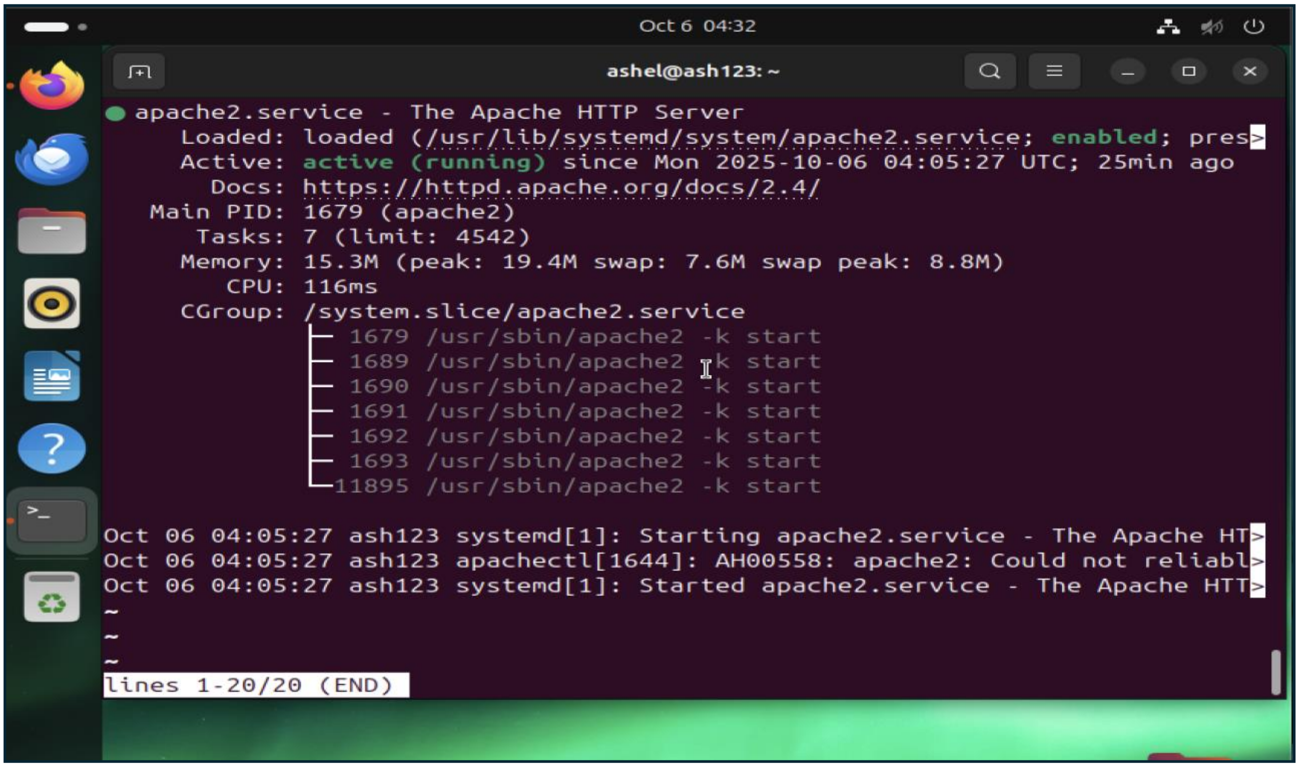
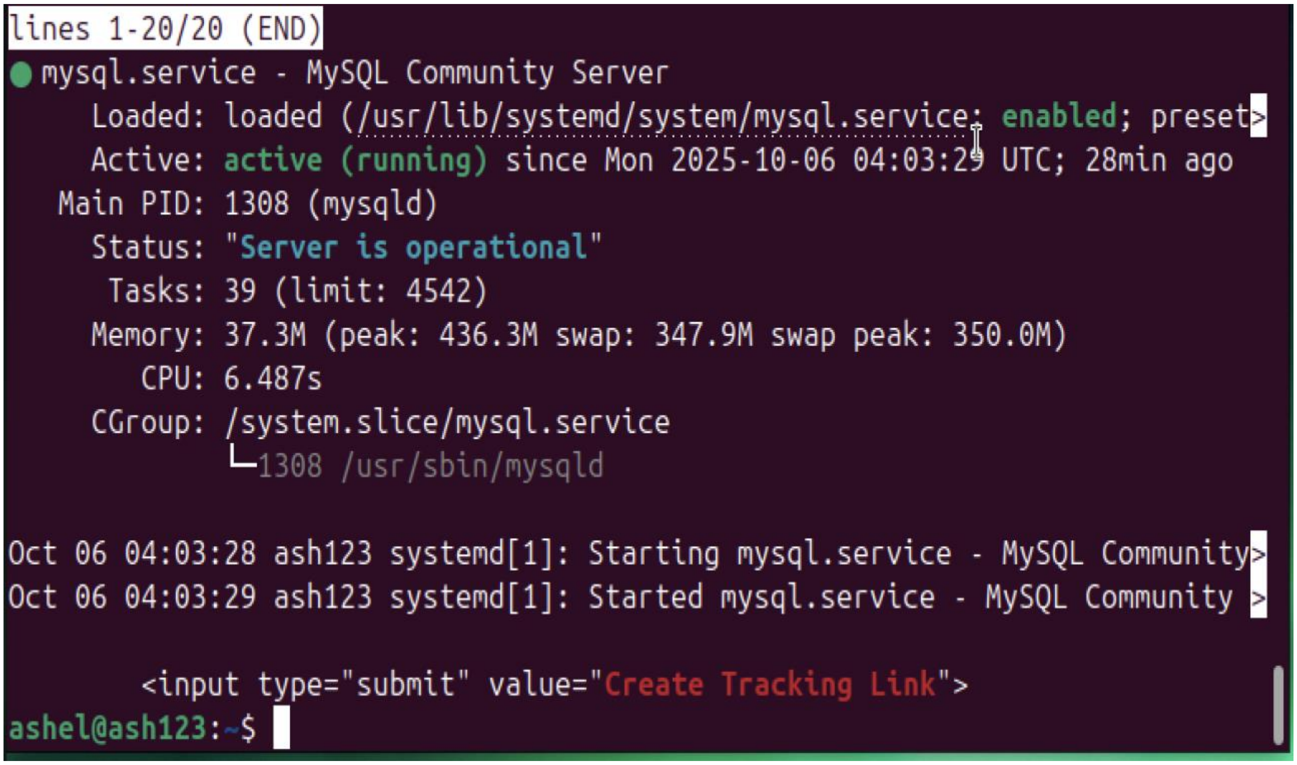
Screen shots for intruder detection alert system.

Current System Status Check

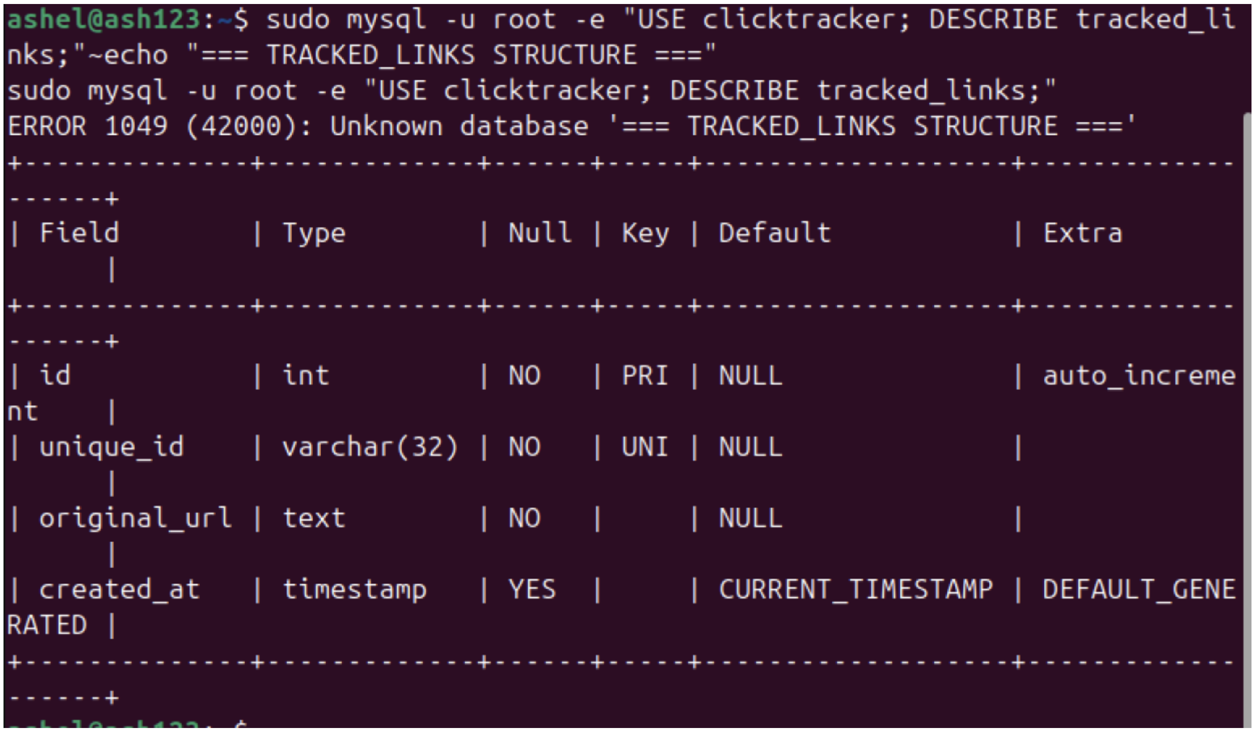


```
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; pres>
     Active: active (running) since Mon 2025-10-06 04:05:27 UTC; 25min ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 1679 (apache2)
      Tasks: 7 (limit: 4542)
     Memory: 15.3M (peak: 19.4M swap: 7.6M swap peak: 8.8M)
        CPU: 116ms
     CGroup: /system.slice/apache2.service
             ├─ 1679 /usr/sbin/apache2 -k start
             ├─ 1689 /usr/sbin/apache2 -k start
             ├─ 1690 /usr/sbin/apache2 -k start
             ├─ 1691 /usr/sbin/apache2 -k start
             ├─ 1692 /usr/sbin/apache2 -k start
             ├─ 1693 /usr/sbin/apache2 -k start
             └─11895 /usr/sbin/apache2 -k start

Oct 06 04:05:27 ash123 systemd[1]: Starting apache2.service - The Apache HT>
Oct 06 04:05:27 ash123 apachectl[1644]: AH00558: apache2: Could not reliabl>
Oct 06 04:05:27 ash123 systemd[1]: Started apache2.service - The Apache HTT>
~
~
~
lines 1-20/20 (END)
```

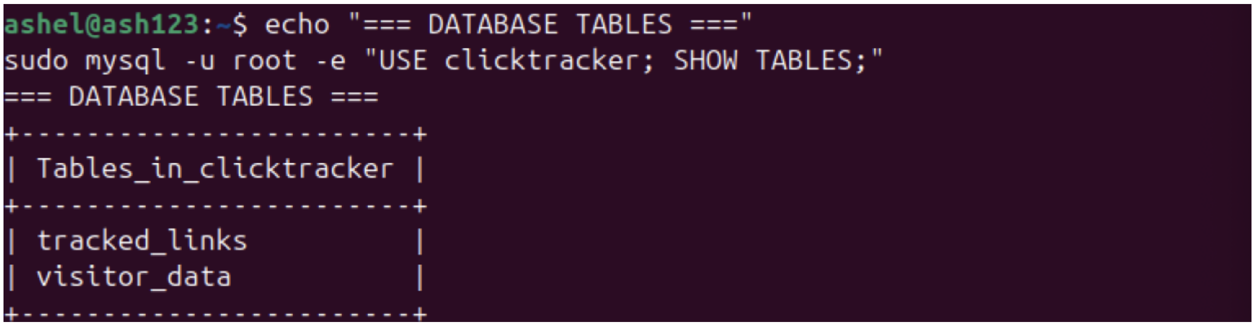


```
lines 1-20/20 (END)
● mysql.service - MySQL Community Server
     Loaded: loaded (/usr/lib/systemd/system/mysql.service; enabled; preset>
     Active: active (running) since Mon 2025-10-06 04:03:29 UTC; 28min ago
   Main PID: 1308 (mysqld)
     Status: "Server is operational"
      Tasks: 39 (limit: 4542)
     Memory: 37.3M (peak: 436.3M swap: 347.9M swap peak: 350.0M)
        CPU: 6.487s
     CGroup: /system.slice/mysql.service
             └─1308 /usr/sbin/mysqld

Oct 06 04:03:28 ash123 systemd[1]: Starting mysql.service - MySQL Community>
Oct 06 04:03:29 ash123 systemd[1]: Started mysql.service - MySQL Community >

        <input type="submit" value="Create Tracking Link">
ashel@ash123:~$
```

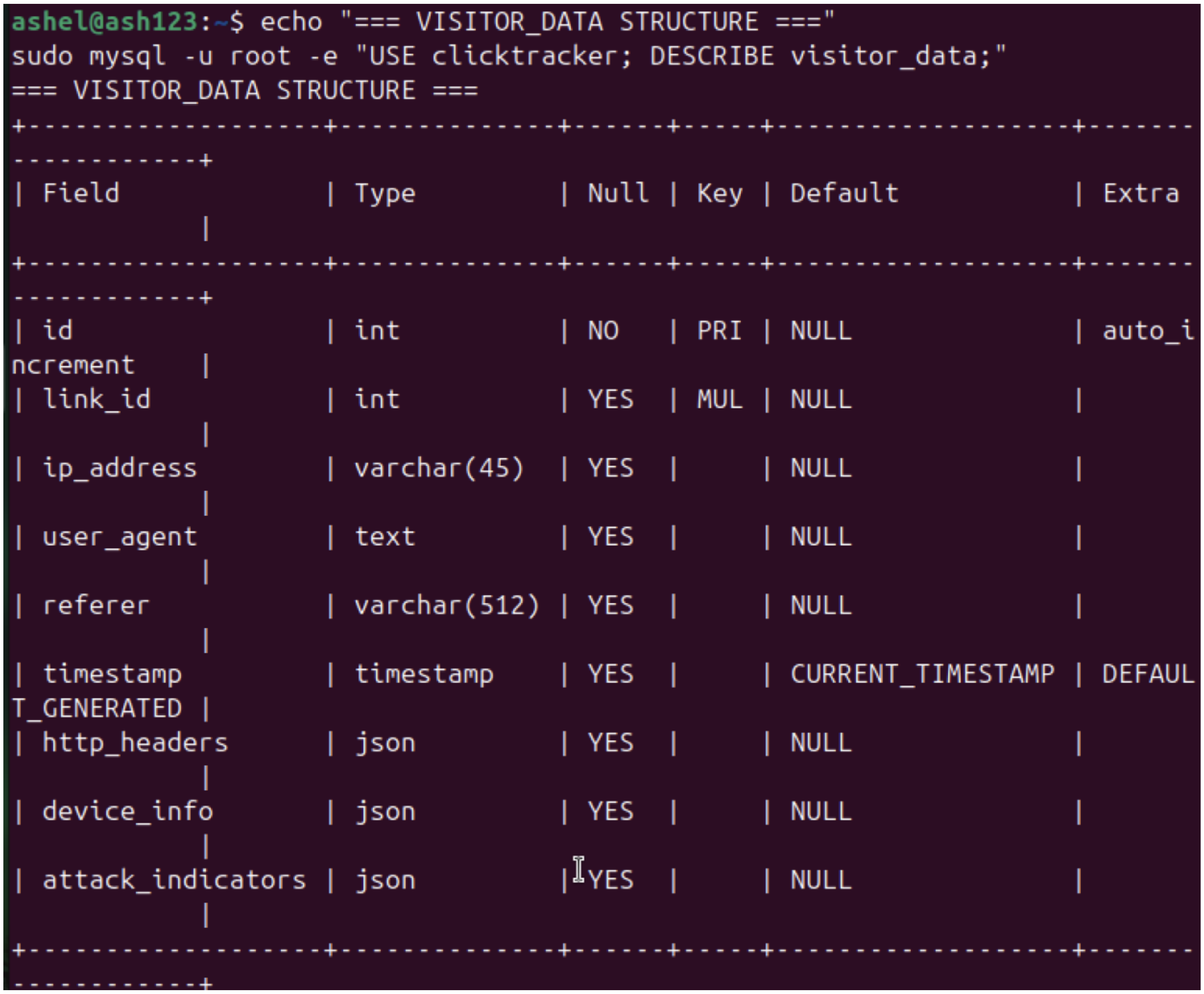
Document Current Working System



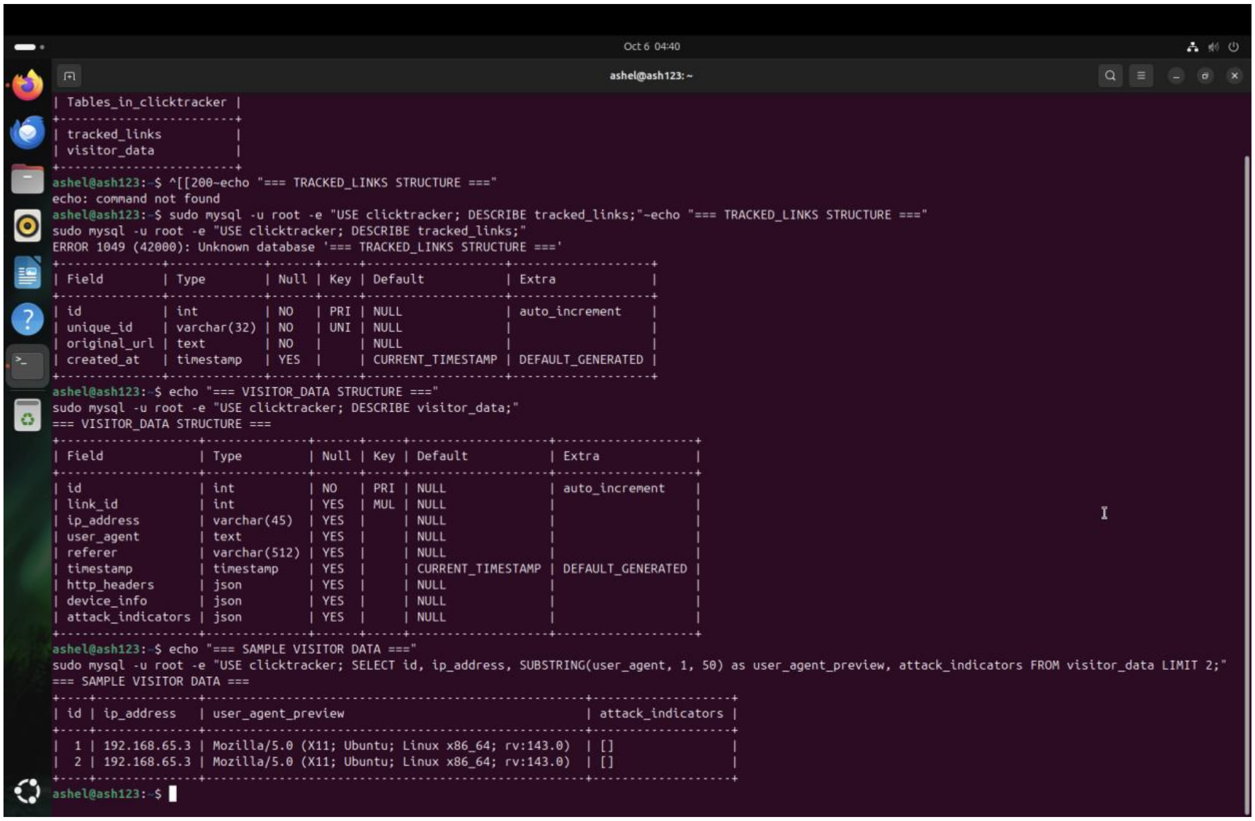
```
ashel@ash123:~$ sudo mysql -u root -e "USE clicktracker; DESCRIBE tracked_li
nks;"~echo "=== TRACKED_LINKS STRUCTURE ==="
sudo mysql -u root -e "USE clicktracker; DESCRIBE tracked_links;"
ERROR 1049 (42000): Unknown database '=== TRACKED_LINKS STRUCTURE ==='
+--------------+-------------+------+-----+-------------------+------------
------+
| Field        | Type        | Null | Key | Default           | Extra
      |
+--------------+-------------+------+-----+-------------------+------------
------+
| id           | int         | NO   | PRI | NULL              | auto_increme
nt    |
| unique_id    | varchar(32) | NO   | UNI | NULL              |
      |
| original_url | text        | NO   |     | NULL              |
      |
| created_at   | timestamp   | YES  |     | CURRENT_TIMESTAMP | DEFAULT_GENE
RATED |
+--------------+-------------+------+-----+-------------------+------------
------+
```



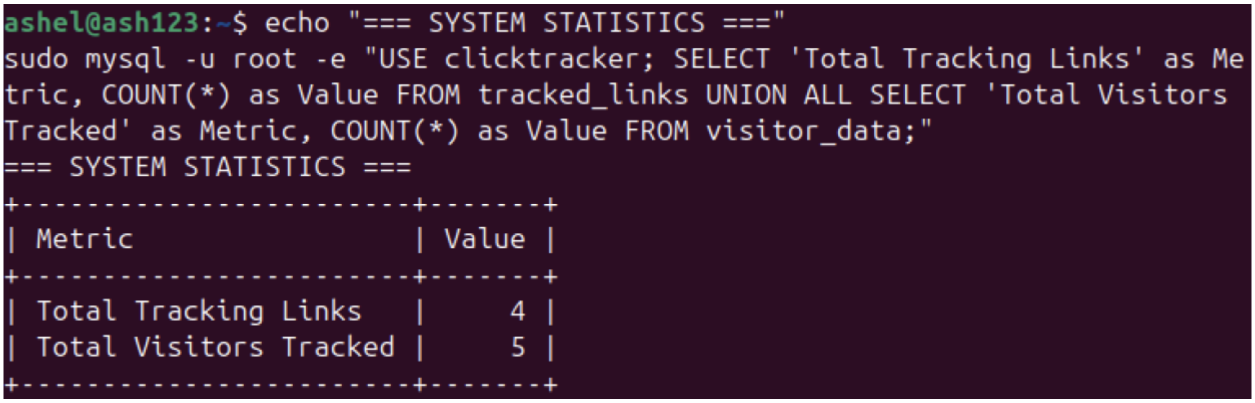
```
ashel@ash123:~$ echo "=== DATABASE TABLES ==="
sudo mysql -u root -e "USE clicktracker; SHOW TABLES;"
=== DATABASE TABLES ===
+-------------------------+
| Tables_in_clicktracker |
+-------------------------+
| tracked_links          |
| visitor_data           |
+-------------------------+
```



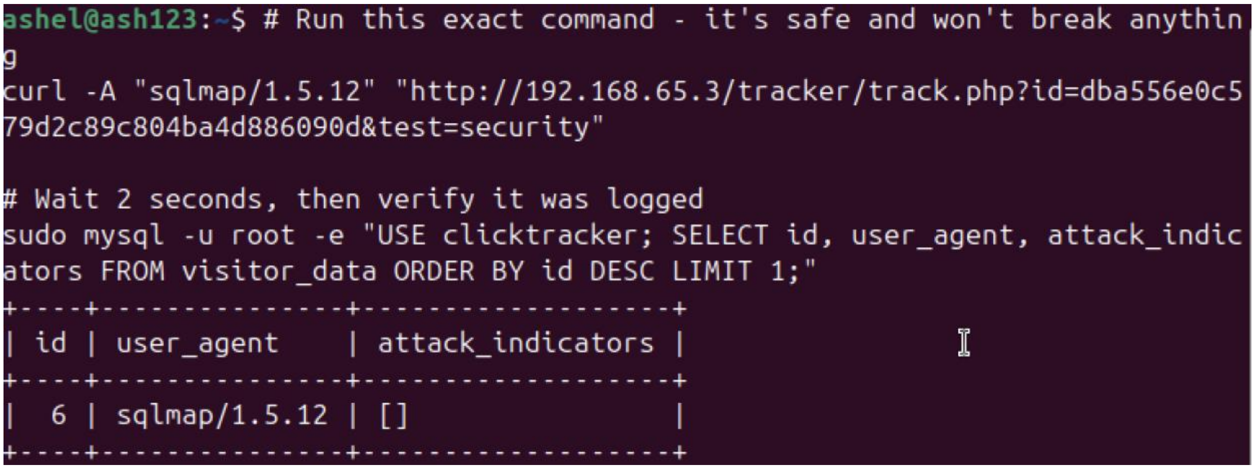
```
ashel@ash123:~$ echo "=== VISITOR_DATA STRUCTURE ==="
sudo mysql -u root -e "USE clicktracker; DESCRIBE visitor_data;"
=== VISITOR_DATA STRUCTURE ===
+-------------------+--------------+------+-----+-------------------+-------
------------+
| Field             | Type         | Null | Key | Default           | Extra
            |
+-------------------+--------------+------+-----+-------------------+-------
------------+
| id                | int          | NO   | PRI | NULL              | auto_i
ncrement    |
| link_id           | int          | YES  | MUL | NULL              |
            |
| ip_address        | varchar(45)  | YES  |     | NULL              |
            |
| user_agent        | text         | YES  |     | NULL              |
            |
| referer           | varchar(512) | YES  |     | NULL              |
            |
| timestamp         | timestamp    | YES  |     | CURRENT_TIMESTAMP | DEFAUL
T_GENERATED |
| http_headers      | json         | YES  |     | NULL              |
            |
| device_info       | json         | YES  |     | NULL              |
            |
| attack_indicators | json         | YES  |     | NULL              |
            |
+-------------------+--------------+------+-----+-------------------+-------
------------+
```



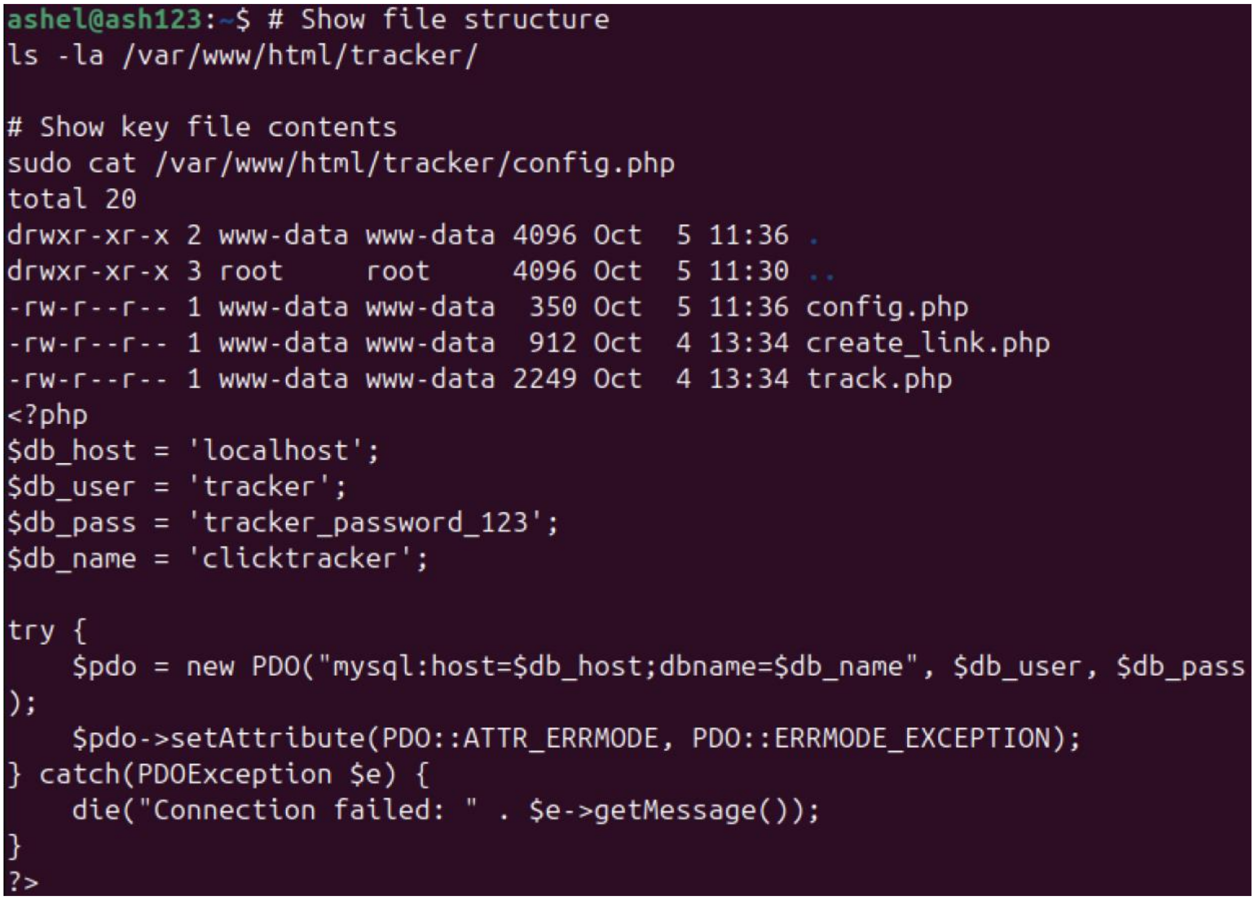
```
| Tables_in_clicktracker |
+------------------------+
| tracked_links          |
| visitor_data           |
+------------------------+
ashel@ash123:~$ ^[[200~echo "=== TRACKED_LINKS STRUCTURE ==="
echo: command not found
ashel@ash123:~$ sudo mysql -u root -e "USE clicktracker; DESCRIBE tracked_links;"~echo "=== TRACKED_LINKS STRUCTURE ==="
sudo mysql -u root -e "USE clicktracker; DESCRIBE tracked_links;"
ERROR 1049 (42000): Unknown database '=== TRACKED_LINKS STRUCTURE ==='
+--------------+-------------+------+-----+-------------------+-------------------+
| Field        | Type        | Null | Key | Default           | Extra             |
+--------------+-------------+------+-----+-------------------+-------------------+
| id           | int         | NO   | PRI | NULL              | auto_increment    |
| unique_id    | varchar(32) | NO   | UNI | NULL              |                   |
| original_url | text        | NO   |     | NULL              |                   |
| created_at   | timestamp   | YES  |     | CURRENT_TIMESTAMP | DEFAULT_GENERATED |
+--------------+-------------+------+-----+-------------------+-------------------+
ashel@ash123:~$ echo "=== VISITOR_DATA STRUCTURE ==="
sudo mysql -u root -e "USE clicktracker; DESCRIBE visitor_data;"
=== VISITOR_DATA STRUCTURE ===
+-------------------+--------------+------+-----+-------------------+-------------------+
| Field             | Type         | Null | Key | Default           | Extra             |
+-------------------+--------------+------+-----+-------------------+-------------------+
| id                | int          | NO   | PRI | NULL              | auto_increment    |
| link_id           | int          | YES  | MUL | NULL              |                   |
| ip_address        | varchar(45)  | YES  |     | NULL              |                   |
| user_agent        | text         | YES  |     | NULL              |                   |
| referer           | varchar(512) | YES  |     | NULL              |                   |
| timestamp         | timestamp    | YES  |     | CURRENT_TIMESTAMP | DEFAULT_GENERATED |
| http_headers      | json         | YES  |     | NULL              |                   |
| device_info       | json         | YES  |     | NULL              |                   |
| attack_indicators | json         | YES  |     | NULL              |                   |
+-------------------+--------------+------+-----+-------------------+-------------------+
ashel@ash123:~$ echo "=== SAMPLE VISITOR DATA ==="
sudo mysql -u root -e "USE clicktracker; SELECT id, ip_address, SUBSTRING(user_agent, 1, 50) as user_agent_preview, attack_indicators FROM visitor_data LIMIT 2;"
=== SAMPLE VISITOR DATA ===
+----+--------------+----------------------------------------------------+-------------------+
| id | ip_address   | user_agent_preview                                 | attack_indicators |
+----+--------------+----------------------------------------------------+-------------------+
|  1 | 192.168.65.3 | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:143.0)  | []                |
|  2 | 192.168.65.3 | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:143.0)  | []                |
+----+--------------+----------------------------------------------------+-------------------+
ashel@ash123:~$ 
```



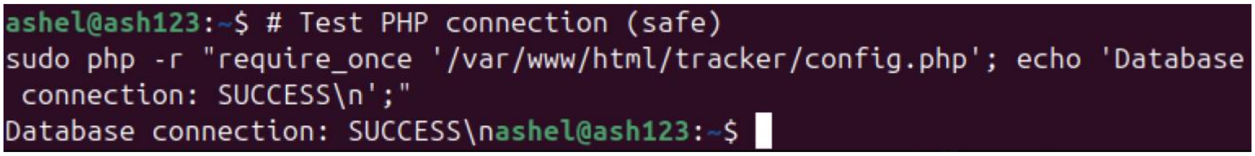
```
ashel@ash123:~$ echo "=== SYSTEM STATISTICS ==="
sudo mysql -u root -e "USE clicktracker; SELECT 'Total Tracking Links' as Me
tric, COUNT(*) as Value FROM tracked_links UNION ALL SELECT 'Total Visitors
Tracked' as Metric, COUNT(*) as Value FROM visitor_data;"
=== SYSTEM STATISTICS ===
+------------------------+-------+
| Metric                 | Value |
+------------------------+-------+
| Total Tracking Links   |     4 |
| Total Visitors Tracked |     5 |
+------------------------+-------+
```



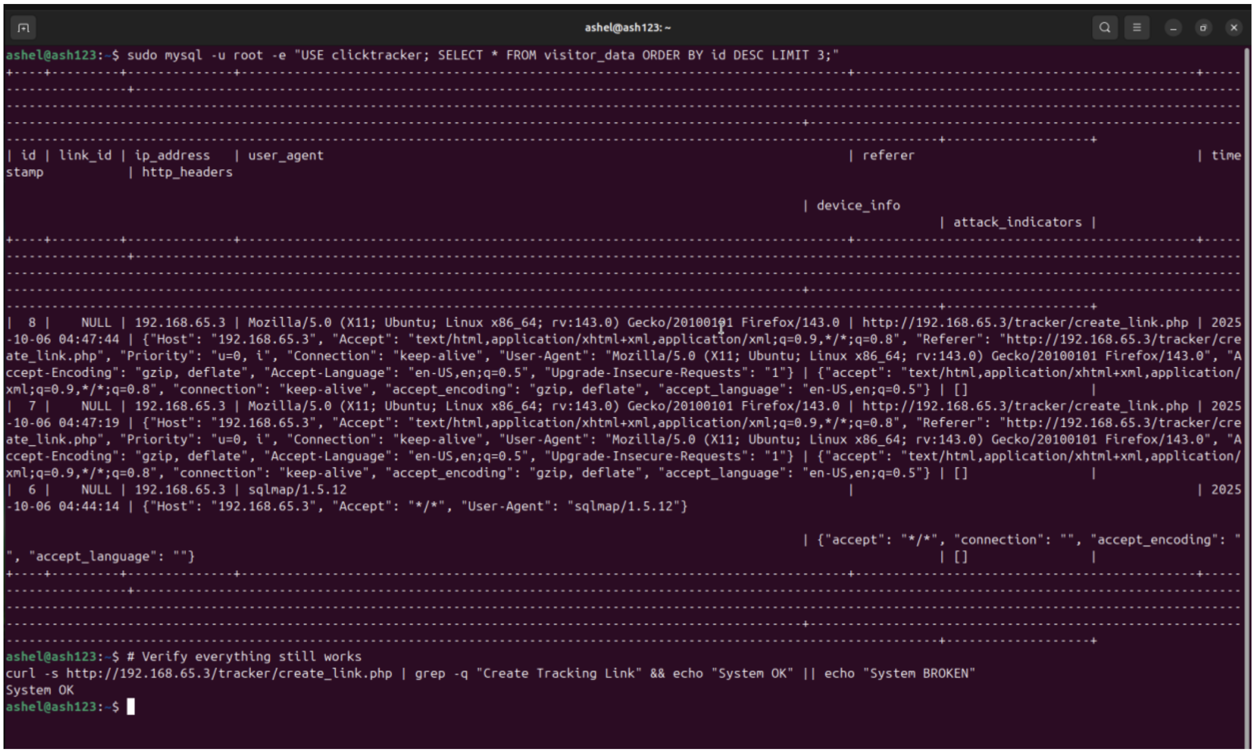
```
ashel@ash123:~$ # Run this exact command - it's safe and won't break anythin
g
curl -A "sqlmap/1.5.12" "http://192.168.65.3/tracker/track.php?id=dba556e0c5
79d2c89c804ba4d886090d&test=security"

# Wait 2 seconds, then verify it was logged
sudo mysql -u root -e "USE clicktracker; SELECT id, user_agent, attack_indic
ators FROM visitor_data ORDER BY id DESC LIMIT 1;"
+----+---------------+-------------------+
| id | user_agent    | attack_indicators |
+----+---------------+-------------------+
|  6 | sqlmap/1.5.12 | []                |
+----+---------------+-------------------+
```



```
ashel@ash123:~$ # Show file structure
ls -la /var/www/html/tracker/

# Show key file contents
sudo cat /var/www/html/tracker/config.php
total 20
drwxr-xr-x 2 www-data www-data 4096 Oct  5 11:36 .
drwxr-xr-x 3 root     root     4096 Oct  5 11:30 ..
-rw-r--r-- 1 www-data www-data  350 Oct  5 11:36 config.php
-rw-r--r-- 1 www-data www-data  912 Oct  4 13:34 create_link.php
-rw-r--r-- 1 www-data www-data 2249 Oct  4 13:34 track.php
<?php
$db_host = 'localhost';
$db_user = 'tracker';
$db_pass = 'tracker_password_123';
$db_name = 'clicktracker';

try {
    $pdo = new PDO("mysql:host=$db_host;dbname=$db_name", $db_user, $db_pass
);
    $pdo->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
} catch(PDOException $e) {
    die("Connection failed: " . $e->getMessage());
}
?>
```

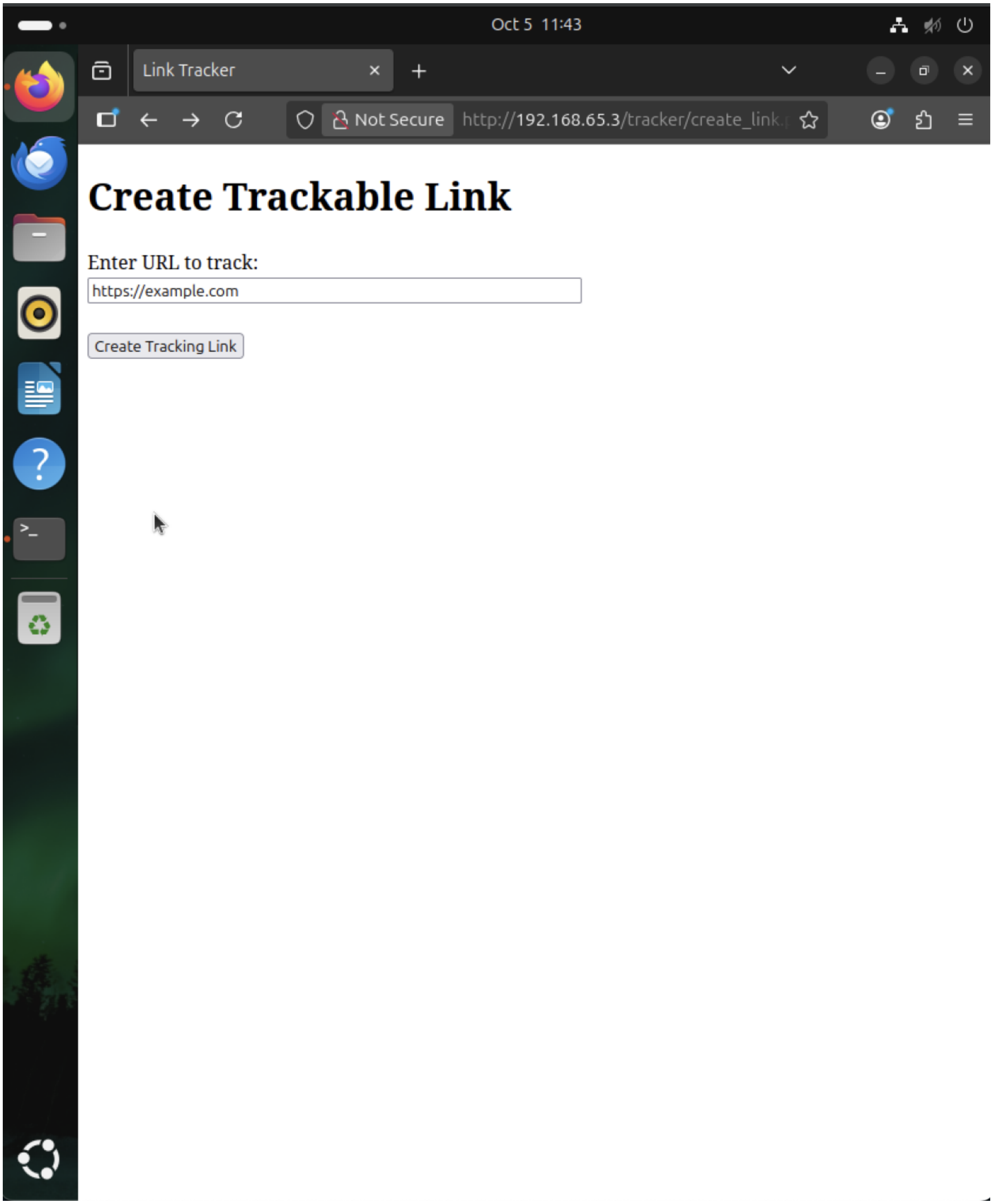


```
ashel@ash123:~$ # Test PHP connection (safe)
sudo php -r "require_once '/var/www/html/tracker/config.php'; echo 'Database
 connection: SUCCESS\n';"
Database connection: SUCCESS\nashel@ash123:~$ 
```



```
ashel@ash123:~$ sudo mysql -u root -e "USE clicktracker; SELECT * FROM visitor_data ORDER BY id DESC LIMIT 3;"
+----+---------+--------------+---------------------------------------------------------------------------------+---------------------------------------------+-----
----------------+-----------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------+----------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------+-------------------+
| id | link_id | ip_address   | user_agent                                                                      | referer                                     | time
stamp           | http_headers

                                                                                                         | device_info
                                                                                                                            | attack_indicators |
+----+---------+--------------+---------------------------------------------------------------------------------+---------------------------------------------+-----
----------------+-----------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------+----------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------+-------------------+
|  8 |    NULL | 192.168.65.3 | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:143.0) Gecko/20100101 Firefox/143.0 | http://192.168.65.3/tracker/create_link.php | 2025
-10-06 04:47:44 | {"Host": "192.168.65.3", "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8", "Referer": "http://192.168.65.3/tracker/cre
ate_link.php", "Priority": "u=0, i", "Connection": "keep-alive", "User-Agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:143.0) Gecko/20100101 Firefox/143.0", "A
ccept-Encoding": "gzip, deflate", "Accept-Language": "en-US,en;q=0.5", "Upgrade-Insecure-Requests": "1"} | {"accept": "text/html,application/xhtml+xml,application/
xml;q=0.9,*/*;q=0.8", "connection": "keep-alive", "accept_encoding": "gzip, deflate", "accept_language": "en-US,en;q=0.5"} | []                |
|  7 |    NULL | 192.168.65.3 | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:143.0) Gecko/20100101 Firefox/143.0 | http://192.168.65.3/tracker/create_link.php | 2025
-10-06 04:47:19 | {"Host": "192.168.65.3", "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8", "Referer": "http://192.168.65.3/tracker/cre
ate_link.php", "Priority": "u=0, i", "Connection": "keep-alive", "User-Agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:143.0) Gecko/20100101 Firefox/143.0", "A
ccept-Encoding": "gzip, deflate", "Accept-Language": "en-US,en;q=0.5", "Upgrade-Insecure-Requests": "1"} | {"accept": "text/html,application/xhtml+xml,application/
xml;q=0.9,*/*;q=0.8", "connection": "keep-alive", "accept_encoding": "gzip, deflate", "accept_language": "en-US,en;q=0.5"} | []                |
|  6 |    NULL | 192.168.65.3 | sqlmap/1.5.12                                                                   |                                             | 2025
-10-06 04:44:14 | {"Host": "192.168.65.3", "Accept": "*/*", "User-Agent": "sqlmap/1.5.12"}

                                                                                                         | {"accept": "*/*", "connection": "", "accept_encoding": "
", "accept_language": ""}                                                                                                   | []                |
+----+---------+--------------+---------------------------------------------------------------------------------+---------------------------------------------+-----
----------------+-----------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------+----------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------+-------------------+
ashel@ash123:~$ # Verify everything still works
curl -s http://192.168.65.3/tracker/create_link.php | grep -q "Create Tracking Link" && echo "System OK" || echo "System BROKEN"
System OK
ashel@ash123:~$
```

Website used for create trackable links:

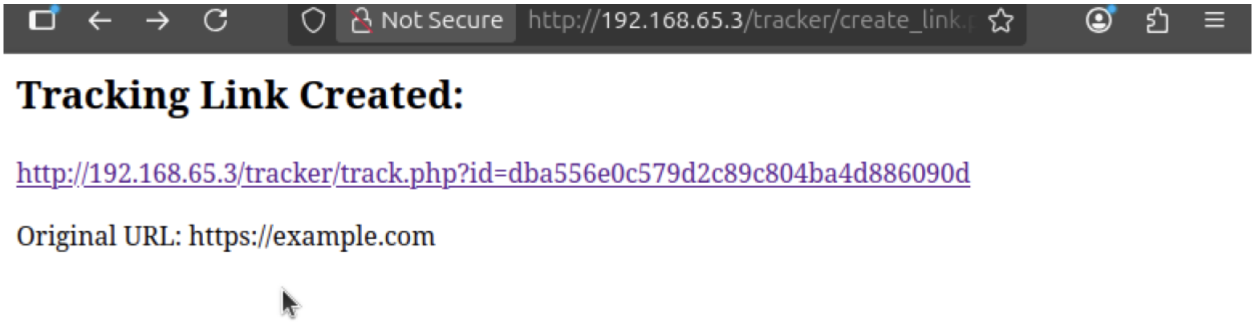


Create Trackable Link

Enter URL to track:

https://example.com

Create Tracking Link

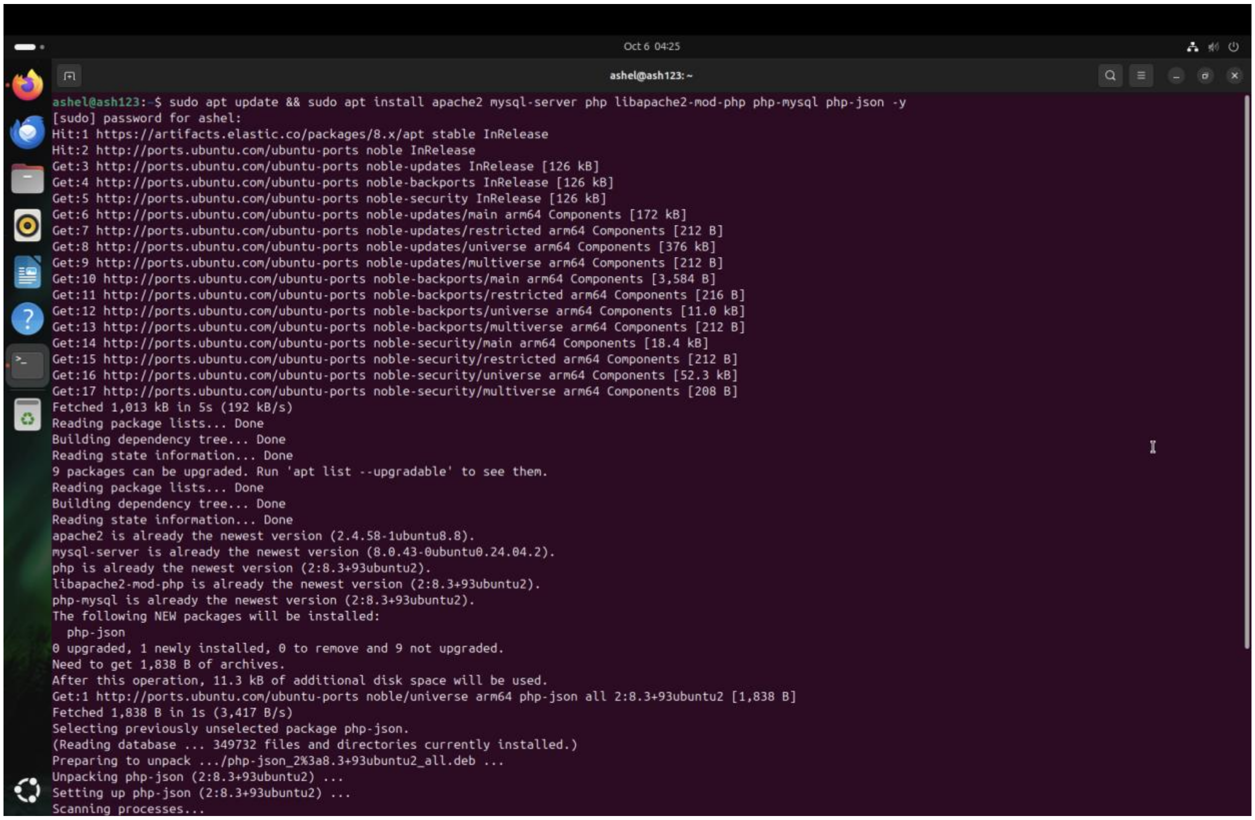


Tracking Link Created:

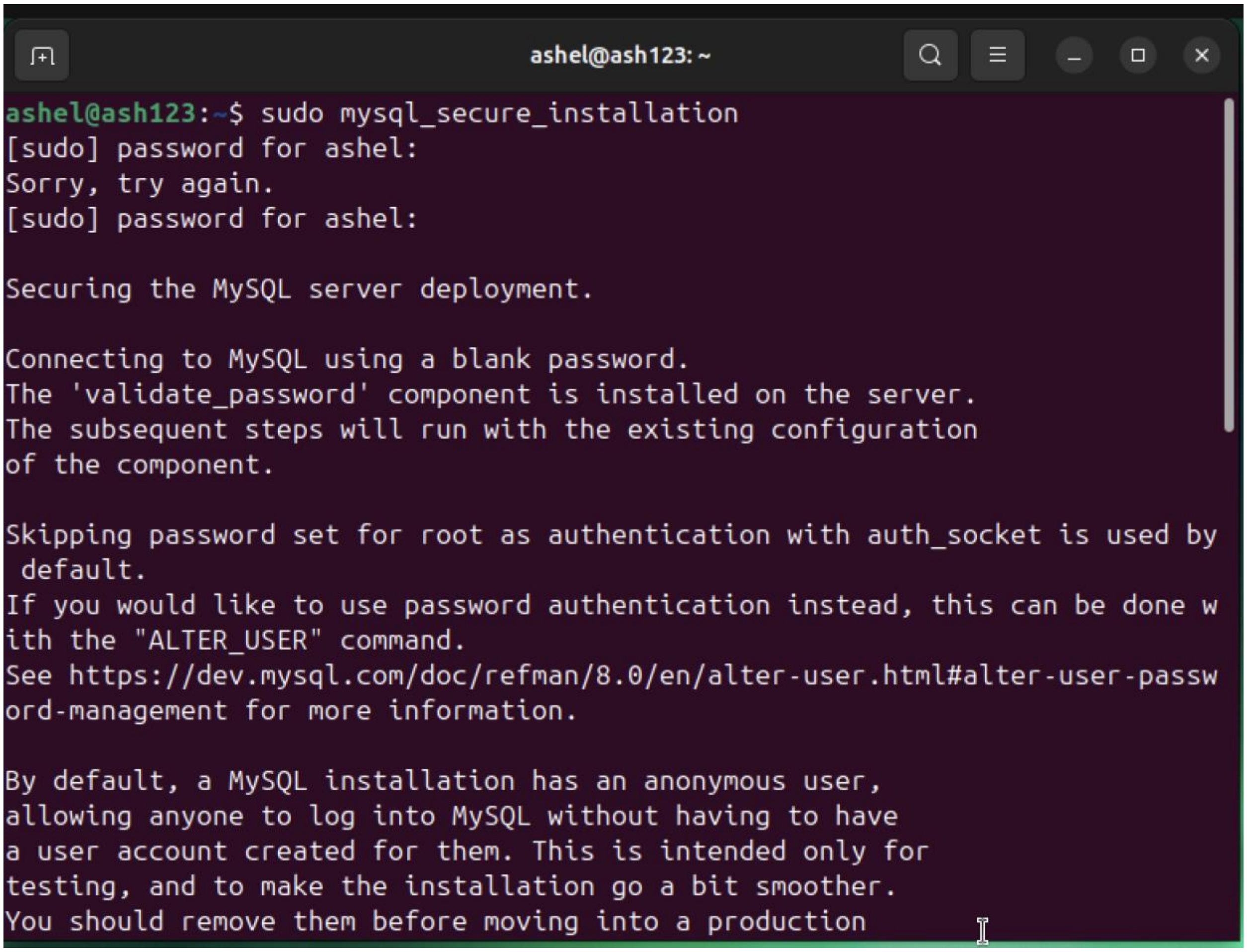
http://192.168.65.3/tracker/track.php?id=dba556e0c579d2c89c804ba4d886090d

Original URL: https://example.com

Additional screen shots:

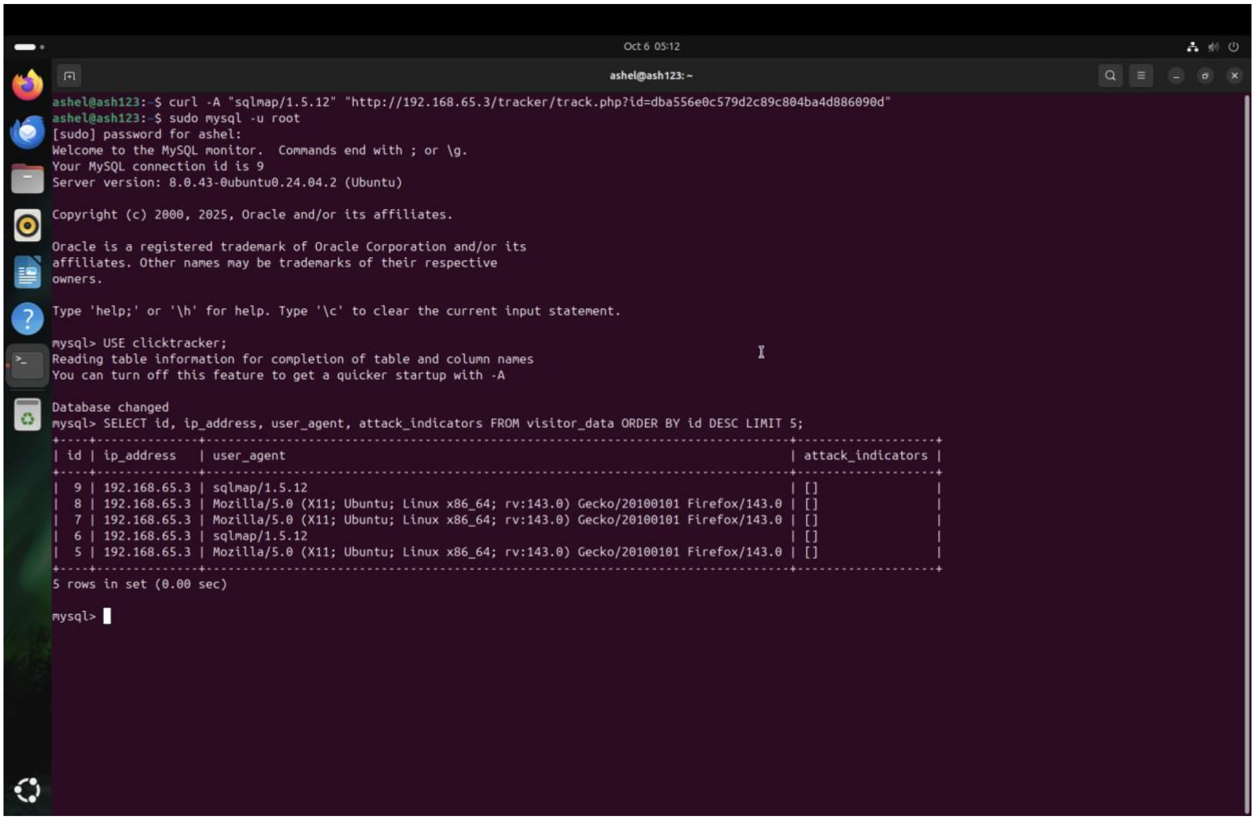


```
ashel@ash123:~$ sudo apt update && sudo apt install apache2 mysql-server php libapache2-mod-php php-mysql php-json -y
[sudo] password for ashel:
Hit:1 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Hit:2 http://ports.ubuntu.com/ubuntu-ports noble InRelease
Get:3 http://ports.ubuntu.com/ubuntu-ports noble-updates InRelease [126 kB]
Get:4 http://ports.ubuntu.com/ubuntu-ports noble-backports InRelease [126 kB]
Get:5 http://ports.ubuntu.com/ubuntu-ports noble-security InRelease [126 kB]
Get:6 http://ports.ubuntu.com/ubuntu-ports noble-updates/main arm64 Components [172 kB]
Get:7 http://ports.ubuntu.com/ubuntu-ports noble-updates/restricted arm64 Components [212 B]
Get:8 http://ports.ubuntu.com/ubuntu-ports noble-updates/universe arm64 Components [376 kB]
Get:9 http://ports.ubuntu.com/ubuntu-ports noble-updates/multiverse arm64 Components [212 B]
Get:10 http://ports.ubuntu.com/ubuntu-ports noble-backports/main arm64 Components [3,584 B]
Get:11 http://ports.ubuntu.com/ubuntu-ports noble-backports/restricted arm64 Components [216 B]
Get:12 http://ports.ubuntu.com/ubuntu-ports noble-backports/universe arm64 Components [11.0 kB]
Get:13 http://ports.ubuntu.com/ubuntu-ports noble-backports/multiverse arm64 Components [212 B]
Get:14 http://ports.ubuntu.com/ubuntu-ports noble-security/main arm64 Components [18.4 kB]
Get:15 http://ports.ubuntu.com/ubuntu-ports noble-security/restricted arm64 Components [212 B]
Get:16 http://ports.ubuntu.com/ubuntu-ports noble-security/universe arm64 Components [52.3 kB]
Get:17 http://ports.ubuntu.com/ubuntu-ports noble-security/multiverse arm64 Components [208 B]
Fetched 1,013 kB in 5s (192 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
9 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.58-1ubuntu8.8).
mysql-server is already the newest version (8.0.43-0ubuntu0.24.04.2).
php is already the newest version (2:8.3+93ubuntu2).
libapache2-mod-php is already the newest version (2:8.3+93ubuntu2).
php-mysql is already the newest version (2:8.3+93ubuntu2).
The following NEW packages will be installed:
  php-json
0 upgraded, 1 newly installed, 0 to remove and 9 not upgraded.
Need to get 1,838 B of archives.
After this operation, 11.3 kB of additional disk space will be used.
Get:1 http://ports.ubuntu.com/ubuntu-ports noble/universe arm64 php-json all 2:8.3+93ubuntu2 [1,838 B]
Fetched 1,838 B in 1s (3,417 B/s)
Selecting previously unselected package php-json.
(Reading database ... 349732 files and directories currently installed.)
Preparing to unpack .../php-json_2%3a8.3+93ubuntu2_all.deb ...
Unpacking php-json (2:8.3+93ubuntu2) ...
Setting up php-json (2:8.3+93ubuntu2) ...
Scanning processes...
```



```
ashel@ash123:~$ sudo mysql_secure_installation
[sudo] password for ashel:
Sorry, try again.
[sudo] password for ashel:

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.
The 'validate_password' component is installed on the server.
The subsequent steps will run with the existing configuration
of the component.

Skipping password set for root as authentication with auth_socket is used by
 default.
If you would like to use password authentication instead, this can be done w
ith the "ALTER_USER" command.
See https://dev.mysql.com/doc/refman/8.0/en/alter-user.html#alter-user-passw
ord-management for more information.

By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
```

Captured intruder list :



```
ashel@ash123:~$ curl -A "sqlmap/1.5.12" "http://192.168.65.3/tracker/track.php?id=dba556e0c579d2c89c804ba4d886090d"
ashel@ash123:~$ sudo mysql -u root
[sudo] password for ashel:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 8.0.43-0ubuntu0.24.04.2 (Ubuntu)

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> USE clicktracker;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SELECT id, ip_address, user_agent, attack_indicators FROM visitor_data ORDER BY id DESC LIMIT 5;
+----+--------------+--------------------------------------------------------------------------------+-------------------+
| id | ip_address   | user_agent                                                                     | attack_indicators |
+----+--------------+--------------------------------------------------------------------------------+-------------------+
|  9 | 192.168.65.3 | sqlmap/1.5.12                                                                  | []                |
|  8 | 192.168.65.3 | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:143.0) Gecko/20100101 Firefox/143.0 | []                |
|  7 | 192.168.65.3 | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:143.0) Gecko/20100101 Firefox/143.0 | []                |
|  6 | 192.168.65.3 | sqlmap/1.5.12                                                                  | []                |
|  5 | 192.168.65.3 | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:143.0) Gecko/20100101 Firefox/143.0 | []                |
+----+--------------+--------------------------------------------------------------------------------+-------------------+
5 rows in set (0.00 sec)

mysql> 
```