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）通过在网上下载到源码，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

3、关键词

unLink	PHP删除文件函数

二、审计过程

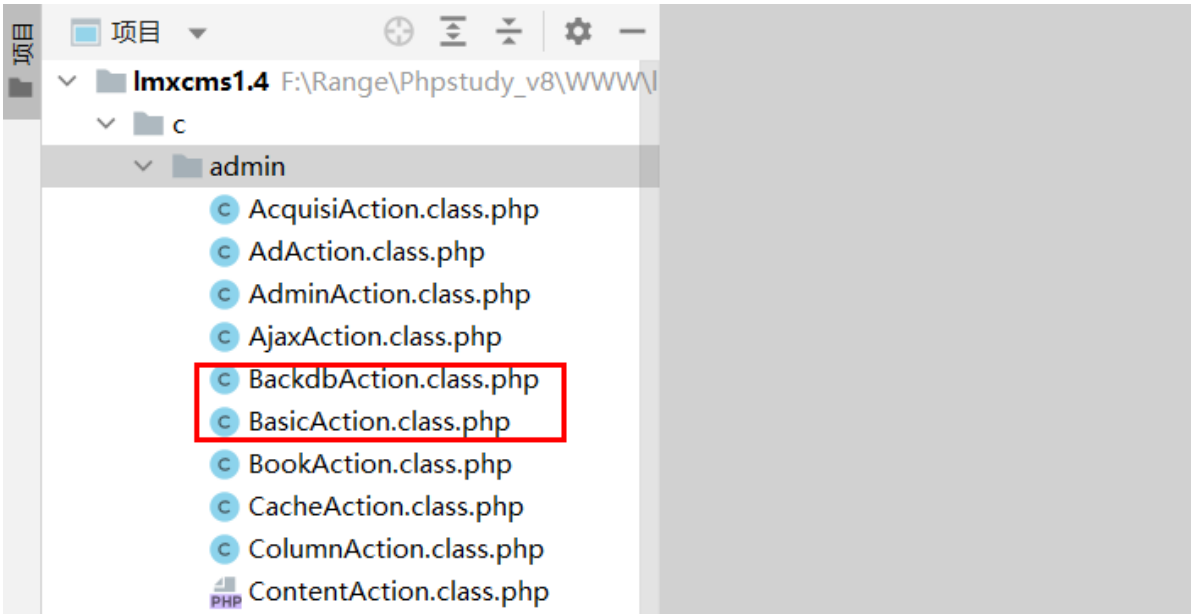
1、通过CNVD中公开的漏洞信息，得知后台的Ba*.cl*.php文件存在任意文件删除

梦想CMS后台Ba***.cl***.php文件存在任意文件删除漏洞

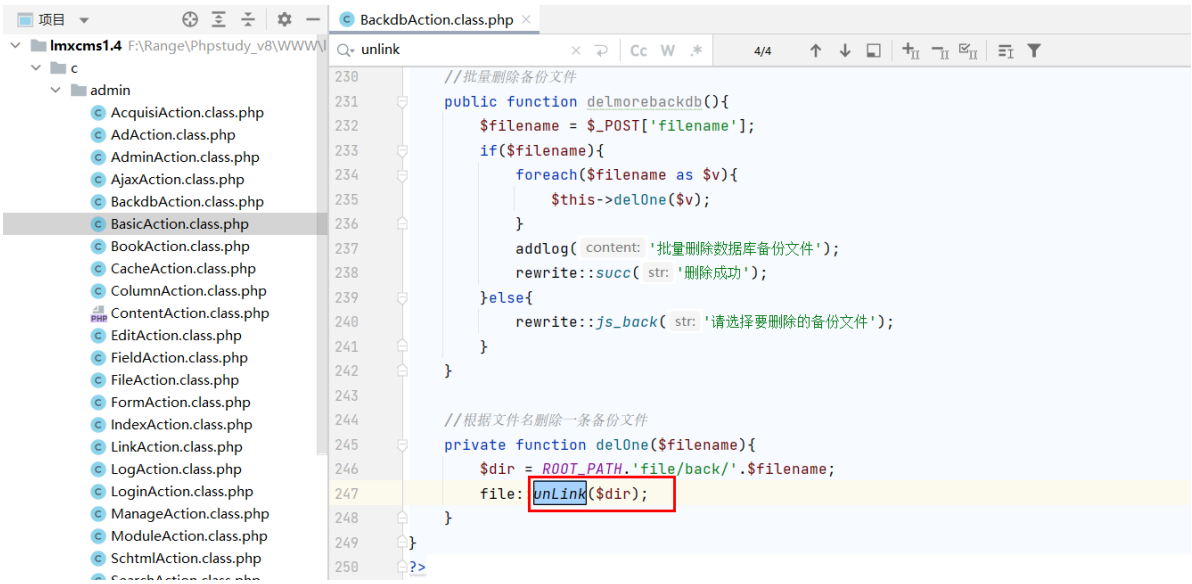
★ 关注(0)

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	梦想CMS（lmxcms）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。 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。
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： http://www.lmxcms.com

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



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

```php
//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);
}
```

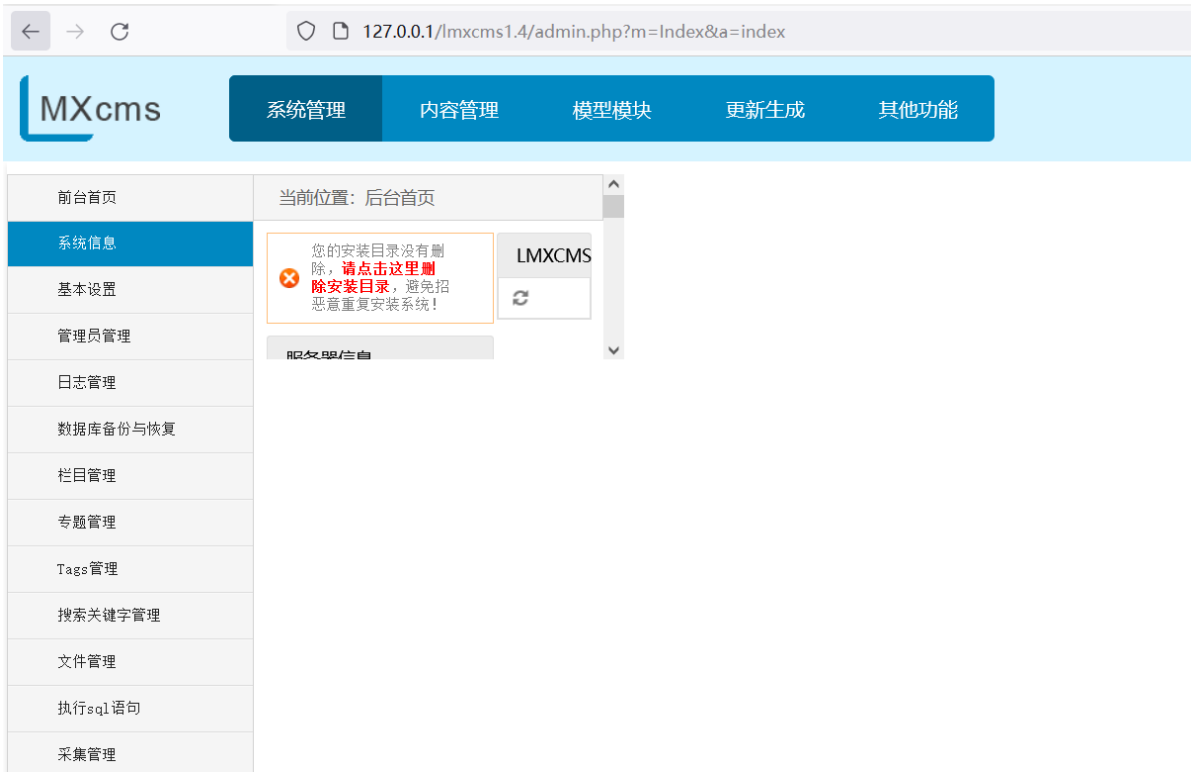
5、右击选中该函数delOne，转到 -> 声明或实例，可以看到该文件在delbackdb()函数中调用了它，通过GET方式传入filename参数，并将得到的filename值作为delOne()函数的实参

- 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

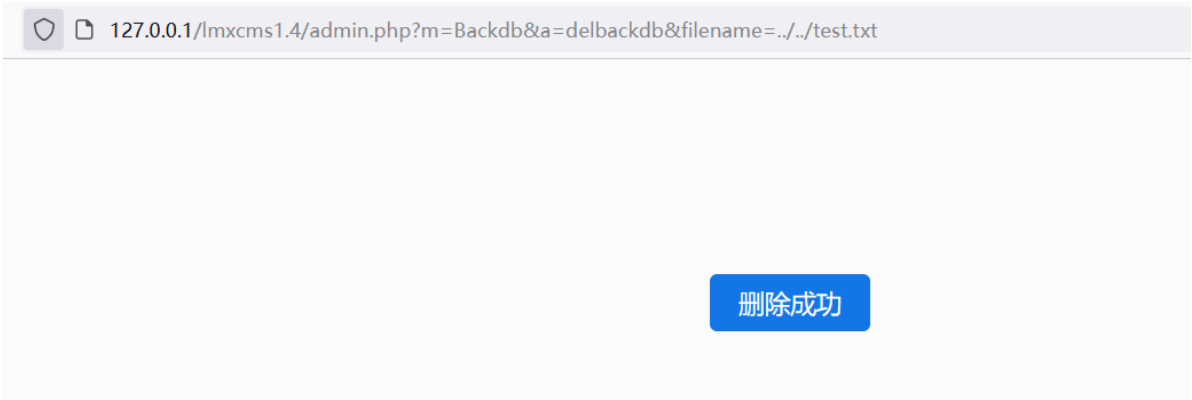
```php
//删除备份文件
public function delbackdb(){
    $filename = trim($_GET['filename']);
    if(!$filename){
        rewrite::js_back( str: '备份文件不存在');
    }
    $this->delOne($filename);
    addlog( content: '删除数据库备份文件');
    rewrite::succ( str: '删除成功');
}
```

三、利用过程

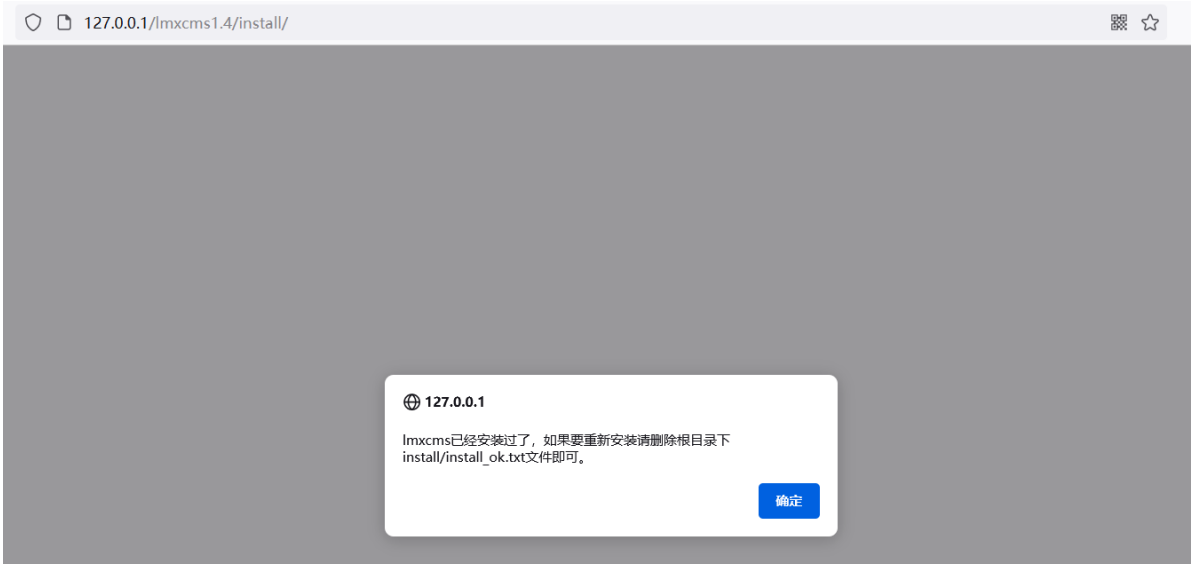
1、已知漏洞点在于网站后台，进入到admin.php，输入安装时的管理员密码进行登录



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

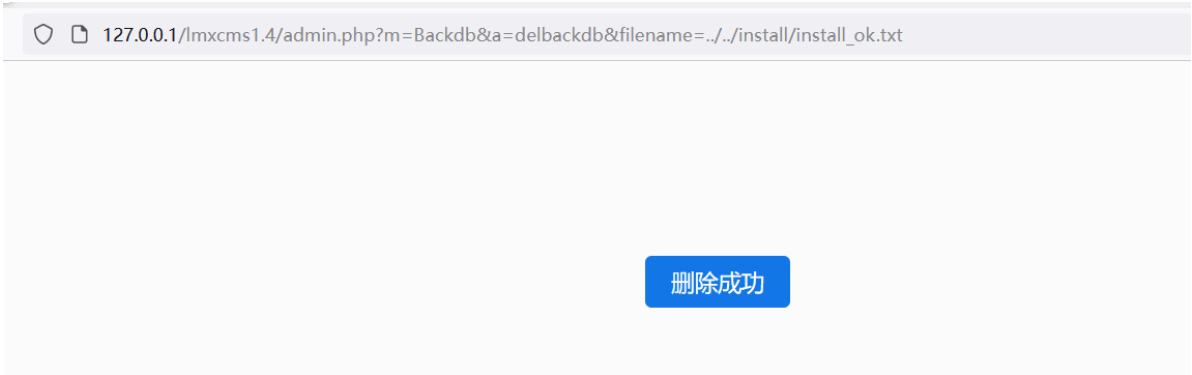


3、那么此时将危害最大化。进入到/install/目录，可以看到如果需要重装系统，只需要删除/install/install_ok.txt 即可



4、构造Paylaod

- 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