




Java注入类漏洞精选技术文章汇总

原创

Ms08067安全实验室  于 2021-05-28 12:00:00 发布  119  收藏 1

文章标签: [xhtml](#) [graphviz](#) [bmp](#) [jdbc](#) [3d](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/shuteer_xu/article/details/117376874

版权

出品 | MS08067实验室 (www.ms08067.com)

下列这些文章是团队在研究Java注入类漏洞时收集的高质量技术文章, 在此推荐给大家。

1. SQL注入

《用javaPreparedStatement就不用担心sql注入了吗? -杨元-博客园》

<https://www.cnblogs.com/iyangyuan/p/4809494.html>

《MyBatis框架中常见的SQL注入-先知社区(aliyun.com)》

<https://xz.aliyun.com/t/2343>

《MyBatis和MyBatis可能导致的sql注入)》

<https://www.sec-in.com/article/1022>

《MyBatis 和SQL 注入的恩恩怨怨 - 安全客, 安全资讯平台 (anquanke.com)》 <https://www.anquanke.com/post/id/190170>

《Hibernate HQL注入攻击入门 - FreeBuf网络安全行业门户》 <https://www.freebuf.com/news/33954.html>

《Hibernate HQL注入与防御(ctf实例) - 卿先生 - 博客园 (cnblogs.com)》 <https://www.cnblogs.com/-qing-/p/11650774.html>

2. 代码注入

《Java代码执行漏洞中类动态加载的应用》

[https://mp.weixin.qq.com/s?](https://mp.weixin.qq.com/s?__biz=MzAwNzk0NTkxNw==&mid=2247484622&idx=1&sn=8ec625711dcf87f0b6abe67483f0534d)

[__biz=MzAwNzk0NTkxNw==&mid=2247484622&idx=1&sn=8ec625711dcf87f0b6abe67483f0534d](https://mp.weixin.qq.com/s?__biz=MzAwNzk0NTkxNw==&mid=2247484622&idx=1&sn=8ec625711dcf87f0b6abe67483f0534d)

《从零开始学java web - struts2 RCE分析· LoRexxar's Blog》 <https://lorexar.cn/2019/09/23/javaweb-S2/>

《Java下奇怪的命令执行 (lmxspace.com)》

<http://www.lmxspace.com/2019/10/08/Java下奇怪的命令执行/>

《Java 回显综述(seebug.org)》

<https://paper.seebug.org/1442/>

《java反序列化RCE回显研究 - 先知社区 (aliyun.com)》

<https://xz.aliyun.com/t/5257>

3.模板注入

《Freemarker模板注入 Bypass - 先知社区 (aliyun.com)》 <https://xz.aliyun.com/t/4846>

《Apache Struts2 Freemarker标签远程执行漏洞分析和复现(S2-053) - 先知社区 (aliyun.com)》

<https://xz.aliyun.com/t/68>

《服务端模板注入攻击 - 知乎 (zhihu.com)》

<https://zhuanlan.zhihu.com/p/28823933>

4.表达式注入

《Java 表达式注入 | Y4er的博客》

<https://y4er.com/post/java-expression-injection/>

《由浅入深SpEL表达式注入漏洞 - Ruilin (rui0.cn)》

<http://rui0.cn/archives/1043>

《浅析EL表达式注入漏洞 - 先知社区 (aliyun.com)》

<https://xz.aliyun.com/t/7692>

《Struts2 中的OGNL、表达式注入及防御》

https://mp.weixin.qq.com/s/8YxQPDU6sx-w_04BrBCEmw

《泛微E-Mobile Ognl 表达式注入 (ioin.in)》

https://docs.ioin.in/writeup/www.sh0w.top/_index_php_archives_14_/index.html

《Spring 全家桶各类 RCE 漏洞浅析》
<https://paper.seebug.org/1422/>

观看《Java代码安全审计（入门篇）》配套讲解视频及技术解答

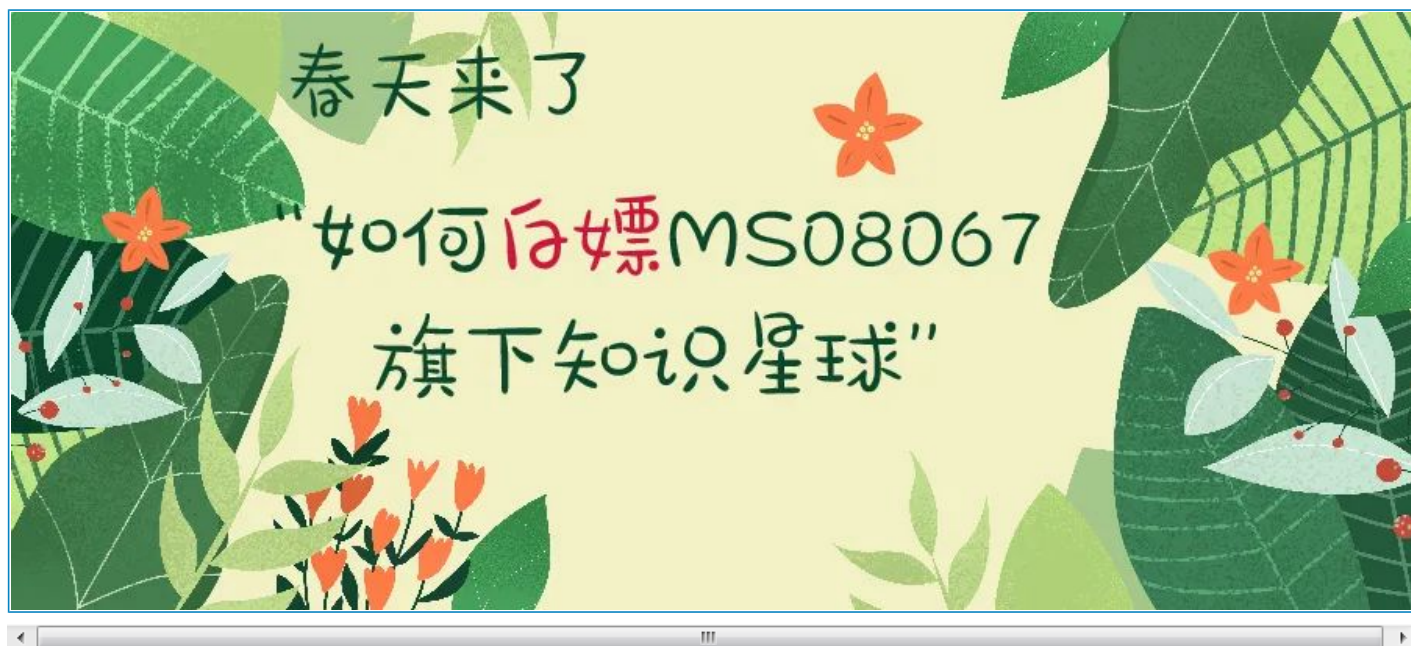
可加入“java代码审计”配套星球

星球建立的根本性目的是“通过较详细的漏洞点剖析以及代码审计的实战演示”帮助读者能够更快的入门Java代码审计，从此迈入Java代码审计的大门。

扫描下方二维码查看星球具体内容，星球附赠全书完整全套源码、工具及环境、配套的Docker镜像！

PS: 广而告之

- 1.同时购买多个星球享受最低至6.3折折扣（第1个原价，第2个8.8折，第3个8.3折，第4个7.8折，第5个7.3折，第6个6.8折，第7个6.3折）
- 2.三人成团，一起购买可在享受第一条折扣基础上再合并打9折
- 3.支持分期付款及花呗付费
- 4.分享有礼，16%分享奖励，以当前价格计，您只需将我们推荐给6位付费新星友，您就完全赚回“门票”支出了



扫描下方二维码加入星球学习

加入后会邀请你进入内部微信群，内部微信群永久有效！



WEB攻防【Ms08067】

星主：徐哥

知识星球

微信扫码预览星球详情



Ms08067安全实验室



0基础逆向【Ms08067】

星主：徐哥

知识星球

微信扫码预览星球详情



Ms08067安全实验室



Java代码安全审计【Ms08067】

星主：徐哥

知识星球

微信扫码预览星球详情



Ms08067安全实验室



内网攻防【Ms08067】

星主：徐哥

知识星球

微信扫码预览星球详情



Ms08067安全实验室



Python 【Ms08067】

星主： 徐哥

知识星球

微信扫码预览星球详情



Ms08067安全实验室



Kali安全 【Ms08067】

星主： 徐哥

知识星球

微信扫码预览星球详情



Ms08067安全实验室

加入星球和5000位同学一起学习

