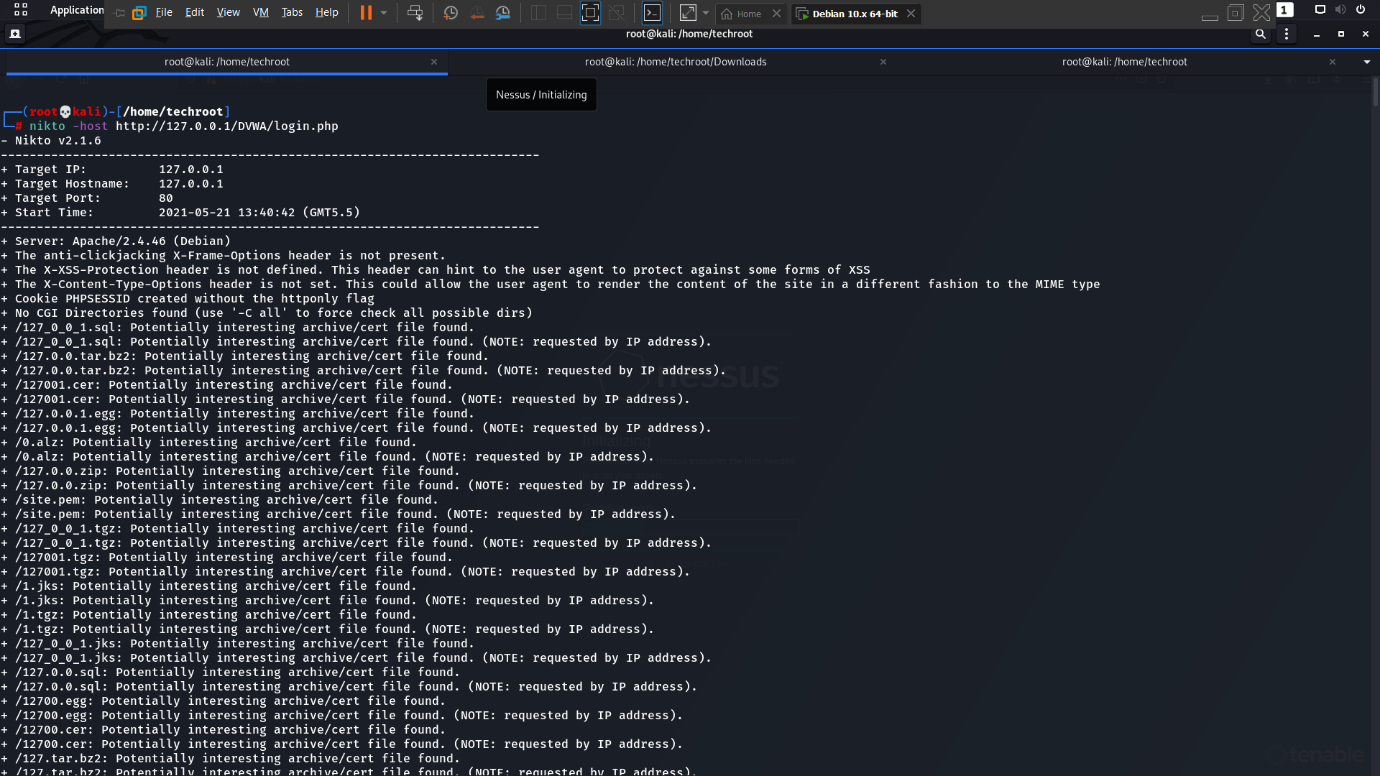
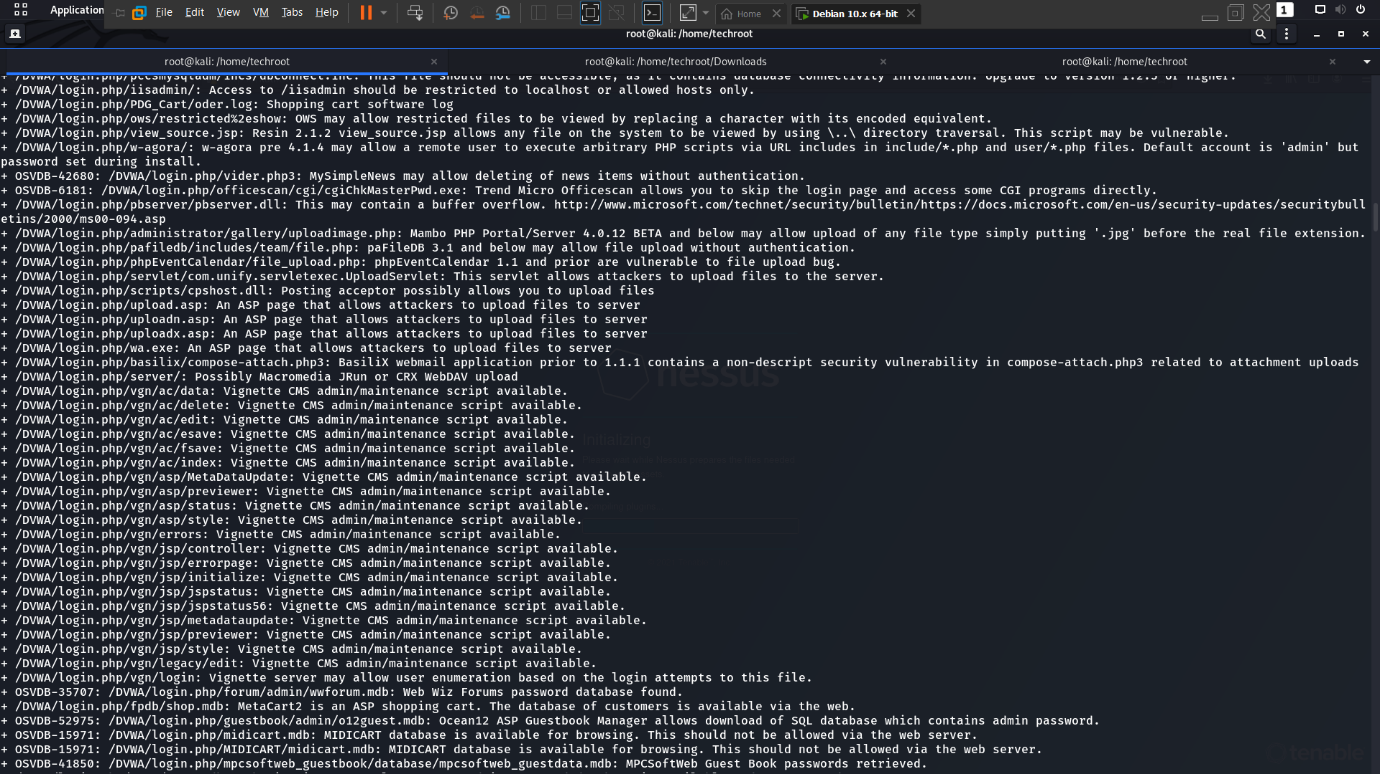
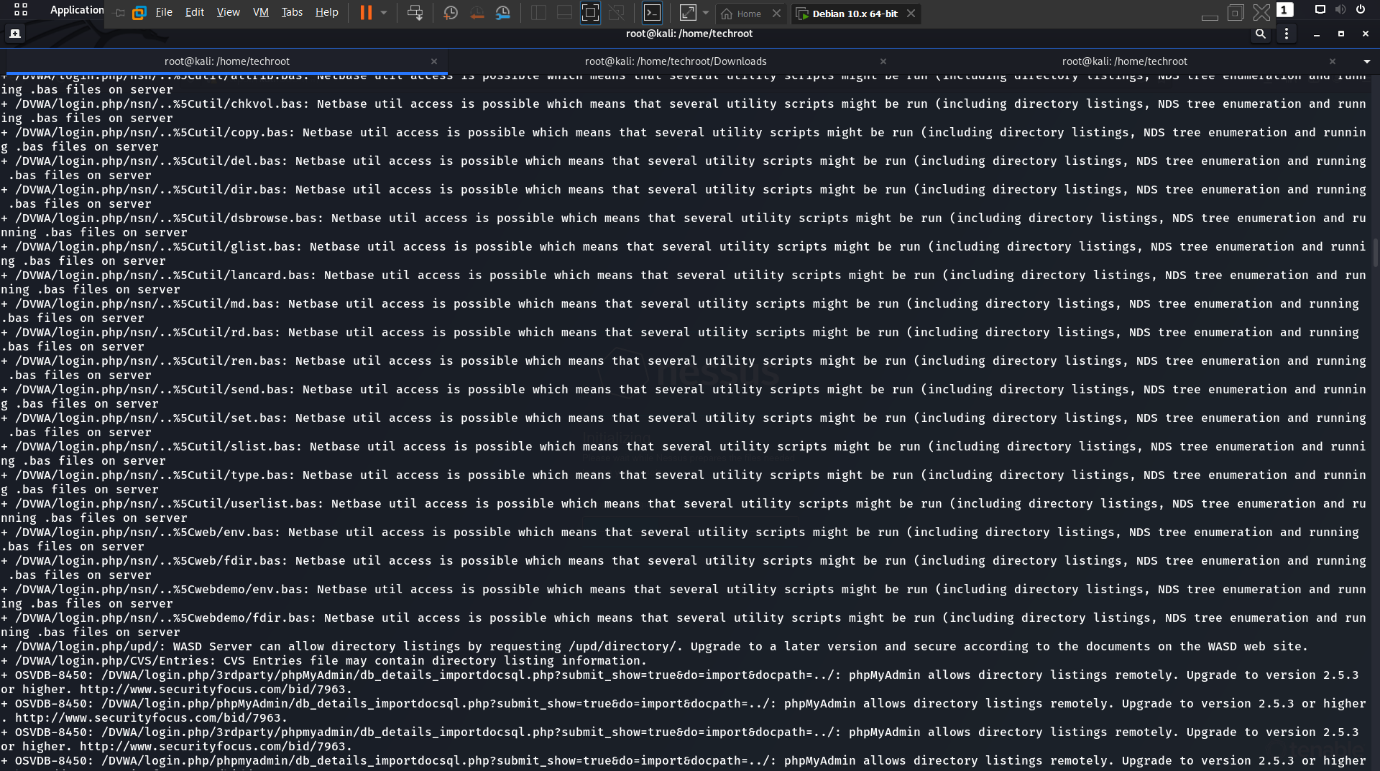
* **VULNERABILITY ASSESSMENT:**
* **Nikto Scan** - #nikto -host <http://127.0.0.1/DVWA/login.php>

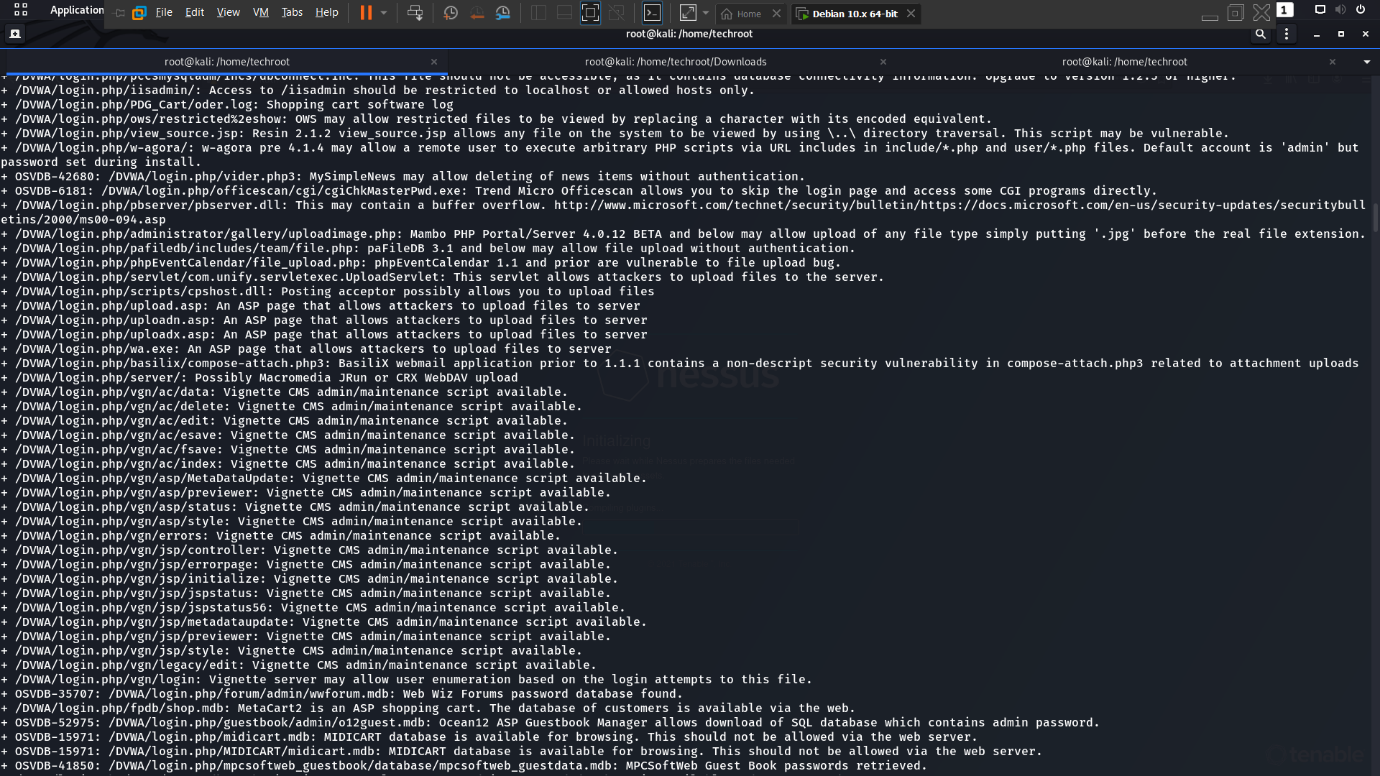
Found much vulnerability during this scan which includes:

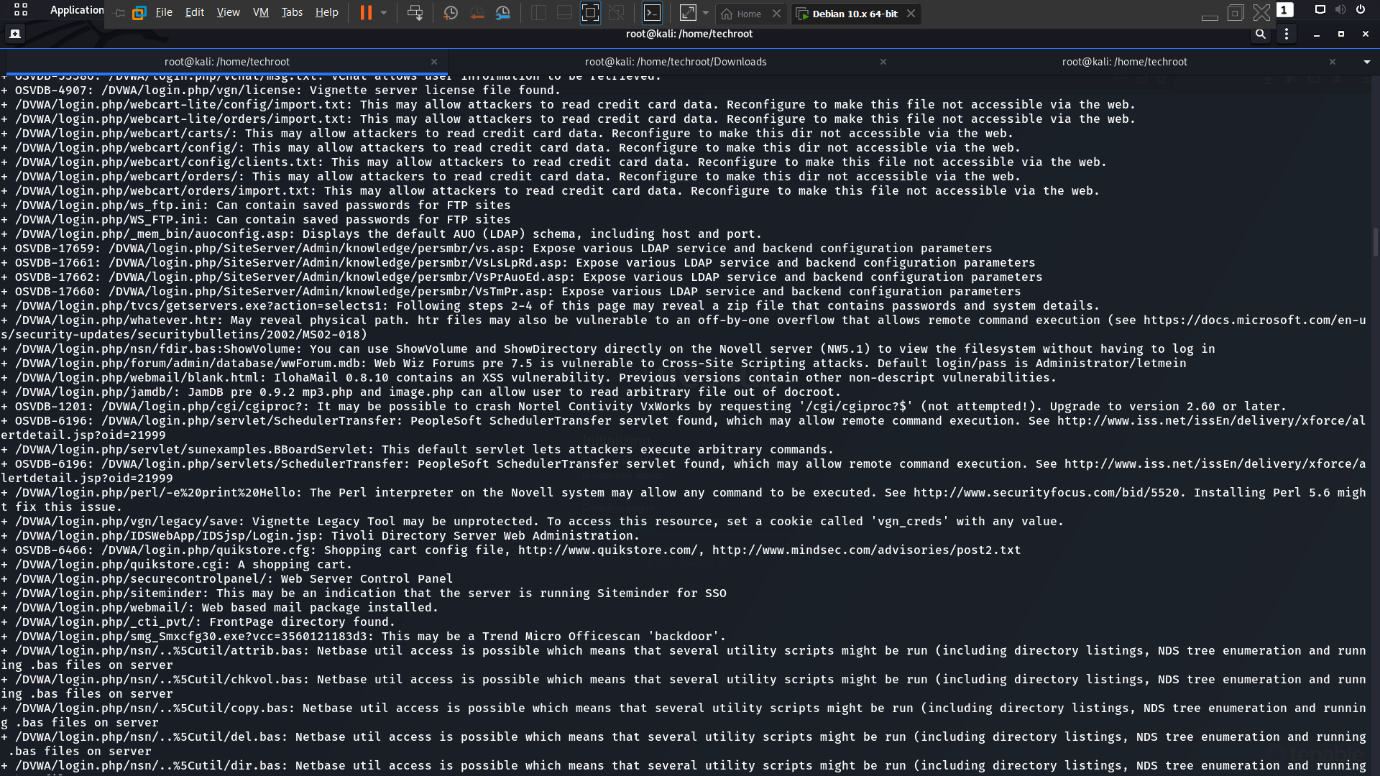
* Different URLs if pen tested can give access to DB id and passwords, hashes, scripts, viewing any file using directory traversing, uploading any file allowing reverse shell, skipping login page and accessing GUI pages directly, passwords of FTP files, reading Credit card data, command execution, expose backend configuration patterns, and many other…

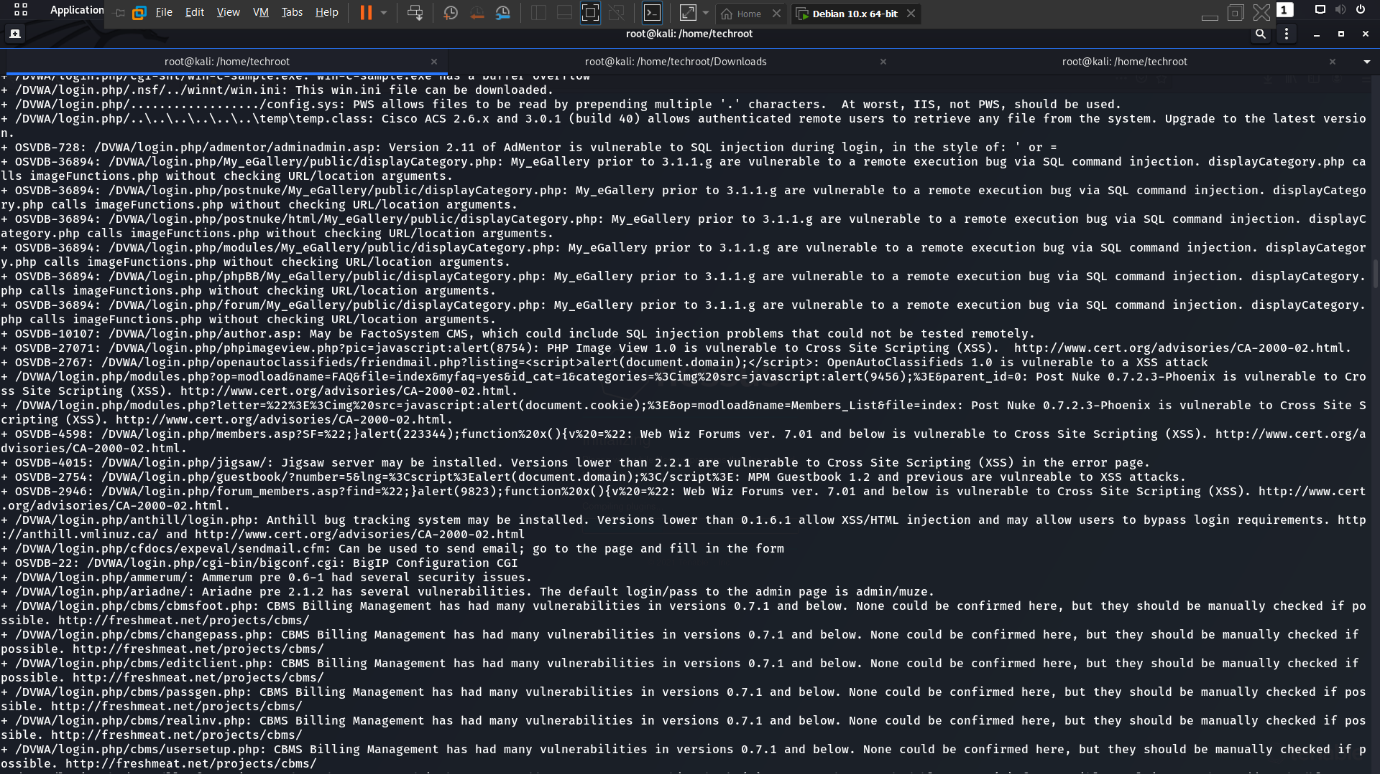


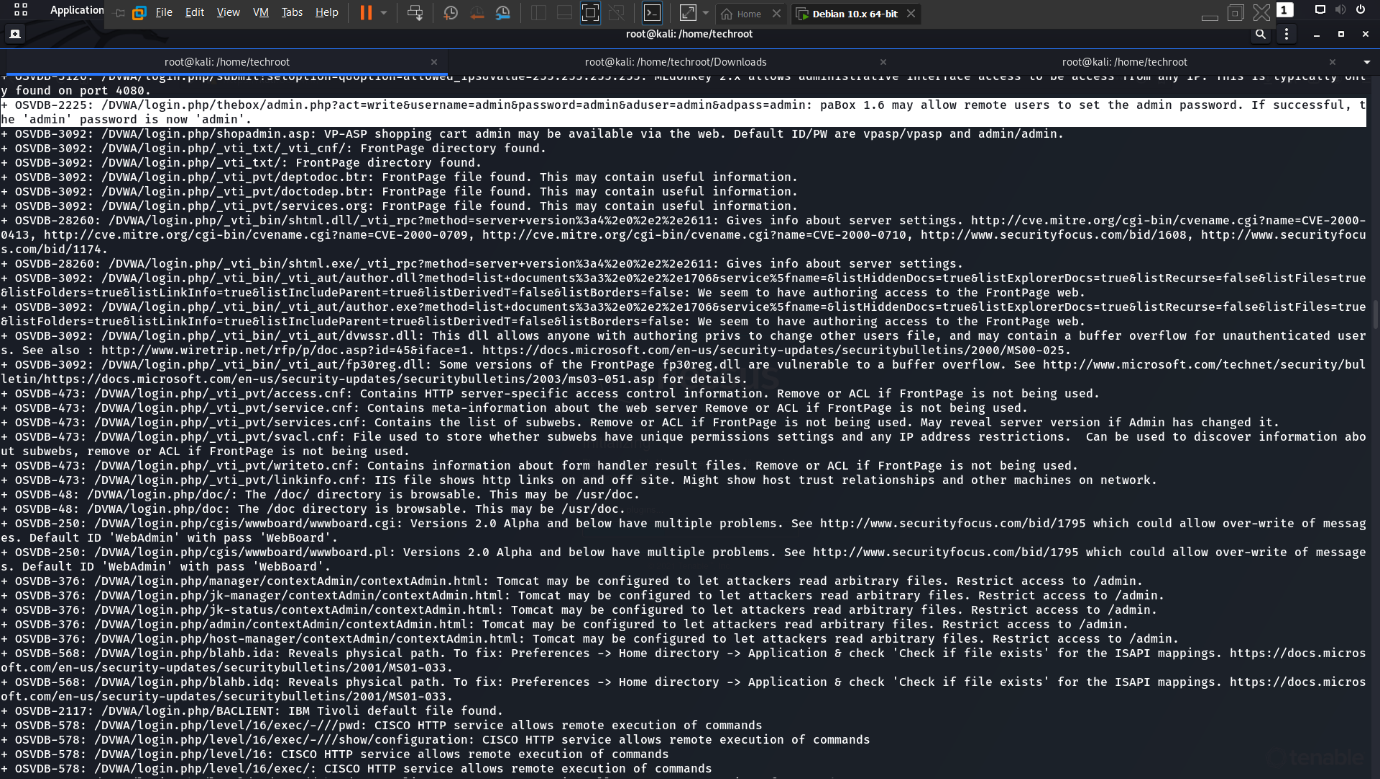


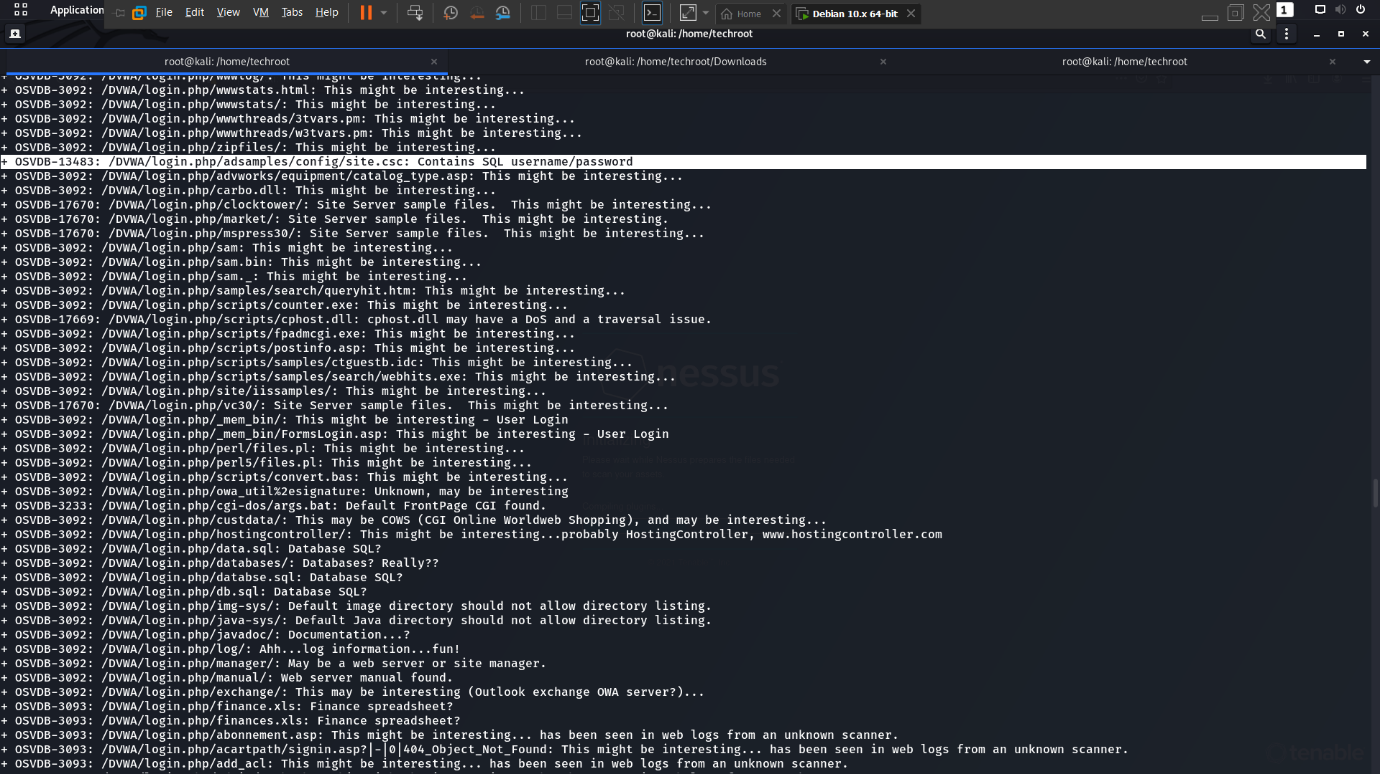


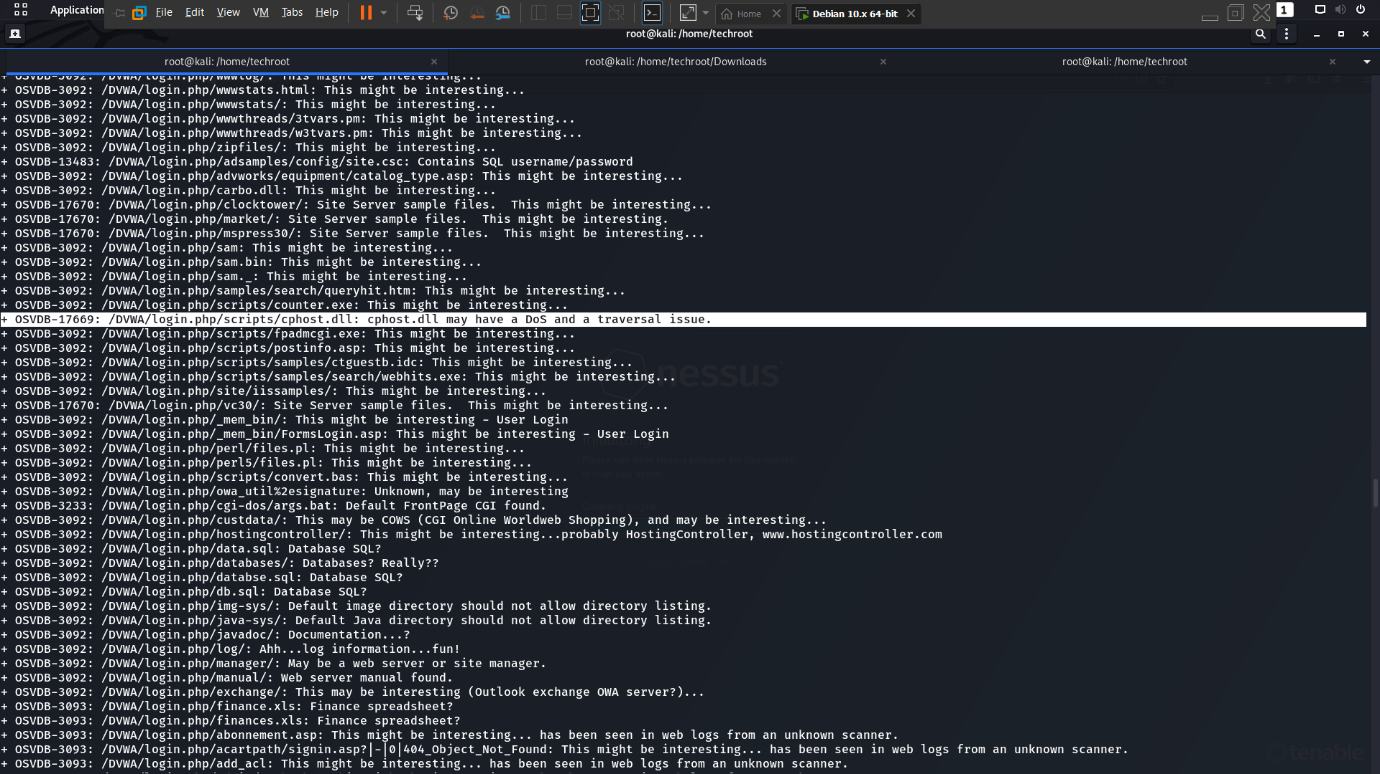






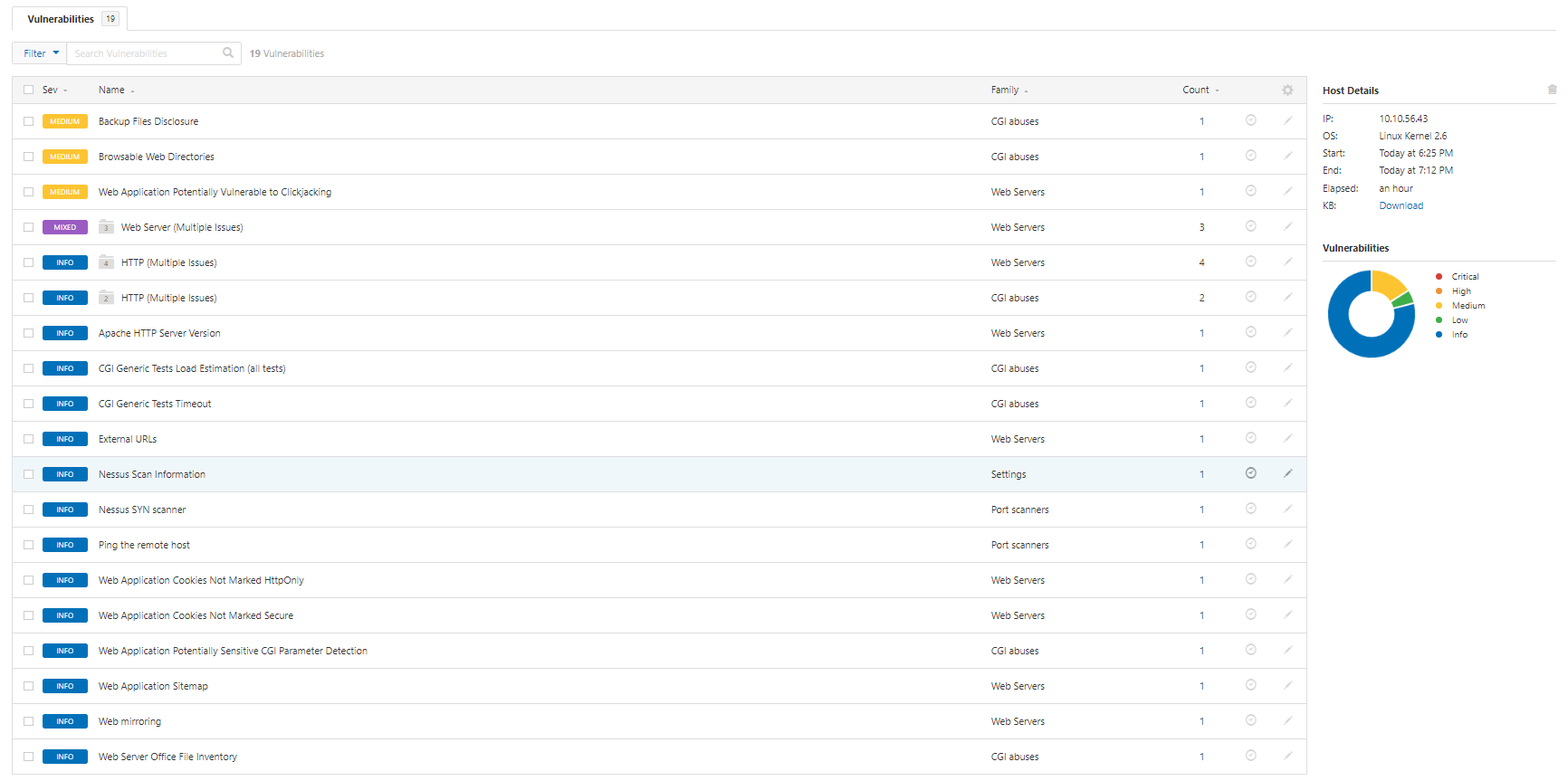






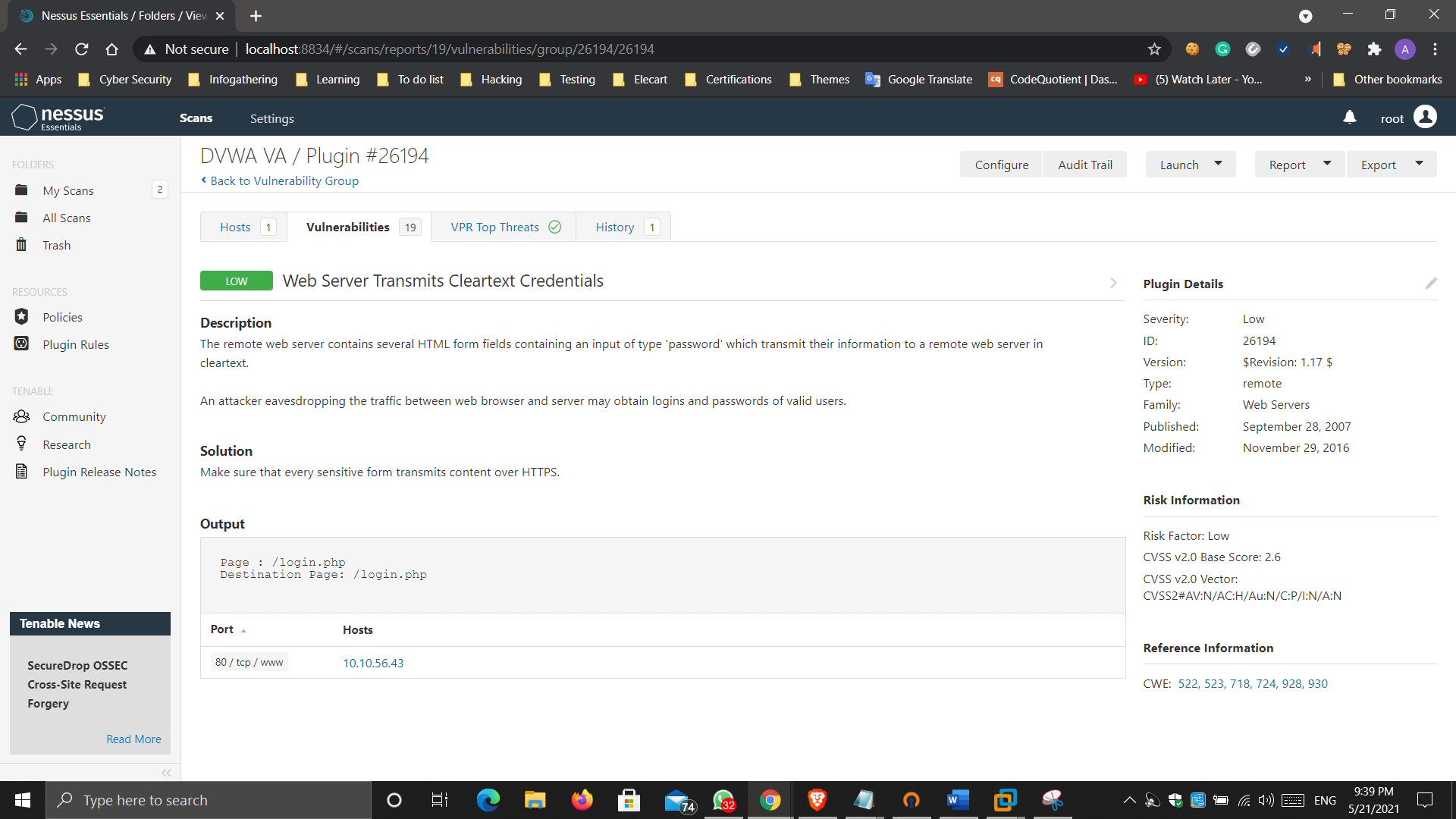
* **NESSUS**

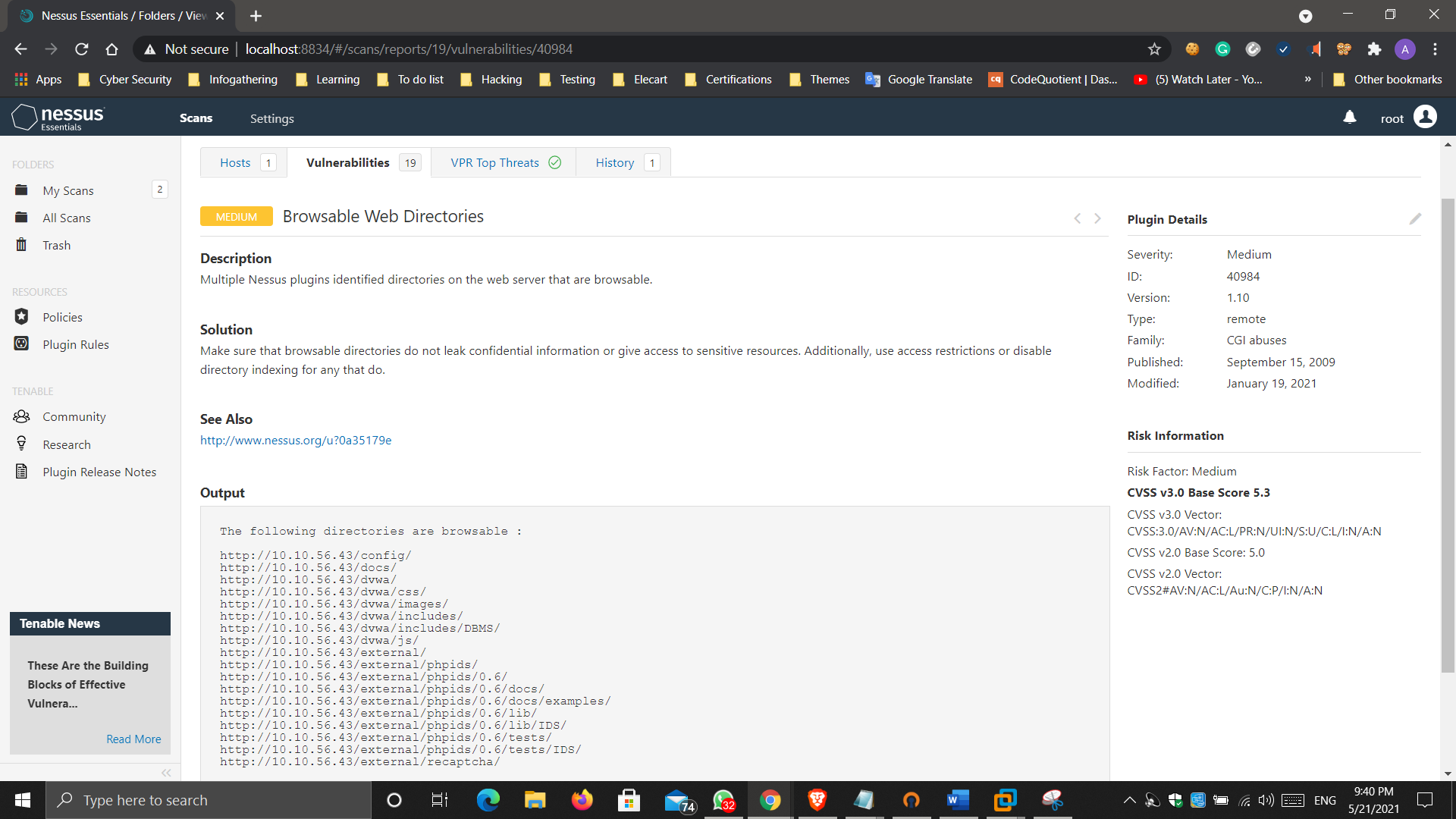
Found 19 vulnerabilities with a count – 3(medium), 1(low), 21(information)



For example, in this low level, it explains us that credentials are transmitted as cleartext by web server and can be exploited in the particular page and a solution to that problem.

Along with this, it also provides us with Risk Information (Bottom-Right of page) in reference to CWE

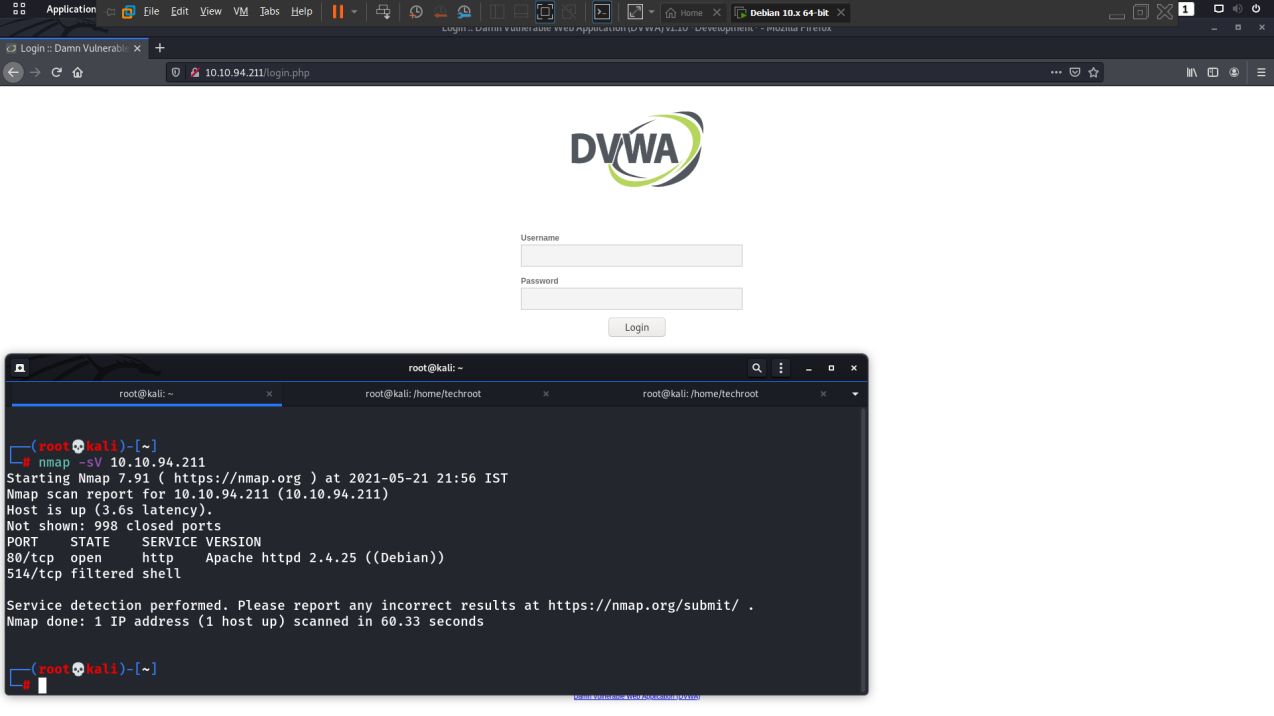




* **NMAP**

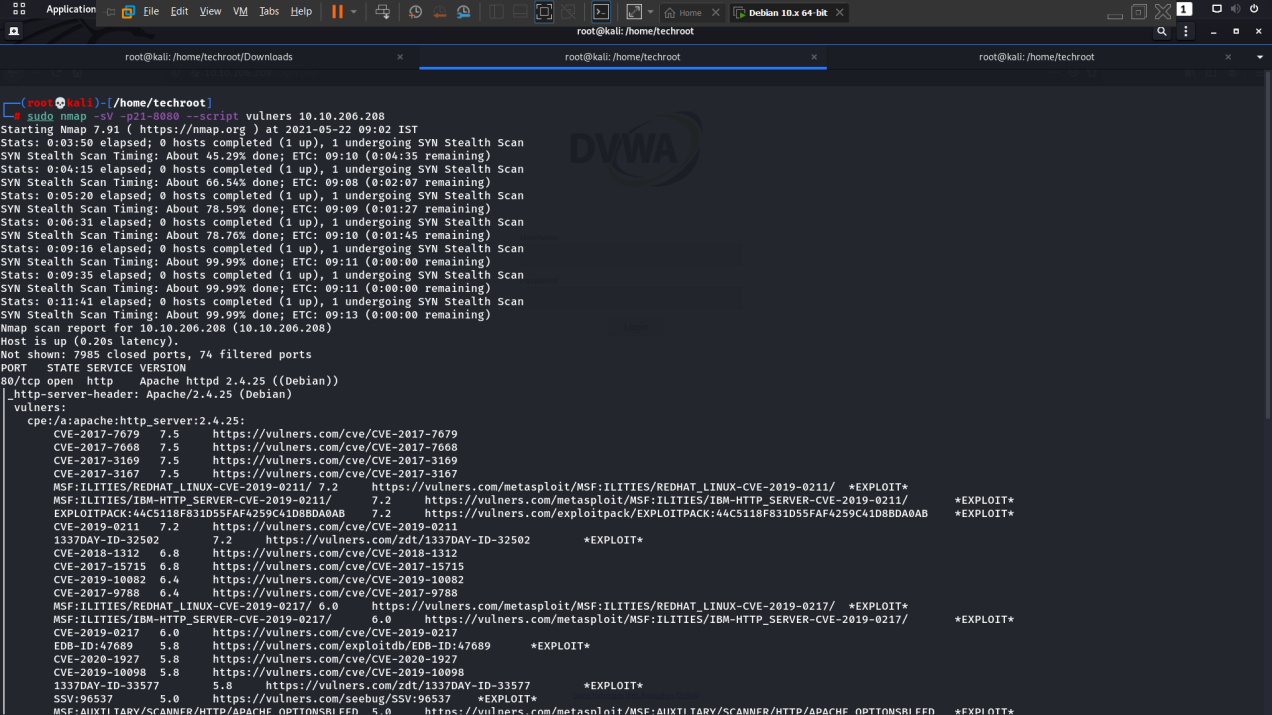
Discovered 80/tcp port open – http(service) - Apache httpd

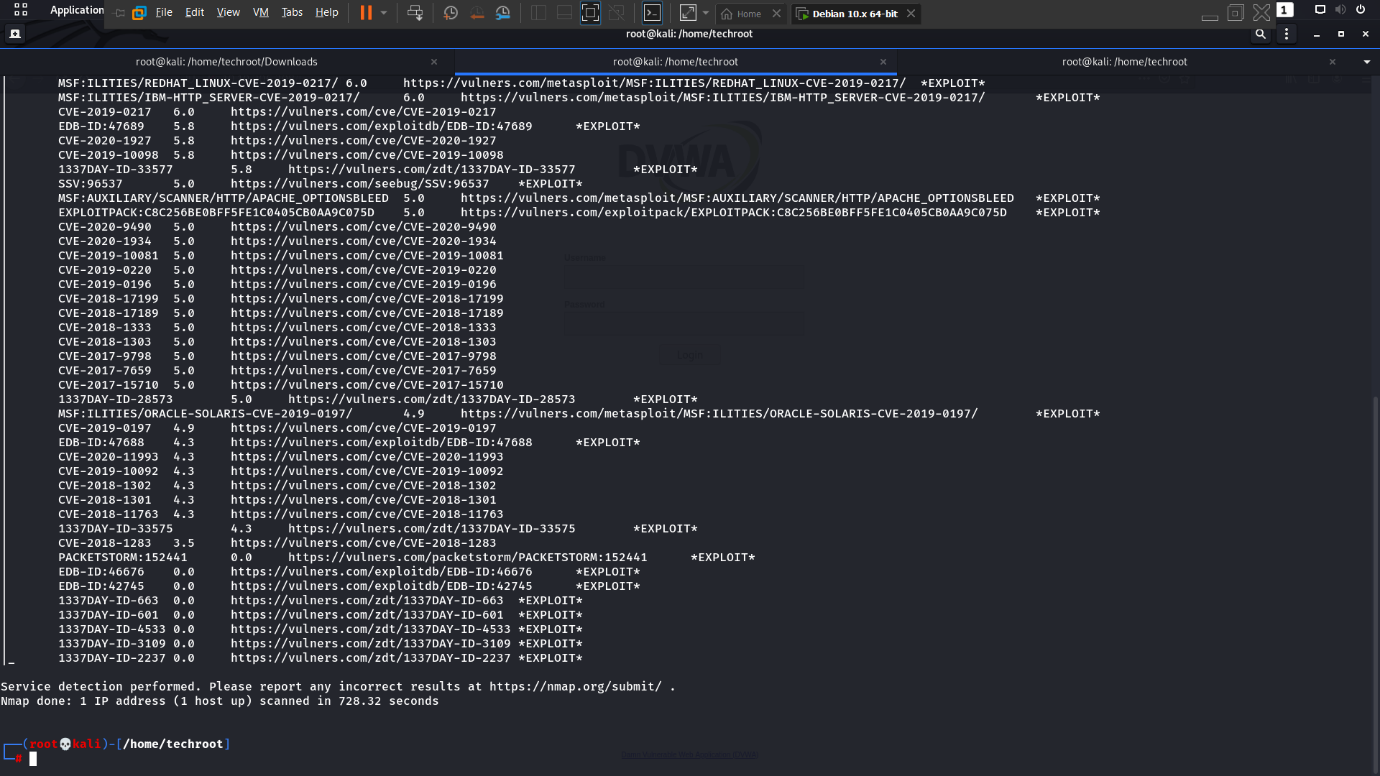
514/tcp port filtered – shell(service)



#sudo nmap -sV -n21-8080 –script vulners 10.10.206.208

Stealth scan gave the full report of vulnerabilities on port 80/tcp (open) – http(service) along with reference of CVE id





Which if explored, provide us with the description of vulnerability.

