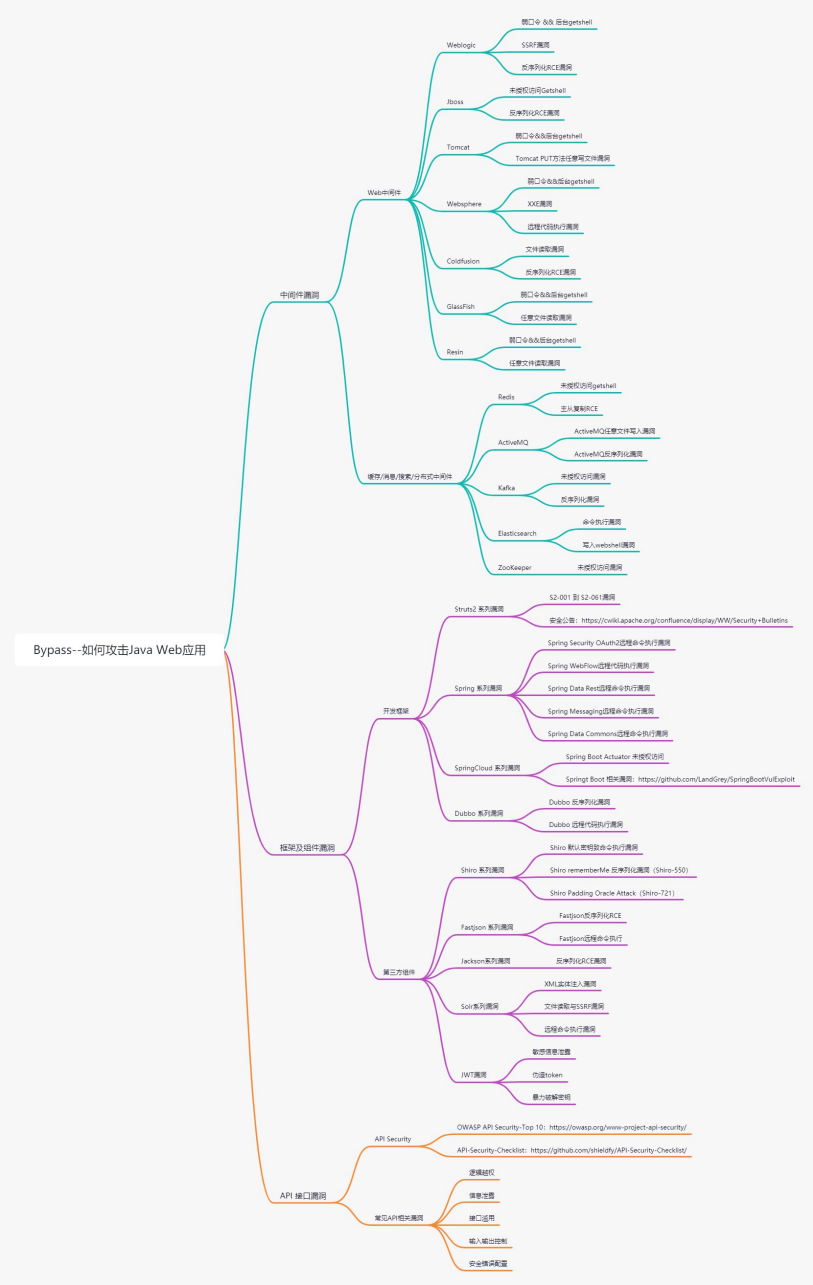
专注于网络安全

一张图告诉你，如何攻击Java Web应用

越来越多的企业采用Java语言构建企业Web应用程序，基于Java主流的框架和技术及可能存在的风险，成为被关注的重点。

本文从黑盒渗透的角度，总结下Java Web应用所知道的一些可能被利用的入侵点。



1、中间件漏洞

基于Java的Web项目部署会涉及一些中间件，一旦中间件配置不当或存在高危漏洞，就会严重影响到整个系统的安全。

1.1 Web中间件

Weblogic系列漏洞： 弱口令 && 后台getshell、 SSRF漏洞、反序列化RCE漏洞

Jboss系列漏洞： 未授权访问Getshell、 反序列化RCE漏洞

Tomcat系列漏洞： 弱口令&&后台getshell、 Tomcat PUT方法任意写文件漏洞

Websphere系列漏洞： 弱口令&&后台getshell、 XXE漏洞、远程代码执行漏洞

Coldfusion系列漏洞： 文件读取漏洞、 反序列化RCE漏洞

GlassFish系列漏洞： 弱口令&&后台getshell、 任意文件读取漏洞

搜索

找找看

谷歌搜索

积分与排名

积分 - 669451

排名 - 561

随笔分类 (367)

CISSP 备考笔记(9)

DevSecOps(8)

ELK学习笔记(2)

Python安全开发(23)

WAF Bypass(25)

安全运维(45)

代码审计(30)

企业安全(37)

权限维持(18)

渗透测试(106)

渗透利器(9)

生活感悟(20)

应急响应(27)

域渗透(8)

随笔档案 (414)

Resin系列漏洞： 弱口令&&后台getshell、 任意文件读取漏洞

1.2 缓存/消息/搜索/分布式中间件

Redis系列漏洞： 未授权访问getshell、 主从复制RCE

ActiveMQ系列漏洞： ActiveMQ任意文件写入漏洞、 ActiveMQ反序列化漏洞

Kafka系列漏洞： 未授权访问漏洞、 反序列化漏洞

Elasticsearch系列漏洞： 命令执行漏洞、 写入webshell漏洞

ZooKeeper系列漏洞： 未授权访问漏洞 框

2、框架及组件漏洞

基于Java开发的Web应用，会使用到各种开发框架和第三方组件，而随着时间推移，这些框架和组件可能早已不再安全了。

2.1 开发框架

2.1.1 Struts2 系列漏洞

S2-001到S2-061漏洞

安全公告：https://cwiki.apache.org/confluence/display/WW/Security+Bulletins

2.1.2 Spring 系列漏洞

Spring Security OAuth2远程命令执行漏洞

Spring WebFlow远程代码执行漏洞 Spring Data Rest远程命令执行漏洞

Spring Messaging远程命令执行漏洞 Spring Data Commons远程命令执行漏洞

2.1.3 SpringCloud 系列漏洞

Spring Boot Actuator 未授权访问

Springt Boot 相关漏洞：https://github.com/LandGrey/SpringBootVulExploit

2.1.4 Dubbo 系列漏洞

Dubbo 反序列化漏洞、Dubbo 远程代码执行漏洞

2.2、第三方组件

2.2.1 Shiro 系列漏洞

Shiro 默认密钥致命令执行漏洞、Shiro rememberMe 反序列化漏洞 (Shiro-550)

Shiro Padding Oracle Attack (Shiro-721)

2.2.2 Fastjson 系列漏洞

Fastjson反序列化RCE、Fastjson远程命令执行

2.2.3 Jackson系列漏洞

反序列化RCE漏洞

2.2.4 Solr系列漏洞

XML实体注入漏洞、文件读取与SSRF漏洞、远程命令执行漏洞

2.2.5 JWT漏洞

2021年9月(4)
2021年8月(5)
2021年7月(2)
2021年6月(1)
2021年5月(3)
2021年3月(3)
2021年2月(7)
2021年1月(10)
2020年12月(3)
2020年11月(11)
2020年10月(4)
2020年9月(6)
2020年8月(7)
2020年7月(9)
2020年6月(6)
更多

阅读排行榜

1. python线程池（threadpool）模块使用笔记(126706)
2. XSS跨站脚本小结(45324)
3. Shiro反序列化漏洞利用汇总（Shiro-550+Shiro-721）(42004)
4. Elasticsearch未授权访问漏洞(35792)

敏感信息泄露、伪造token、暴力破解密钥

3、API 接口漏洞

基于前后端分离的开发模式，都需要通过调用后端提供的接口来进行业务交互，api接口安全测试是一项非常重要的任务。

3.1 API Security

```
OWASP API Security-Top 10: https://owasp.org/www-project-api-security/
API-Security-Checklist: https://github.com/shieldfy/API-Security-Checklist/
```

3.2 常见API相关漏洞

逻辑越权 信息泄露 接口滥用 输入输出控制 安全错误配置

本文由Bypass整理发布，转载请保留出处。欢迎关注我的个人微信公众号：Bypass --，浏览更多精彩文章。

分类： 渗透测试

Bypass
关注 - 9
粉丝 - 345
+加关注

0 0

« 上一篇： 静态代码分析工具清单
» 下一篇： 微信小程序反编译解包教程

posted @ 2021-07-11 19:55 Bypass 阅读(289) 评论(0) 编辑 收藏 举报

5. 手机验证码常见漏洞总结(34430)

评论排行榜

1. python线程池（threadpool）模块使用笔记(4)
2. 揭秘骗局：这是一张会变的图片(3)
3. JWT攻击手册：如何入侵你的Token(2)
4. 搭建rsyslog日志服务器(2)
5. 蜜罐搭建(2)

推荐排行榜

1. python线程池（threadpool）模块使用笔记(6)
2. Shiro反序列化漏洞利用汇总（Shiro-550+Shiro-721）(3)
3. 跨站脚本（XSS）备忘单-2019版(3)
4. JWT攻击手册：如何入侵你的Token(3)
5. Redis主从复制getshell技巧(2)

最新评论

1. Re:揭秘骗局：这是一张会变的图片

我也一样的方式被骗，求指教。qq1070253646

--尊大大

2. Re:由OSS AccessKey泄露引发的思考

可以

--h0er

3. Re:Docker逃逸--脏牛漏洞POC测试

你好，我想问下我运行之后显示this vDSO

· 技术管理进阶——管人还是管事?
· 以终为始：如何让你的开发符合预期
· 五个维度打造研发管理体系
· 不会SQL也能做数据分析？浅谈语义解析领域的机会与挑战
· Spring IoC Container 原理解析

最新新闻:
· 宁德时代的鱿鱼游戏（2021-10-21 22:38）
· 法拉第未来中国前员工收到补薪！网友：贾跃亭还钱了（2021-10-21 22:33）
· 登顶中国互联网新首富 对张一鸣意味着什么（2021-10-21 22:32）
· 蚂蚁反诈治理报告：已在全国100个县城、3200个社区开展防骗教育（2021-10-21 22:28）
· "腾讯清理大师"等14款移动应用存在隐私不合规行为（2021-10-21 22:20）
» 更多新闻...

version isn't supported add first entry point instructions to prologue 这个应该怎...

--wlnancy

4. Re:Linux 入侵痕迹清理技巧

dalao， 这里是/var/log/messages不是/var/log/message。这里写错了，但是下面是正确的。 除此之外，/var/log/cron.log和/var/spool/mail...

--夜尽终会天明

5. Re:蜜罐搭建

我在： 2021年 4月 11日 18:30:57 看过本篇博客!

--努力变胖-HWP