铁三入门测试题writeup

原创

JBlock 于 2018-01-25 19:34:47 发布 10123 收藏

分类专栏： 漏洞 html 漏洞挖掘 文章标签： 测试 密码 管理 源码

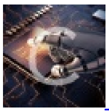
本文链接：https://blog.csdn.net/JBlock/article/details/79165754

版权

漏洞 同时被 3 个专栏收录

12 篇文章 0 订阅

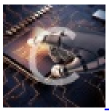
订阅专栏



html

9 篇文章 0 订阅

订阅专栏



漏洞挖掘

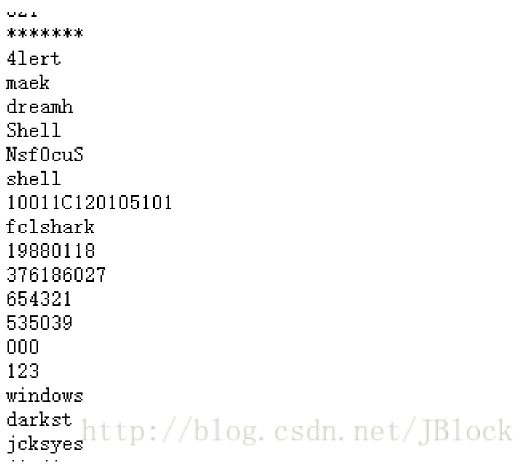
13 篇文章 0 订阅

订阅专栏

1.你是管理员吗？

解题链接：http://ctf4.shiyanbar.com/web/root/index.php

打开链接，我们发现是一个登陆页面，第一步先看页面源码，发现一个password.txt,这里面可能有东西，访问一下http://ctf4.shiyanbar.com/web/root/password.txt发现一个密码字典。



```
*******
4lert
maek
dreamh
Shell
Nsf0cuS
shell
10011C120105101
fclshark
19880118
376186027
654321
535039
000
123
windows
darkst
jcksyes
```

然后用bp爆破密码为Nsf0cuS,我们在bp的repeater里面把密码修改成Nsf0cuS,go一下

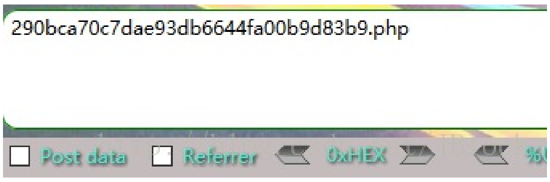
```
<form method="POST" action="">
<input type="text" name="username"
value="admin"></input><br><br>
<input type="password" name="password" maxlength="5" value=""
></input>
<input type="submit" value="□□"></input>
<br>
<br>
```

但在返回的页面里面发现密码的长度不能超过5，所以只能绕过前端在bp里面改包了。

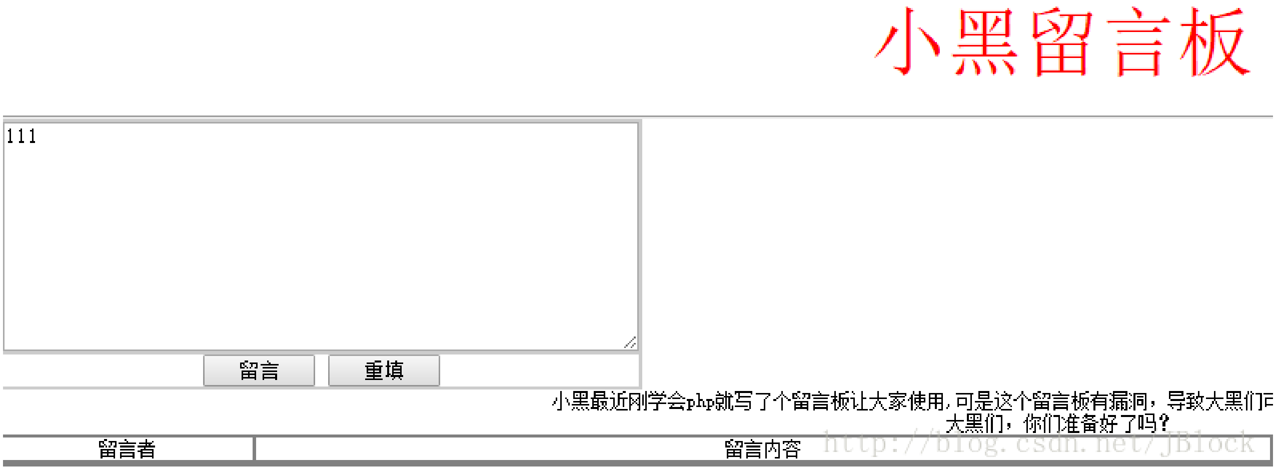
```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 25 Jan 2018 09:12:35 GMT
Content-Type: text/html
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.36
Set-Cookie:
newpage=MjkwYmNhNzBjN2RhZTkzZGI2NjQ0ZmEwMGI5ZDgzYjkucGhw;
expires=Thu, 25-Jan-2018 09:13:35 GMT; Max-Age=60
Content-Length: 1756

<html>
<head>
    <title>password.txt</title>
    <meta http-equiv="Content-Type" content="text/html;
charset=utf-8" />

</head>
<body alink="gold" bgcolor="#000000" link="gold"
text="#008000" vlink="#00c000" charset="utf-8" >
<center>
<div style="LEFT: 50%; MARGIN: -170px 0px 0px -370px; WIDTH:
780px; POSITION: absolute; TOP: 40%; HEIGHT: 330px">
<table width="668" border="0" cellpadding="3" cellspacing="3"
class="main">
  <tr>
   </tr>
<tr><td>
<center><h1>WELCOME<h1></center>
<br>
```

发现一个set-cookie就要有趣了，一般这里面都隐藏的有东西。

我们对其进行newpage后面部分base64解码得


290bca70c7dae93db6644fa00b9d83b9.php

这里面应该有东西，所以我们访问一下
http://ctf4.shiyanbar.com/web/root/290bca70c7dae93db6644fa00b9d83b9.php

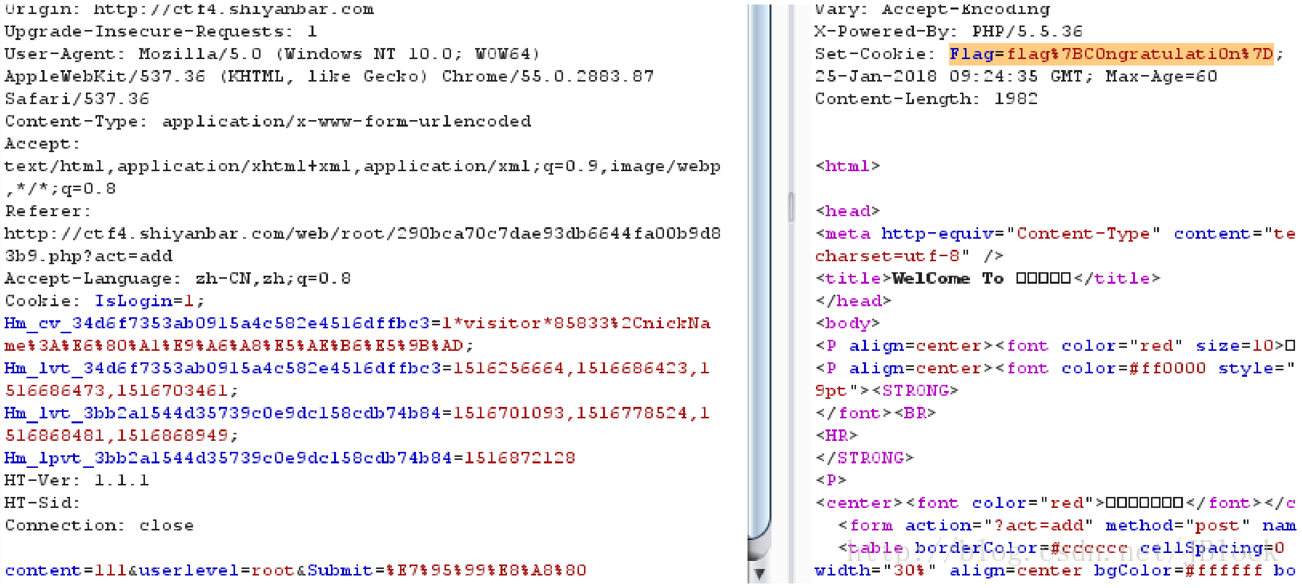

小黑留言板

111

小黑最近刚学会php就写了个留言板让大家使用,可是这个留言板有漏洞，导致大黑们F
大黑们，你们准备好了吗？

上面既然都说有漏洞了，咱就随便发个言，抓个包看看。
我们又发现有一个set-cookie，有个IsLogin的状态，看名字想必是为了标识root用户的登陆状态，此时是0，我们把它改为1，并把用户改为root。Go一下！

```
Content-Type: text/html
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.36
Set-Cookie: IsLogin=0; expires=Thu, 25-Jan-2018 09:23:26 GM
Max-Age=60
Content-Length: 1990


<html>

<head>
<meta http-equiv="Content-Type" content="text/html;
charset=utf-8" />
<title>WelCome To □□□□□</title>
</head>
<body>
<P align=center><font color="red" size=10>□□□□□</font></P>
<P align=center><font color=#ff0000 style="FONT-SIZE:
9pt"><STRONG>
</font><BR>
```



```
Origin: http://ctf4.shiyanbar.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87
Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Referer:
http://ctf4.shiyanbar.com/web/root/290bca70c7dae93db6644fa00b9d8
3b9.php?act=add
Accept-Language: zh-CN,zh;q=0.8
Cookie: IsLogin=1;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*85833%2CnickNa
me%3A%E6%80%A1%E9%A6%A8%E5%AE%B6%E5%9B%AD;
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1516256664,1516686423,1
516686473,1516703461;
Hm_lvt_3bb2a1544d35739c0e9dc158cdb74b84=1516701093,1516778524,1
516868481,1516868949;
Hm_lpvt_3bb2a1544d35739c0e9dc158cdb74b84=1516872128
HT-Ver: 1.1.1
HT-Sid:
Connection: close

content=111&userlevel=root&Submit=%E7%95%99%E8%A8%80
```

```
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.36
Set-Cookie: Flag=flag%7BC0ngratulati0n%7D;
25-Jan-2018 09:24:35 GMT; Max-Age=60
Content-Length: 1982


<html>


<head>
<meta http-equiv="Content-Type" content="te
charset=utf-8" />
<title>WelCome To □□□□□</title>
</head>
<body>
<P align=center><font color="red" size=10>□
<P align=center><font color=#ff0000 style="
9pt"><STRONG>
</font><BR>
<HR>
</STRONG>
<P>
<center><font color="red">□□□□□□□</font></c
  <form action="?act=add" method="post" nam
  <table borderColor=#cccccc cellSpacing=0
width="30%" align=center bgColor=#ffffff bo
```

得到flag=flag%7BC0ngratulati0n%7D

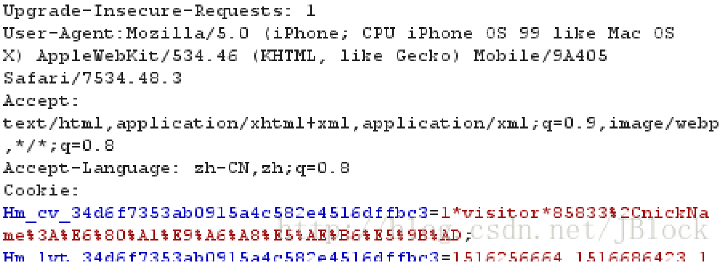
因为还未经过浏览器处理，所以还需对其进行url解码得

flag{C0ngratulati0n}

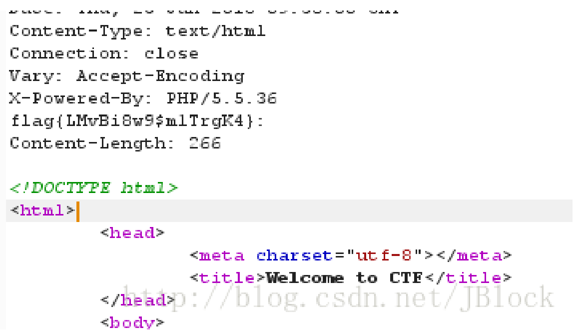
2.IOS

解题链接：http://ctf4.shiyanbar.com/web/IOS/index.php

这一题主要考察chrome浏览器本身也能模拟ios的数据包，所以我们抓包，然后把User-Agent标识改成ios99的就可以了。



```
Upgrade-Insecure-Requests: 1
User-Agent:Mozilla/5.0 (iPhone; CPU iPhone OS 99 like Mac OS
X) AppleWebKit/534.46 (KHTML, like Gecko) Mobile/9A405
Safari/7534.48.3
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8
Cookie:
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*85833%2CnickNa
me%3A%E6%80%A1%E9%A6%A8%E5%AE%B6%E5%9B%AD;
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1516256664,1516686423,1
```



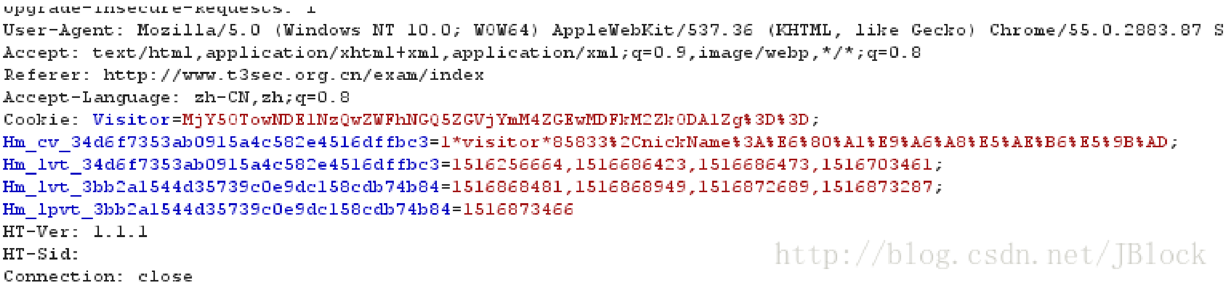
```
Content-Type: text/html
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.36
flag{LMvBi8w9$m1TrgK4}:
Content-Length: 266

<!DOCTYPE html>
<html>
        <head>
                <meta charset="utf-8"></meta>
                <title>Welcome to CTF</title>
        </head>
        <body>
```

flag{LMvBi8w9$m1TrgK4}

3.照猫画虎

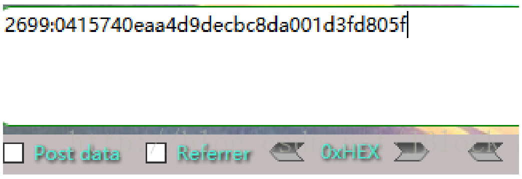
解题链接：http://ctf4.shiyanbar.com/web/copy/index.php

这一题思路也很简单，题如其名，照猫画虎，我们web题的第一步就是先看网页源码，这一题源码并没什么线索，所以我们就抓个包看看。

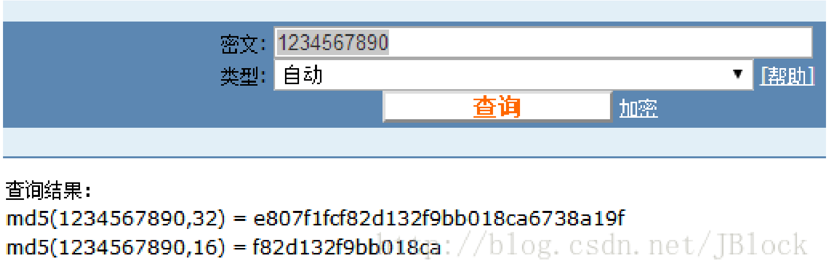


```
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 S
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://www.t3sec.org.cn/exam/index
Accept-Language: zh-CN,zh;q=0.8
Cookie: Visitor=MjY5OTowNDE1NzQwZWFhNGQ5ZGVjYmM4ZGEwMDFkM2ZkODA1Zg%3D%3D;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*85833%2CnickName%3A%E6%80%A1%E9%A6%A8%E5%AE%B6%E5%9B%AD;
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1516256664,1516686423,1516686473,1516703461;
Hm_lvt_3bb2a1544d35739c0e9dc158cdb74b84=1516868481,1516868949,1516872689,1516873287;
Hm_lpvt_3bb2a1544d35739c0e9dc158cdb74b84=1516873466
HT-Ver: 1.1.1
HT-Sid:
Connection: close
```

一般cookie和User-Agent是我们关注的重点，此时我们发现cookie中visitor项是经过base64转码的，我们对其解码：



2699:0415740eaa4d9decbc8da001d3fd805f

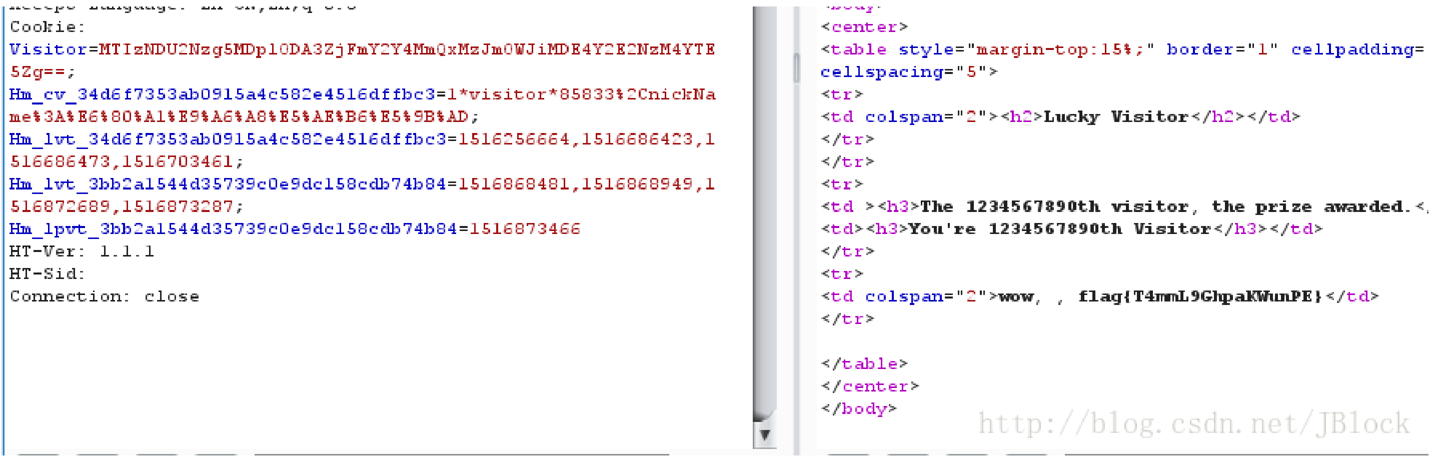


密文：1234567890

类型：自动

查询结果：
md5(1234567890,32) = e807f1fcf82d132f9bb018ca6738a19f
md5(1234567890,16) = f82d132f9bb018ca

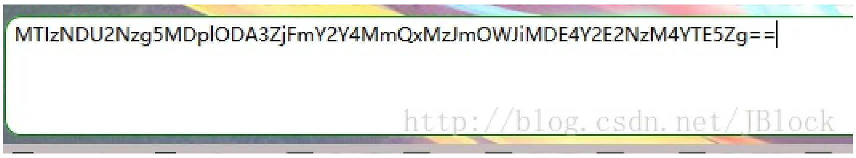
后面的一串明显是2699的32位MD5值。然后我们把请求发给repeater，看看服务器返回来的页面。



```
Cookie:
Visitor=MTIzNDU2Nzg5MDplODA3ZjFmY2Y4MmQxMzJmOWJiMDE4Y2E2NzM4YTE
5Zg==;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*85833%2CnickNa
me%3A%E6%80%A1%E9%A6%A8%E5%AE%B6%E5%9B%AD;
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1516256664,1516686423,1
516686473,1516703461;
Hm_lvt_3bb2a1544d35739c0e9dc158cdb74b84=1516868481,1516868949,1
516872689,1516873287;
Hm_lpvt_3bb2a1544d35739c0e9dc158cdb74b84=1516873466
HT-Ver: 1.1.1
HT-Sid:
Connection: close
```

```
<center>
<table style="margin-top:15%;" border="1" cellpadding=
cellspacing="5">
<tr>
<td colspan="2"><h2>Lucky Visitor</h2></td>
</tr>
</tr>
<tr>
<td ><h3>The 1234567890th visitor, the prize awarded.<
<td><h3>You're 1234567890th Visitor</h3></td>
</tr>
<tr>
<td colspan="2">wow, , flag{T4mmL9GhpaKWunPE}</td>
</tr>

</table>
</center>
</body>
```

发现只有当1234567890名访问才可以，明显是让我们修改cookie进行欺骗。我们对1234567890进行MD5加密，再对其base64转码构造payload。

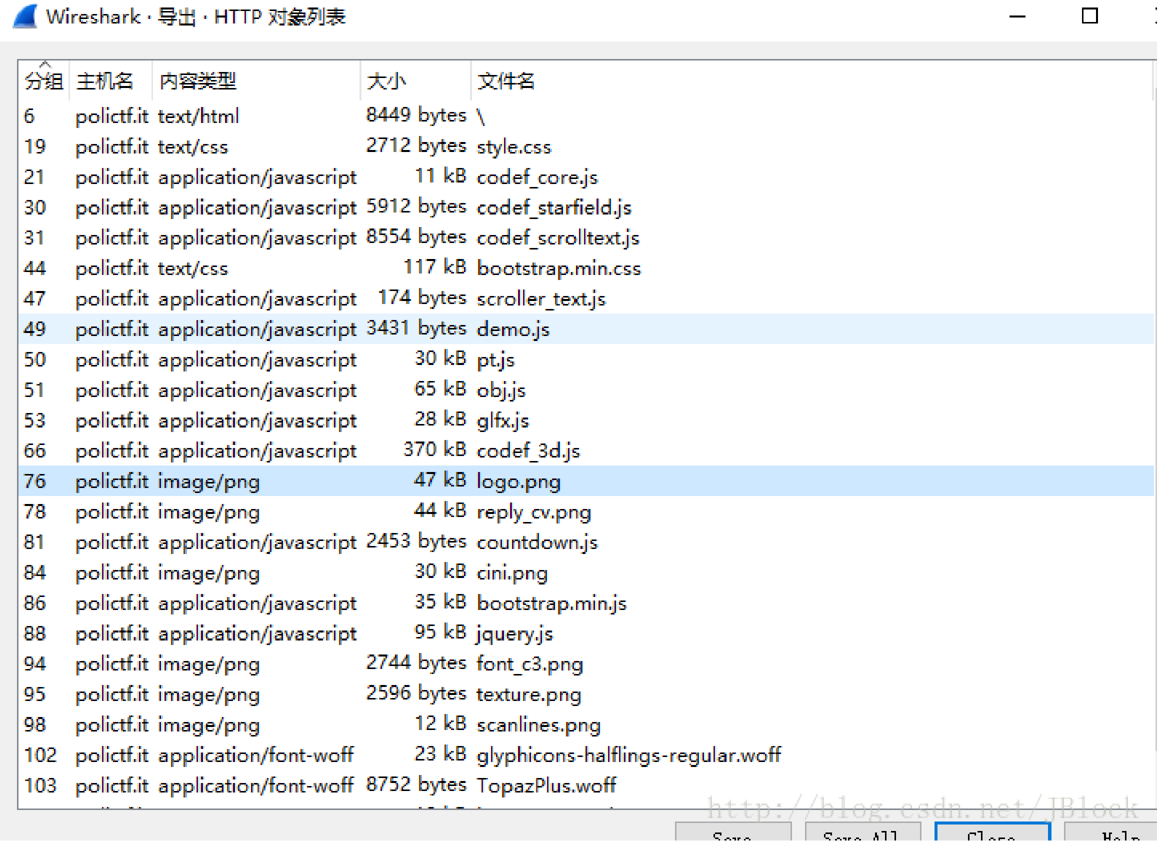


```
MTIzNDU2Nzg5MDplODA3ZjFmY2Y4MmQxMzJmOWJiMDE4Y2E2NzM4YTE5Zg==
```

flag{T4mmL9GhpaKWunPE}
4.问题就在这（20分）
【题目描述】：找答案 GPG key: GhairfAvvewvukDetolicDer-OcNayd#
【解题链接】：http://ctf4.shiyanbar.com/ste/gpg/john.tar.gz.gpg
这首先是考察gpg文件参考http://www.ruanyifeng.com/blog/2013/07/gpg.html
输入密钥key得到一个压缩包。

名称	压缩前	压缩后	类型	修改日期
.. (上级目录)			文件夹	
john-in-the-middle.pcap	395.0 KB	395.0 KB	Wireshark captu...	2015-04-24 00:08

接下来进行数据分析，跟踪一下http流，这里在linux里可以使用binwalk辅助分析，但在这一题不复杂，所以在windows使用wireshark中进行分析。

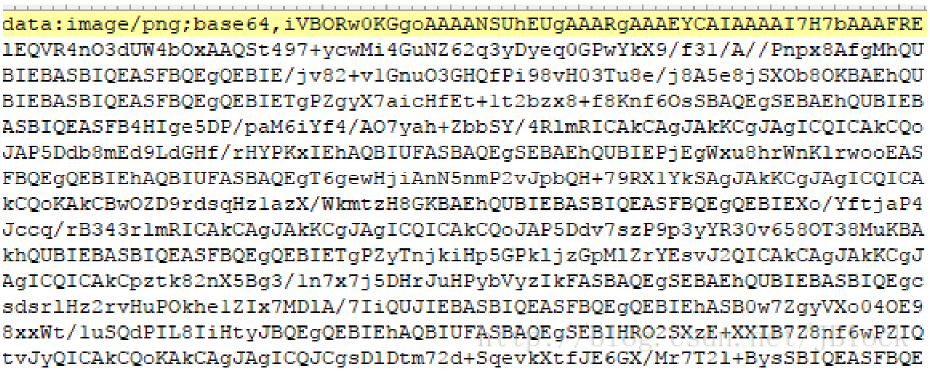


分组	主机名	内容类型	大小	文件名
6	polictf.it	text/html	8449 bytes	\
19	polictf.it	text/css	2712 bytes	style.css
21	polictf.it	application/javascript	11 kB	codef_core.js
30	polictf.it	application/javascript	5912 bytes	codef_starfield.js
31	polictf.it	application/javascript	8554 bytes	codef_scrolltext.js
44	polictf.it	text/css	117 kB	bootstrap.min.css
47	polictf.it	application/javascript	174 bytes	scroller_text.js
49	polictf.it	application/javascript	3431 bytes	demo.js
50	polictf.it	application/javascript	30 kB	pt.js
51	polictf.it	application/javascript	65 kB	obj.js
53	polictf.it	application/javascript	28 kB	glfx.js
66	polictf.it	application/javascript	370 kB	codef_3d.js
76	polictf.it	image/png	47 kB	logo.png
78	polictf.it	image/png	44 kB	reply_cv.png
81	polictf.it	application/javascript	2453 bytes	countdown.js
84	polictf.it	image/png	30 kB	cini.png
86	polictf.it	application/javascript	35 kB	bootstrap.min.js
88	polictf.it	application/javascript	95 kB	jquery.js
94	polictf.it	image/png	2744 bytes	font_c3.png
95	polictf.it	image/png	2596 bytes	texture.png
98	polictf.it	image/png	12 kB	scanlines.png
102	polictf.it	application/font-woff	23 kB	glyphicons-halflings-regular.woff
103	polictf.it	application/font-woff	8752 bytes	TopazPlus.woff

经过分析，发现只有一个logo.png对我们是有用的，
我们把它dump下来，然后对其进行隐写分析，放进stegsolve中分析

flag: flag{J0hn_th3_Sn1ff3r}
5.你最美
【题目描述】：无

【解题链接】：http://ctf4.shiyanbar.com/misc/123/123.exe
直接丢到16进制编辑器，发现是经过base64转码的png，在线解码保存为png图片。发现是一个二扫码扫码得flag。



```
data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAARgAAAEYCAIAAAAI7H7bAAAFRE
lEQVR4nO3dUW4bOxAAQSt497+ycwMi4GuNZ62q3yDyeq0GPwYkX9/f31/A//Pnpx8AfgMhQU
BIEBASBIQEASFBQEgQEBIE/jv82+v1GnuO3GHQfPi98vH03Tu8e/j8A5e8jSXOb8OKBAEhQU
BIEBASBIQEASFBQEgQEBIETgPZgyX7aicHfEt+1t2bzx8+f8Knf6OsSBAQEgSEBAEhQUBIEB
ASBIQEASFB4HIge5DP/paM6iYf4/AO7yah+ZbbSY/4RlmRICAkCCgJAkKCgJAgICQoJAP5Ddb8mEd9LdGHf/rHYPKxIEhAQBIUFASBAQEgT6gewHjiAnN5nmP2vJpbQH+79RX1YkCAgJAkKCgJAgJAgICQoJAP5Ddv7szP9p3yYR30v658OT38MuKBA
khQUBIEBASBIQEASFBQEgQEBIETgPZyTnjkiHp5GPklj zGpM1ZrYEsvJ2QICAkCAgJAkKCgJ
AgICQICAkCpztk82nX5Bg3/1n7x7j5DHrJuHPybVyzIkFASBAQEgSEBAEhQUBIEBASBIQEgc
sdsrlHz2rvHuPOkhe1ZIx7MD1A/7IiQUJIEBASBIQEASFBQEgQEBIEhASB0w7ZgyVXo04OE9
8xxWt/1uSQdPIL8IiHtyJBQEgQEBIEhAQBIUFASBAQEgSEBIHRO2SXzE+XXIB7Z8nf6wPZIQ
tvJyQICAkCQoKAkCAgJAgICQJCgsD1Dtm72d+SqevkXtfJE6GX/Mr7T21+BysSBIQEASFBQE
```

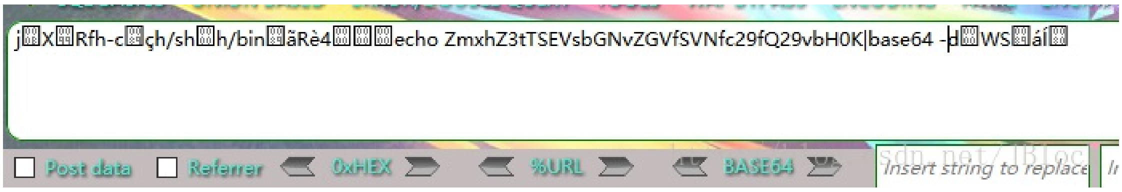
flag{you are beautiful}

6.shellcode

【题目描述】：无

【解题链接】：http://ctf4.shiyanbar.com/re/shellcode/shellcode.txt

先对其url解码，再对部分进行base64转码



```
j□□X□Rfh-c□çh/sh□h/bin□ãRè4□□□echo ZmxhZ3tTSEVsbGNvZGVfSVNfc29fQ29vbH0K|base64 -d□WS□áí□
```

```
j□□X□Rfh-c□çh/sh□h/bin□ãRè4□□□echoflag{SHEllcode_IS_so_Cool}
|base64 -d□WS□áí□
```

flag{SHEllcode_IS_so_Cool}