登录

2017年要结束了，我们是否来个年度经典漏洞汇总？

hades / 2017-12-06 16:16:00 / 浏览数 4008 安全技术 技术讨论 顶(1) 踩(0)

把大家认为比较经典的漏洞，类型不限（Php、Java、Python）都可以提名，并给出相应的分析文章地址（网上的文章都可以），方便后期的整理归类。

来吧 各抒己见吧 gogogo

来自我的推荐：

缓存函数

ThinkPHP5.0.10-3.2.3缓存函数设计缺陷可导致Getshell

随机数

php mt_rand()随机数安全

PHP-GD函数

ThinkerPHP后台InputControllerclassphp存在远程任意代码执行漏洞

点击收藏 | 0 关注 | 0

上一篇：Fix Time For Java... 下一篇：蜜罐与内网安全从0到1（四）

1. 6 条回复

刘德华 2017-12-06 16:28:22

我就先来了，都是公开的漏洞

1.Discuz! 任意文件删除漏洞
2.FFmpeg 任意文件读取漏洞
3.Apache Struts2 任意代码执行漏洞 S2-045,S2-046
4.MS17-010
5.Typecho install.php 反序列化漏洞
6.PHPCMS V9 注册模块getshell 漏洞
7.PHPCMS V9 下载模块 SQL注入漏洞

0 回复Ta

hades 2017-12-06 16:39:34

@刘德华 带上文章分析地址吧 和 漏洞类型吧 尬

0 回复Ta


guanji 2017-12-06 19:57:14

6.PHPCMS V9 注册模块getshell 漏洞 https://zhuanlan.zhihu.com/p/26646050

0 回复Ta


Mountain 2017-12-07 22:27:00

前排支持

0 回复Ta


zksmile2333 2017-12-12 11:41:41

其实一直觉得P神的 gayhub 是一个学习漏洞不错的地方，环境 测试方法都有

https://github.com/vulhub/vulhub

0 回复Ta

chris 2017-12-12 16:34:59

搞事，搞事，搞事 ‹ ›

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