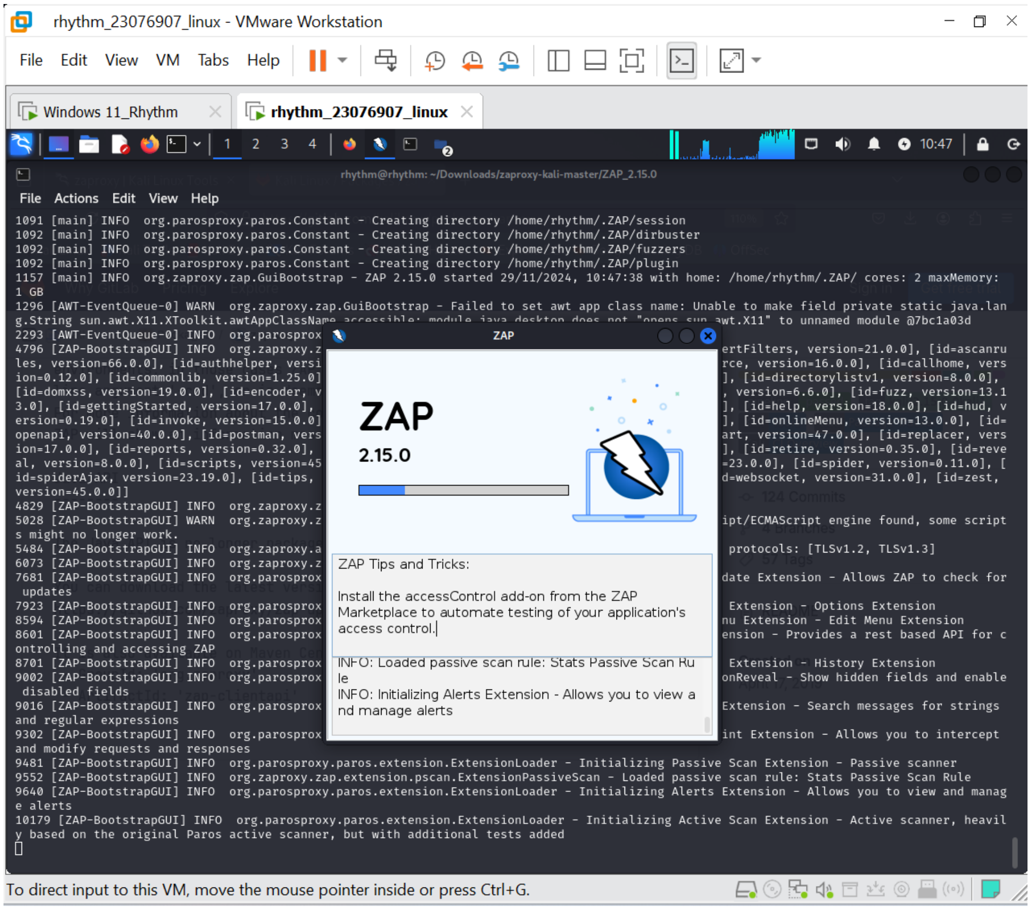
Activity 1: Using the ZAP Proxy

In this exercise, you will install the ZAP interception proxy on your system and use it to intercept and modify a request before it is sent to a website.

1. Visit the OWASP ZAP project homepage at https://owasp.org/www-project-developer-guide/draft/verification/tools/zed_attack_proxy/
2. Download and install the version of ZAP appropriate for your operating system.

   Installing ZAP on Kali Linux


rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
Windows 11_Rhythm
rhythm_23076907_linux
1 2 3 4
10:47
rhythm@rhythm: ~/Downloads/zaproxy-kali-master/ZAP_2.15.0
File Actions Edit View Help
ZAP
ZAP
2.15.0

```
1091 [main] INFO  org.parosproxy.paros.Constant - Creating directory /home/rhythm/.ZAP/session
1092 [main] INFO  org.parosproxy.paros.Constant - Creating directory /home/rhythm/.ZAP/dirbuster
1092 [main] INFO  org.parosproxy.paros.Constant - Creating directory /home/rhythm/.ZAP/fuzzers
1092 [main] INFO  org.parosproxy.paros.Constant - Creating directory /home/rhythm/.ZAP/plugin
1157 [main] INFO  org.zaproxy.zap.GuiBootstrap - ZAP 2.15.0 started 29/11/2024, 10:47:38 with home: /home/rhythm/.ZAP/ cores: 2 maxMemory:
1 GB
1296 [AWT-EventQueue-0] WARN  org.zaproxy.zap.GuiBootstrap - Failed to set awt app class name: Unable to make field private static java.lan
g.String sun.awt.X11.XToolkit.awtAppClassName accessible: module java.desktop does not "opens sun.awt.X11" to unnamed module @7bc1a03d
2293 [AWT-EventQueue-0] INFO  org.parosprox
4796 [ZAP-BootstrapGUI] INFO  org.zaproxy.z                           ertFilters, version=21.0.0], [id=ascanru
les, version=66.0.0], [id=authhelper, versi                           rce, version=16.0.0], [id=callhome, vers
ion=0.12.0], [id=commonlib, version=1.25.0]                           ], [id=directorylistv1, version=8.0.0],
[id=domxss, version=19.0.0], [id=encoder, v                           , version=6.6.0], [id=fuzz, version=13.1
3.0], [id=gettingStarted, version=17.0.0],                            ], [id=help, version=18.0.0], [id=hud, v
ersion=0.19.0], [id=invoke, version=15.0.0]                           ], [id=onlineMenu, version=13.0.0], [id=
openapi, version=40.0.0], [id=postman, vers                           art, version=47.0.0], [id=replacer, vers
ion=17.0.0], [id=reports, version=0.32.0],                            ], [id=retire, version=0.35.0], [id=reve
al, version=8.0.0], [id=scripts, version=45                           =23.0.0], [id=spider, version=0.11.0], [
id=spiderAjax, version=23.19.0], [id=tips,                            d=websocket, version=31.0.0], [id=zest,
version=45.0.0]]
4829 [ZAP-BootstrapGUI] INFO  org.zaproxy.z
5028 [ZAP-BootstrapGUI] WARN  org.zaproxy.z                           ipt/ECMAScript engine found, some script
s might no longer work.
5484 [ZAP-BootstrapGUI] INFO  org.zaproxy.a                            protocols: [TLSv1.2, TLSv1.3]
6073 [ZAP-BootstrapGUI] INFO  org.zaproxy.z
7681 [ZAP-BootstrapGUI] INFO  org.parosprox                           date Extension - Allows ZAP to check for
 updates
7923 [ZAP-BootstrapGUI] INFO  org.parosprox                            Extension - Options Extension
8594 [ZAP-BootstrapGUI] INFO  org.parosprox                           nu Extension - Edit Menu Extension
8601 [ZAP-BootstrapGUI] INFO  org.parosprox                           ension - Provides a rest based API for c
ontrolling and accessing ZAP
8701 [ZAP-BootstrapGUI] INFO  org.parosprox                            Extension - History Extension
9002 [ZAP-BootstrapGUI] INFO  org.parosprox                           onReveal - Show hidden fields and enable
 disabled fields
9016 [ZAP-BootstrapGUI] INFO  org.parosprox                           Extension - Search messages for strings
and regular expressions
9302 [ZAP-BootstrapGUI] INFO  org.parosprox                           int Extension - Allows you to intercept
and modify requests and responses
9481 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Passive Scan Extension - Passive scanner
9552 [ZAP-BootstrapGUI] INFO  org.zaproxy.zap.extension.pscan.ExtensionPassiveScan - Loaded passive scan rule: Stats Passive Scan Rule
9640 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Alerts Extension - Allows you to view and manag
e alerts
10179 [ZAP-BootstrapGUI] INFO  org.parosproxy.paros.extension.ExtensionLoader - Initializing Active Scan Extension - Active scanner, heavil
y based on the original Paros active scanner, but with additional tests added
```

ZAP Tips and Tricks:

Install the accessControl add-on from the ZAP Marketplace to automate testing of your application's access control.

```
INFO: Loaded passive scan rule: Stats Passive Scan Ru
le
INFO: Initializing Alerts Extension - Allows you to view a
nd manage alerts
```

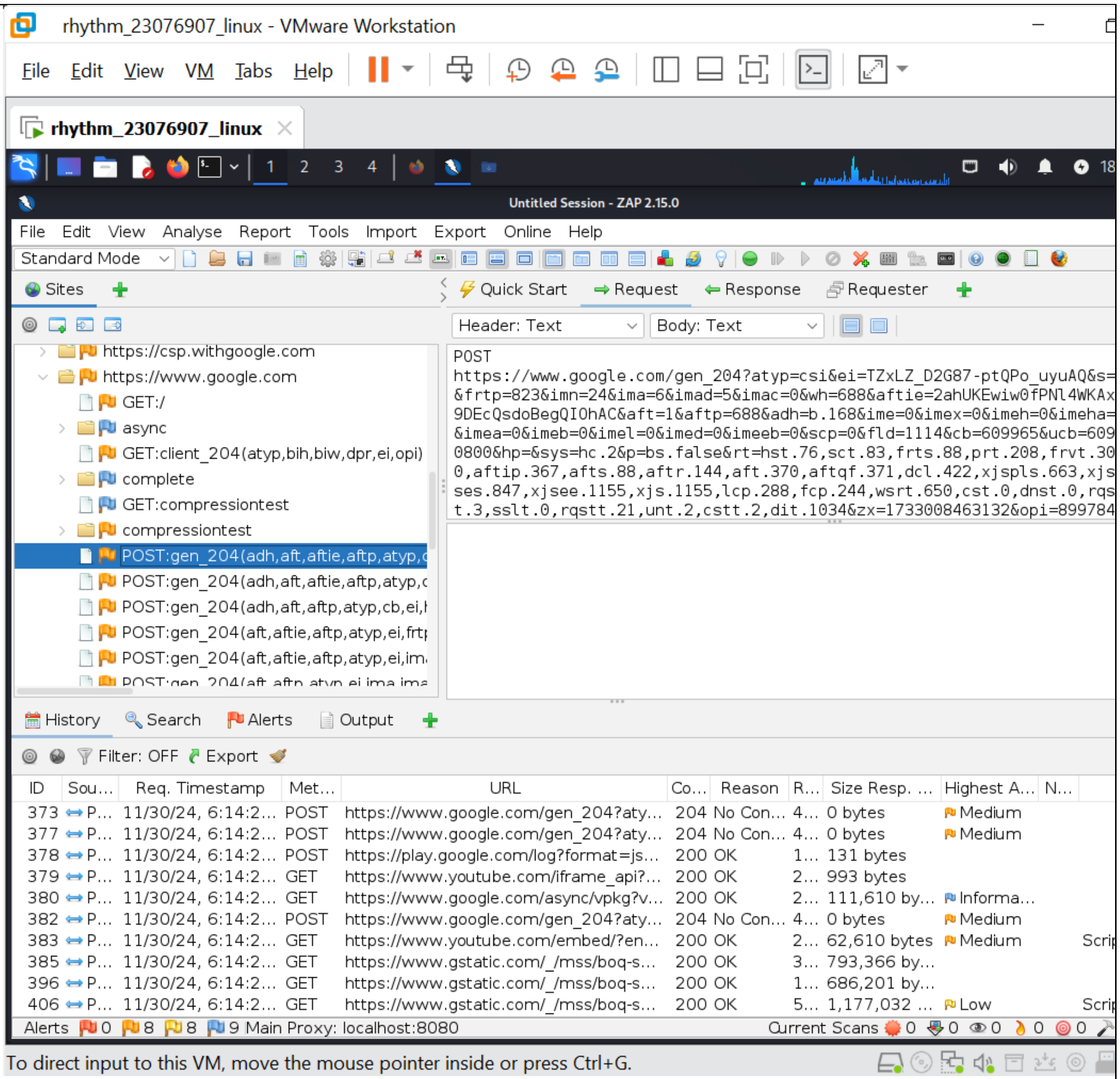
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

3. Review the OWASP ZAP Getting Started Guide at:

   https://www.zaproxy.org/getting-started/
4. You may go through the following PDF document about ZAP.

   PDF

   20200120-OWASPD
   orset-ZAP-DanielW.¡
5. Use ZAP to intercept a request sent from your browser to a search engine. Using ZAP, modify the request to change the search term sent to the remote site. **Take the screen shot.**
6. View the results.



rhythm_23076907_linux - VMware Workstation

Untitled Session - ZAP 2.15.0

Standard Mode

```
https://csp.withgoogle.com
https://www.google.com
    GET:/
    async
    GET:client_204(atyp,bih,biw,dpr,ei,opi)
    complete
    GET:compressiontest
    compressiontest
    POST:gen_204(adh,aft,aftie,aftp,atyp,c
    POST:gen_204(adh,aft,aftie,aftp,atyp,c
    POST:gen_204(adh,aft,aftp,atyp,cb,ei,l
    POST:gen_204(aft,aftie,aftp,atyp,ei,frt
    POST:gen_204(aft,aftie,aftp,atyp,ei,im
    POST:gen_204(aft,aftp,atyp,ei,ima,ima
```

Header: Text

Body: Text

```
POST
https://www.google.com/gen_204?atyp=csi&ei=TZxLZ_D2G87-ptQPo_uyuAQ&s=
&frtp=823&imn=24&ima=6&imad=5&imac=0&wh=688&aftie=2ahUKEwiw0fPNl4WKAx
9DEcQsdoBegQIOhAC&aft=1&aftp=688&adh=b.168&ime=0&imex=0&imeh=0&imeha=
&imea=0&imeb=0&imel=0&imed=0&imeeb=0&scp=0&fld=1114&cb=609965&ucb=609
0800&hp=&sys=hc.2&p=bs.false&rt=hst.76,sct.83,frts.88,prt.208,frvt.30
0,aftip.367,afts.88,aftr.144,aft.370,aftqf.371,dcl.422,xjspls.663,xjs
ses.847,xjsee.1155,xjs.1155,lcp.288,fcp.244,wsrt.650,cst.0,dnst.0,rqs
t.3,sslt.0,rqstt.21,unt.2,cstt.2,dit.1034&zx=1733008463132&opi=899784
```

Filter: OFF Export

ID	Sou...	Req. Timestamp	Met...	URL	Co...	Reason	R...	Size Resp. ...	Highest A...	N...
373	⇔ P...	11/30/24, 6:14:2...	POST	https://www.google.com/gen_204?aty...	204	No Con...	4...	0 bytes	Medium	
377	⇔ P...	11/30/24, 6:14:2...	POST	https://www.google.com/gen_204?aty...	204	No Con...	4...	0 bytes	Medium	
378	⇔ P...	11/30/24, 6:14:2...	POST	https://play.google.com/log?format=js...	200	OK	1...	131 bytes		
379	⇔ P...	11/30/24, 6:14:2...	GET	https://www.youtube.com/iframe_api?...	200	OK	2...	993 bytes		
380	⇔ P...	11/30/24, 6:14:2...	GET	https://www.google.com/async/vpkg?v...	200	OK	2...	111,610 by...	Informa...	
382	⇔ P...	11/30/24, 6:14:2...	POST	https://www.google.com/gen_204?aty...	204	No Con...	4...	0 bytes	Medium	
383	⇔ P...	11/30/24, 6:14:2...	GET	https://www.youtube.com/embed/?en...	200	OK	2...	62,610 bytes	Medium	Scri
385	⇔ P...	11/30/24, 6:14:2...	GET	https://www.gstatic.com/_/mss/boq-s...	200	OK	3...	793,366 by...		
396	⇔ P...	11/30/24, 6:14:2...	GET	https://www.gstatic.com/_/mss/boq-s...	200	OK	1...	686,201 by...		
406	⇔ P...	11/30/24, 6:14:2...	GET	https://www.gstatic.com/_/mss/boq-s...	200	OK	5...	1,177,032 ...	Low	Scri

Alerts 0 8 8 9 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

File Edit View VM Tabs Help
rhythm_23076907_linux
1 2 3 4
File Edit View Analyse Report Tools Import Export Online Help
Sites
Quick Start Request Response Requester
History Search Alerts Output

Q1: Did your browser display the results for the term that you typed into the browser, or did it display the results for the search term that you changed using ZAP?

Ans: Yes I have searched various website and all link has shown to my zaps

Activity 2: Creating a Cross-Site Scripting Vulnerability

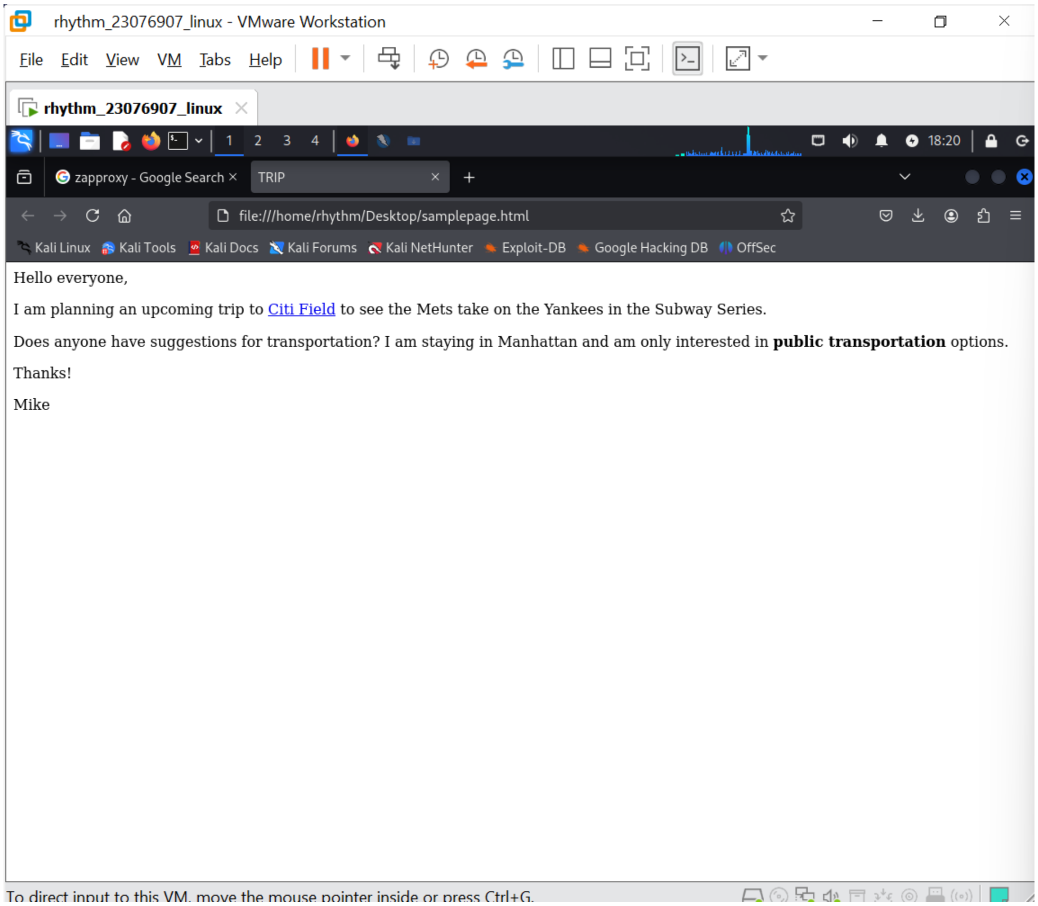
In this activity, you will create a cross-site scripting vulnerability using an HTML page saved on your local computer.sam

1. Using a text editor of your choice, create an HTML file containing some simple content of your choice. For example, you might want to model your code after the following sample page:

<p>Hello everyone,</p>
<p>I am planning an upcoming trip to <A HREF= 'https://www.mlb.com/mets/ballpark'>Citi Field</A> to see the Mets take on the Yankees in the Subway Series.</p>
<p>Does anyone have suggestions for transportation? I am staying in Manhattan and am only interested in <B>public transportation</B> options.</p>

```
<p>Thanks!</p>
<p>Mike</p>
```

2. Open the file stored on your local computer and view it using your favorite browser.



rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
rhythm_23076907_linux
1 2 3 4
18:20
zapproxy - Google Search
TRIP
file:///home/rhythm/Desktop/samplepage.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Hello everyone,

I am planning an upcoming trip to Citi Field to see the Mets take on the Yankees in the Subway Series.

Does anyone have suggestions for transportation? I am staying in Manhattan and am only interested in **public transportation** options.

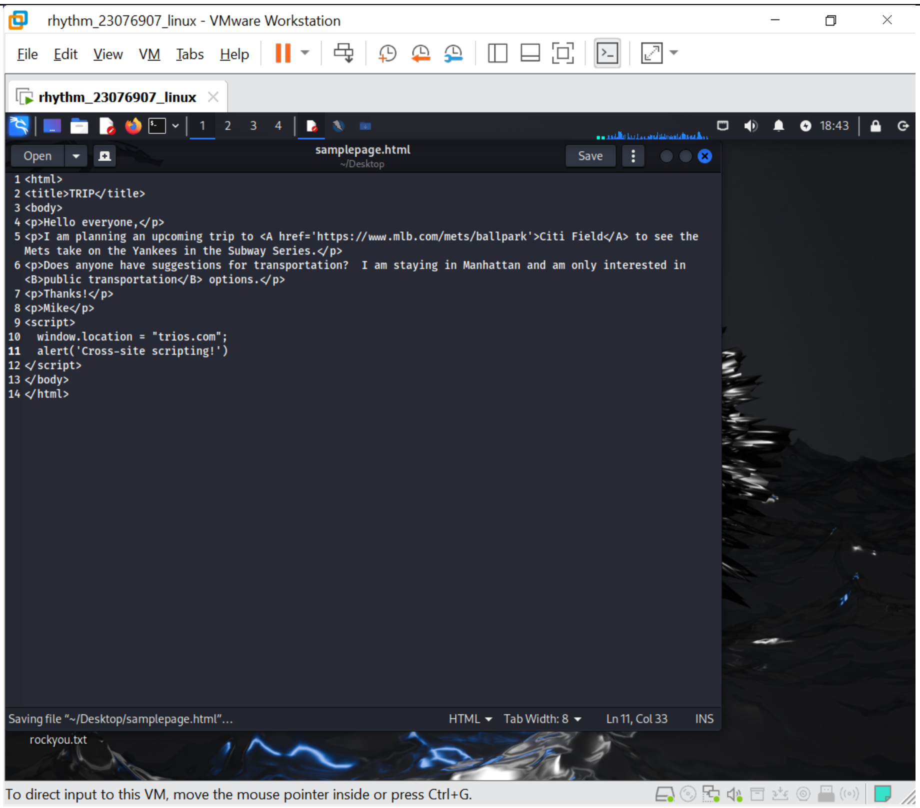
Thanks!

Mike

3. In your text editor, modify the file that you created in step 1 to include a cross-site scripting attack. You may wish to refer to the example in the section “Cross-Site Scripting (XSS)” did earlier, if you need assistance.

```
<p>Hello everyone,</p>
<p>I am planning an upcoming trip to <A HREF=
'https://www.mlb.com/mets/ballpark'>Citi Field</A> to see the Mets take on the
Yankees in the Subway Series.</p>
<p>Does anyone have suggestions for transportation?  I am staying in Manhattan and
am only interested in <B>public transportation</B> options.</p>
<p>Thanks!</p>
<p>Mike</p>
<SCRIPT>alert('Cross-site scripting!')</SCRIPT>
```

(You must change the last line to another line or lines of HTML code to include a cross site scripting attack.) **Take the screen shot of the modified code**.


rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
rhythm_23076907_linux
1 2 3 4
18:43
Open
samplepage.html
~/Desktop
Save
HTML
Tab Width: 8
Ln 11, Col 33
INS
rockyou.txt
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

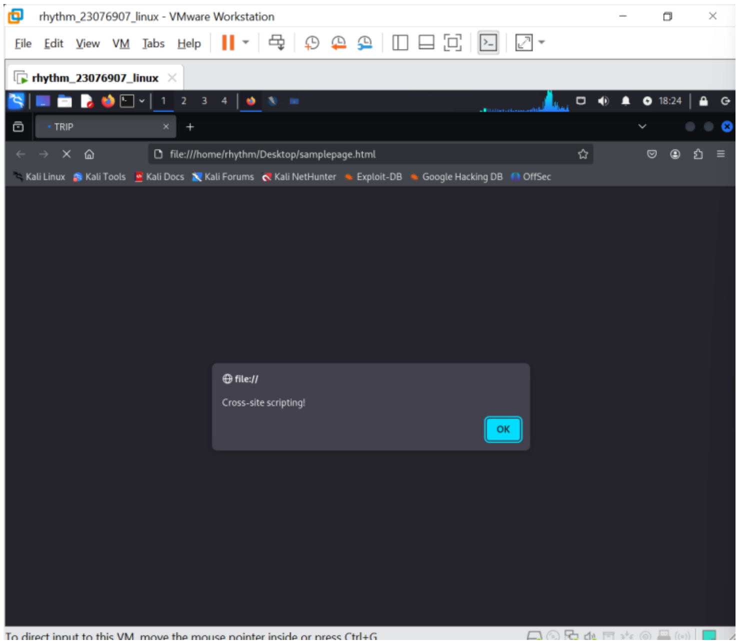
```
<html>
<title>TRIP</title>
<body>
<p>Hello everyone,</p>
<p>I am planning an upcoming trip to <A href='https://www.mlb.com/mets/ballpark'>Citi Field</A> to see the
Mets take on the Yankees in the Subway Series.</p>
<p>Does anyone have suggestions for transportation?  I am staying in Manhattan and am only interested in
<B>public transportation</B> options.</p>
<p>Thanks!</p>
<p>Mike</p>
<script>
  window.location = "trios.com";
  alert('Cross-site scripting!')
</script>
</body>
</html>
```

Saving file "~/Desktop/samplepage.html"...

I have changed it into changing link when ever user try to login same login page will redirect to trios.com and make a alert as cross-site scripting

But if I remove alert and simply put this script then its gonna redirect to trios.com without giving me alert ()

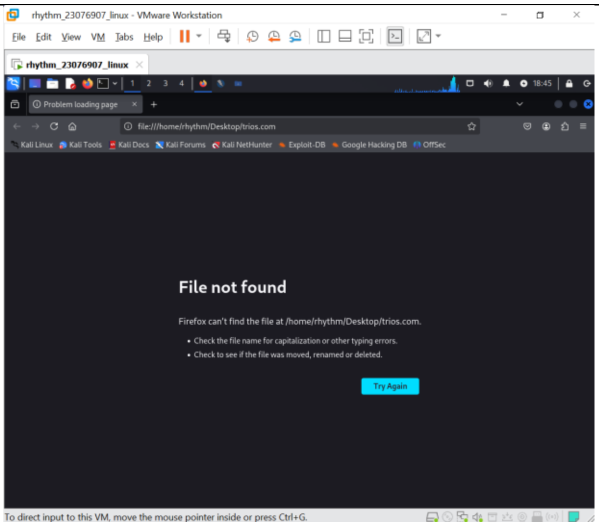
4. After saving the modified file, refresh the page in your browser. **Take the screen shot.**


rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
rhythm_23076907_linux
1 2 3 4
18:24
TRIP
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OK
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

file:///home/rhythm/Desktop/samplepage.html

file://

Cross-site scripting!


rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
rhythm_23076907_linux
Problem loading page
file:///home/rhythm/Desktop/trios.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

File not found

Firefox can't find the file at /home/rhythm/Desktop/trios.com.

- Check the file name for capitalization or other typing errors.
- Check to see if the file was moved, renamed or deleted.

Try Again

Q2: Did you see the impact of your cross-site scripting attack?

Ans Yes I see the impact using CSS attack and it can be use for Manipulation the user as open other link.s

Activtiy#3: Exploiting Insecure Direct Object Reference (URL Manipulation)

First, we need to setup the lab. environment by creating a LAMP Server in Kali:

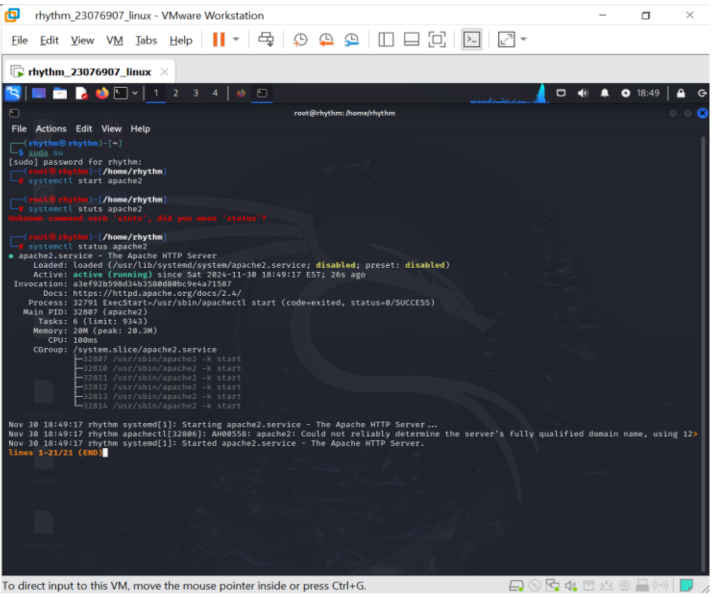
- Start Kali vm in VMWare or VirtualBox.
- Make sure Apache webserver is installed, it should be by default, so try to start it, if the service is not found then use apt-get to install it.

  systemctl start apache2

  The standard password is set as: kali

  (If you have changed Kali's password previously, then use that one.)
- After starting Apache, check the status to make sure it is up and running.

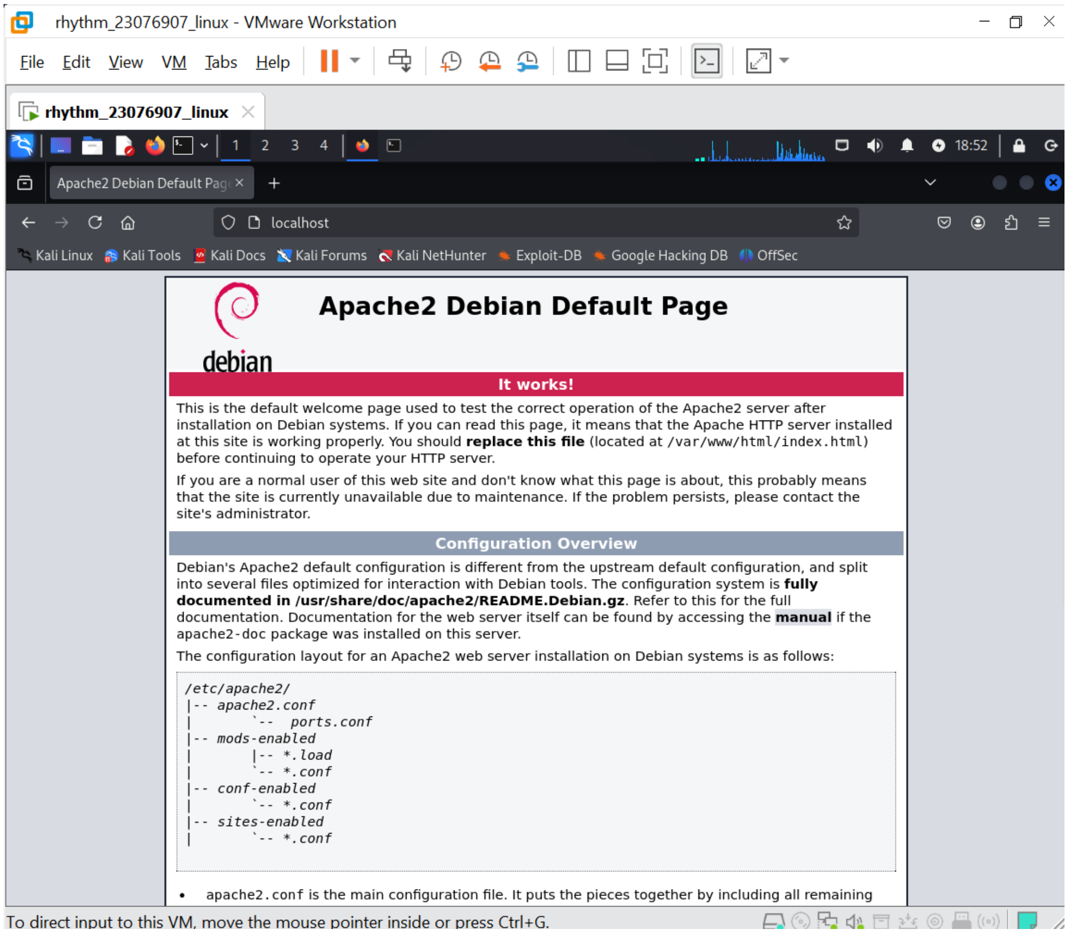
  systemctl status apache2


rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
rhythm_23076907_linux
18:49
root@rhythm: /home/rhythm
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
┌──(rhythm㉿rhythm)-[~]
└─$ sudo su
[sudo] password for rhythm:
┌──(root㉿rhythm)-[/home/rhythm]
└─# systemctl start apache2

┌──(root㉿rhythm)-[/home/rhythm]
└─# systemctl stuts apache2
Unknown command verb 'stuts', did you mean 'status'?

┌──(root㉿rhythm)-[/home/rhythm]
└─# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-11-30 18:49:17 EST; 26s ago
 Invocation: a3ef92b598d34b3580d80bc9e4a71587
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 32791 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 32807 (apache2)
      Tasks: 6 (limit: 9343)
     Memory: 20M (peak: 20.3M)
        CPU: 100ms
     CGroup: /system.slice/apache2.service
             ├─32807 /usr/sbin/apache2 -k start
             ├─32810 /usr/sbin/apache2 -k start
             ├─32811 /usr/sbin/apache2 -k start
             ├─32812 /usr/sbin/apache2 -k start
             ├─32813 /usr/sbin/apache2 -k start
             └─32814 /usr/sbin/apache2 -k start

Nov 30 18:49:17 rhythm systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 30 18:49:17 rhythm apachectl[32806]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 12>
Nov 30 18:49:17 rhythm systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)
```

S

- Open a web browser and go to the “localhost” address to make sure the website is up and running, it should show the default Apache2 Debian page.


rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
rhythm_23076907_linux
1 2 3 4
18:52
Apache2 Debian Default Pag
localhost
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
debian
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|        `--  ports.conf
|-- mods-enabled
|        |-- *.load
|        `-- *.conf
|-- conf-enabled
|        `-- *.conf
|-- sites-enabled
|        `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining

- Now that Apache is installed and running, make sure that mysql is installed. Try to start the mysql service, if it is not found, install it with apt-get.

  systemctl start mysqls

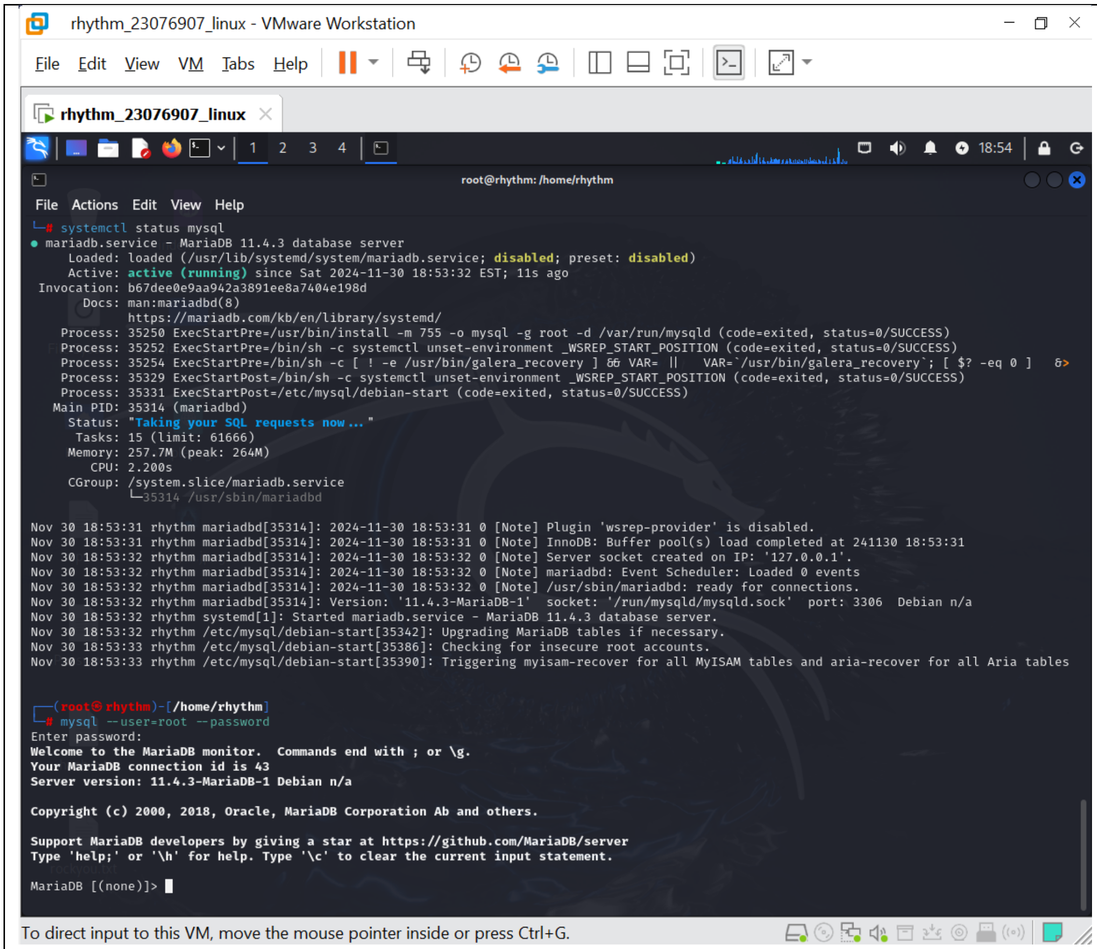
  The standard password is set as: kali

- Check the status of mysql to make sure it is running.

  systemctl status mysql

- Now that mysql is up and running, we have to setup the database. Login to mysql as the root user.

  sudo mysql --user=root –password



rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
rhythm_23076907_linux
1 2 3 4
18:54
root@rhythm: /home/rhythm
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

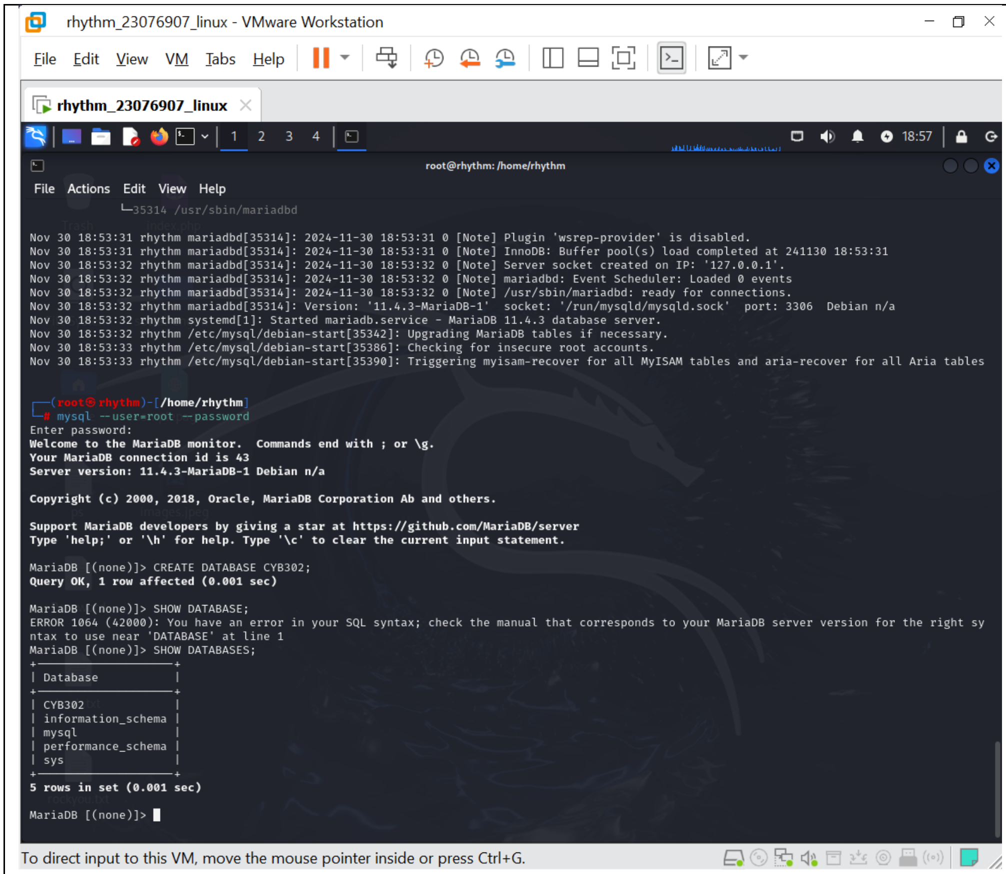
```
└─# systemctl status mysql
● mariadb.service - MariaDB 11.4.3 database server
     Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-11-30 18:53:32 EST; 11s ago
 Invocation: b67dee0e9aa942a3891ee8a7404e198d
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
    Process: 35250 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)
    Process: 35252 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
    Process: 35254 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||   VAR=`/usr/bin/galera_recovery`; [ $? -eq 0 ]   &>
    Process: 35329 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
    Process: 35331 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
   Main PID: 35314 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 15 (limit: 61666)
     Memory: 257.7M (peak: 264M)
        CPU: 2.200s
     CGroup: /system.slice/mariadb.service
             └─35314 /usr/sbin/mariadbd

Nov 30 18:53:31 rhythm mariadbd[35314]: 2024-11-30 18:53:31 0 [Note] Plugin 'wsrep-provider' is disabled.
Nov 30 18:53:31 rhythm mariadbd[35314]: 2024-11-30 18:53:31 0 [Note] InnoDB: Buffer pool(s) load completed at 241130 18:53:31
Nov 30 18:53:32 rhythm mariadbd[35314]: 2024-11-30 18:53:32 0 [Note] Server socket created on IP: '127.0.0.1'.
Nov 30 18:53:32 rhythm mariadbd[35314]: 2024-11-30 18:53:32 0 [Note] mariadbd: Event Scheduler: Loaded 0 events
Nov 30 18:53:32 rhythm mariadbd[35314]: 2024-11-30 18:53:32 0 [Note] /usr/sbin/mariadbd: ready for connections.
Nov 30 18:53:32 rhythm mariadbd[35314]: Version: '11.4.3-MariaDB-1'  socket: '/run/mysqld/mysqld.sock'  port: 3306  Debian n/a
Nov 30 18:53:32 rhythm systemd[1]: Started mariadb.service - MariaDB 11.4.3 database server.
Nov 30 18:53:32 rhythm /etc/mysql/debian-start[35342]: Upgrading MariaDB tables if necessary.
Nov 30 18:53:33 rhythm /etc/mysql/debian-start[35386]: Checking for insecure root accounts.
Nov 30 18:53:33 rhythm /etc/mysql/debian-start[35390]: Triggering myisam-recover for all MyISAM tables and aria-recover for all Aria tables


┌──(root㉿rhythm)-[/home/rhythm]
└─# mysql --user=root --password
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 43
Server version: 11.4.3-MariaDB-1 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> 
```

- Create the database - call it CYB302. NOTE the capital, it is important to make sure it is capitalized because the PHP files that connect to the database is case-sensitive. Also make sure to use the semi-colon ; to end the statement

    CREATE DATABASE CYB302;

- Verify that the database was created correctly by using the show databases command.

    SHOW DATABASES;



rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
rhythm_23076907_linux
1 2 3 4
18:57
root@rhythm: /home/rhythm
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
        └─35314 /usr/sbin/mariadbd

Nov 30 18:53:31 rhythm mariadbd[35314]: 2024-11-30 18:53:31 0 [Note] Plugin 'wsrep-provider' is disabled.
Nov 30 18:53:31 rhythm mariadbd[35314]: 2024-11-30 18:53:31 0 [Note] InnoDB: Buffer pool(s) load completed at 241130 18:53:31
Nov 30 18:53:32 rhythm mariadbd[35314]: 2024-11-30 18:53:32 0 [Note] Server socket created on IP: '127.0.0.1'.
Nov 30 18:53:32 rhythm mariadbd[35314]: 2024-11-30 18:53:32 0 [Note] mariadbd: Event Scheduler: Loaded 0 events
Nov 30 18:53:32 rhythm mariadbd[35314]: 2024-11-30 18:53:32 0 [Note] /usr/sbin/mariadbd: ready for connections.
Nov 30 18:53:32 rhythm mariadbd[35314]: Version: '11.4.3-MariaDB-1'  socket: '/run/mysqld/mysqld.sock'  port: 3306  Debian n/a
Nov 30 18:53:32 rhythm systemd[1]: Started mariadb.service - MariaDB 11.4.3 database server.
Nov 30 18:53:32 rhythm /etc/mysql/debian-start[35342]: Upgrading MariaDB tables if necessary.
Nov 30 18:53:33 rhythm /etc/mysql/debian-start[35386]: Checking for insecure root accounts.
Nov 30 18:53:33 rhythm /etc/mysql/debian-start[35390]: Triggering myisam-recover for all MyISAM tables and aria-recover for all Aria tables


┌──(root㉿rhythm)-[/home/rhythm]
└─# mysql --user=root --password
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 43
Server version: 11.4.3-MariaDB-1 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE CYB302;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> SHOW DATABASE;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right sy
ntax to use near 'DATABASE' at line 1
MariaDB [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| CYB302             |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.001 sec)

MariaDB [(none)]> █
```

- Now we have to create a user for accessing the database and setup the user's privileges. The username is "mohamed" and the password is "S!d@q!##". Copy and paste this command, it is actually several commands linked together by statement terminating semi-colons ; make sure they all respond with Query OK. Do not change anything in the below commands at all.

  CREATE USER 'mohamed'@'%' IDENTIFIED BY 'S!d@q!##';GRANT SELECT ON *.* TO 'mohamed'@'%';ALTER USER 'mohamed'@'%' REQUIRE NONE WITH MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0 MAX_USER_CONNECTIONS 0;GRANT ALL PRIVILEGES ON `mohamed`.* TO 'mohamed'@'%';

- Now create the tables. First select the database.

  USE CYB302;

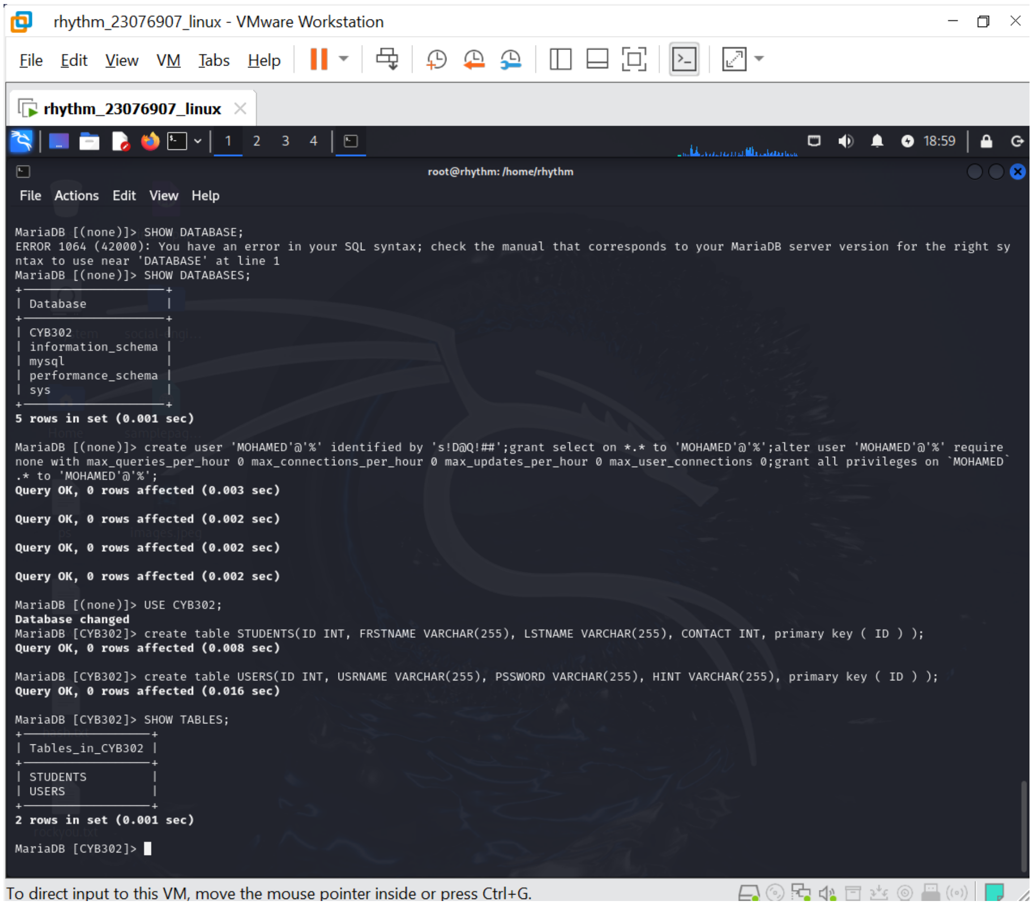
- Now make two tables, a students table that holds first and last name of students, and a users table that holds users usernames and passwords.

  CREATE TABLE students(id int, frstname varchar(255), lstname varchar(255), contact int, PRIMARY KEY (id));

  CREATE TABLE users(id int, usrname varchar(255), pssword varchar(255), hint varchar(255), PRIMARY KEY (id));

- Finally verify the tables were created correctly by display the tables.

SHOW TABLES; (Take the screen shot)


rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
rhythm_23076907_linux
1 2 3 4
18:59
root@rhythm: /home/rhythm
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

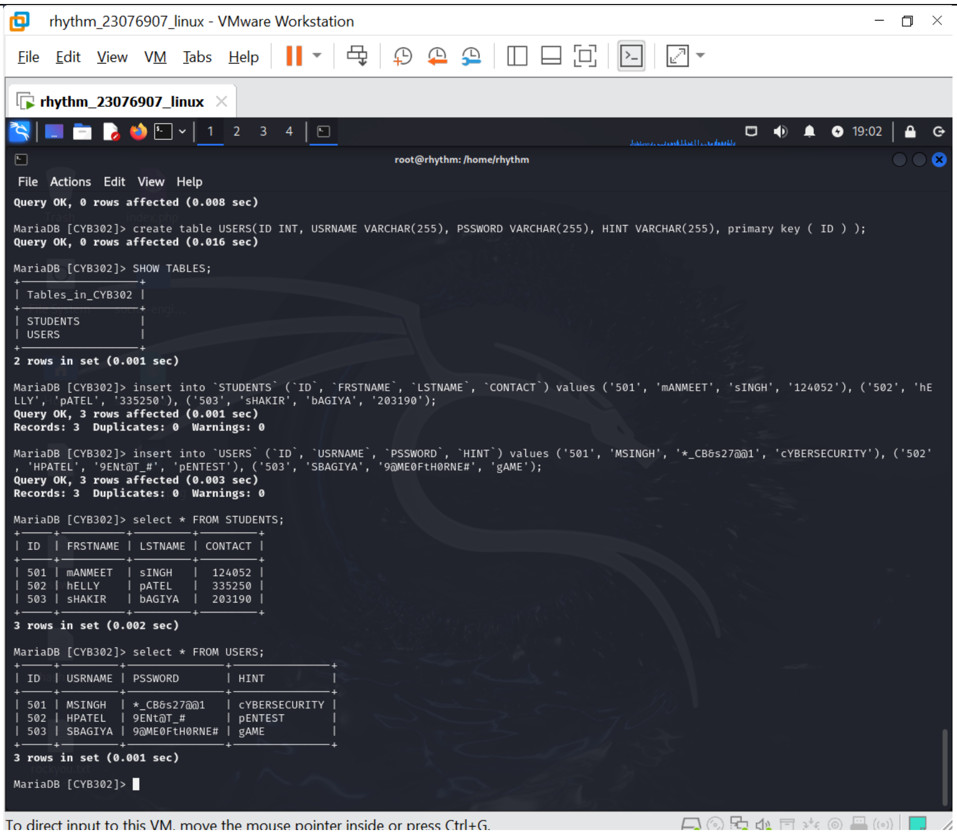
```
MariaDB [(none)]> SHOW DATABASE;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right sy
ntax to use near 'DATABASE' at line 1
MariaDB [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| CYB302             |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.001 sec)

MariaDB [(none)]> create user 'MOHAMED'@'%' identified by 's!D@Q!##';grant select on *.* to 'MOHAMED'@'%';alter user 'MOHAMED'@'%' require
none with max_queries_per_hour 0 max_connections_per_hour 0 max_updates_per_hour 0 max_user_connections 0;grant all privileges on `MOHAMED`
.* to 'MOHAMED'@'%';
Query OK, 0 rows affected (0.003 sec)

Query OK, 0 rows affected (0.002 sec)

Query OK, 0 rows affected (0.002 sec)

Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> USE CYB302;
Database changed
MariaDB [CYB302]> create table STUDENTS(ID INT, FRSTNAME VARCHAR(255), LSTNAME VARCHAR(255), CONTACT INT, primary key ( ID ) );
Query OK, 0 rows affected (0.008 sec)

MariaDB [CYB302]> create table USERS(ID INT, USRNAME VARCHAR(255), PSSWORD VARCHAR(255), HINT VARCHAR(255), primary key ( ID ) );
Query OK, 0 rows affected (0.016 sec)

MariaDB [CYB302]> SHOW TABLES;
+------------------+
| Tables_in_CYB302 |
+------------------+
| STUDENTS         |
| USERS            |
+------------------+
2 rows in set (0.001 sec)

MariaDB [CYB302]> 
```

- Insert some data into the “students” table and the “users” table. Feel free to change the values to other names, usernames, and passwords.

  INSERT INTO `students` (`id`, `frstname`, `lstname`, `contact`) VALUES ('501', 'Manmeet', 'Singh', '124052'), ('502', 'Helly', 'Patel', '335250'), ('503', 'Shakir', 'Bagiya', '203190');

  INSERT INTO `users` (`id`, `usrname`, `pssword`, `hint`) VALUES ('501', 'msingh', '*_cb&S27@@1', 'Cybersecurity'), ('502', 'hpatel', '9enT@t_#', 'Pentest'), ('503', 'sbagiya', '9@me0fTh0rne#', 'Game');

- Read back the data from the tables to make sure that it was inserted correctly.
  SELECT * from students;
  SELECT * from users;
  (Take the screen shot showing output of both above-mentioned commands)


rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
rhythm_23076907_linux
1 2 3 4
19:02
root@rhythm: /home/rhythm
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
Query OK, 0 rows affected (0.008 sec)

MariaDB [CYB302]> create table USERS(ID INT, USRNAME VARCHAR(255), PSSWORD VARCHAR(255), HINT VARCHAR(255), primary key ( ID ) );
Query OK, 0 rows affected (0.016 sec)

MariaDB [CYB302]> SHOW TABLES;
+----------------+
| Tables_in_CYB302 |
+----------------+
| STUDENTS       |
| USERS          |
+----------------+
2 rows in set (0.001 sec)

MariaDB [CYB302]> insert into `STUDENTS` (`ID`, `FRSTNAME`, `LSTNAME`, `CONTACT`) values ('501', 'mANMEET', 'sINGH', '124052'), ('502', 'hE
LLY', 'pATEL', '335250'), ('503', 'sHAKIR', 'bAGIYA', '203190');
Query OK, 3 rows affected (0.001 sec)
Records: 3  Duplicates: 0  Warnings: 0

MariaDB [CYB302]> insert into `USERS` (`ID`, `USRNAME`, `PSSWORD`, `HINT`) values ('501', 'MSINGH', '*_CB&s27@@1', 'cYBERSECURITY'), ('502'
, 'HPATEL', '9ENt@T_#', 'pENTEST'), ('503', 'SBAGIYA', '9@ME0FtH0RNE#', 'gAME');
Query OK, 3 rows affected (0.003 sec)
Records: 3  Duplicates: 0  Warnings: 0

MariaDB [CYB302]> select * FROM STUDENTS;
+-----+----------+---------+---------+
| ID  | FRSTNAME | LSTNAME | CONTACT |
+-----+----------+---------+---------+
| 501 | mANMEET  | sINGH   |  124052 |
| 502 | hELLY    | pATEL   |  335250 |
| 503 | sHAKIR   | bAGIYA  |  203190 |
+-----+----------+---------+---------+
3 rows in set (0.002 sec)

MariaDB [CYB302]> select * FROM USERS;
+-----+---------+---------------+---------------+
| ID  | USRNAME | PSSWORD       | HINT          |
+-----+---------+---------------+---------------+
| 501 | MSINGH  | *_CB&s27@@1   | cYBERSECURITY |
| 502 | HPATEL  | 9ENt@T_#      | pENTEST       |
| 503 | SBAGIYA | 9@ME0FtH0RNE# | gAME          |
+-----+---------+---------------+---------------+
3 rows in set (0.001 sec)

MariaDB [CYB302]> 
```

- Finally, exit out of the mysql command terminal.

  esxit

- Download the following tws PHP files form.php and doit.php

- Open a terminal and change directory to your Downloads directory. Make sure that the two files are there in the downloads directory by using the **ls command**.
- Make a new directory called "**cyb**" in the webserver root directory with the following command:

  sudo mkdir /var/www/html/cyb

  Note that the /var/www/html directory is the default webserver root directory for apache, also make sure you use **sudo** with the **mkdir** command because this directory is owned by root and regular users will not have permission to make new directories.
- s

  sudo mv doit.php form.php /var/www/html/cyb

  Note once again that you must use **sudo** since the directory is owned by the root user.
- Restart the Apache webserver

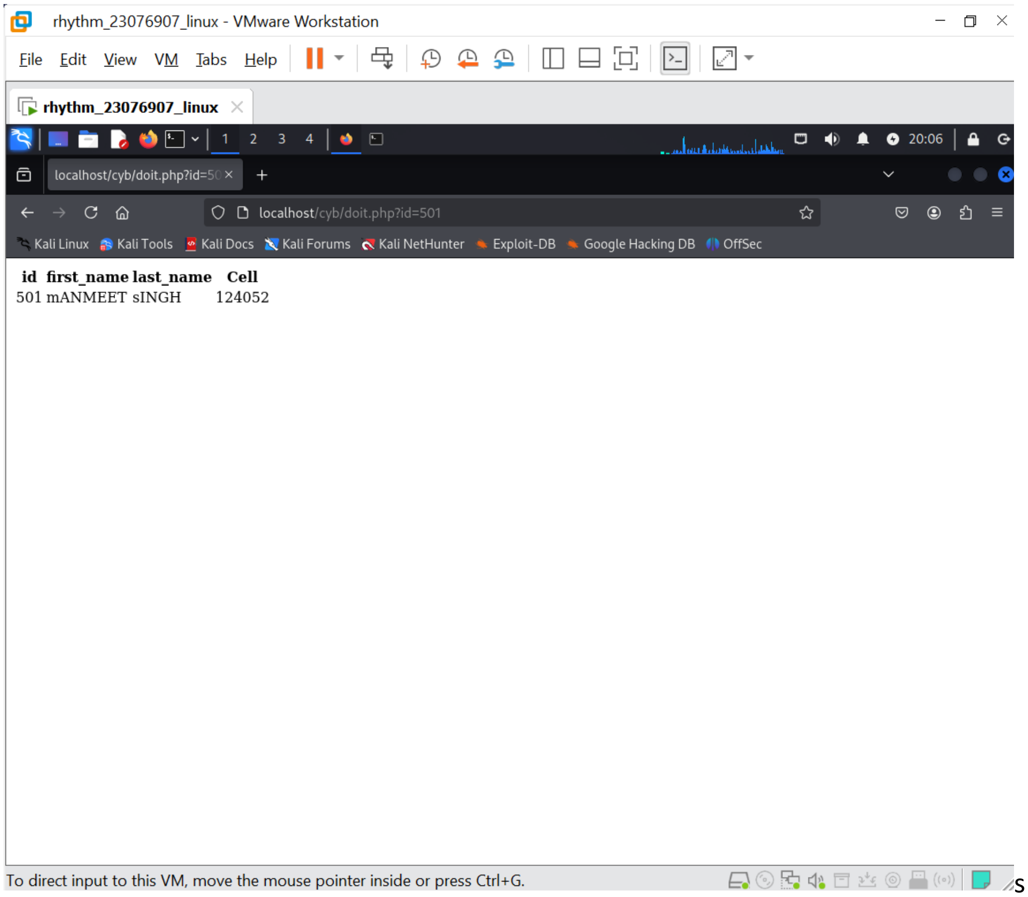
  systemctl restart apache2

  Now visit the address "localhost/cyb/form.php" in your web browser, you should see the form page.

URL Manipulation:

URL manipulation is a starting point with SQL injection that allows you to change the variables that websites use to communicate between the back and front end.

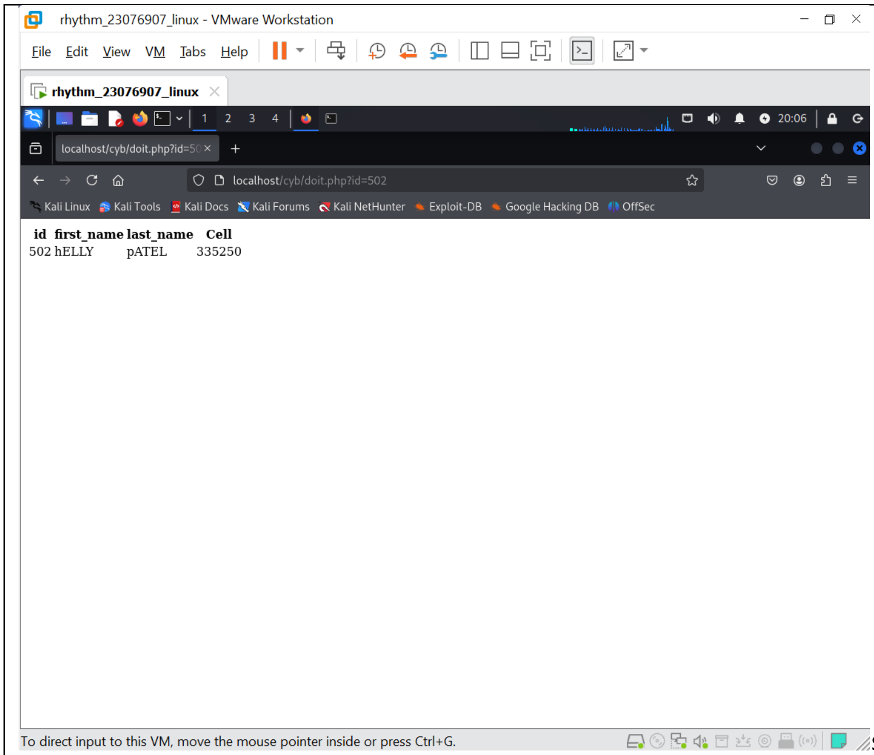
- Navigate to the site "**localhost/cyb/form.php**" and enter the number 501 in the ID field, click submit. **Take the screen shot.**
  Notice how the resulting PHP code returns a pagse that lists the record associated with ID number 501.


rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
rhythm_23076907_linux
20:06
localhost/cyb/doit.php?id=50
localhost/cyb/doit.php?id=501
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
 id  first_name last_name  Cell
501 mANMEET sINGH       124052
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- Modify the URL to show you the record associated with the following ID numbers:
  - 502 **(Take the screen shot)**


rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
rhythm_23076907_linux
1 2 3 4
20:06
localhost/cyb/doit.php?id=50
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

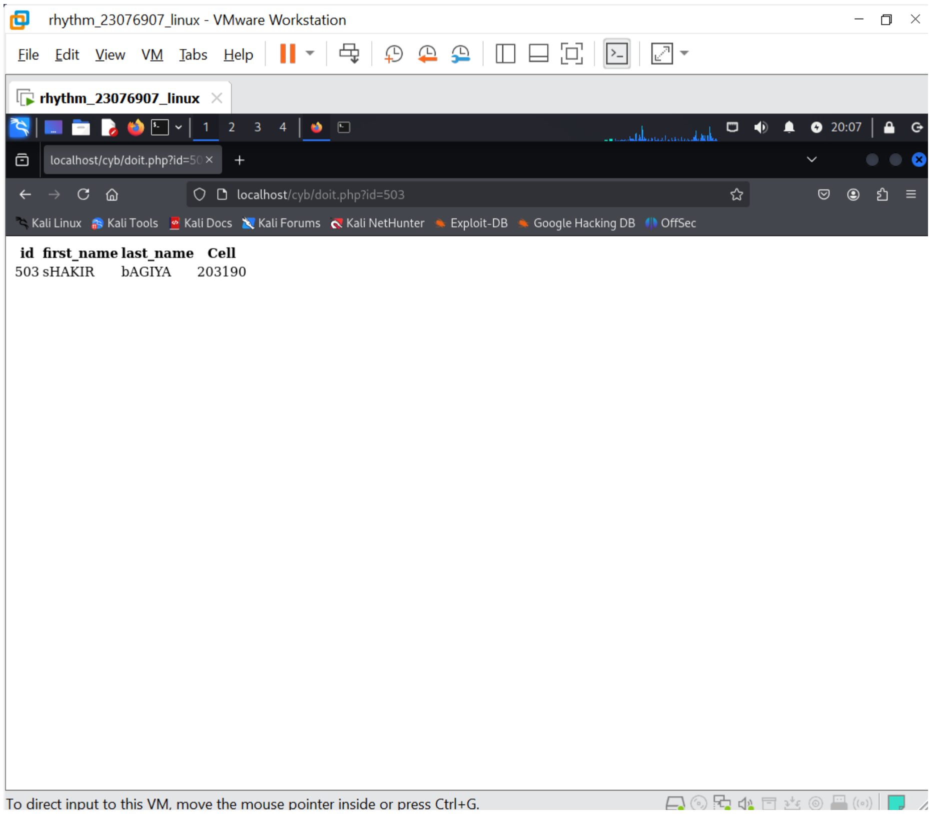
localhost/cyb/doit.php?id=502

```
id  first_name last_name  Cell
502 hELLY      pATEL      335250
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

S

- ○ 503 **(Take the screen shot)**


rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
rhythm_23076907_linux
1 2 3 4
20:07
localhost/cyb/doit.php?id=50
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

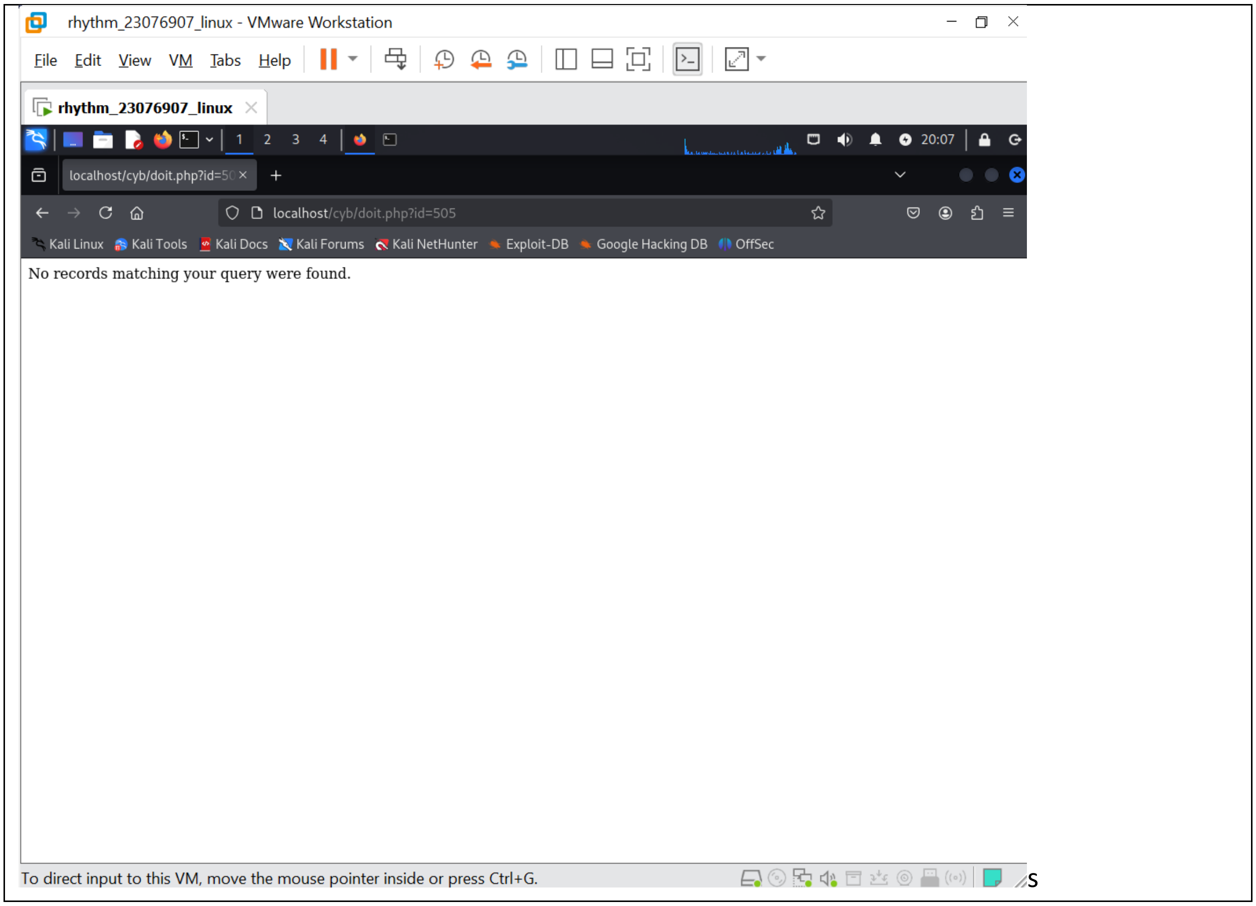
localhost/cyb/doit.php?id=503

```
id  first_name last_name  Cell
503 sHAKIR     bAGIYA     203190
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

S

- ○ 505 **(Take the screen shot)**



rhythm_23076907_linux - VMware Workstation
File Edit View VM Tabs Help
rhythm_23076907_linux
1 2 3 4
20:07
localhost/cyb/doit.php?id=50
localhost/cyb/doit.php?id=505
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
No records matching your query were found.
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

s