【fairy】实验吧web题——hash爆破

原创

meng_x1 于 2018-09-20 21:15:06 发布 679 收藏
分类专栏： wp 文章标签： 实验吧 ctf wp writeup

最近沉迷于爆破= =

题目链接“http://ctf5.shiyanbar.com/ppc/sd.php

给你一个sha1值，它是0-100000之间的整数的md5值再求取sha1值，请在2秒内提交该整数值

给你一个sha1值，它是0-100000之间的整数的md5值再求取sha1值，请在2秒内提交该整数值

请在2秒内提交该整数： 123 提交

ea3a27c33882feade84e856d9fa77e63ee046765

Time expired!

题干表述的很清楚，就是让你碰撞出hash值对应的原来的值。

emmmm。又到了写脚本的时候了！！！

我们很容易发现提交数据为post请求，抓包分析一下post数据的参数：

```
POST /ppc/sd.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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://ctf5.shiyanbar.com/ppc/sd.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Cookie: PHPSESSID=801b38jcv0r3vgh2hh1oc5jnm4
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

inputNumber=123&submit=%E6%8F%90%E4%BA%A4
```


我们看见除了inputNumber字段接受你所填写的数据，还有个submit字段。

ok，一切分析清楚，最后的流程：

获取界面html→正则出hash值→循环碰撞→碰撞出结果后构建post→post数据→获取返回html即可获取flag

```
</table>
<div name='sha1' style="color:red">bc8c3097a9dc0e46b4b7de0eed39998adf7d5deb</div>
</form>
You are winner, the flag is CTF{BlAsT_FasT_Pr0gRamE}</body>
</html>
```


最后附上脚本：

```
#coding=utf-8
import requests
import hashlib
import re

url="http://ctf5.shiyanbar.com/ppc/sd.php"
se=requests.Session()
sqlurl=se.get(url)
sqlurl.encoding='utf-8'
print sqlurl.text

hash = re.compile(r'color:red">(.*?)</div>', re.DOTALL).findall(sqlurl.text)
hash1=hash[0]
print hash1

for i in range(0,100000):
 k=str(i)
 hashmd5 = hashlib.md5(k).hexdigest()
 hashsha1 = hashlib.sha1(hashmd5).hexdigest()
 if hashsha1 == hash1:
  post = {'inputNumber':i,'submit':'%E6%8F%90%E4%BA%A4'}
  flag=se.post(url,data=post)
  flag.encoding='utf-8'
  print flag.text
```

over～