黑客丛林之旅

原创

浅零半泣 于 2017-09-12 21:35:30 发布

分类专栏： CTF

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

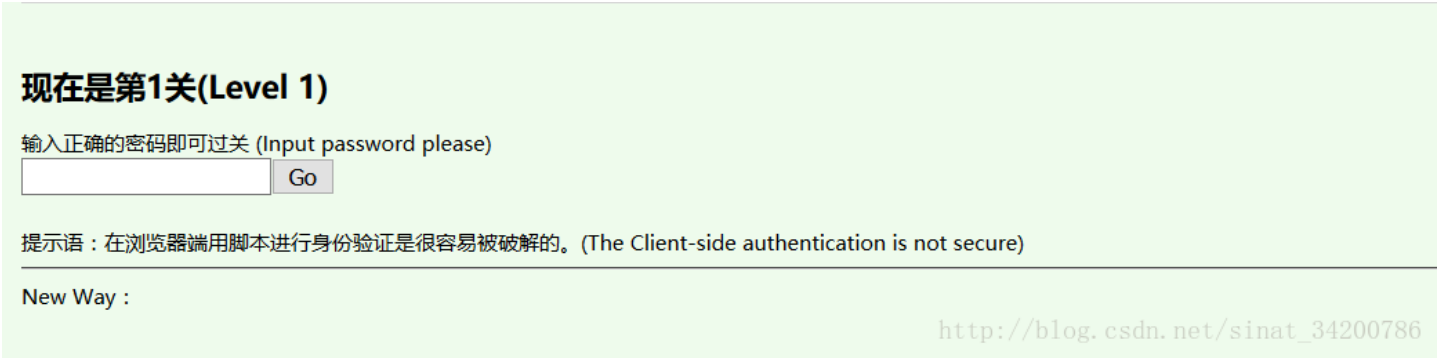
黑客丛林之旅——挑战的不仅仅是黑客技术

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



解题思路

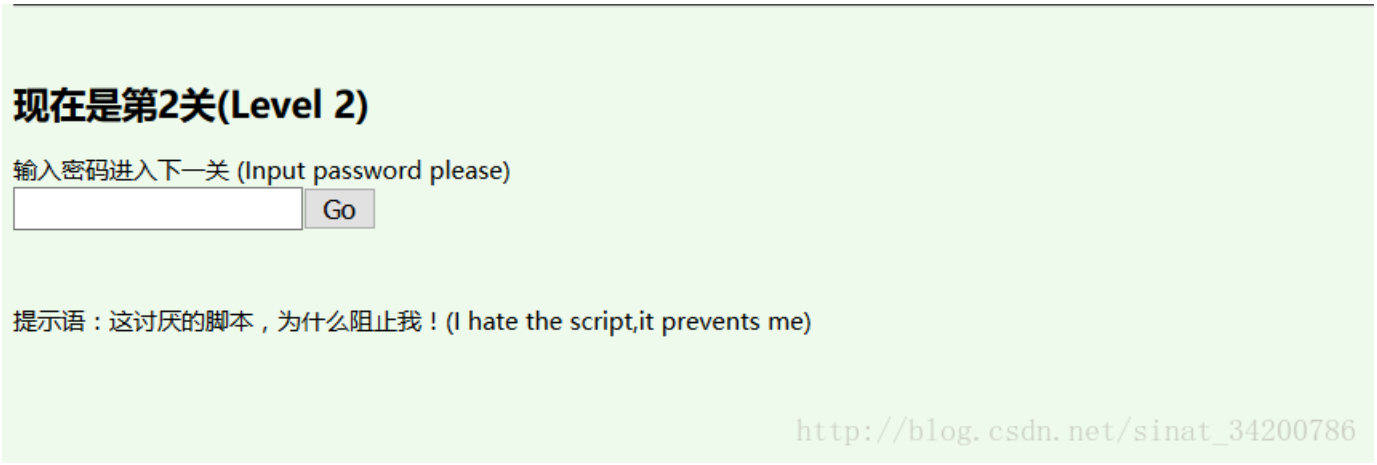
审查页面源码即可

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



解题思路

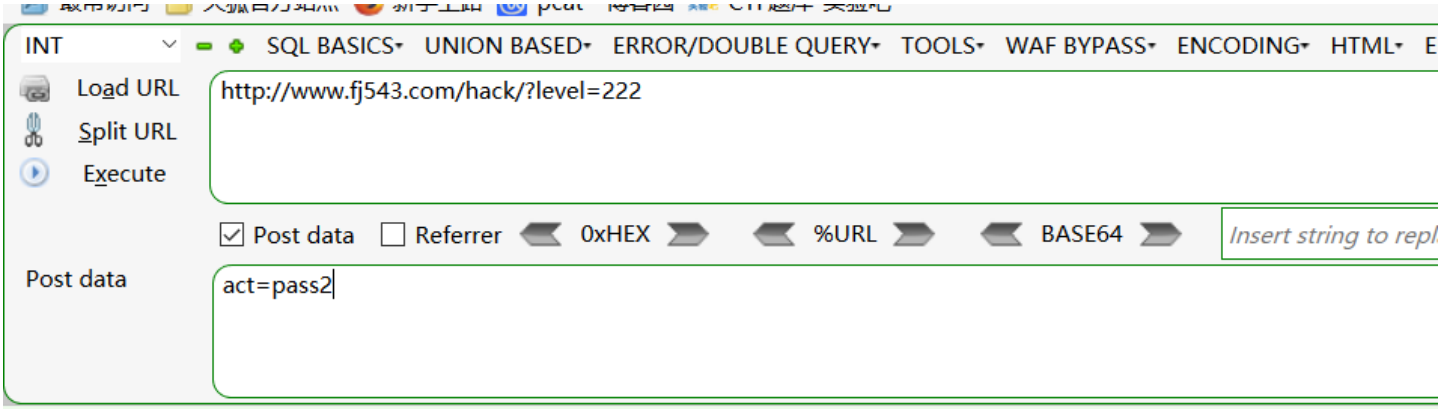
页面源代码中发现隐藏表单，直接post隐藏表单的内容

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)
```


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)

Go

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

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?)

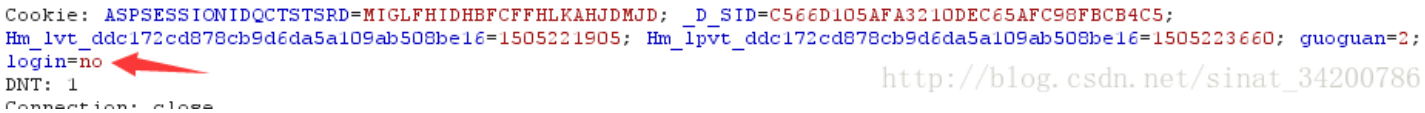
New Way：
我知道管理员很懒，密码应该很简单。可是他懒到连登录界面都没做.....

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
```



发现cookie一栏里有个login=no，改为yes即可

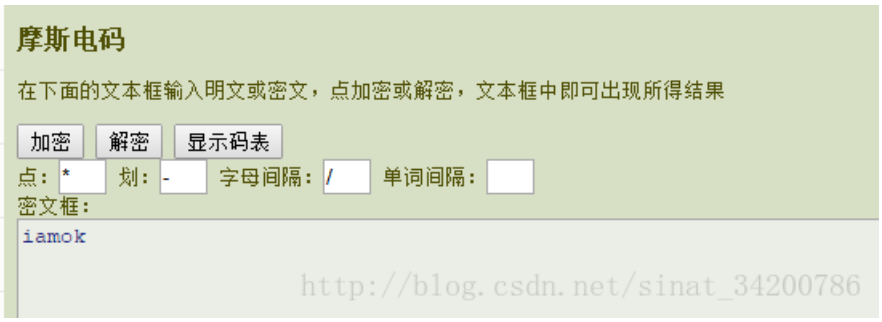
第四关

原题

解题思路

莫斯电码而已

WriteUp



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)

Go

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)

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

第六关

原题

现在是第6关(Level 6)

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

password= Go

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

New Way：

level="7"+vnc

解题思路

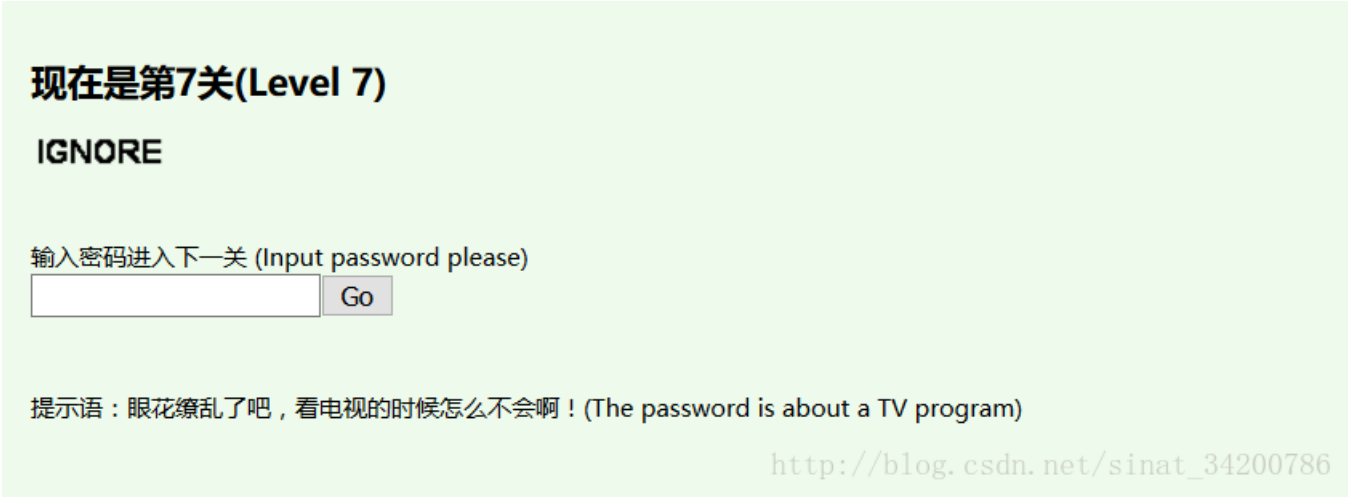
```
默认端口
```

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

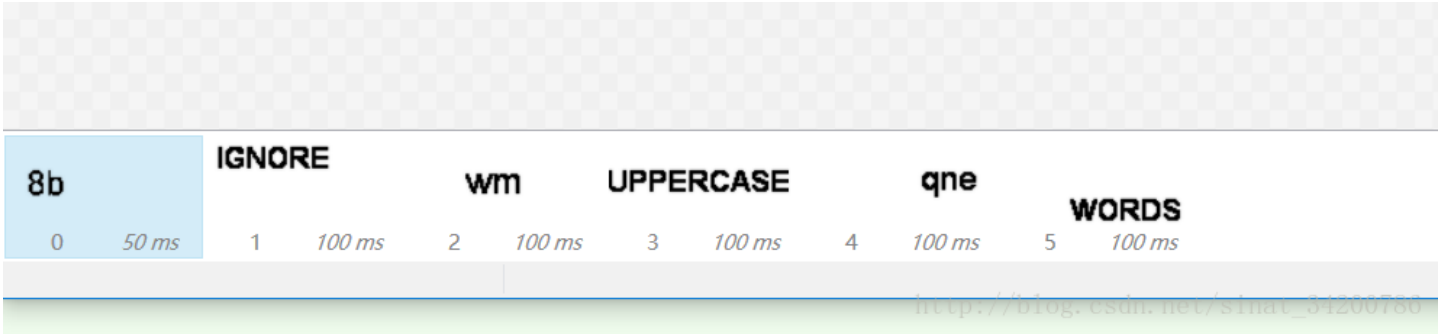


解题思路

```
gif一帧一帧看即可
```

WriteUp

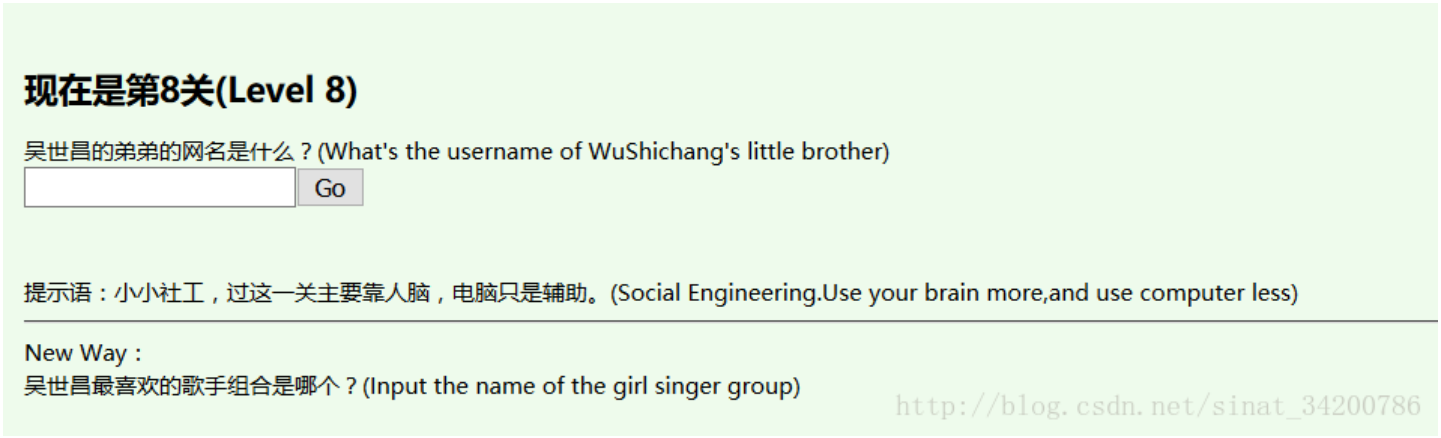
```
把gif分解成帧，发现提示
```




```
直接按提示提交就可以了
```

第八关

原题



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)

Go

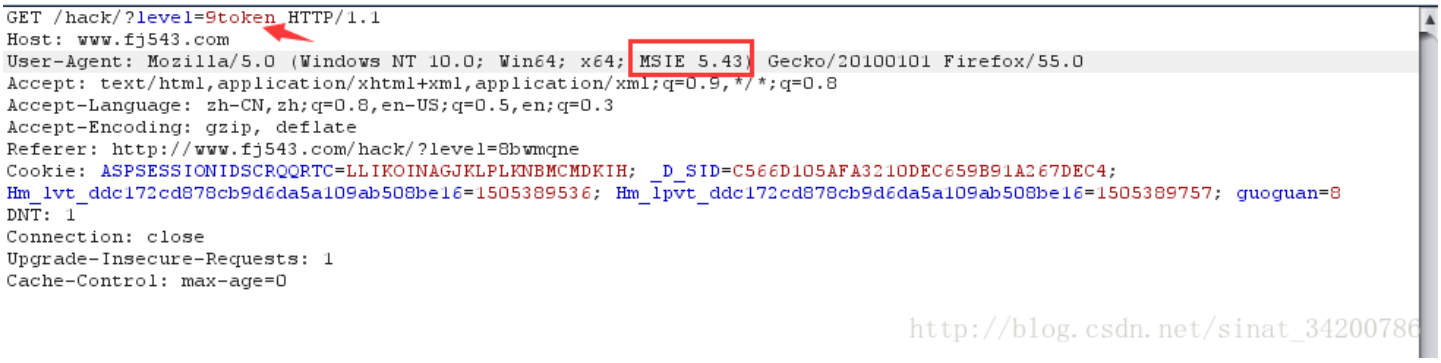
提示语：使用IE 5.43版本的浏览器访问?level=9token可以得到令牌。(Use IE 5.43 version to browse ?level=9token)

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
```



您的令牌(Token):level9496302

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

第十关

原题

现在是第10关(Level 10)

请输入令牌：(Input the token please)

Go

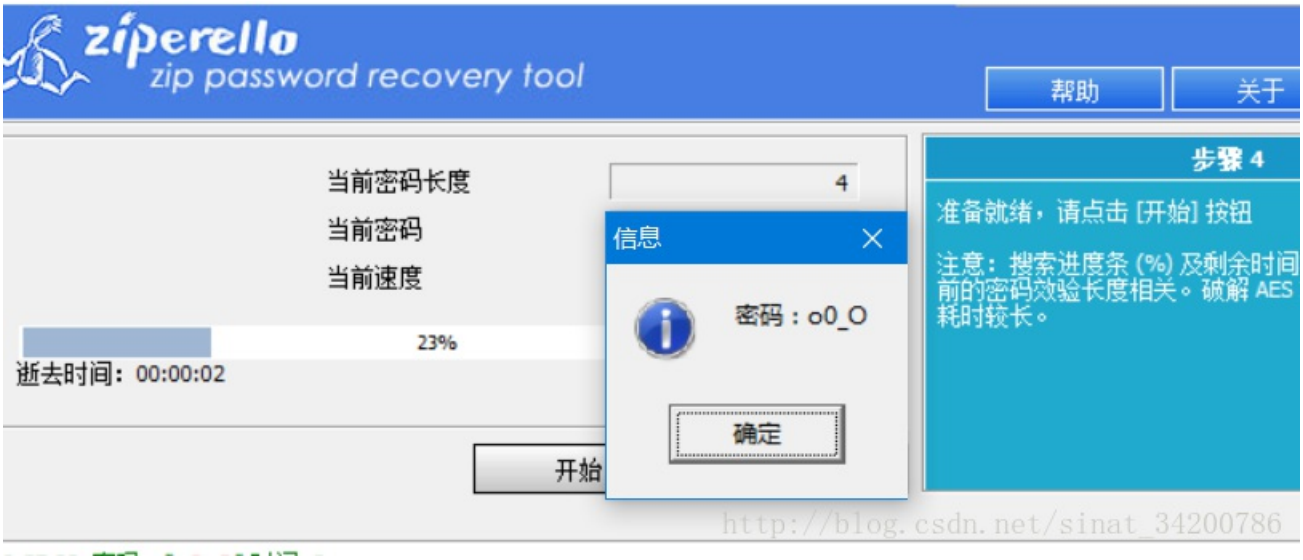
提示语：请下载令牌生成器(Token Generator)。解压密码不长,但很复杂。(Download it.The zip password is short,but very complex)

解题思路

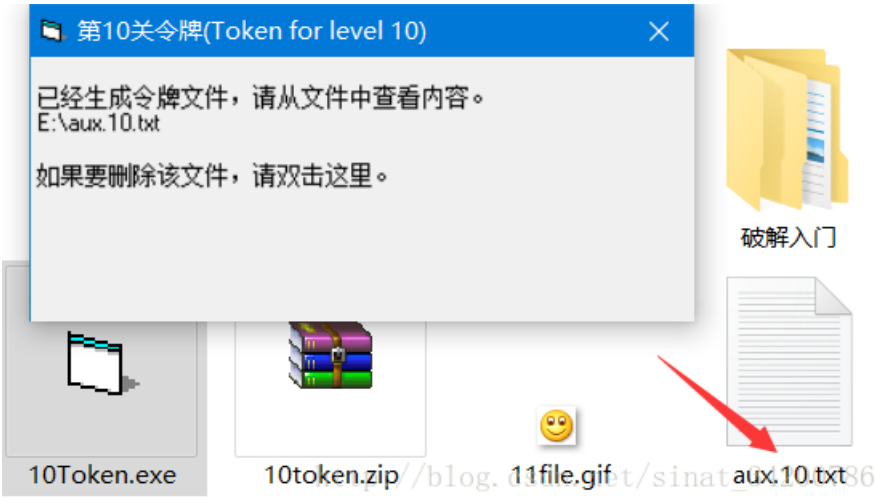
爆破，命令行type指令

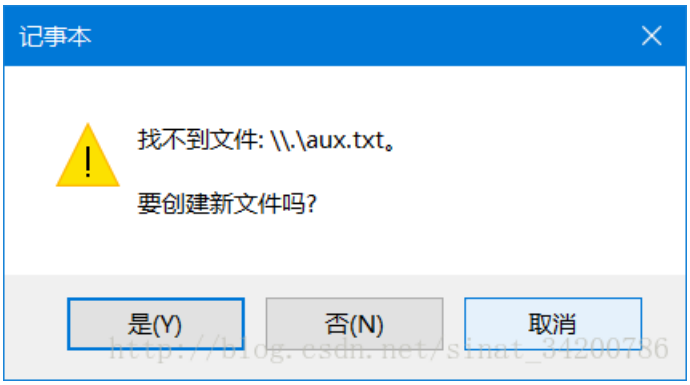
WriteUp

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





这时需要用到命令行的type指令

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11关(Level 11)

输入密码进入下一关 (Input password please)

Go

提示语：一个表情，却是有声有色。(I like the beautiful face and the voice)

解题思路

```
简单隐写
```

WriteUp

```
一个24*24的gif怎么会有70多kB?
很明显隐藏有其他数据
不过binwalk却没发现什么，那么通过gif的格式结构搜索特定数值，这时发现隐藏的数据
```

```
00006E0  D4 FD 0B 74 C2 1B 41 74 81 D2 6D C1 21 B0 84 C0  Oý.tA.At.OmA!°„A
00006F0  19 FF 4E 1C 64 53 4D E0 8B 9C 03 D7 04 D2 D8 F0  .ÿN.dSMà‹œ.×.ÒØð
0000700  E0 84 7F 40 FA 0A 1E 4C B8 B0 61 81 F7 0E 06 04  à„.@ú..L¸°a.÷...
0000710  00 3B 0D 0A 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D  .;..------------
0000720  2D 2D 2D 2D 2D 2D 2D 2D 70 61 73 73 77 6F 72 64  --------password
0000730  20 65 6E 64 2C 61 6E 64 20 70 61 73 73 77 6F 72   end,and passwor
0000740  64 20 73 74 61 72 74 2D 2D 2D 2D 2D 2D 2D 2D 2D  d start---------
0000750  2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 0D 0A 52 49 46 46  ----------..RIFF
0000760  46 24 1D 01 00 57 41 56 45 66 6D 74 20 10 00 00  F$...WAVEfmt ...
0000770  00 01 00 01 00 40 1F 00 00 80 3E 00 00 02 00 10  .....@....€>.....
0000780  00 64 61 74 61 00 1D 01 00 00 00 00 00 00 00 00  .data...........
```



```
可以知道隐藏了一个wav格式的音频文件，分离出音频文件，打开音频听提示即可
```

第十二关

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)

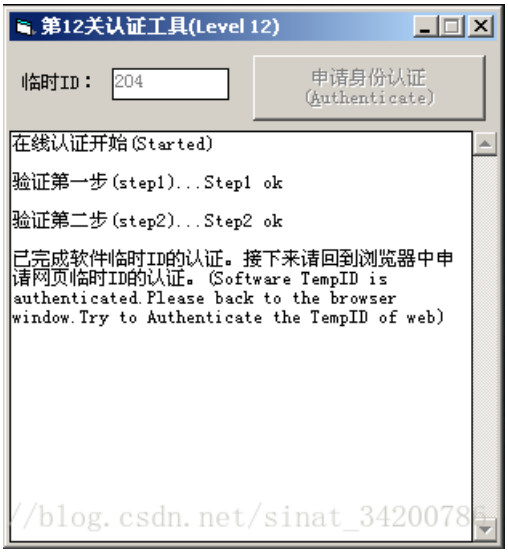
提示语：你的网页临时ID是**235**.半小时内有效，若失效请刷新网页。(This is your TempID of web)

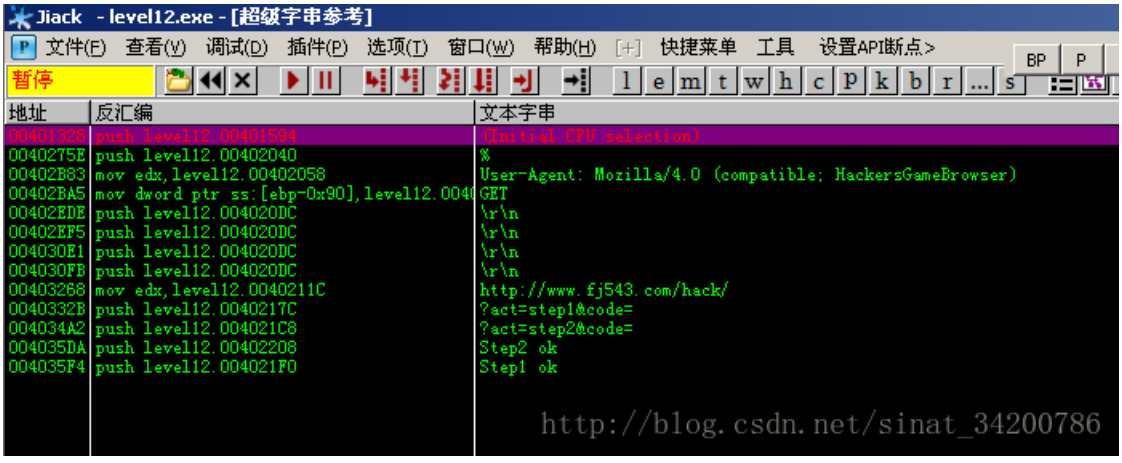
解题思路

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: HackersGameBrower)'
```

```
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 = {'ASPSESSIONIDSCRQQRTC':'BLNFHKCCLKAHGNCLHGFDFFLM',
          '_D_SID':'C566D105AFA3210DEC658FCF929AADF9',
          'Hm_lvt_ddc172cd878cb9d6da5a109ab508be16':'1505537184',
          'Hm_lpvt_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
```

```
[redacted].py
Step1 ok
Step2 ok 245
```



```
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)

第十三关

原题

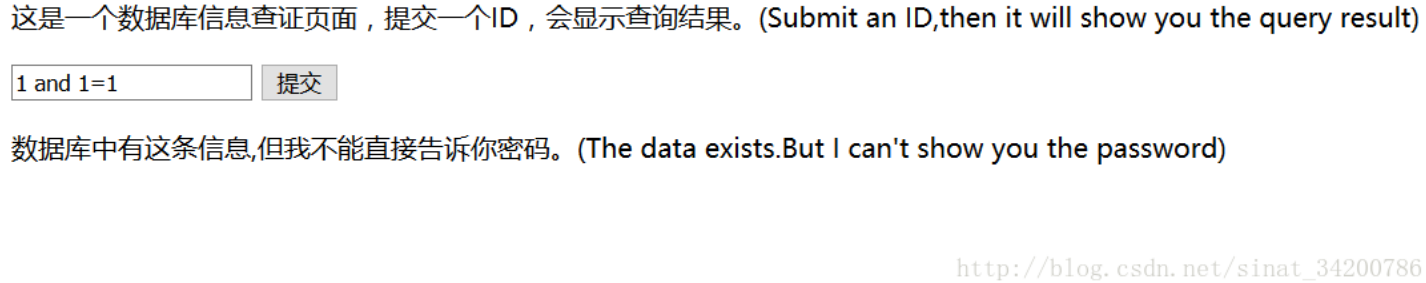
解题思路

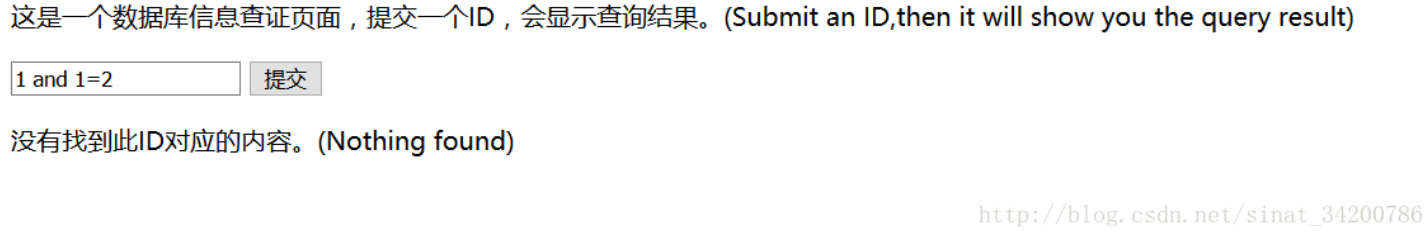
```
sql注入，猜测列名，爆破
```

WriteUp

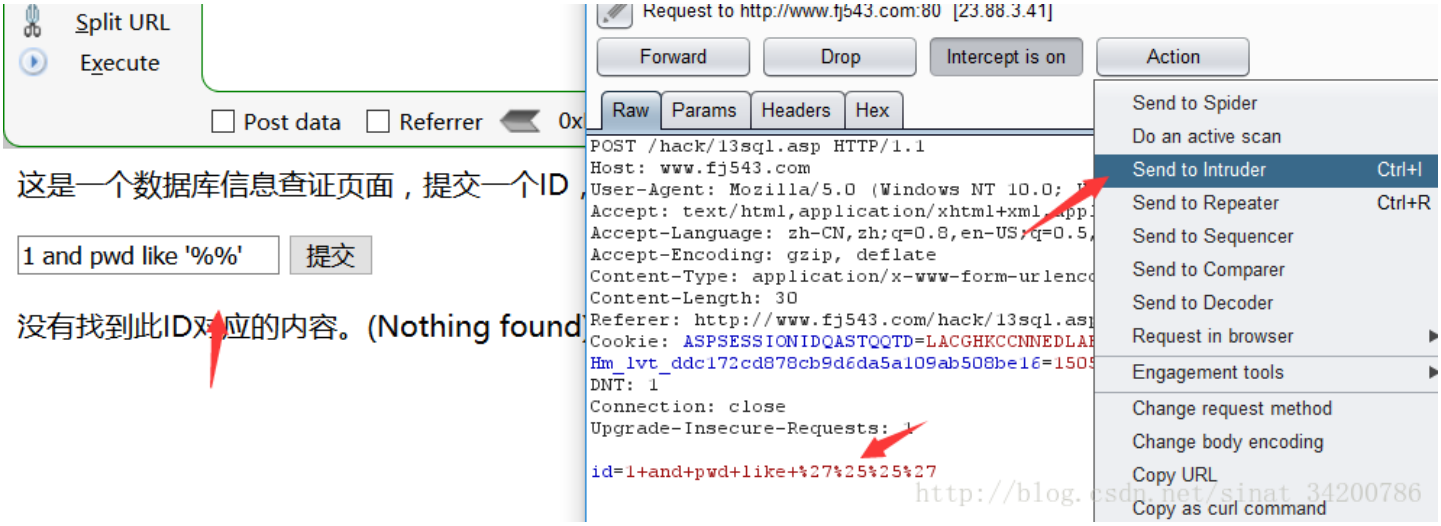
本关参考资料

```
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
```






```
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
```



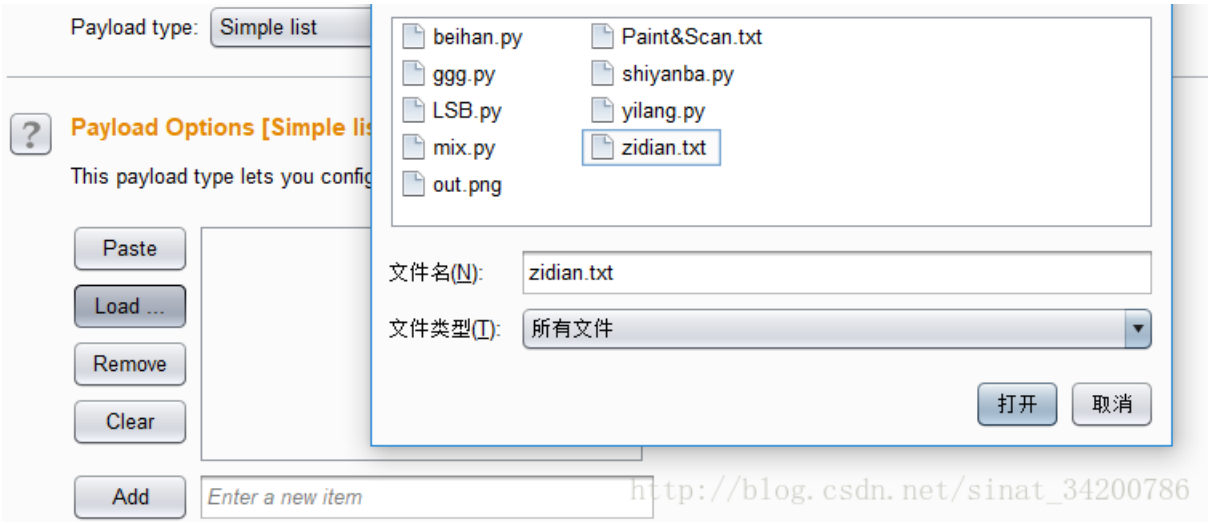
将范围限定为a-z A-Z 0-9，进行爆破

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

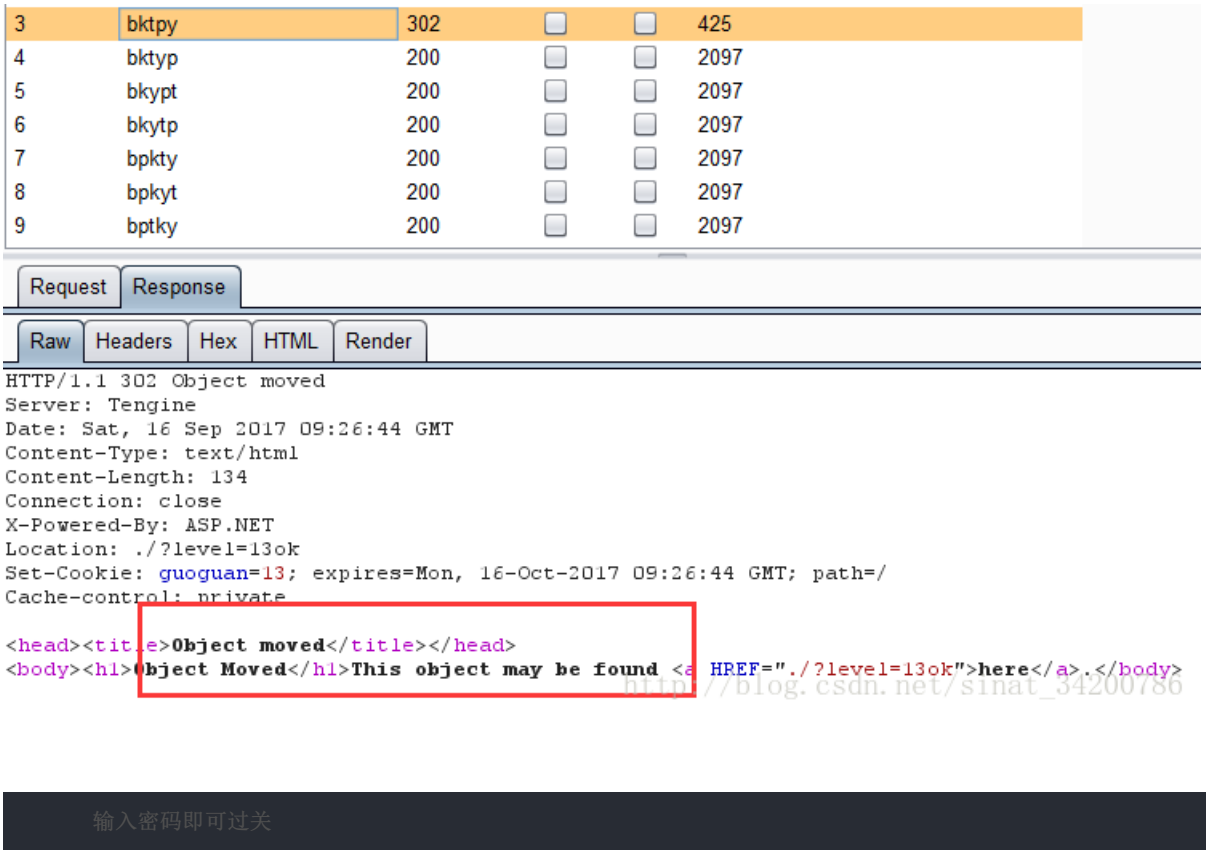
Request	Payload	Status	Error	Timeout	Length	Comment
2	b	200			652	
11	k	200			652	
16	p	200			652	
20	t	200			652	
25	y	200			652	
29	B	200			652	
38	K	200			652	
43	P	200			652	
47	T	200			652	
52	Y	200			652	


```
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



爆破出密码



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!)

第十四关

原题

现在是第14关(Level 14)

请输入令牌：(Input the token please)

Go

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

解题思路

```
逆向
```

WriteUp

本关参考资料

```
又是逆向。。，学会了再补过程
```
