



Search or jump to...



Pull requests

Issues

Marketplace

Explore



r0eXpeR/redteam_vul

Watch 6

Star 92

Fork 20

Code Issues Pull requests Actions Projects Wiki Security Insights

main

1 branch

0 tags

Go to file

Add file

Code



r0eXpeR Update README.md

cc9fd84 13 days ago

3 commits



README.md

Update README.md

13 days ago

README.md

About

红队作战中比较常遇到的一些重点系统漏洞整理。

redteam security hacking

Readme

Releases

No releases published

Packages

No packages published

红队中易被攻击的一些重点系统漏洞整理

一、OA系统

泛微(Weaver-Ecology-OA)

- ◆ 泛微OA E-cology RCE(CNVD-2019-32204) - 影响版本7.0/8.0/8.1/9.0
- ◆ 泛微OA WorkflowCenterTreeData接口注入(限oracle数据库)
- ◆ 泛微ecology OA数据库配置信息泄露
- ◆ 泛微OA云桥任意文件读取 - 影响2018-2019 多个版本
- ◆ 泛微 e-cology OA 前台SQL注入漏洞
- ◆ 泛微OA系统 com.eweaver.base.security.servlet.LoginAction 参数keywordid SQL注入漏洞
- ◆ 泛微 OA sysinterface/codeEdit.jsp 页面任意文件上传

致远(Seeyon)

- ◆ 致远OA-A8 htmlofficeservlet getshell 漏洞
- ◆ 致远OA Session泄露漏洞
- ◆ 致远OA A6 search_result.jsp sql注入漏洞
- ◆ 致远OA A6 setextno.jsp sql注入漏洞
- ◆ 致远OA A6 重置数据库账号密码漏洞
- ◆ 致远OA A8 未授权访问
- ◆ 致远OA A8-v5 任意用户密码修改
- ◆ 致远OA A8-m 后台万能密码
- ◆ 致远OA 帆软报表组件 前台XXE漏洞

蓝凌OA

暂无(希望大佬能提供)

通达OA

- ◆ 通达OA任意文件删除&文件上传RCE分析(2020年hw 8月0day)
- ◆ 通达OA任意文件上传/文件包含GetShell
- ◆ 通达OA<11.5版本 任意用户登录
- ◆ 通达OA 11.2后台getshell
- ◆ 通达OA 11.7 后台sql注入getshell漏洞

金蝶OA

- ◆ 金蝶协同办公系统 GETSHELL漏洞

二、E-mail

Exchange

- ◆ CVE-2020-17083 Microsoft Exchange Server 远程执行代码漏洞
- ◆ Microsoft Exchange远程代码执行漏洞 (CVE-2020-16875)
- ◆ CVE-2020-0688_微软EXCHANGE服务的远程代码执行漏洞
- ◆ Microsoft Exchange任意用户伪造漏洞
- ◆ Exchange 历史漏洞合集

coremail

- ◆ coremail 配置信息泄露及接口未授权漏洞
- ◆ Coremail的存储型XSS漏洞
- ◆ Coremail 历史漏洞合集

三、web中间件

Apache

- ◆ Apache Solr RCE—【CVE-2019-0192】
- ◆ CVE-2018-1335:Apache Tika 命令注入
- ◆ Apache Axis1(<=1.4版本) RCE
- ◆ Apache Solr 模版注入漏洞(RCE)
- ◆ Apache Shiro权限绕过漏洞(CVE-2020-11989)
- ◆ Shiro remeberMe反序列化漏洞(Shiro-550)
- ◆ Apache历史漏洞合集

Tomcat

- ◆ Tomcat信息泄漏和远程代码执行漏洞【CVE-2017-12615/CVE-2017-12616】
- ◆ Tomcat Ghostcat - AJP协议文件读取/文件包含漏洞

- ◆ Tomcat全版本命令执行漏洞 CVE-2019-0232
- ◆ Tomcat后台部署war木马getshell
- ◆ CVE-2016-1240 Tomcat本地提权漏洞
- ◆ Tomcat历史漏洞合集

Weblogic

- ◆ CVE-2020-14882 Weblogic 未经授权绕过RCE
- ◆ Weblogic 远程命令执行漏洞分析(CVE-2019-2725)
- ◆ CVE-2019-2618任意文件上传漏洞
- ◆ WebLogic XMLDecoder反序列化漏洞(CVE-2017-10271)
- ◆ Weblogic任意文件读取漏洞(CVE-2019-2615)与文件上传漏洞(CVE-2019-2618)
- ◆ Weblogic coherence组件iiop反序列化漏洞 (CVE-2020-14644)
- ◆ Weblogic历史漏洞合集

JBoss

- ◆ CVE-2017-7504-JBoss JMXInvokerServlet 反序列化
- ◆ JBoss 5.x/6.x 反序列化漏洞(CVE-2017-12149)
- ◆ JBoss 4.x JBossMQ JMS 反序列化漏洞(CVE-2017-7504)
- ◆ JBOSS远程代码执行漏洞
- ◆ JBoss JMX Console未授权访问Getshell
- ◆ JBoss历史漏洞合集

四、源代码管理

GitLab

- ◆ GitLab任意文件读取漏洞CVE-2020-10977
- ◆ GitLab远程代码执行漏洞分析 -【CVE-2018-14364】
- ◆ GitLab 任意文件读取 (CVE-2016-9086) 和任意用户token泄露漏洞
- ◆ GitLab历史漏洞合集

SVN

- ◆ SVN源码泄露漏洞

五、项目管理系统

禅道

- ◆ CNVD-C-2020-121325 禅道开源版文件上传漏洞
- ◆ 禅道9.1.2 免登陆SQL注入漏洞
- ◆ 禅道 ≤ 12.4.2 后台管理员权限Getshell
- ◆ 禅道9.1.2 权限控制逻辑漏洞
- ◆ 禅道826版本一定条件getshell
- ◆ 禅道远程代码执行漏洞
- ◆ 禅道11.6任意文件读取

Jira

- ◆ Atlassian Jira漏洞大杂烩
- ◆ Jira服务工作台路径遍历导致的敏感信息泄露漏洞(CVE-2019-14994)
- ◆ Jira未授权SSRF漏洞(CVE-2019-8451)
- ◆ Atlassian JIRA服务器模板注入漏洞(CVE-2019-11581)
- ◆ CVE-2019-8449 JIRA 信息泄露漏洞
- ◆ Jira历史漏洞合集

六、数据库

Redis

- ◆ Redis未授权访问漏洞利用总结
- ◆ Redis 4.x RCE
- ◆ redis利用姿势收集
- ◆ Redis历史漏洞合集

Mysql

- ◆ Mysql提权(CVE-2016-6663、CVE-2016-6664组合实践)
- ◆ Mysql数据库渗透及漏洞利用总结
- ◆ Mysql 注入专辑
- ◆ PhpMyadmin的几种getshell方法
- ◆ 高版本MySQL之UDF提权
- ◆ Mysql历史漏洞合集

Mssql

- ◆ Mssql利用姿势整理(史上最全)
- ◆ Mssql数据库命令执行总结
- ◆ 利用mssql模拟登录提权
- ◆ 高级的MSSQL注入技巧
- ◆ MSSQL使用CLR程序集来执行命令

Author:Unomi 持续更新中.....☺ 欢迎Star

