triOS COLLEGE
BUSINESS ♠ TECHNOLOGY ♠ HEALTHCARE

Course: CYB302

Ethical Hacking
(Canadian Context)

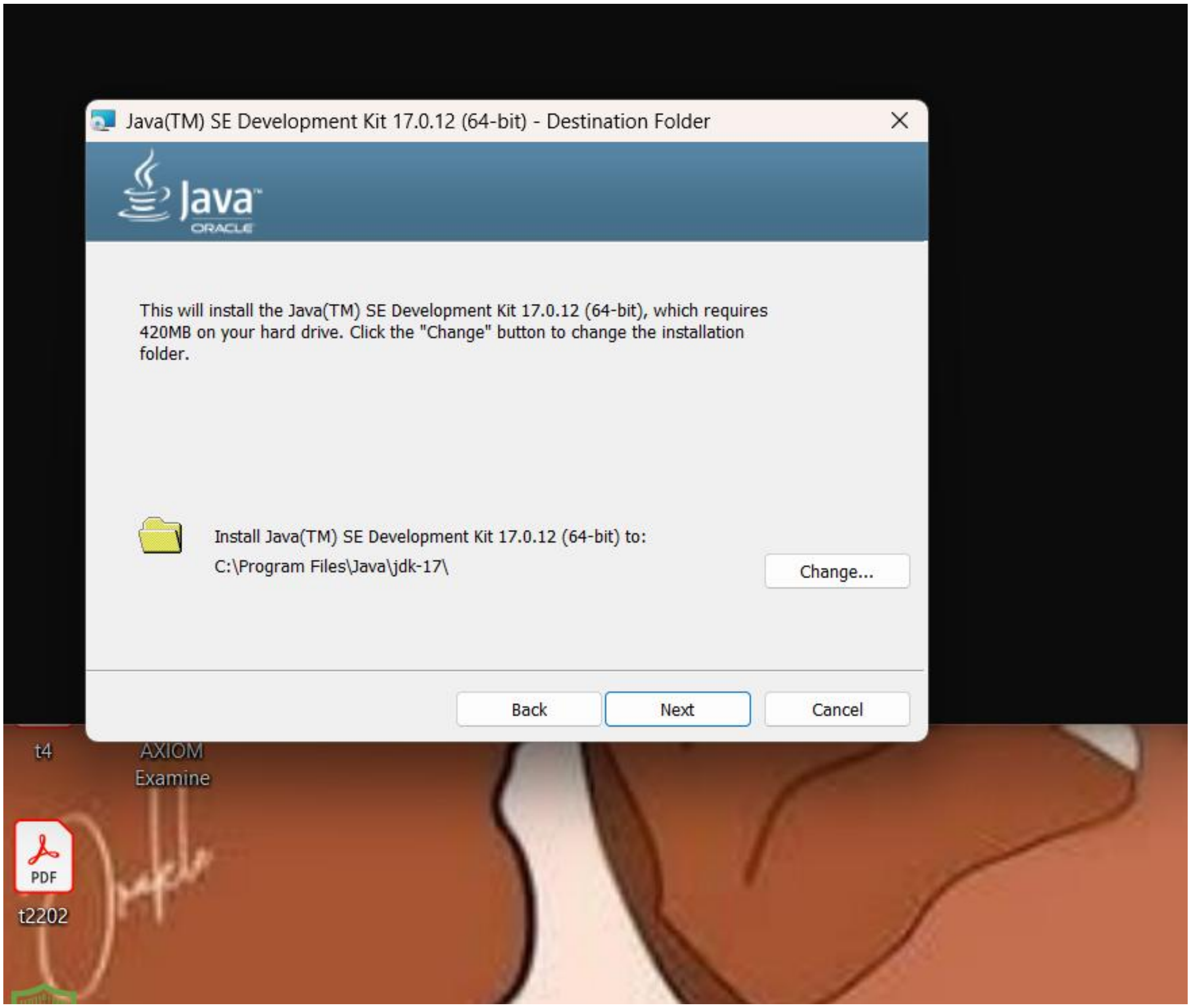
Lab 9: Exploiting Application Vulnerabilities using ZAP, XSS and URL manipulation.

Coordinator and Instructor:

Muhamma Saleem

Student Name:	**Olushola Enoch Bayode**
Student ID:	**23077087**
Section:	**3rd Semester**

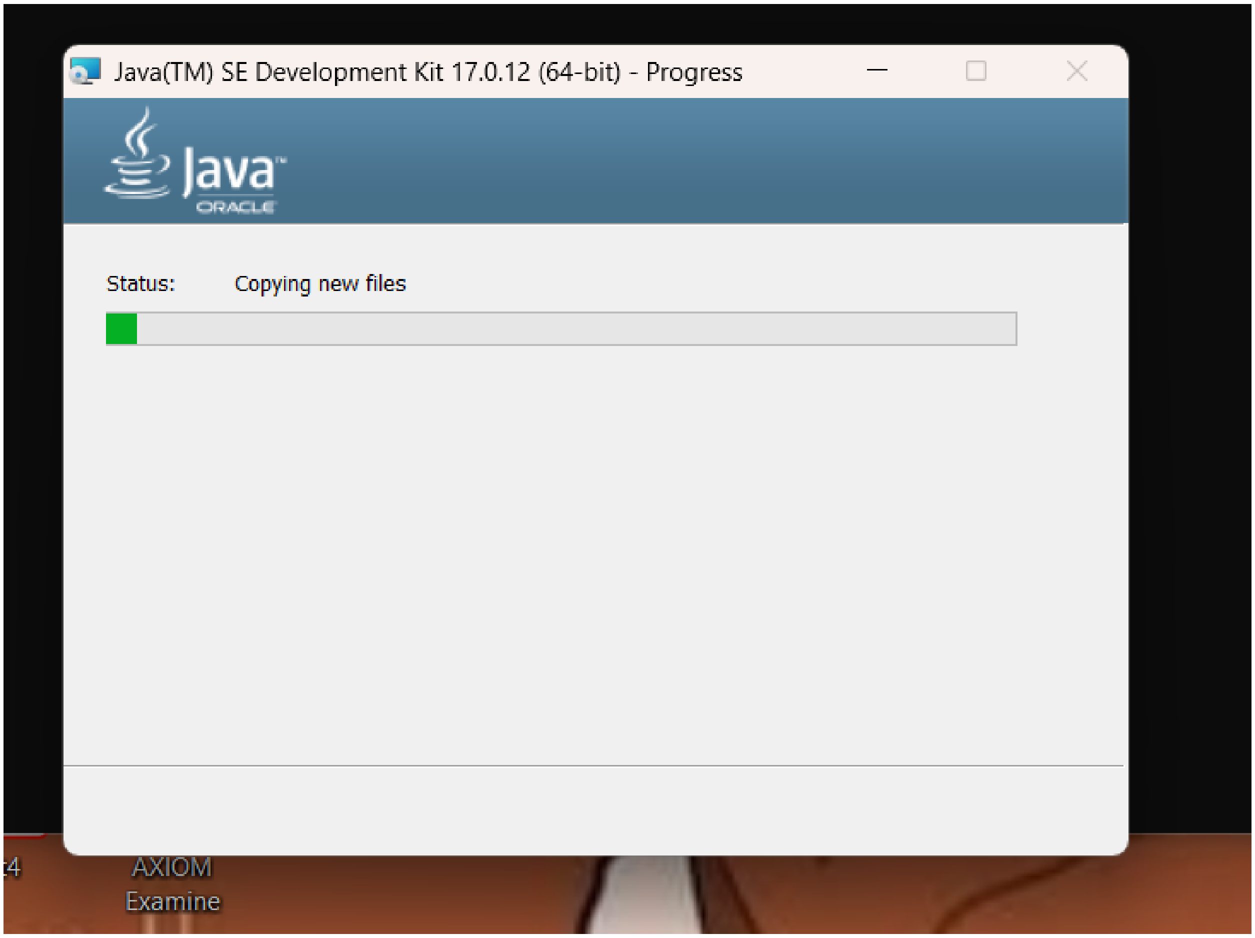
Activity 1: Using the ZAP Proxy



Java(TM) SE Development Kit 17.0.12 (64-bit) - Destination Folder

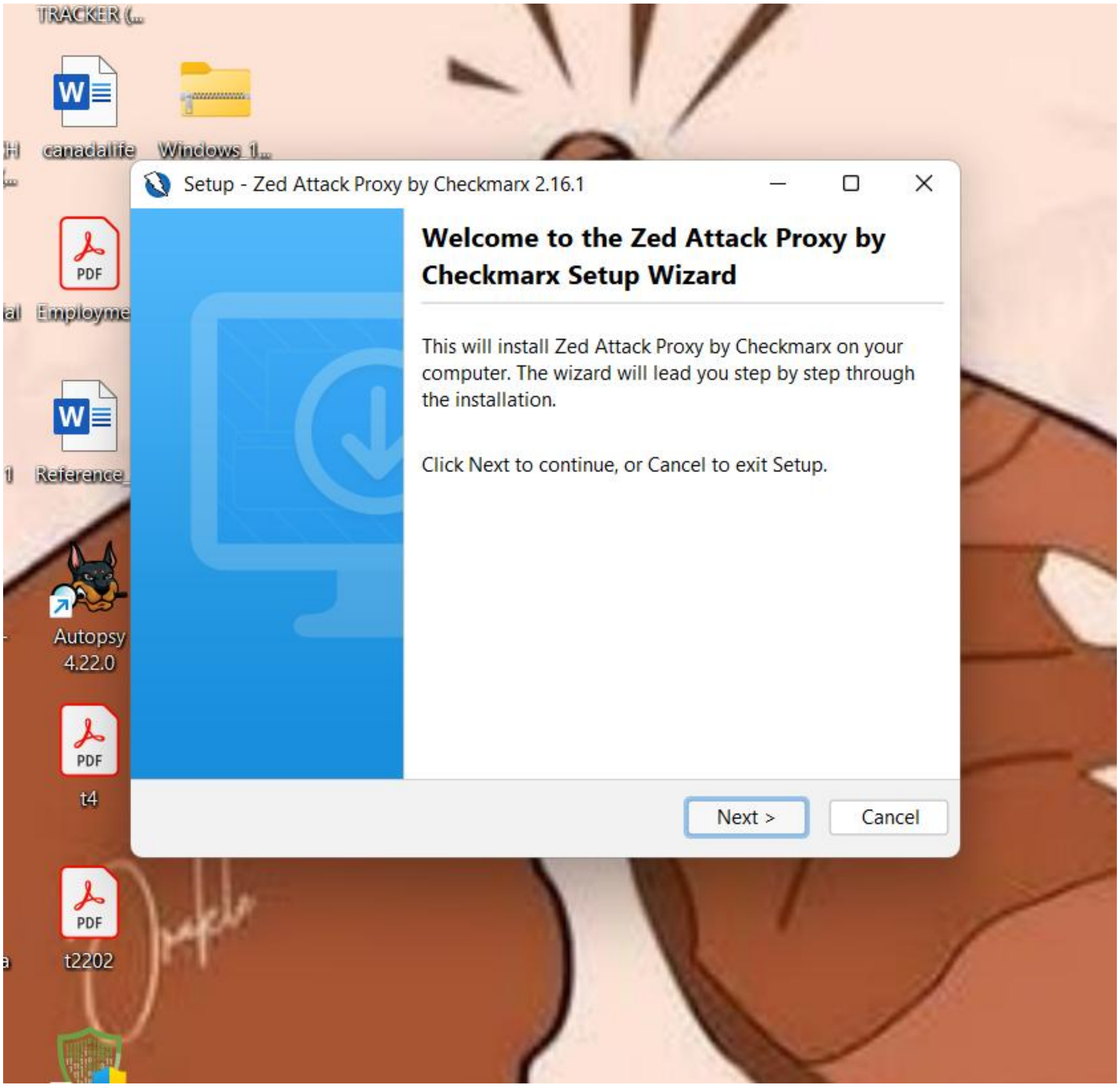
This will install the Java(TM) SE Development Kit 17.0.12 (64-bit), which requires 420MB on your hard drive. Click the "Change" button to change the installation folder.

Install Java(TM) SE Development Kit 17.0.12 (64-bit) to:
C:\Program Files\Java\jdk-17\



Java(TM) SE Development Kit 17.0.12 (64-bit) - Progress

Status: Copying new files

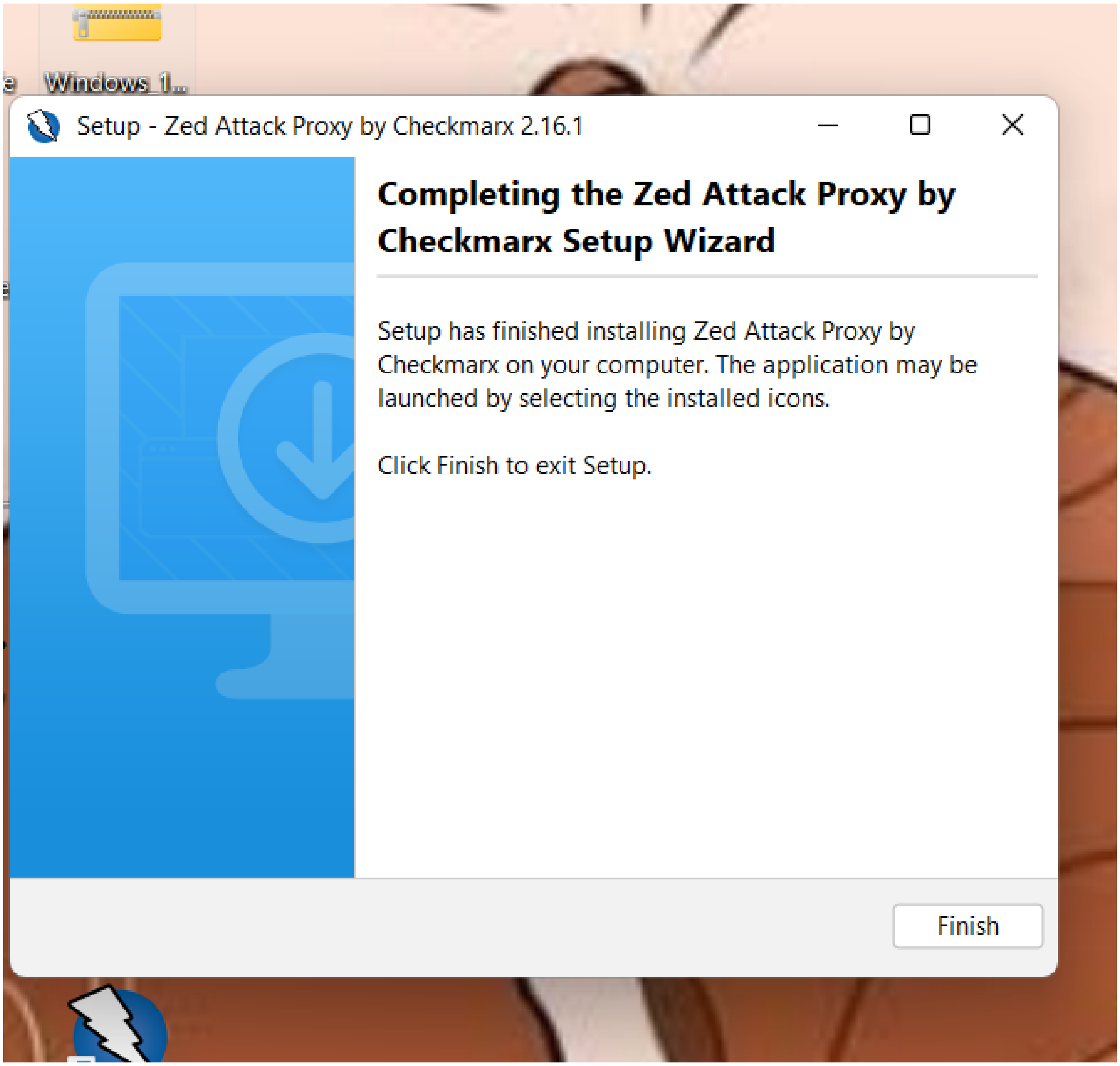


Setup - Zed Attack Proxy by Checkmarx 2.16.1

Welcome to the Zed Attack Proxy by Checkmarx Setup Wizard

This will install Zed Attack Proxy by Checkmarx on your computer. The wizard will lead you step by step through the installation.

Click Next to continue, or Cancel to exit Setup.

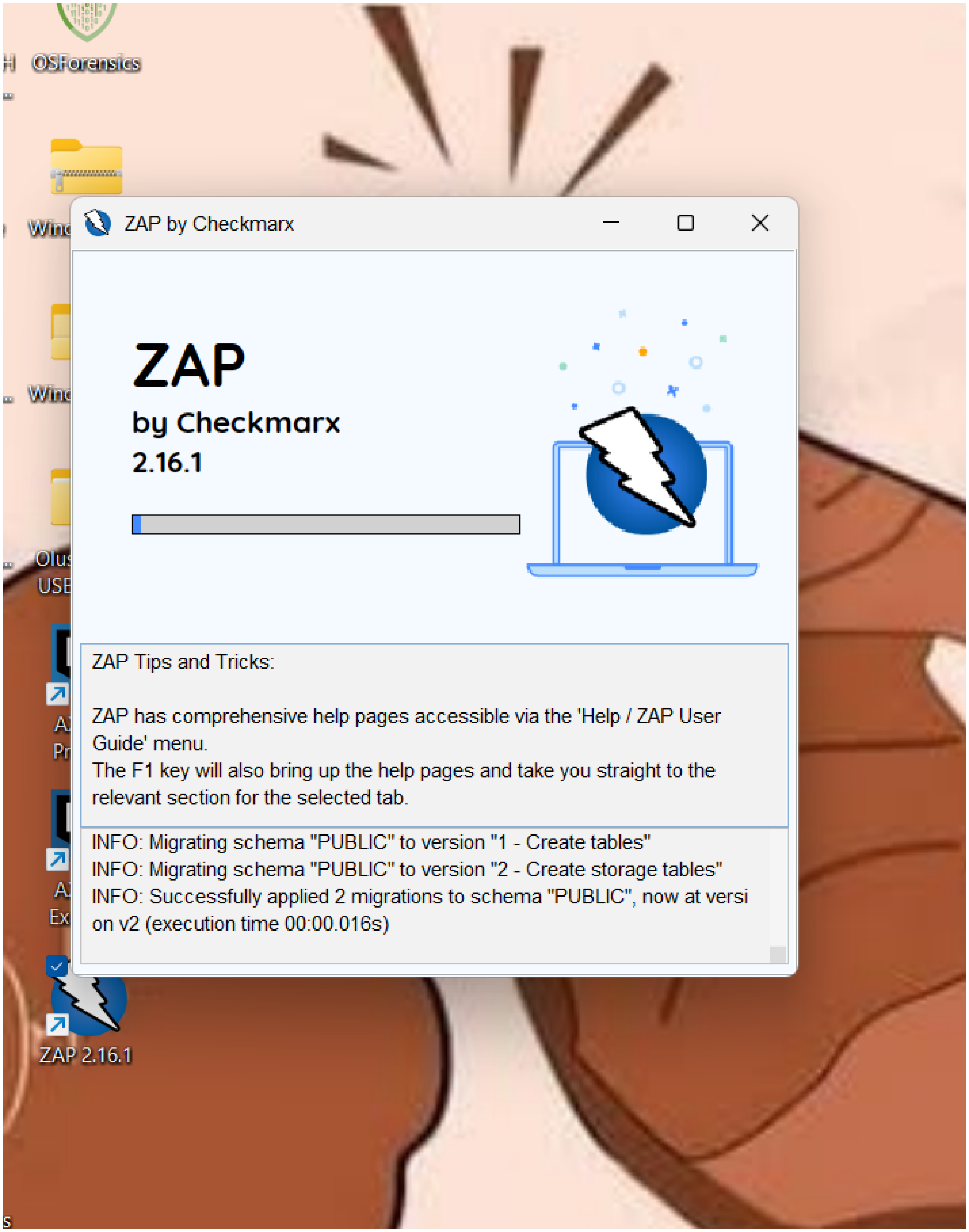


Setup - Zed Attack Proxy by Checkmarx 2.16.1

Completing the Zed Attack Proxy by Checkmarx Setup Wizard

Setup has finished installing Zed Attack Proxy by Checkmarx on your computer. The application may be launched by selecting the installed icons.

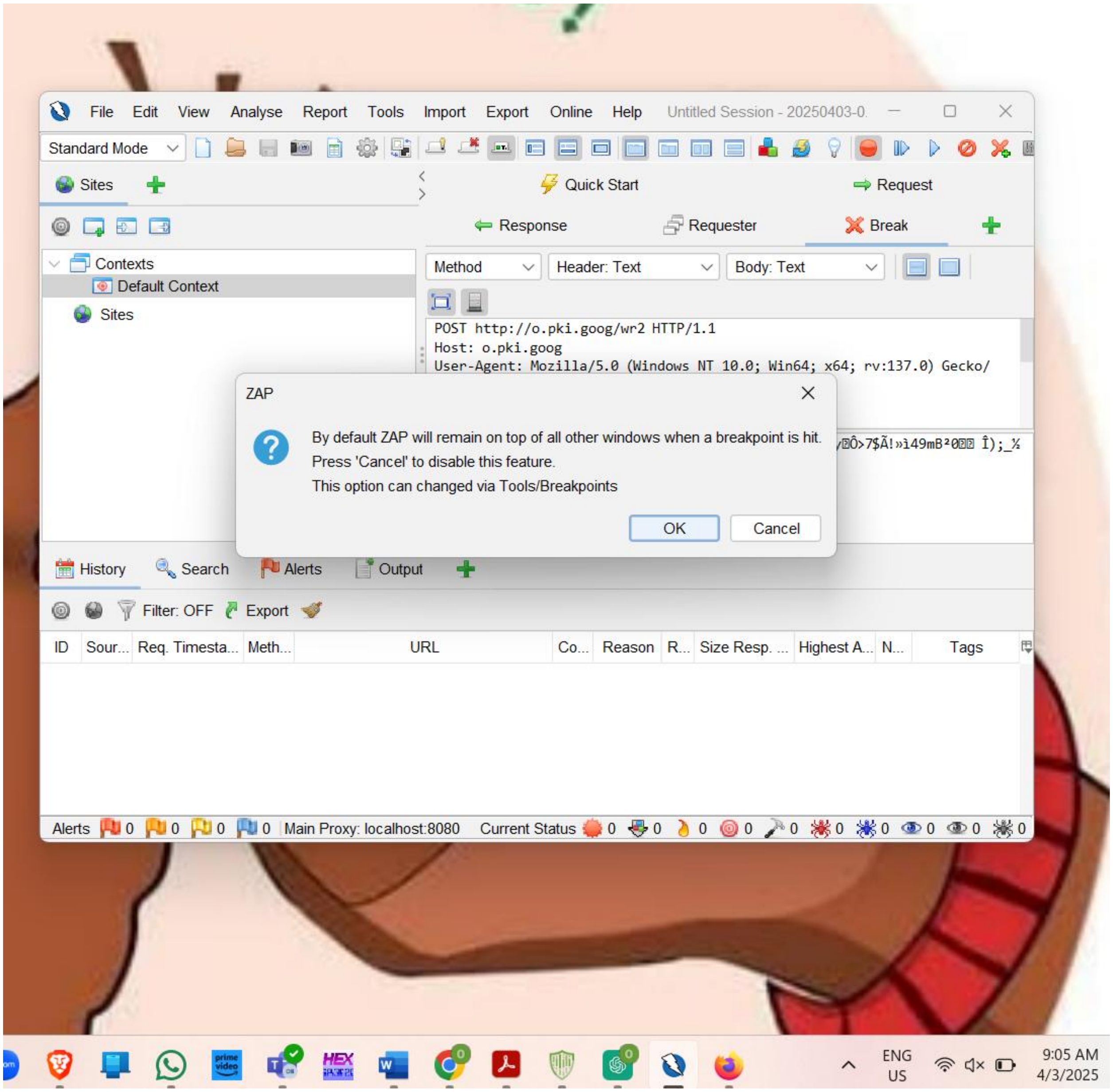
Click Finish to exit Setup.



ZAP Tips and Tricks:

ZAP has comprehensive help pages accessible via the 'Help / ZAP User Guide' menu.
The F1 key will also bring up the help pages and take you straight to the relevant section for the selected tab.

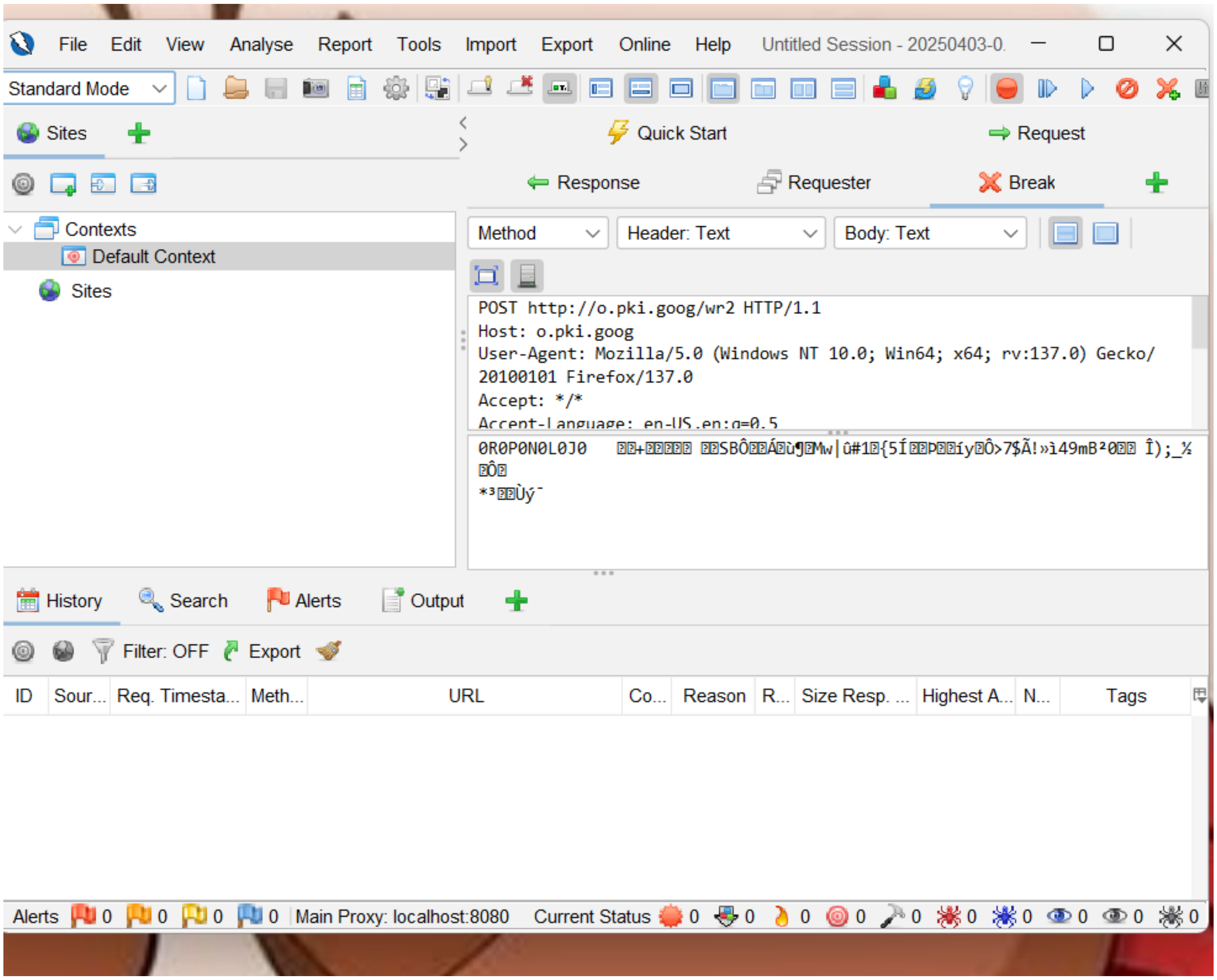
```
INFO: Migrating schema "PUBLIC" to version "1 - Create tables"
INFO: Migrating schema "PUBLIC" to version "2 - Create storage tables"
INFO: Successfully applied 2 migrations to schema "PUBLIC", now at versi
on v2 (execution time 00:00.016s)
```



```
POST http://o.pki.goog/wr2 HTTP/1.1
Host: o.pki.goog
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/
```

```
yÐÔ>7$Ã!»ì49mB²0ÐÐ Î);_½
```

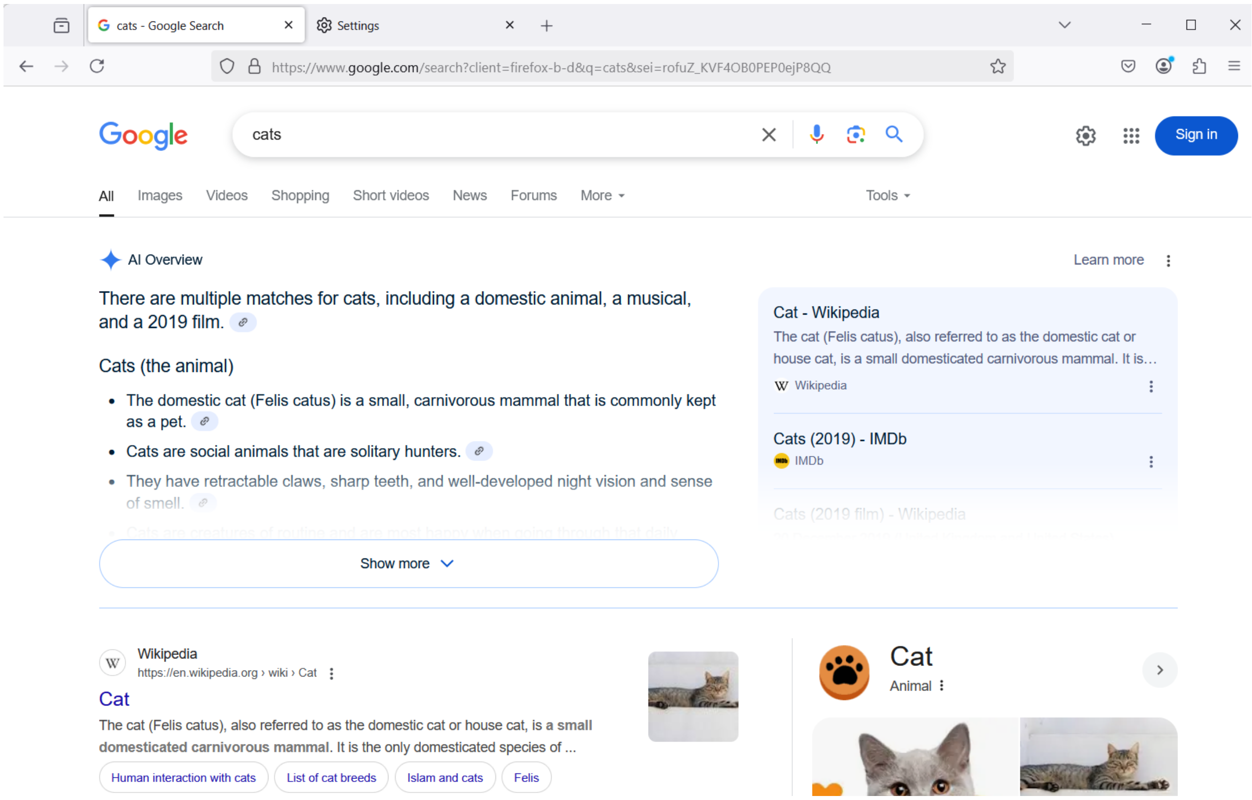
By default ZAP will remain on top of all other windows when a breakpoint is hit.
Press 'Cancel' to disable this feature.
This option can changed via Tools/Breakpoints



Method | Header: Text | Body: Text

```
POST http://o.pki.goog/wr2 HTTP/1.1
Host: o.pki.goog
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/
20100101 Firefox/137.0
Accept: */*
Accept-Language: en-US,en;q=0.5
```

```
0R0P0N0L0J0   □□+□□□□□ □□SBÔ□□Á□ù¶□Mw|û#1□{5Í□□Þ□□íy□Ô>7$Ã!»ì49mB²0□□ Î);_½
□Ô□
*³□□Ùý¯
```



https://www.google.com/search?client=firefox-b-d&q=cats&sei=rofuZ_KVF4OB0PEP0ejP8QQ

cats

AI Overview

There are multiple matches for cats, including a domestic animal, a musical, and a 2019 film.

Cats (the animal)

- The domestic cat (Felis catus) is a small, carnivorous mammal that is commonly kept as a pet.
- Cats are social animals that are solitary hunters.
- They have retractable claws, sharp teeth, and well-developed night vision and sense of smell.
- Cats are creatures of routine and are most happy when going through that daily

Cat - Wikipedia
The cat (Felis catus), also referred to as the domestic cat or house cat, is a small domesticated carnivorous mammal. It is…
Wikipedia

Cats (2019) - IMDb
IMDb

Cats (2019 film) - Wikipedia
20 December 2019 (United Kingdom and United States)

Wikipedia
https://en.wikipedia.org › wiki › Cat

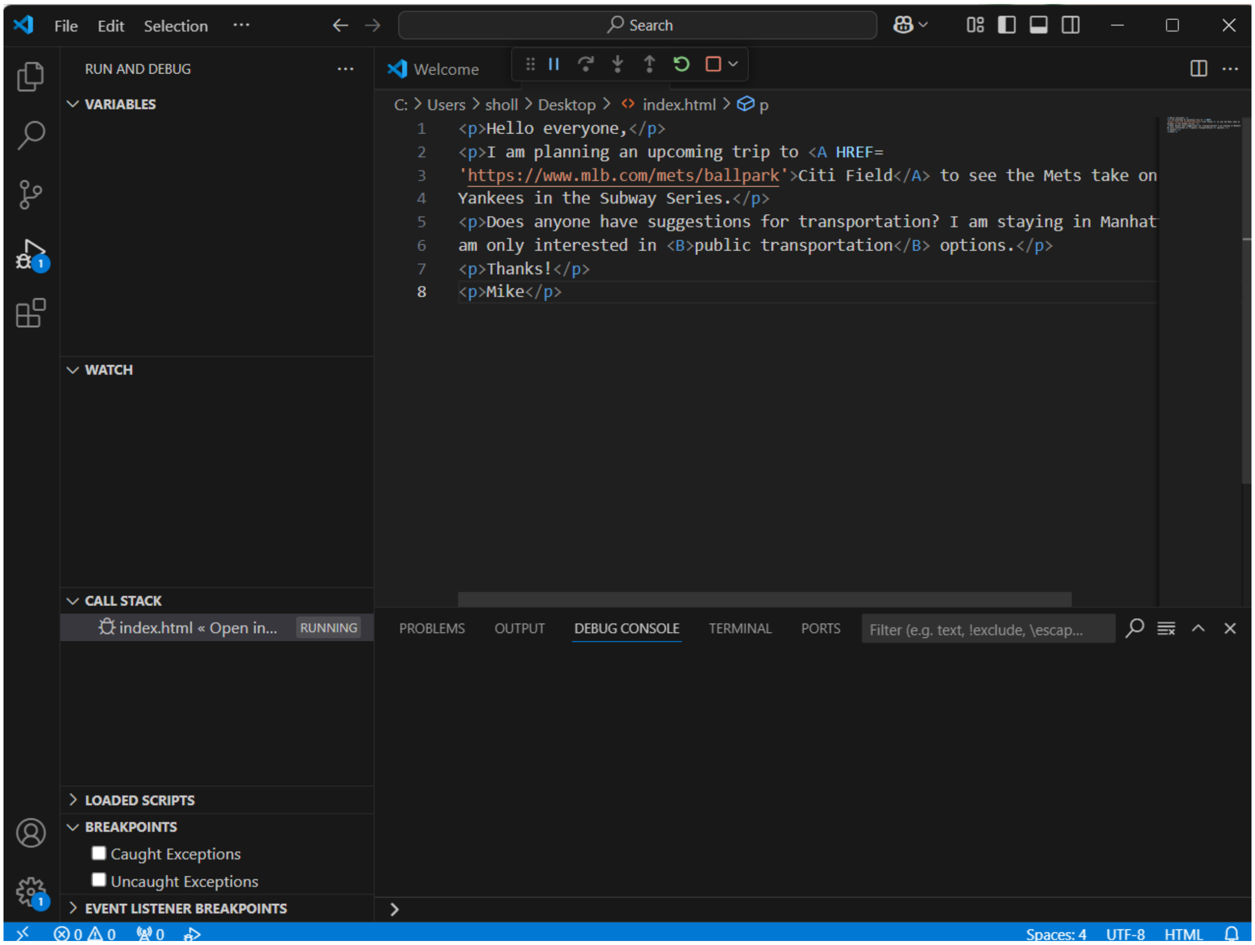
Cat

The cat (Felis catus), also referred to as the domestic cat or house cat, is **a small domesticated carnivorous mammal**. It is the only domesticated species of ...

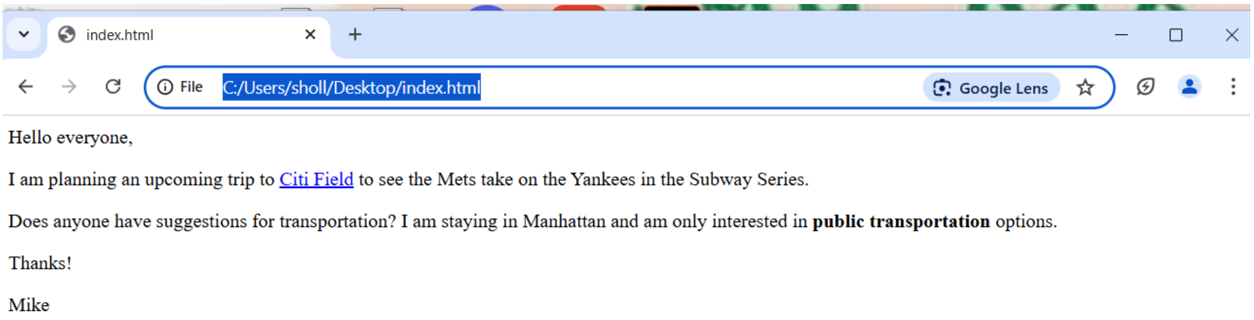
Human interaction with cats | List of cat breeds | Islam and cats | Felis

Cat
Animal

Activity 2: Creating a Cross-Site Scripting Vulnerability



```
<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
Yankees in the Subway Series.</p>
<p>Does anyone have suggestions for transportation? I am staying in Manhat
am only interested in <B>public transportation</B> options.</p>
<p>Thanks!</p>
<p>Mike</p>
```



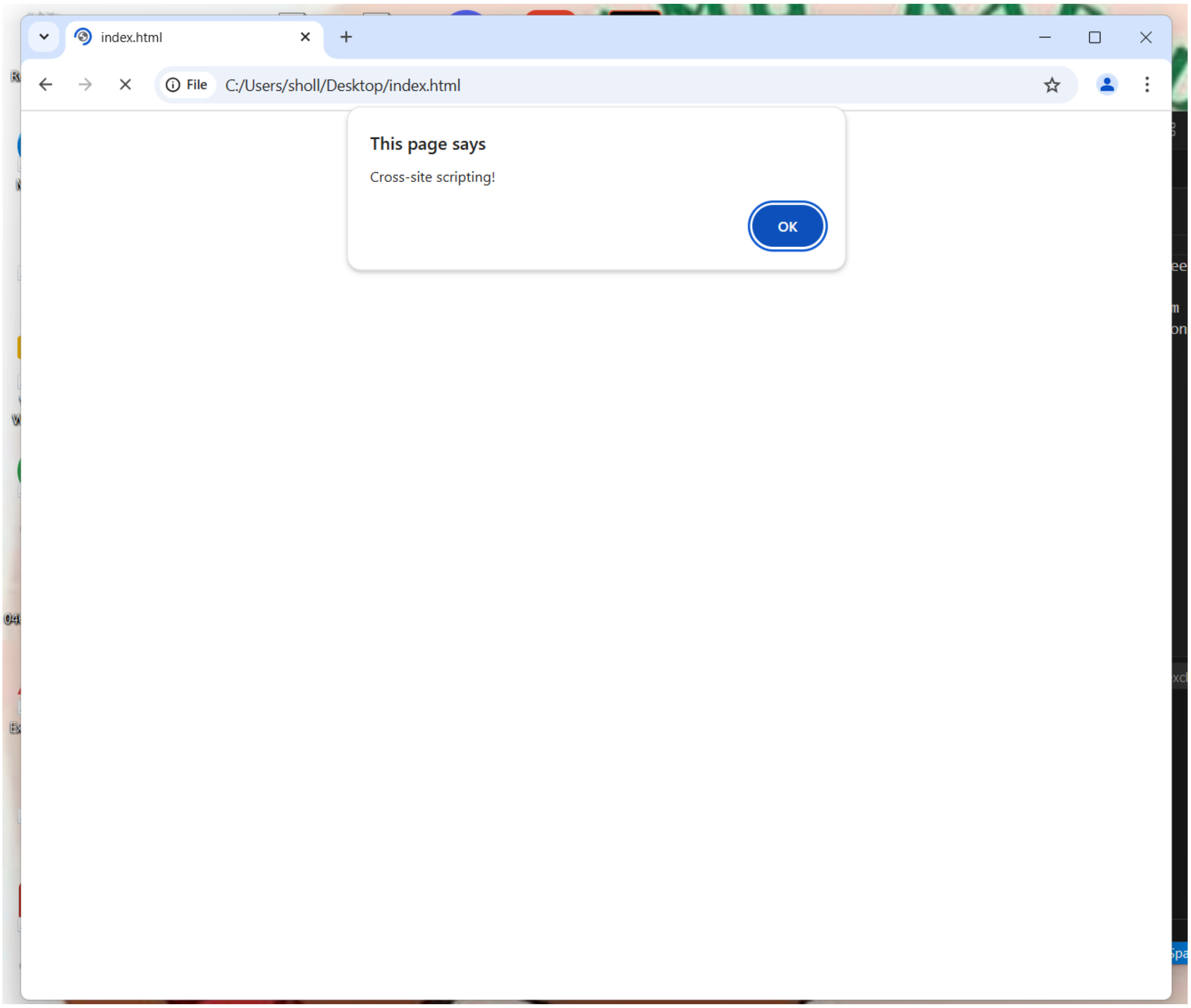
Hello everyone,

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.

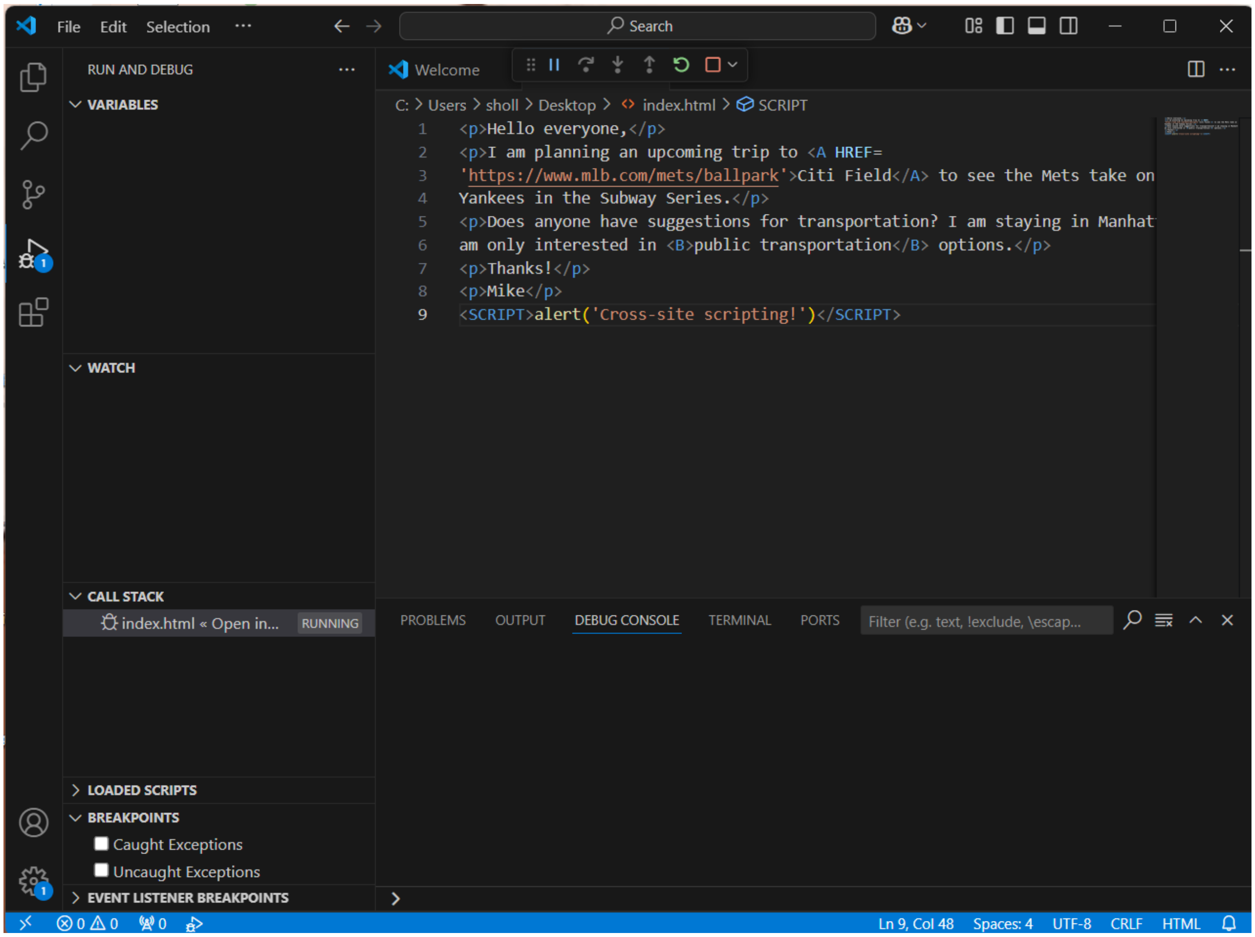
Thanks!

Mike



This page says

Cross-site scripting!



☐ Caught Exceptions

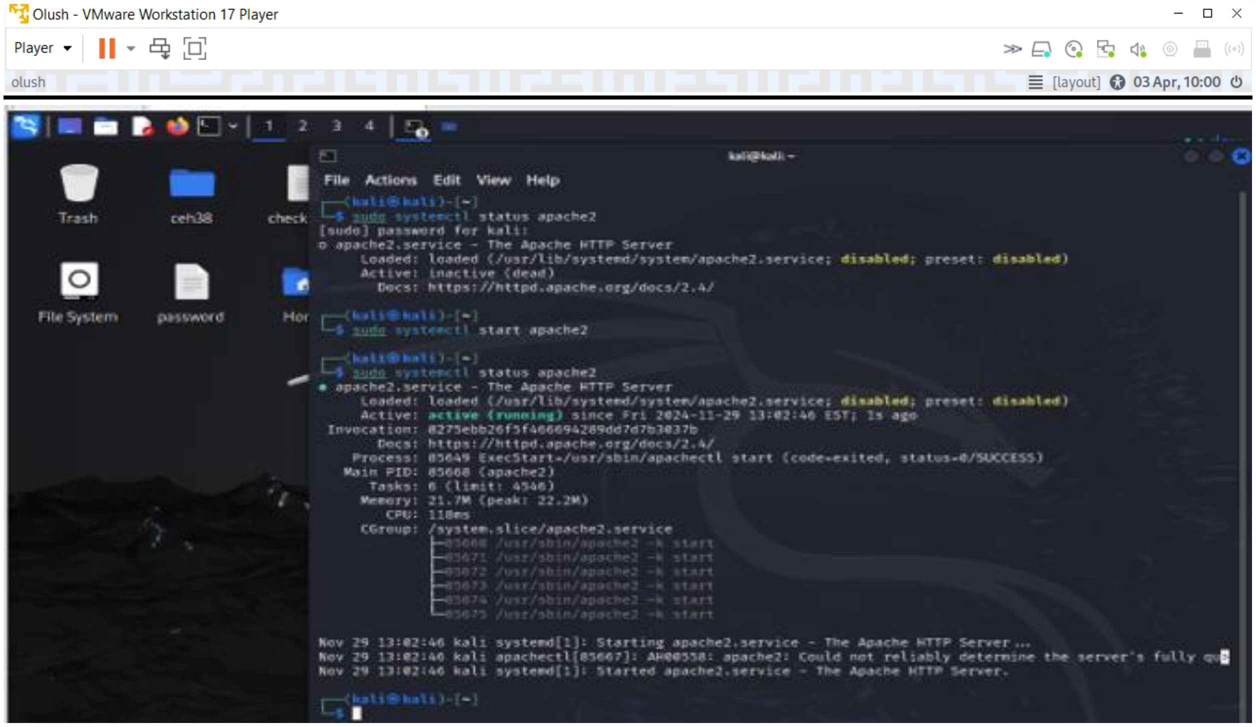
☐ Uncaught Exceptions

```
<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
Yankees in the Subway Series.</p>
<p>Does anyone have suggestions for transportation? I am staying in Manhat
am only interested in <B>public transportation</B> options.</p>
<p>Thanks!</p>
<p>Mike</p>
<SCRIPT>alert('Cross-site scripting!')</SCRIPT>
```

Did you see the impact of your cross-site scripting attack? Yes.

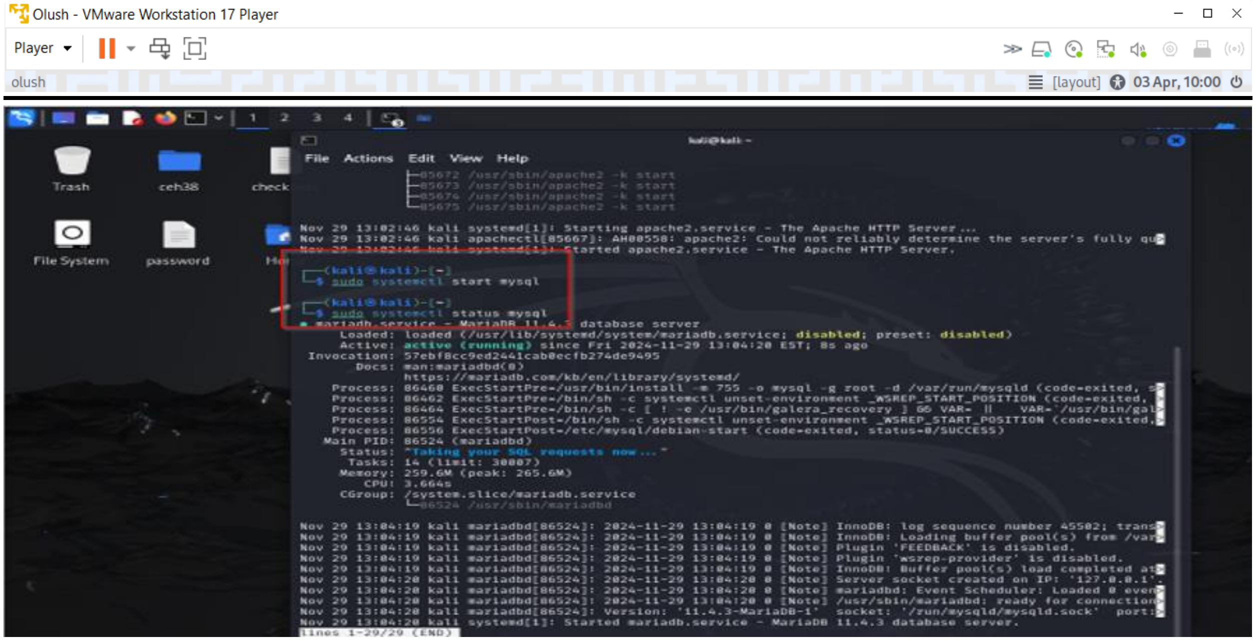
Activtiy#3: Exploiting Insecure Direct Object Reference (URL Manipulation)

Apache started and running:



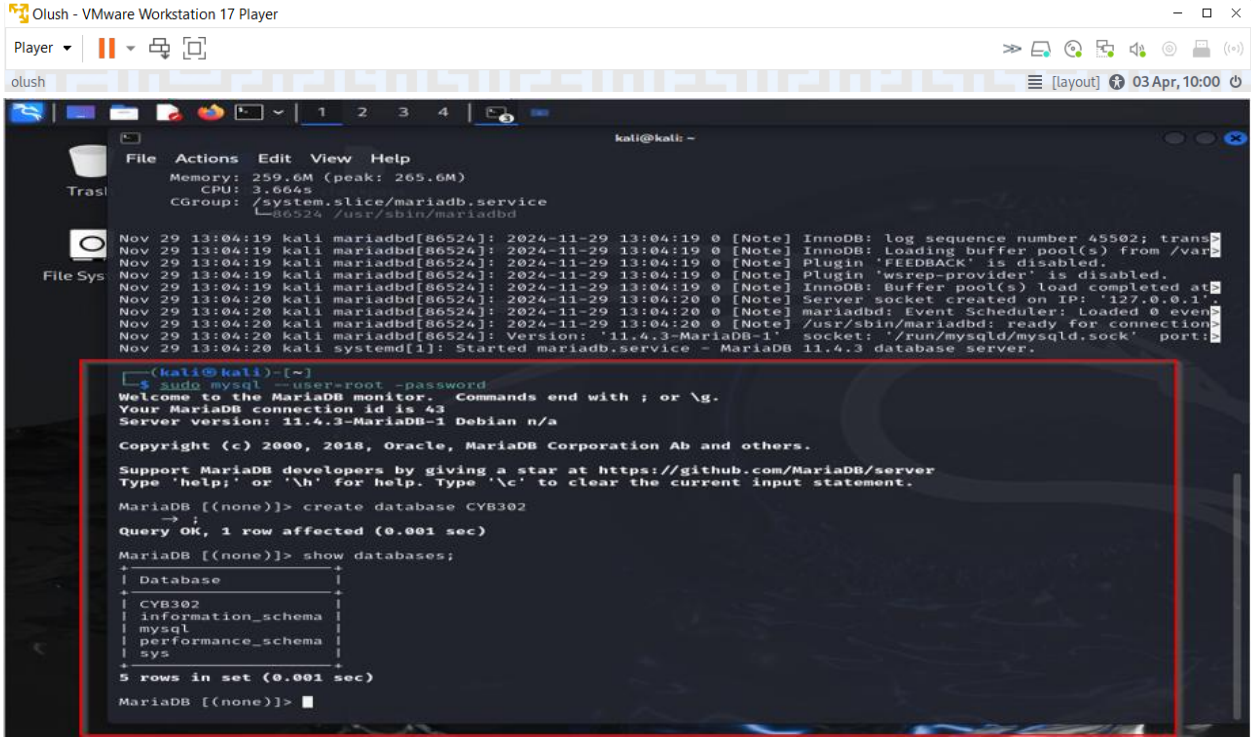
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status apache2
[sudo] password for kali:
○ apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: https://httpd.apache.org/docs/2.4/

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start apache2

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Fri 2024-11-29 13:02:46 EST; 1s ago
 Invocation: 0275ebb26f5f466694289dd7d7b3037b
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 85649 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 85668 (apache2)
      Tasks: 6 (limit: 4546)
     Memory: 21.7M (peak: 22.2M)
        CPU: 118ms
     CGroup: /system.slice/apache2.service
             ├─85668 /usr/sbin/apache2 -k start
             ├─85671 /usr/sbin/apache2 -k start
             ├─85672 /usr/sbin/apache2 -k start
             ├─85673 /usr/sbin/apache2 -k start
             ├─85674 /usr/sbin/apache2 -k start
             └─85675 /usr/sbin/apache2 -k start

Nov 29 13:02:46 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 29 13:02:46 kali apachectl[85667]: AH00558: apache2: Could not reliably determine the server's fully qu
Nov 29 13:02:46 kali systemd[1]: Started apache2.service - The Apache HTTP Server.

┌──(kali㉿kali)-[~]
└─$ 
```

Mysql started and Runing in kali:



```
             ├─85672 /usr/sbin/apache2 -k start
             ├─85673 /usr/sbin/apache2 -k start
             ├─85674 /usr/sbin/apache2 -k start
             └─85675 /usr/sbin/apache2 -k start

Nov 29 13:02:46 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 29 13:02:46 kali apachectl[85667]: AH00558: apache2: Could not reliably determine the server's fully qu
Nov 29 13:02:46 kali systemd[1]: Started apache2.service - The Apache HTTP Server.

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start mysql

┌──(kali㉿kali)-[~]
└─$ sudo 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 Fri 2024-11-29 13:04:20 EST; 8s ago
 Invocation: 57ebf8cc9ed2441cab0ecfb274de9495
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
    Process: 86460 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, s
    Process: 86462 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited,
    Process: 86464 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||   VAR=`/usr/bin/gal
    Process: 86554 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited,
    Process: 86556 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
   Main PID: 86524 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 14 (limit: 30007)
     Memory: 259.6M (peak: 265.6M)
        CPU: 3.664s
     CGroup: /system.slice/mariadb.service
             └─86524 /usr/sbin/mariadbd

Nov 29 13:04:19 kali mariadbd[86524]: 2024-11-29 13:04:19 0 [Note] InnoDB: log sequence number 45502; trans
Nov 29 13:04:19 kali mariadbd[86524]: 2024-11-29 13:04:19 0 [Note] InnoDB: Loading buffer pool(s) from /var
Nov 29 13:04:19 kali mariadbd[86524]: 2024-11-29 13:04:19 0 [Note] Plugin 'FEEDBACK' is disabled.
Nov 29 13:04:19 kali mariadbd[86524]: 2024-11-29 13:04:19 0 [Note] Plugin 'wsrep-provider' is disabled.
Nov 29 13:04:19 kali mariadbd[86524]: 2024-11-29 13:04:19 0 [Note] InnoDB: Buffer pool(s) load completed at
Nov 29 13:04:20 kali mariadbd[86524]: 2024-11-29 13:04:20 0 [Note] Server socket created on IP: '127.0.0.1'.
Nov 29 13:04:20 kali mariadbd[86524]: 2024-11-29 13:04:20 0 [Note] mariadbd: Event Scheduler: Loaded 0 even
Nov 29 13:04:20 kali mariadbd[86524]: 2024-11-29 13:04:20 0 [Note] /usr/sbin/mariadbd: ready for connection
Nov 29 13:04:20 kali mariadbd[86524]: Version: '11.4.3-MariaDB-1'  socket: '/run/mysqld/mysqld.sock'  port:
Nov 29 13:04:20 kali systemd[1]: Started mariadb.service - MariaDB 11.4.3 database server.
lines 1-29/29 (END)
```

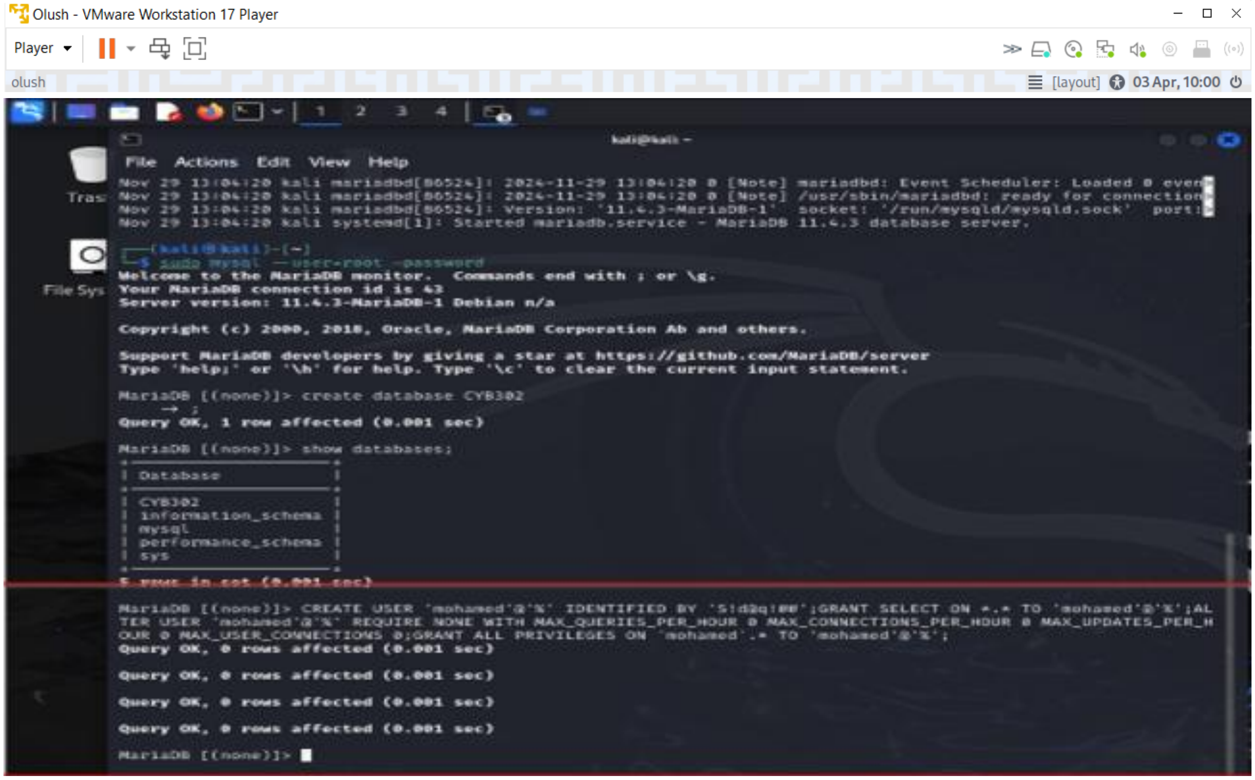
Database created in mysql:



Olush - VMware Workstation 17 Player
Player
olush
[layout]
03 Apr, 10:00
File Sys
kali@kali: ~
File Actions Edit View Help

```
         Memory: 259.6M (peak: 265.6M)
            CPU: 3.664s
         CGroup: /system.slice/mariadb.service
                 └─86524 /usr/sbin/mariadbd

Nov 29 13:04:19 kali mariadbd[86524]: 2024-11-29 13:04:19 0 [Note] InnoDB: log sequence number 45502; trans>
Nov 29 13:04:19 kali mariadbd[86524]: 2024-11-29 13:04:19 0 [Note] InnoDB: Loading buffer pool(s) from /var>
Nov 29 13:04:19 kali mariadbd[86524]: 2024-11-29 13:04:19 0 [Note] Plugin 'FEEDBACK' is disabled.
Nov 29 13:04:19 kali mariadbd[86524]: 2024-11-29 13:04:19 0 [Note] Plugin 'wsrep-provider' is disabled.
Nov 29 13:04:19 kali mariadbd[86524]: 2024-11-29 13:04:19 0 [Note] InnoDB: Buffer pool(s) load completed at>
Nov 29 13:04:20 kali mariadbd[86524]: 2024-11-29 13:04:20 0 [Note] Server socket created on IP: '127.0.0.1'.
Nov 29 13:04:20 kali mariadbd[86524]: 2024-11-29 13:04:20 0 [Note] mariadbd: Event Scheduler: Loaded 0 even>
Nov 29 13:04:20 kali mariadbd[86524]: 2024-11-29 13:04:20 0 [Note] /usr/sbin/mariadbd: ready for connection>
Nov 29 13:04:20 kali mariadbd[86524]: Version: '11.4.3-MariaDB-1'  socket: '/run/mysqld/mysqld.sock'  port:>
Nov 29 13:04:20 kali systemd[1]: Started mariadb.service - MariaDB 11.4.3 database server.

┌──(kali㉿kali)-[~]
└─$ sudo mysql --user=root -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 databases;
+--------------------+
| Database           |
+--------------------+
| CYB302             |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.001 sec)

MariaDB [(none)]> █
```

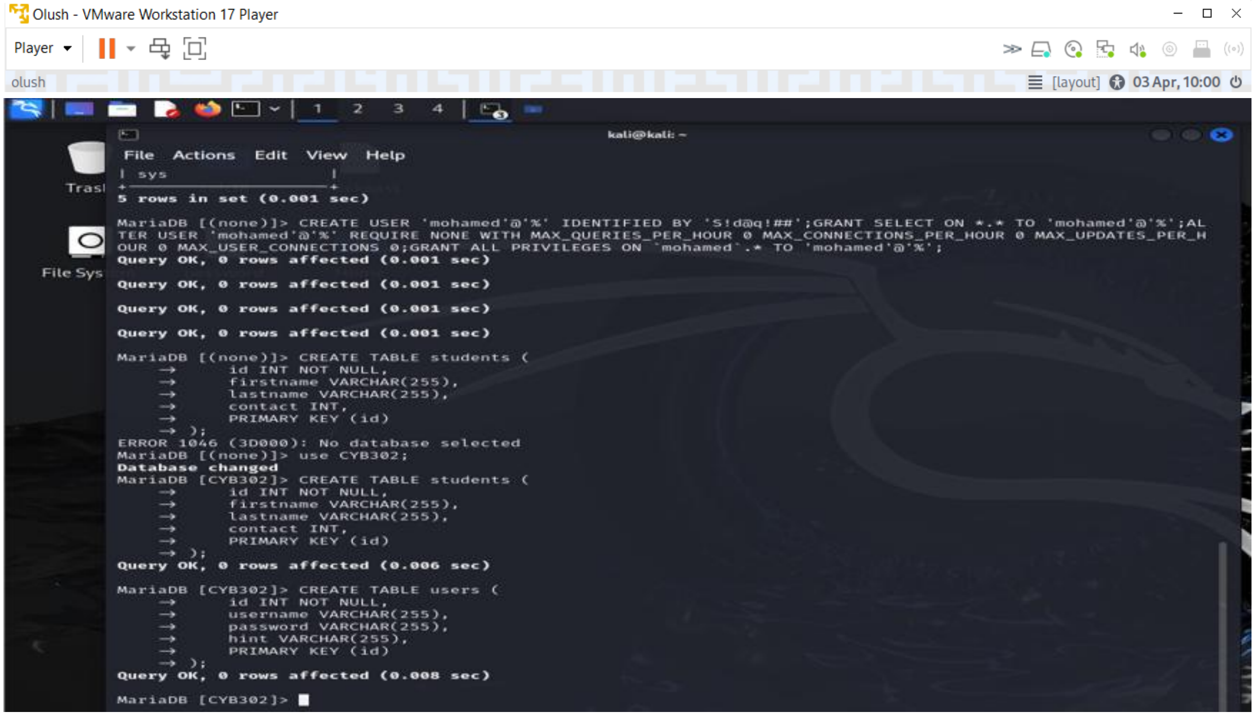
User (mohamed') and privilege created:



Olush - VMware Workstation 17 Player
Player
olush
[layout]
03 Apr, 10:00
File Sys
kali@kali: ~
File Actions Edit View Help

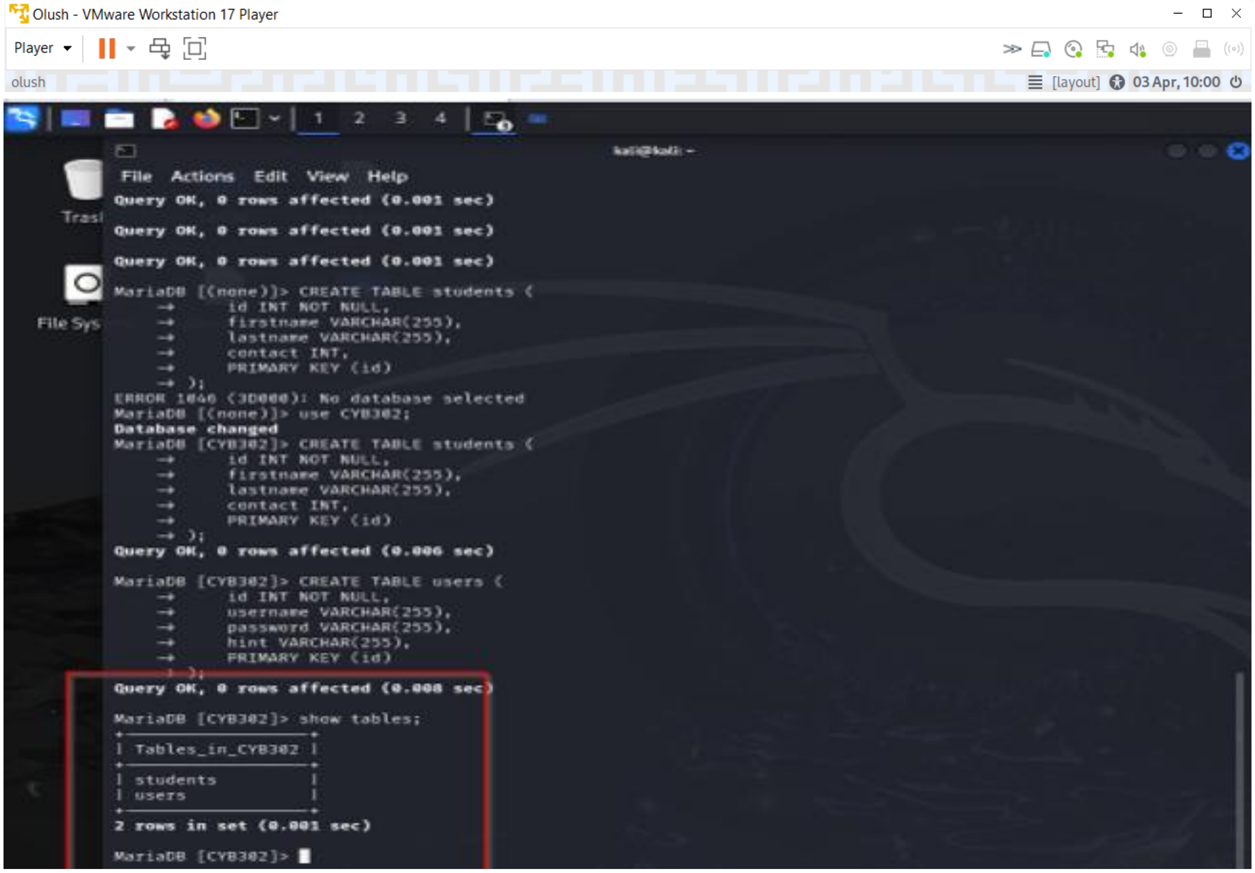
```
Nov 29 13:04:20 kali mariadbd[86524]: 2024-11-29 13:04:20 0 [Note] mariadbd: Event Scheduler: Loaded 0 even>
Nov 29 13:04:20 kali mariadbd[86524]: 2024-11-29 13:04:20 0 [Note] /usr/sbin/mariadbd: ready for connection>
Nov 29 13:04:20 kali mariadbd[86524]: Version: '11.4.3-MariaDB-1'  socket: '/run/mysqld/mysqld.sock'  port:>
Nov 29 13:04:20 kali systemd[1]: Started mariadb.service - MariaDB 11.4.3 database server.

┌──(kali㉿kali)-[~]
└─$ sudo mysql --user=root -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 databases;
+--------------------+
| Database           |
+--------------------+
| CYB302             |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.001 sec)

MariaDB [(none)]> CREATE USER 'mohamed'@'%' IDENTIFIED BY 'S!d2q!##';GRANT SELECT ON *.* TO 'mohamed'@'%';AL
TER USER 'mohamed'@'%' REQUIRE NONE WITH MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_H
OUR 0 MAX_USER_CONNECTIONS 0;GRANT ALL PRIVILEGES ON `mohamed`.* TO 'mohamed'@'%';
Query OK, 0 rows affected (0.001 sec)

Query OK, 0 rows affected (0.001 sec)

Query OK, 0 rows affected (0.001 sec)

Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> █
```

Table “student” & “user” created on CYB302 databse:



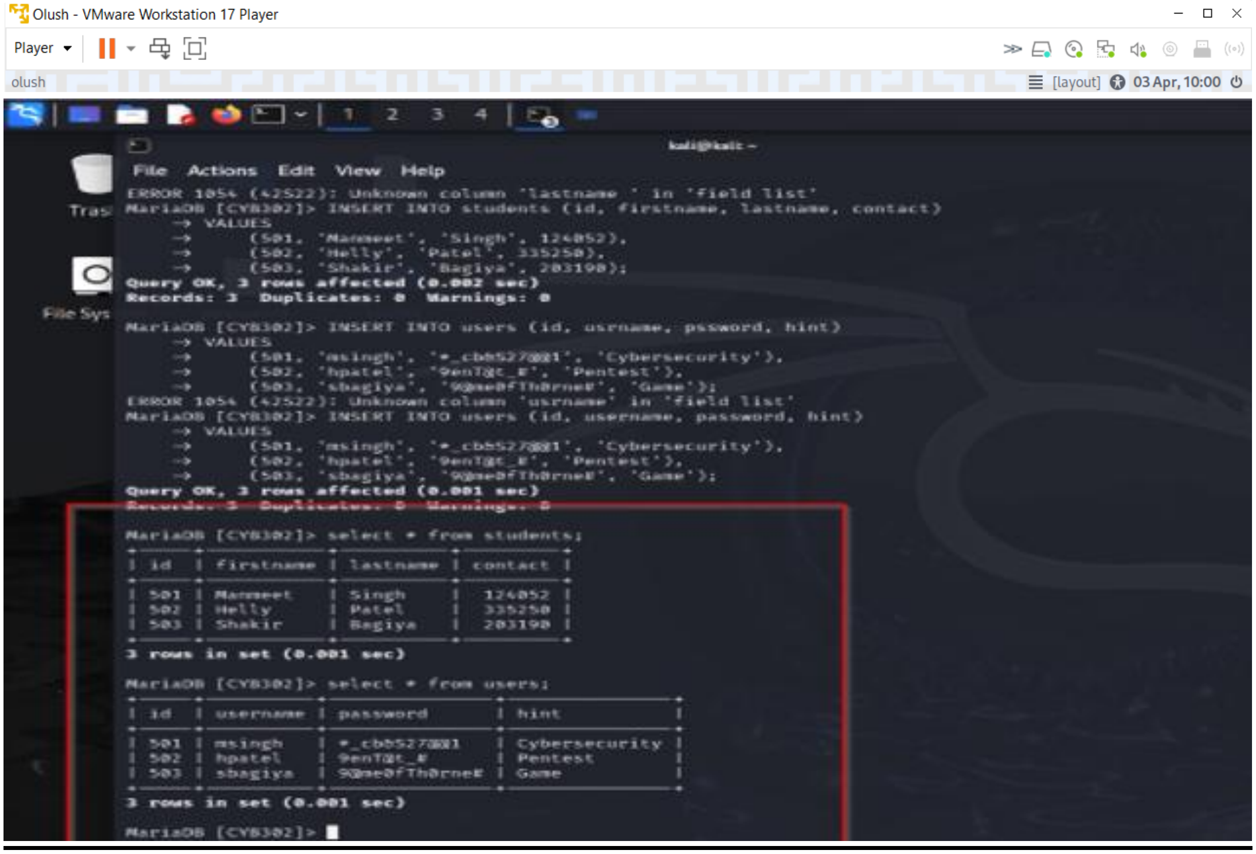
```
| sys                |
+--------------------+
5 rows in set (0.001 sec)

MariaDB [(none)]> CREATE USER 'mohamed'@'%' IDENTIFIED BY 'S!d@q!##';GRANT SELECT ON *.* TO 'mohamed'@'%';AL
TER USER 'mohamed'@'%' REQUIRE NONE WITH MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_H
OUR 0 MAX_USER_CONNECTIONS 0;GRANT ALL PRIVILEGES ON `mohamed`.* TO 'mohamed'@'%';
Query OK, 0 rows affected (0.001 sec)

Query OK, 0 rows affected (0.001 sec)

Query OK, 0 rows affected (0.001 sec)

Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> CREATE TABLE students (
    →       id INT NOT NULL,
    →       firstname VARCHAR(255),
    →       lastname VARCHAR(255),
    →       contact INT,
    →       PRIMARY KEY (id)
    → );
ERROR 1046 (3D000): No database selected
MariaDB [(none)]> use CYB302;
Database changed
MariaDB [CYB302]> CREATE TABLE students (
    →       id INT NOT NULL,
    →       firstname VARCHAR(255),
    →       lastname VARCHAR(255),
    →       contact INT,
    →       PRIMARY KEY (id)
    → );
Query OK, 0 rows affected (0.006 sec)

MariaDB [CYB302]> CREATE TABLE users (
    →       id INT NOT NULL,
    →       username VARCHAR(255),
    →       password VARCHAR(255),
    →       hint VARCHAR(255),
    →       PRIMARY KEY (id)
    → );
Query OK, 0 rows affected (0.008 sec)

MariaDB [CYB302]> █
```

<u>Showing created tables: students & user:</u>



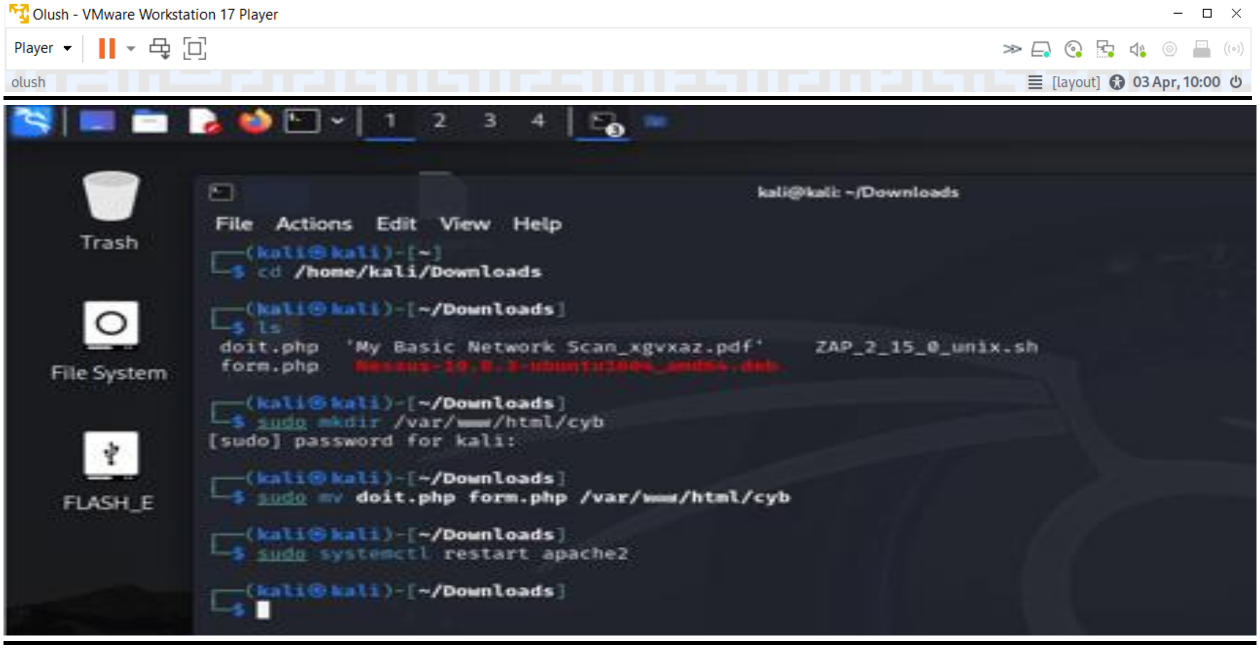
```
Query OK, 0 rows affected (0.001 sec)

Query OK, 0 rows affected (0.001 sec)

Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> CREATE TABLE students (
    →       id INT NOT NULL,
    →       firstname VARCHAR(255),
    →       lastname VARCHAR(255),
    →       contact INT,
    →       PRIMARY KEY (id)
    → );
ERROR 1046 (3D000): No database selected
MariaDB [(none)]> use CYB302;
Database changed
MariaDB [CYB302]> CREATE TABLE students (
    →       id INT NOT NULL,
    →       firstname VARCHAR(255),
    →       lastname VARCHAR(255),
    →       contact INT,
    →       PRIMARY KEY (id)
    → );
Query OK, 0 rows affected (0.006 sec)

MariaDB [CYB302]> CREATE TABLE users (
    →       id INT NOT NULL,
    →       username VARCHAR(255),
    →       password VARCHAR(255),
    →       hint VARCHAR(255),
    →       PRIMARY KEY (id)
    → );
Query OK, 0 rows affected (0.008 sec)

MariaDB [CYB302]> show tables;
+------------------+
| Tables_in_CYB302 |
+------------------+
| students         |
| users            |
+------------------+
2 rows in set (0.001 sec)

MariaDB [CYB302]> 
```

<u>Insert some data into the “students” table and the “users” table:</u>


Olush - VMware Workstation 17 Player
Player
olush
[layout]
03 Apr, 10:00
Trash
File Sys
kali@kali: ~
File Actions Edit View Help

```
ERROR 1054 (42S22): Unknown column 'lastname ' in 'field list'
MariaDB [CYB302]> INSERT INTO students (id, firstname, lastname, contact)
    -> VALUES
    ->      (501, 'Manmeet', 'Singh', 124052),
    ->      (502, 'Helly', 'Patel', 335250),
    ->      (503, 'Shakir', 'Bagiya', 203198);
Query OK, 3 rows affected (0.002 sec)
Records: 3  Duplicates: 0  Warnings: 0

MariaDB [CYB302]> INSERT INTO users (id, usrname, pssword, hint)
    -> VALUES
    ->      (501, 'msingh', '*_cb0527@@1', 'Cybersecurity'),
    ->      (502, 'hpatel', '9enT@t_E', 'Pentest'),
    ->      (503, 'sbagiya', '9@me0fTh0rne#', 'Game');
ERROR 1054 (42S22): Unknown column 'usrname' in 'field list'
MariaDB [CYB302]> INSERT INTO users (id, username, password, hint)
    -> VALUES
    ->      (501, 'msingh', '*_cb0527@@1', 'Cybersecurity'),
    ->      (502, 'hpatel', '9enT@t_E', 'Pentest'),
    ->      (503, 'sbagiya', '9@me0fTh0rne#', 'Game');
Query OK, 3 rows affected (0.001 sec)
Records: 3  Duplicates: 0  Warnings: 0

MariaDB [CYB302]> select * from students;
+-----+-----------+----------+---------+
| id  | firstname | lastname | contact |
+-----+-----------+----------+---------+
| 501 | Manmeet   | Singh    |  124052 |
| 502 | Helly     | Patel    |  335250 |
| 503 | Shakir    | Bagiya   |  203198 |
+-----+-----------+----------+---------+
3 rows in set (0.001 sec)

MariaDB [CYB302]> select * from users;
+-----+----------+---------------+---------------+
| id  | username | password      | hint          |
+-----+----------+---------------+---------------+
| 501 | msingh   | *_cb0527@@1   | Cybersecurity |
| 502 | hpatel   | 9enT@t_#      | Pentest       |
| 503 | sbagiya  | 9@me0fTh0rne# | Game          |
+-----+----------+---------------+---------------+
3 rows in set (0.001 sec)

MariaDB [CYB302]> 
```

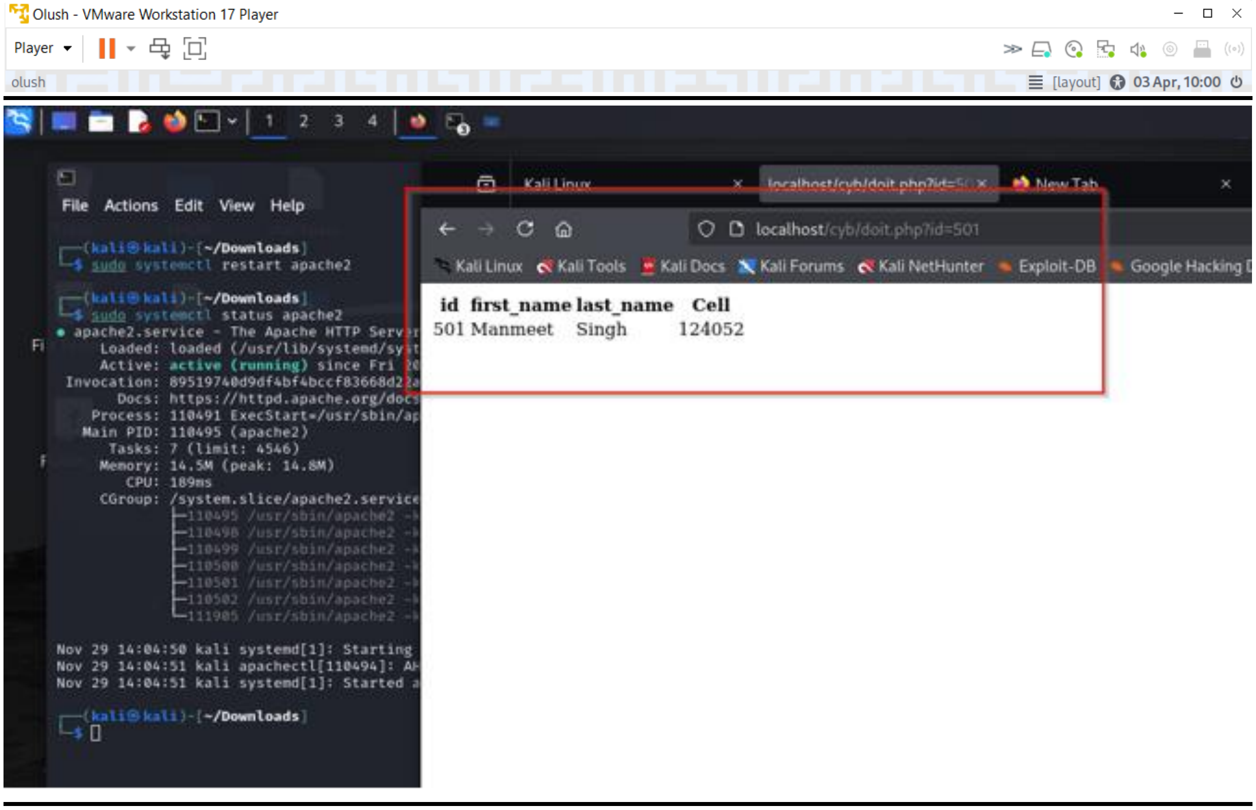
Downloading files and setting apache webserver:



```
┌──(kali㉿kali)-[~]
└─$ cd /home/kali/Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
 doit.php  'My Basic Network Scan_xgvxaz.pdf'    ZAP_2_15_0_unix.sh
 form.php   Nessus-10.8.3-ubuntu1604_amd64.deb

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo mkdir /var/www/html/cyb
[sudo] password for kali:

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo mv doit.php form.php /var/www/html/cyb

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl restart apache2

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

URL Manipulation:

Accessing localhost/cyb/form.php and inserting 501 to view user:



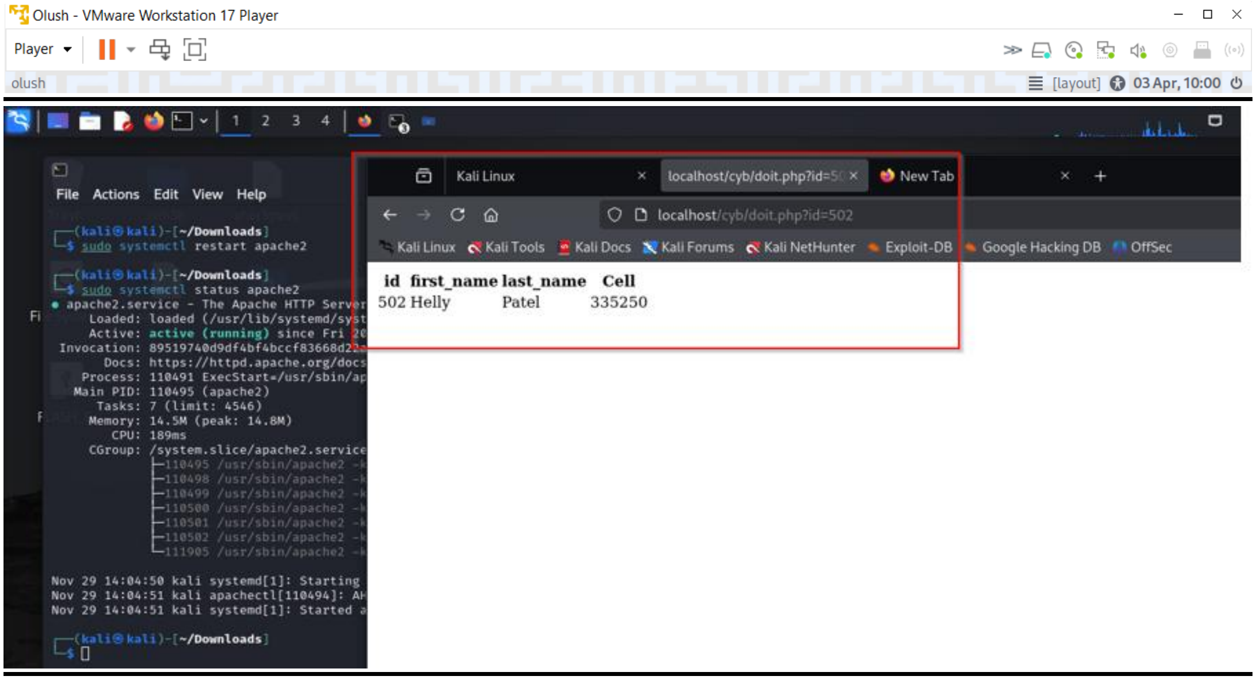
Olush - VMware Workstation 17 Player
Player
olush
[layout]
03 Apr, 10:00
File Actions Edit View Help
Kali Linux
localhost/cyb/doit.php?id=50
New Tab
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking D

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl restart apache2

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Serv
     Loaded: loaded (/usr/lib/systemd/syst
     Active: active (running) since Fri 20
 Invocation: 89519740d9df4bf4bccf83668d22a
       Docs: https://httpd.apache.org/doc
    Process: 110491 ExecStart=/usr/sbin/ap
   Main PID: 110495 (apache2)
      Tasks: 7 (limit: 4546)
     Memory: 14.5M (peak: 14.8M)
        CPU: 189ms
     CGroup: /system.slice/apache2.service
             ├─110495 /usr/sbin/apache2 -k
             ├─110498 /usr/sbin/apache2 -k
             ├─110499 /usr/sbin/apache2 -k
             ├─110500 /usr/sbin/apache2 -k
             ├─110501 /usr/sbin/apache2 -k
             ├─110502 /usr/sbin/apache2 -k
             └─111905 /usr/sbin/apache2 -k

Nov 29 14:04:50 kali systemd[1]: Starting
Nov 29 14:04:51 kali apachectl[110494]: AH
Nov 29 14:04:51 kali systemd[1]: Started a

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

localhost/cyb/doit.php?id=501

```
id  first_name last_name   Cell
501 Manmeet    Singh       124052
```

Accessing localhost/cyb/form.php and inserting 502 to view user:



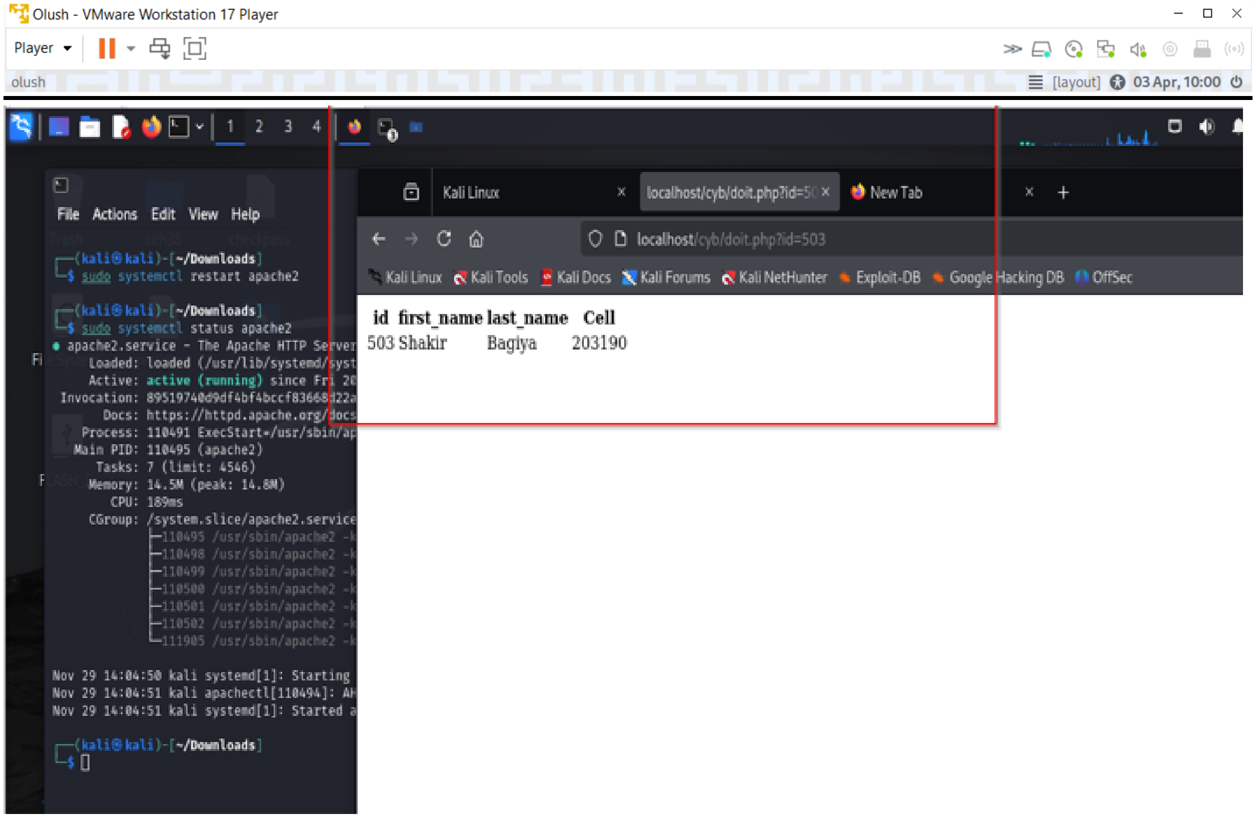
Olush - VMware Workstation 17 Player
Player
olush
[layout]
03 Apr, 10:00
File Actions Edit View Help
Kali Linux
localhost/cyb/doit.php?id=50
New Tab
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl restart apache2

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/syst
     Active: active (running) since Fri 20
 Invocation: 89519740d9df4bf4bccf83668d2
       Docs: https://httpd.apache.org/docs
    Process: 110491 ExecStart=/usr/sbin/ap
   Main PID: 110495 (apache2)
      Tasks: 7 (limit: 4546)
     Memory: 14.5M (peak: 14.8M)
        CPU: 189ms
     CGroup: /system.slice/apache2.service
             ├─110495 /usr/sbin/apache2 -k
             ├─110498 /usr/sbin/apache2 -k
             ├─110499 /usr/sbin/apache2 -k
             ├─110500 /usr/sbin/apache2 -k
             ├─110501 /usr/sbin/apache2 -k
             ├─110502 /usr/sbin/apache2 -k
             └─111905 /usr/sbin/apache2 -k

Nov 29 14:04:50 kali systemd[1]: Starting
Nov 29 14:04:51 kali apachectl[110494]: AH
Nov 29 14:04:51 kali systemd[1]: Started a

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

localhost/cyb/doit.php?id=502

```
id  first_name last_name  Cell
502 Helly      Patel      335250
```

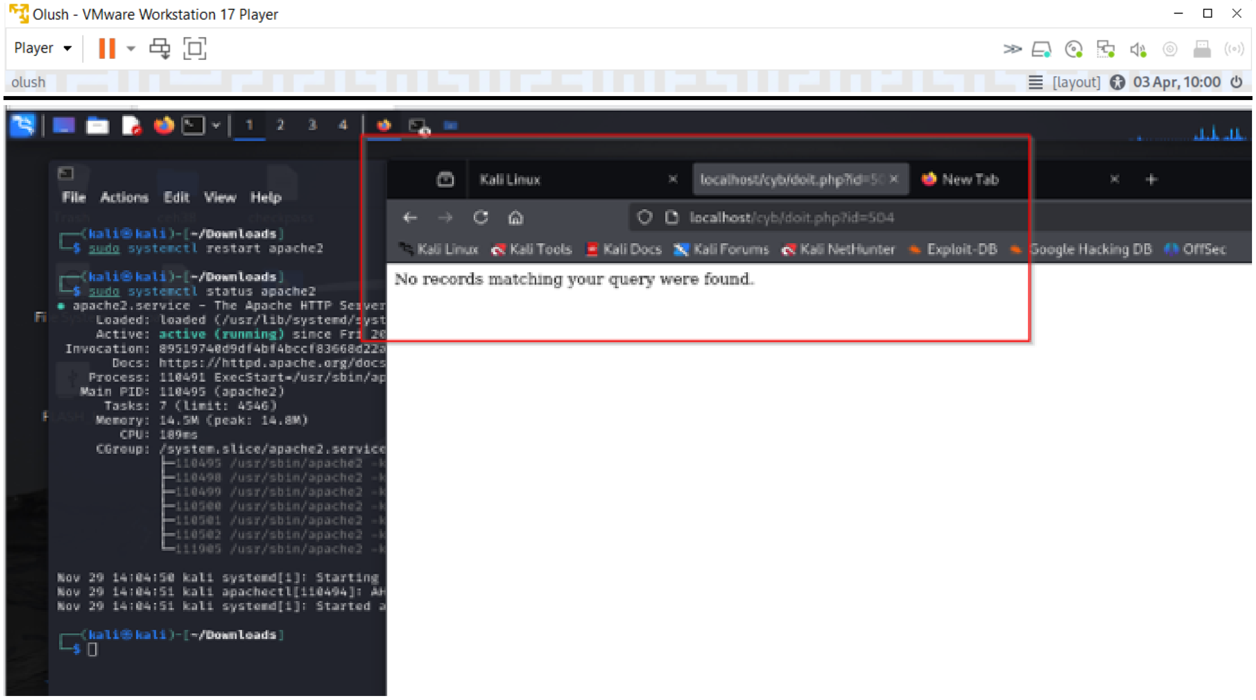
Accessing localhost/cyb/form.php and inserting 503 to view user:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl restart apache2

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/syst
     Active: active (running) since Fri 20
 Invocation: 89519740d9df4bf4bccf83668d22a
       Docs: https://httpd.apache.org/docs
    Process: 110491 ExecStart=/usr/sbin/ap
   Main PID: 110495 (apache2)
      Tasks: 7 (limit: 4546)
     Memory: 14.5M (peak: 14.8M)
        CPU: 189ms
     CGroup: /system.slice/apache2.service
             ├─110495 /usr/sbin/apache2 -k
             ├─110498 /usr/sbin/apache2 -k
             ├─110499 /usr/sbin/apache2 -k
             ├─110500 /usr/sbin/apache2 -k
             ├─110501 /usr/sbin/apache2 -k
             ├─110502 /usr/sbin/apache2 -k
             └─111905 /usr/sbin/apache2 -k

Nov 29 14:04:50 kali systemd[1]: Starting
Nov 29 14:04:51 kali apachectl[110494]: AH
Nov 29 14:04:51 kali systemd[1]: Started a

┌──(kali㉿kali)-[~/Downloads]
└─$ ▯
```

id	first_name	last_name	Cell
503	Shakir	Bagiya	203190

Acessing localhost/cyb/form.php and inserting 504 to view user:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl restart apache2

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/syst
     Active: active (running) since Fri 20
 Invocation: 89519740d9df4bf4bccf83668d22a
       Docs: https://httpd.apache.org/docs
    Process: 110491 ExecStart=/usr/sbin/ap
   Main PID: 110495 (apache2)
      Tasks: 7 (limit: 4546)
     Memory: 14.5M (peak: 14.8M)
        CPU: 189ms
     CGroup: /system.slice/apache2.service
             ├─110495 /usr/sbin/apache2 -k
             ├─110498 /usr/sbin/apache2 -k
             ├─110499 /usr/sbin/apache2 -k
             ├─110500 /usr/sbin/apache2 -k
             ├─110501 /usr/sbin/apache2 -k
             ├─110502 /usr/sbin/apache2 -k
             └─111905 /usr/sbin/apache2 -k

Nov 29 14:04:50 kali systemd[1]: Starting
Nov 29 14:04:51 kali apachectl[110494]: AH
Nov 29 14:04:51 kali systemd[1]: Started a

┌──(kali㉿kali)-[~/Downloads]
└─$ ▯
```

No records matching your query were found.