【经典合集】社区原创贡献公示栏

hades / 2017-05-27 02:55:40 / 浏览数 12955 安全技术 漏洞分析 顶(0) 踩(0)

文章太多难免有些疏忽，导致文章沉底，请大伙多多包涵。如有丢失，欢迎大伙自荐，请私信我地址

@从容 ——WafBypass之道

【独家连载】我的WafBypass之道（SQL注入篇）

【独家连载】我的WafBypass之道（upload篇）

【独家连载】我的WafBypass之道（Misc篇）

@Sofia

【独家】php一句话后门过狗姿势万千之后门构造与隐藏【一】

【独家】php一句话后门过狗姿势万千之传输层加工【二】

@math1as

- 初探 relative path overwrite
- 【独家】XSS Bypass Cookbook
- 【独家】初探CSPBypass一些细节总结

@lcamry——SQLi Labs注入天书

【独家连载】mysql注入天书（一）Basic Challenges

【独家连载】mysql注入天书（二）Advanced injection

【独家连载】mysql注入天书（三）Stacked injection

【独家连载】mysql注入天书（四）Challenges

【独家】Mysql注入天书 PDF版本

@菠菜

【独家】Loki窃密木马家族分析

CVE-2017-7269—IIS 6.0 WebDAV远程代码执行漏洞分析

【独家】2017年最佳算法提名勒索软件（sega）分析

【独家】揭开CryptoShield 勒索软件的真实面目

【独家】针对俄罗斯社科院的定向勒索分析

火眼分析工具FLARE-QDB介绍

静态分析揭开Joanap木马的神秘面纱

@rainfire

- 【独家】0CTF2017 EasiestPrintf PWN技巧分析

【独家】二进制漏洞利用中的ROP技术研究与实例分析

【独家】某驱动逆向题目调试分析

Capcom Rootkit实现原理与分析(翻译）

@diffway

- 【独家】Wannacry 勒索软件分析
- 【独家】spore勒索软件分析
- 【独家】zepto勒索软件分析

@墨眉_凌迟

- 【独家】某记账App iOS客户端内购破解

@forever80s

- [某云pc客户端命令执行挖掘过程

@testme

- 从XSSer的角度测试上传文件功能

@索马里的海贼

-【11.9再次更新】CmsEasy前台无限制GetShell
-[【独家】智能硬件分析-京东来点光波入网
-DarkEye开源 免费的cloudeye.me

@v1ct0r

-CmsEasy前台无限制GetShell【Getshell的补充说明】

@wnagzihxain

- 【独家】闲聊阿里加固（一）

@doggy

- 浅谈json参数解析对waf绕过的影响

@jax777

- 【独家】关于命令注入的测试payload生成

@aqcxbom

安卓Hook函数的复杂参数如何给定？

@sanwenkit

- 通过双重跳板漫游隔离内网
- 【独家】ApachePOI的XXE漏洞本地调试（cve20165000）

@熊猫正正

- 【独家】Linux勒索样本KillDisk分析报告

@phithon

- 从Pwnhub诞生聊Django安全编码
- 【独家】Python格式化字符串漏洞（Django为例）

@shuteer

- Metasploit、Powershell之AlwaysInstallElevated提权实战
- Metasploit驰骋内网直取域管首级
- Metasploit权限提升全剧终
- 内网漫游之SOCKS代理大结局

@evi1cg

- 隐匿的攻击之-Domain Fronting
- Exec OS Command Via MSSQL

@阿松

浅谈Discuz插件代码安全（内附0day）

Chrome中"自动填充"安全性研究

@小憨

- Phpcms_V9任意文件上传(N day ...)
- Drupal 7.x Service模块SQLi & RCE 漏洞分析及EXP
- 基于MitM的RDP降级攻击
- ntfs - 3g本地提权漏洞（CVE - 2017 - 0358）

@nmask

- 分享微软MS漏洞对应的KB号（2010-2017年漏洞）
- 色情资源引发的百度网盘之战
- 文件包含漏洞(绕过姿势)
- Struts2_045漏洞批量检测脚本
- Phantomjs爬过的那些坑

@potato

- Phpcms_V9任意文件上传 漏洞分析
- phpcmsV9.5.8 后台两个低权限拿shell
- Phpcms_V9任意文件上传 -临时解决方案
- s2045漏洞分析

@cryin

- Magento2 CSRF导致任意文件上传漏洞简单分析
- phpcms v9.6.0 wap模块 SQL注入分析
- S2-046漏洞调试及初步分析
- Struts2漏洞利用原理及OGNL机制研究
- SDL软件安全设计初窥

@backlion

- Cobalt Strike搭建和使用以及bybass杀软

@heeeeen

- 【独家】原创蓝牙App漏洞系列分析之一CVE20170601

@blackwolf

- CVE原创分析b2evolution目录遍历bypass之CVE20175539
- CVE原创分析初探CVE漏洞之CVE20175480

@该隐

- 禅道9.1.2最新版免登陆SQL注入漏洞
- 禅道权限控制逻辑漏洞
- 禅道826版本一定条件getshell
- 禅道826版本SQL注入，登录绕过

@m0l1ce

- Wooyun All Bugs 10-16年所有漏洞（更新完成）

@monika

- [[原创][巨人肩膀上的矮子]XSS挑战之旅---游戏通关攻略（更新至18关）
- 一套实用的渗透测试岗位面试题

@jkgh006

- Java软WAF框架

@泳少

- 【独家】我的企业安全推动
- 【独家】一个有意思的APPLE XSS（CVE-2016-7762）的 分析与思考

@tinyfisher

- NSA 0day ETERNALBLUE 漏洞利用

@好的资源帖

- 甲方企业整体安全建设思路及坑点
- 安全书籍合集（PDF版）
- 网络安全监控实战：深入理解事件检测与响应 PDF版本
- Wireshark数据包分析实战详解
- Apache Tomcat的安全相关东西
- SFDC黑无止境之业务逻辑"漏洞"PPT分享及其他
- Linux环境下常见漏洞利用技术
- 密码找回和跨域的知识导图
- web相关的一些笔记
- 移动APP安全与SDL
- SecWiki技术分享——漏洞挖掘之逻辑漏洞
- burpsuite收集到的录像、文档以及视频资料
- BurpSuite实战指南
- 基线检查表&安全加固规范（V1.1）
- 攻击JavaWeb应用1-9[JavaWeb安全系列]

@sm0nk

- 解读2017OWASPTop10漏洞体系含接口安全
- 黑客入侵应急分析手工排查

@季雨林

- 互联网定位技术小谈
- 互联网定位技术-wifi定位介绍

@simeon

- 信息收集之SVN源代码社工获取及渗透实战

@茶码古刀

- PR的盛宴之下，不能缺席的是技术的纯真——WannaCry事件之反思

@sevck

- 一条命令引发的思考
- 老洞新姿势，记一次漏洞挖掘和利用(PHPMailer RCE)
- 浏览器中一些好玩的洞(IE/Safari)

@jeary

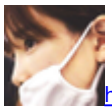
- Web日志安全分析浅谈

@紫霞仙子

- [福利贴] 精华帖或长期活跃送永久cloudeye账号 [2017-06-15更新]

上一篇：Loki窃密木马家族分析 下一篇：WAF5月挑战赛来啦 【暂停】

1. 14 条回复


hades 2017-05-27 03:43:22

感谢先知社区所有的原创贡献者

0 回复Ta


tinyfisher 2017-05-30 01:51:14

果断收藏

0 回复Ta


hades 2017-05-31 01:10:27

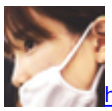
必需的嘛

0 回复Ta


泳少 2017-06-15 07:56:21

看到上榜了。吓死我

0 回复Ta


hades 2017-06-15 08:47:19

没湿，起来继续(。･ㅁ･)ﾉﾞ嗨

0 回复Ta


sevck 2017-06-18 04:14:31

竟然没我

0 回复Ta


hades 2017-06-18 04:21:09

我的锅。。马上添上

0 回复Ta


笑然 2017-07-04 06:58:19

好东西

0 回复Ta


mendickxiao 2017-07-09 02:03:12

果断收藏

0 回复Ta


xigua 2017-07-14 06:54:10

收藏,膜拜大佬们

0 回复Ta


sophone 2017-07-24 08:19:12

学习姿势

0 回复Ta


好好学习 2017-07-24 09:54:04

收藏一波

0 回复Ta


c0de 2017-09-06 04:30:12

很厉害的样子

0 回复Ta


suolong 2017-09-08 06:42:12

好东西收藏~

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