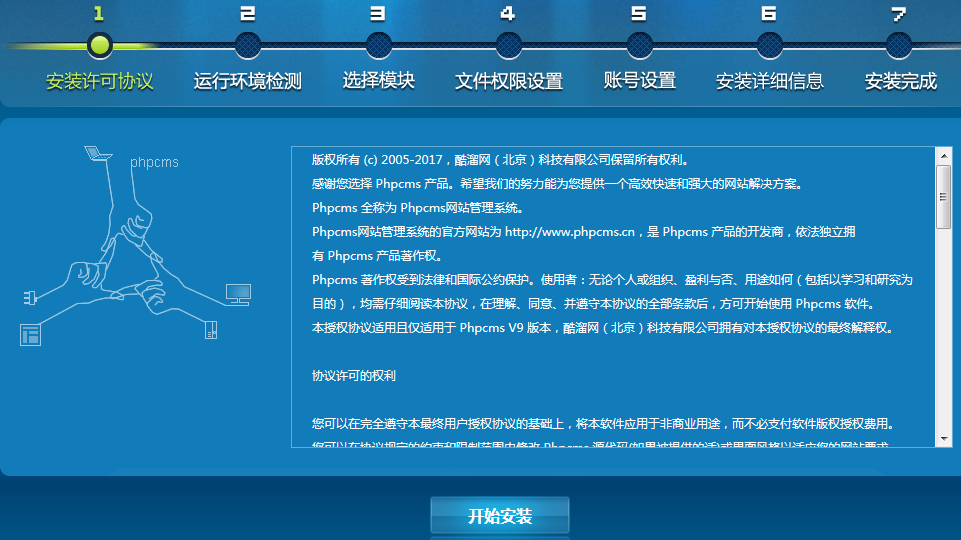
# 会员头像上传拿webshell

测试靶机：phpcms\_v9.3.4\_UTF8

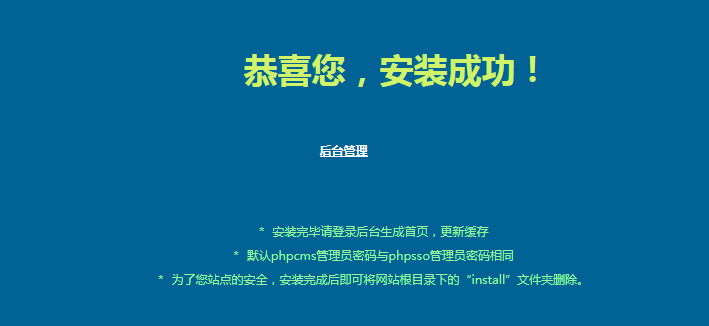
## 靶机安装









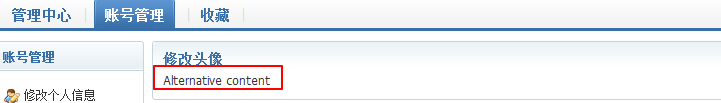


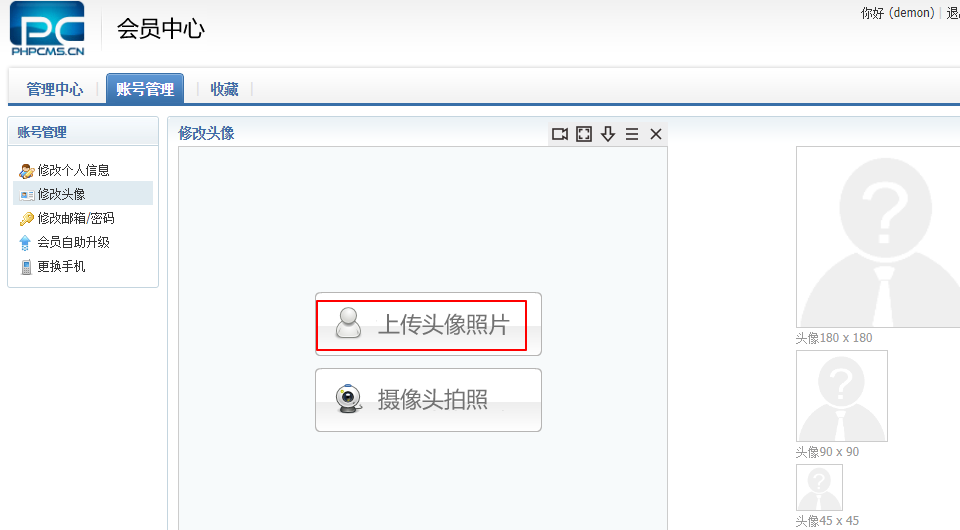
访问主页，找到账号注册





找到上传头像，如果没有显示出来，换个浏览器或者重新登录一下，火狐不行用谷歌





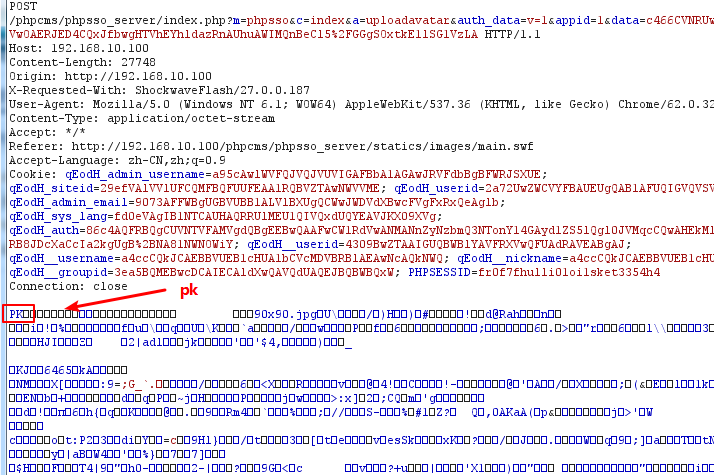
将大马 Alexa.php 放进一个文件夹压缩成zip包，然后随便上传一张图片，用burp抓包



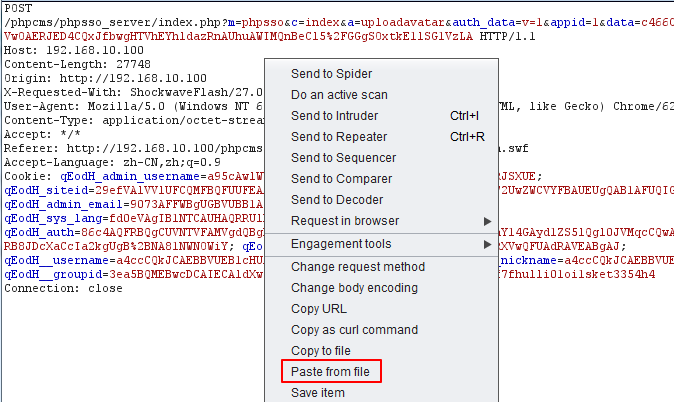
点击保存图形，brup上就可以抓到包



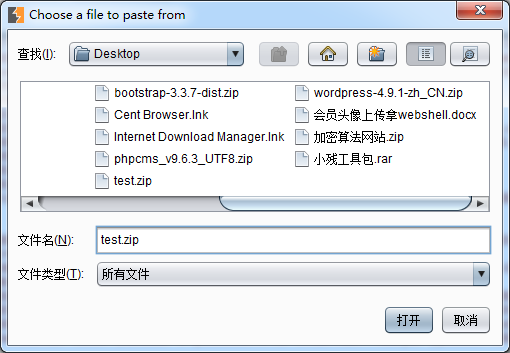
注意抓到包的内容是有PK带头的，则很有可能存在压缩包上传漏洞，有些版本没有pk带头无法上传成功，抓到后，将pk（包括pk）后面的内容全部删除



右键paste from file 粘贴我们的存放大马的zip压缩包

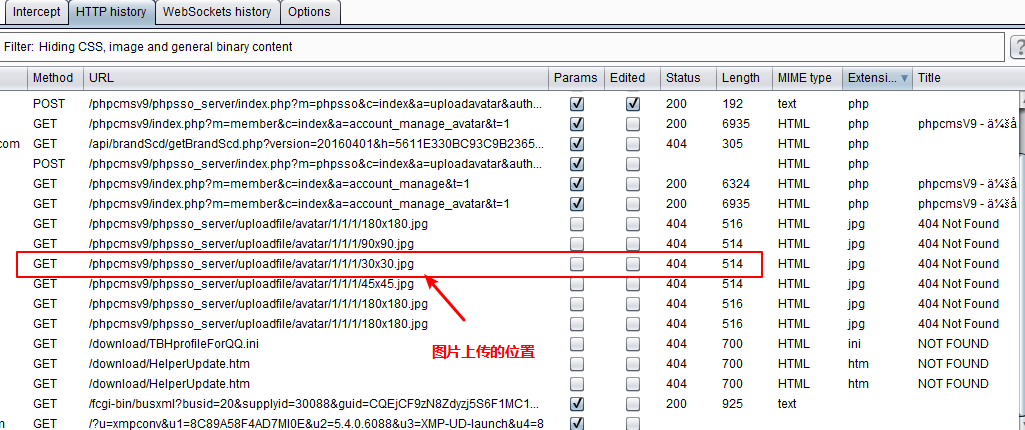


粘贴后的包头部也是有带PK的





全部转发放行，查看burp的历史记录，找到图片的上传位置



右键复制URL，将30x30.jpg 文件名改成zip解压后的路径文件名： test/Alexa.php 如下：

http://192.168.10.100/phpcms/phpsso\_server/uploadfile/avatar/1/1/1/test/Alexa.php

浏览器访问就可以看到大马了，成功拿webshell

