

# 一、环境搭建

## 1、环境介绍

源码: lmxcms 1.4  
操作系统: windows10  
靶场环境: PHPStudy v8  
审计工具: PHPStorm

## 2、搭建过程

- 1) 通过在网下载源码, 开启PHPStudy并将源码放置在www目录中
- 2) 访问<http://127.0.0.1/lmxcms1.4/install>, 进入安装页面, 根据提示完成安装即可

127.0.0.1/lmxcms1.4/install/

🔍 ☆

梦想MXcms 真免费、无授权  
lmxcms.com

lmxcms 1.4 网站系统 安装程序

1 安装使用协议 2 系统环境效验 3 参数配置 4 正在安装 5 安装完成

用户安装协议

感谢您选择使用“梦想cms”网站管理系统(以下简称lmxcms), lmxcms将打造更加人性化的cms网站系统, 而且lmxcms并不收取任何费用, 只用于交流学习, 真正的完全免费使用。  
如果您不同意以下协议中的任何一条规定, 请勿复制、下载、安装、修改、传播或以其他方式使用lmxcms。

许可您的权利:

1、您可以将lmxcms应用于任何商业用途、非商业用途、个人网站, 而不必支付任何费用。  
2、您可以根据需要对lmxcms进行必要的修改和美化, 以适应您的网站要求。  
3、您拥有使用lmxcms构建的网站中的全部内容的所有权, 并独立承担与内容相关的法律责任。

约束和限制:

1、您不得对lmxcms的源码进行出租、出售、抵押或发放子许可证。  
2、无论任何情况下, 希望您在后台保留lmxcms的相关链接和版权标识, lmxcms的发展离不开您的支持与帮助!

127.0.0.1/lmxcms1.4/install/?m=Index&a=index\_5

🔍 ☆

梦想MXcms 真免费、无授权  
lmxcms.com

lmxcms 1.0 网站系统 安装程序

1 安装使用协议 2 系统环境效验 3 参数配置 4 正在安装 5 安装完成

安装成功!

请【手动删除“/install”目录、删除“/c/install”目录】, 或者进入网站管理后台删除, 避免被恶意二次安装

后台管理 — 网站首页

Powered by lmxcms 1.4 ©2014 lmxcms Inc.

### 3、关键词

unLink

PHP删除文件函数

## 二、审计过程

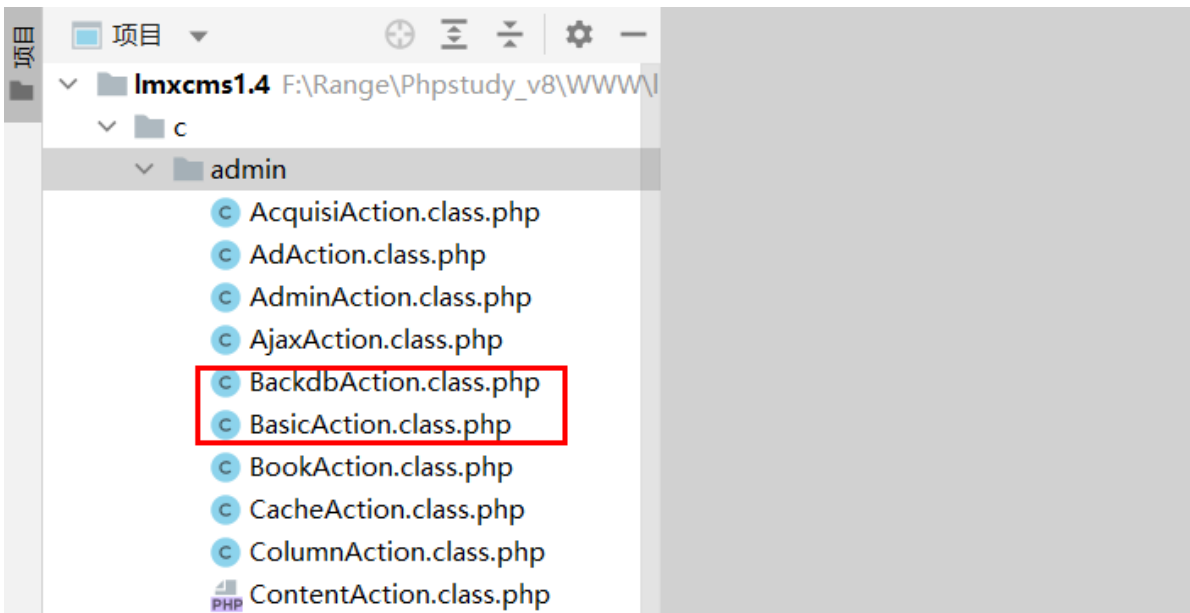
1、通过CNVD中公开的漏洞信息，得知后台的Ba\*\*\*.cl\*\*\*.php文件存在任意文件删除

## 梦想CMS后台Ba\*\*\*.cl\*\*\*.php文件存在任意文件删除漏洞

★ 关注(0)

CNVD-ID	CNVD-2020-59469
公开日期	2020-12-01
危害级别	低 (AV:N/AC:H/Au:S/C:N/I:P/A:N)
影响产品	梦想CMS LMXCMS V1.4
漏洞描述	<p>梦想CMS (Imxcms) 使用php语言和mysql数据库开发，并且采用了主流的MVC设计模式。</p> <p>梦想CMS后台Ba***.cl***.php文件存在任意文件删除漏洞。攻击者可利用漏洞删除服务器任意文件。</p>
漏洞类型	通用型漏洞
参考链接	
漏洞解决方案	厂商尚未提供漏洞修补方案，请关注厂商主页及时更新： <a href="http://www.lmxcms.com">http://www.lmxcms.com</a>

2、打开源码，可以看到两个匹配上的文件



### 3、通过关键词 unlink 函数进行定位，两个文件都是存在该函数的

```
230 //批量删除备份文件
231 public function delmorebackdb(){
232     $filename = $_POST['filename'];
233     if($filename){
234         foreach($filename as $v){
235             $this->delOne($v);
236         }
237         addlog( content: '批量删除数据库备份文件');
238         rewrite::succ( str: '删除成功');
239     }else{
240         rewrite::js_back( str: '请选择要删除的备份文件');
241     }
242 }
243 //根据文件名删除一条备份文件
244 private function delOne($filename){
245     $dir = ROOT_PATH.'file/back/'.$filename;
246     file::unlink($dir);
247 }
248 }
249 }
250 }
```

### 4、先看第一个文件，BackdbAction.class.php下的delOne()函数

- 这里的意思是使用unlink函数删除 \$dir变量
- \$dir变量是网站 ROOT\_PATH（网站根目录）下的file/back/下的\$filename变量文件

```
//根据文件名删除一条备份文件
private function delOne($filename){
    $dir = ROOT_PATH.'file/back/'.$filename;
    file::unlink($dir);
}
```

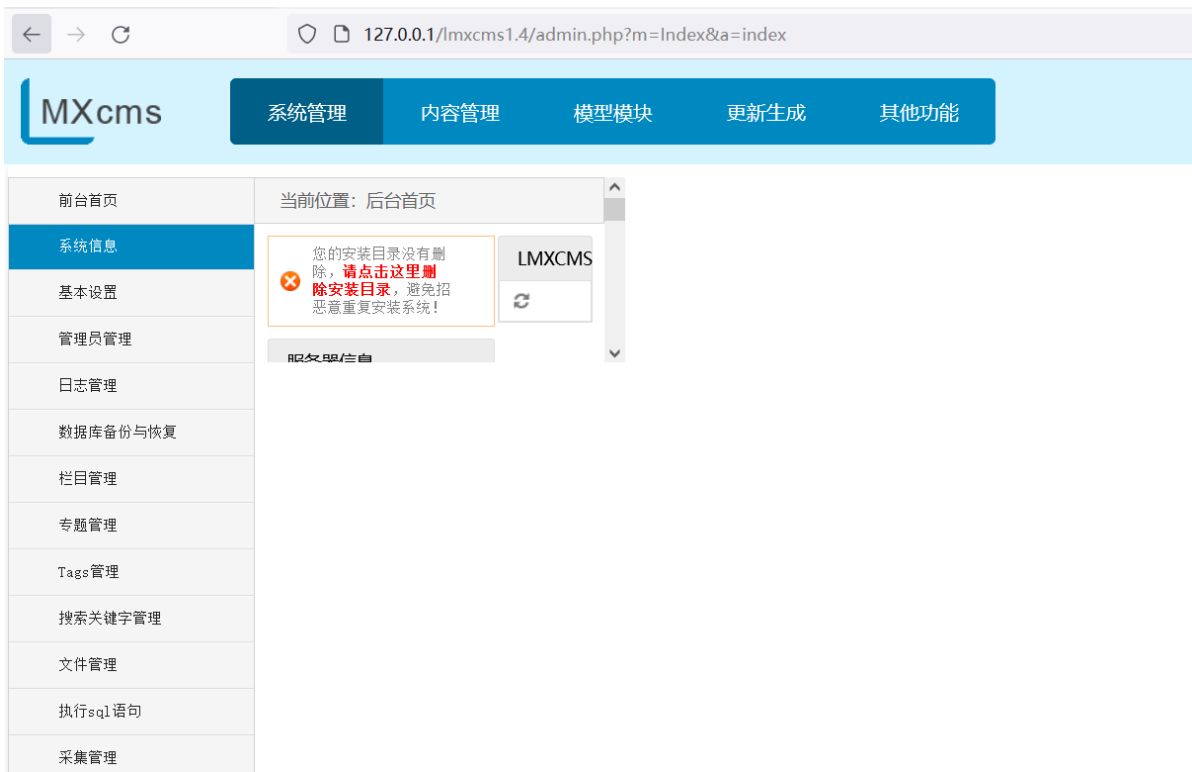
5、右击选中该函数delOne，转到 -> 声明或实例，可以看到该文件在delbackdb()函数中调用了它，通过GET方式传入filename参数，并将得到的filename值作为delOne()函数的实参

- 也就是说，通过GET传入filename值，拼接到file/back/目录下，进行删除文件
- 但是这里没有对filename的值进行过滤，也就是说可以通过../的方式目录穿越，从而达到任意文件删除

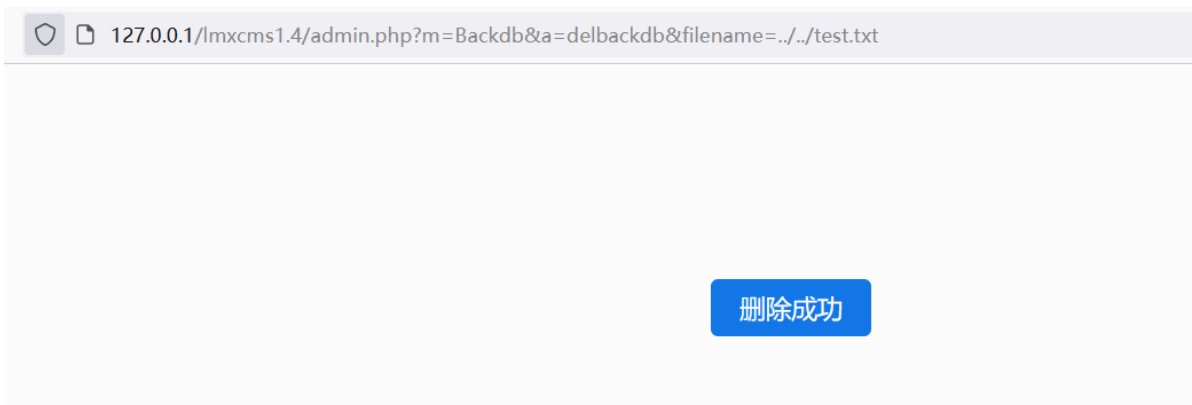
```
//删除备份文件
public function delbackdb(){
    $filename = trim($_GET['filename']);
    if(!$filename){
        rewrite::js_back( str: '备份文件不存在');
    }
    $this->delOne($filename);
    addlog( content: '删除数据库备份文件');
    rewrite::succ( str: '删除成功');
}
```

### 三、利用过程

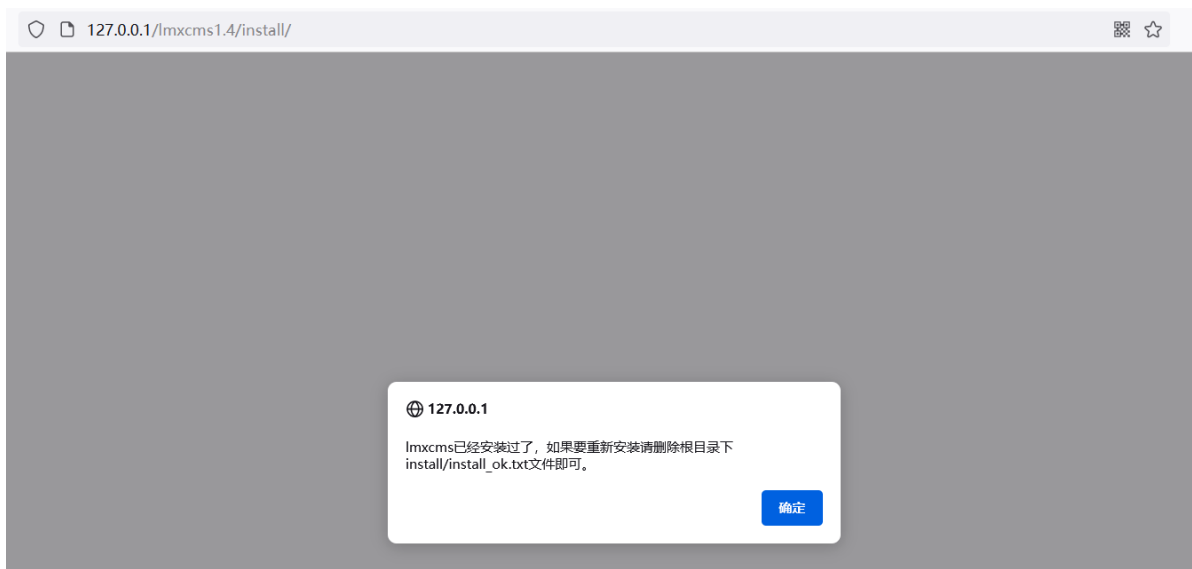
1、已知漏洞点在于网站后台，进入到admin.php，输入安装时的管理员密码进行登录



2、由于该网站是MVC架构，传入m的值为当前文件名（去除Action）Backdb，a的值为当前删除操作的函数delbackdb，filename为CMS根目录下的test.txt（自己创建的），相对于file/back/的相对路径就是../../test.txt，提示删除成功



3、那么此时将危害最大化。进入到/install/目录，可以看到如果需要重装系统，只需要删除/install/install\_ok.txt 即可



#### 4、构造Payload

- `http://127.0.0.1/lmxcms1.4/admin.php?m=Backdb&a=delbackdb&filename=../../install/install_ok.txt`



5、再次进入install目录，系统进入重装环节，此时安装的时候输入自己的数据库地址 和 管理员账号密码，也就是接管了这个网站



## 四、参考链接

审计教程: <https://www.freebuf.com/vuls/254825.html>

