360数字安全
数字安全的领导者

2025攻防演练必修漏洞合集

360数字安全集团 ●漏洞情报服务

目　录 | Contents

一、前言

在数字化威胁持续演进的当下，攻防演练已成为检验企业安全体系实战能力的关键环节。传统漏洞清单往往聚焦于漏洞描述与修复建议，却忽略了攻击者如何利用漏洞突破防线、横向渗透的真实路径。攻击者不再依赖单一漏洞，而是通过组合漏洞利用、社会工程、工具武器化等手段构建完整攻击链。若无法预判攻击者的场景化思维，防守方极易陷入“补丁疲于奔命，威胁依然潜伏”的被动局面。

值此 2025 年网络安全攻防演练即将启动之际，360 漏洞云突破传统漏洞清单的静态分析模式，依托于对近千起真实攻防案例的深度研究及红队实战经验积累，创新性地将漏洞特性、攻击场景与利用手法进行三维关联，构建出"漏洞即战术"的动态化分析框架。报告不仅涵盖高危漏洞的技术细节，更着重拆解攻击者如何在不同业务环境中（如金融系统的供应链入口、制造业的 OT 资产暴露面）筛选目标漏洞、定制武器化载荷（如内存马注入、凭证窃取）、串联利用链（如初始访问→权限提升→横向移动），并关联 ATT&CK 战术阶段与检测盲区。通过行业差异化攻击剧本（Playbook）与工具链剖析（如 Cobalt Strike、Metasploit 模块调用），帮助企业从攻击者视角重构防御逻辑，将有限的资源精准投入到对抗成本最高的关键环节。

本清单的核心目标是让漏洞清单“活”起来，努力还原漏洞在真实攻防中的“杀伤力坐标”——它为何被攻击者选中？如何与业务弱点结合？防守方如何从流量、日志、行为等维度捕捉其利用痕迹？无论是攻防演练前的针对性布防，还是日常防御体系的短板排查，本报告均提供可落地的场景化指引。我们相信，唯有将漏洞置于攻击链中审视，才能真正实现“知攻知防，百战不殆”。

二、总述：攻防演练核心目标与攻击链模型

1. 攻防演练的核心目标：从“合规检查”到“对抗博弈”的范式升级

传统安全演练多聚焦于合规性验证与单点漏洞修复，而现代攻防演练的核心目标已升级为动态对抗能力检验，具体涵盖三大维度：

防御体系有效性验证：通过模拟攻击者思维与高阶战术（如 APT 攻击、0day 漏洞利用），检验安全防护设备（如 WAF、EDR）的检测覆盖率、响应时效性及策略盲区；

业务风险暴露面收敛：识别关键业务链路中“漏洞利用链与业务逻辑缺陷（如身份验证绕过、数据接口未鉴权）叠加形成的定向突破路径”，避免“技术漏洞已修复，业务风险仍开放”的典型误区；

实战化应急响应能力淬炼：基于攻击链的阶段性特征（如初始入侵→横向移动→数据窃取），构建“监测—分析—阻断—溯源”的闭环处置流程，提升团队在对抗高压下的协同能力与决策速度。

2. 攻击链模型：从“单点防御”到“链式对抗”的范式重构

攻击链模型（如洛克希德·马丁的 Cyber Kill Chain、MITRE ATT&CK 框架）将攻击行为拆解为阶段性战术动作，其价值在于：

攻击路径可视化：通过映射攻击者从侦察、武器化投递、漏洞利用到横向渗透的完整链条，暴露防御体系中“单点强、链路弱”的致命短板（例如：EDR 可检测恶意进程，但缺乏对合法工具滥用行为的关联分析）；

防御机会窗口定位：在攻击链的每一环节（如“初始访问”阶段的钓鱼邮件投递、“权限提升”阶段的本地提权漏洞利用）预置针对性检测与拦截策略，实现“链式防御”而非“孤立封堵”；

业务上下文关联分析：结合行业特性（如金融行业的 API 开放生态、制造业的 OT 资产暴露面），分析攻击链如何与业务逻辑弱点（如供应链系统接口未鉴权、运维通道明文传输）耦合形成定向攻击场景，推动风险治理从“技术漏洞清单”向“业务威胁图谱”进化。

3. 攻防演练与攻击链模型的融合实践

在攻防演练中，攻击链模型既是攻击方的“战术指南”，也是防守方的“防御蓝图”，其落地需围绕以下原则展开：

以攻促防，链式布控：基于攻击链阶段设计红队战术（如利用 Log4j2 漏洞建立据点后，通过 NTLM Relay 攻击横向渗透域控），同步验证防守方在各环节的监测与阻断能力（如日志是否留存 JNDI 请求、网络设备能否识别异常 SMB 流量）；

量化对抗成本效益比：通过“攻击成功率—攻击耗时—防守方检测率”等指标，评估不同攻击链路径的威胁等级（例如：利用公开 EXP 的漏洞突破成本低但防守方修复率高，应优先加固；而依赖社工的钓鱼攻击虽成功率低但绕过率极高，需强化用户意识与邮件网关策略）；

动态迭代防御剧本：将演练中暴露的攻击链路径转化为防守方的“防御剧本”（Playbook），例如：针对“漏洞利用+内存马注入”组合攻击，固化内存马行为特征检测规则；针对“云原生场景下的容器逃逸攻击链”，优化运行时监控与 Pod 隔离策略。

三、需立即修复的超高风险漏洞

1 命令注入漏洞

a) 漏洞场景

命令注入漏洞是一种高危安全风险，攻击者通过篡改用户输入参数，将恶意指令注入应用程序的系统调用中，从而直接控制服务器操作系统；漏洞产生的核心条件包括：

1. **未验证的用户输入**：应用程序直接接收外部输入（如 URL 参数、表单字段）并拼接至系统命令中，未实施白名单校验或危险字符过滤（如;、&）。
2. **危险函数调用**：使用可执行系统命令的 API（如 PHP 的 exec()、Python 的 os.system()），且未采用参数化方式传递用户输入。例如，Java 的 Runtime.getRuntime().exec()若直接拼接字符串，易被注入命令分隔符。
3. **权限配置不当**：应用程序以高权限（如 root）运行，导致注入的命令具备破坏性操作能力（如删除生产环境容器、窃取数据库）。

b) 攻击手段

命令注入漏洞通过篡改用户输入参数将恶意指令嵌入系统命令执行，攻击手段多样且危害严重，常见攻击方法如下：

1. **命令拼接与分隔符利用**，攻击者通过注入命令分隔符（如;、&&、|）将恶意指令附加到合法命令中。
2. **盲注与带外通信**，当无回显时，攻击者通过时间延迟（如 sleep 5）或带外通信（DNS/HTTP 请求）确认漏洞。
3. **环境变量劫持与编码绕过**，劫持 PATH 变量，将恶意程序伪装成系统命令（如 ls），触发时执行反弹 Shell。此外，十六进制或 Base64 编码可绕过黑名单过滤。

攻击者还可借助工具实现自动化，如 Burp Suite 探测注入点、Commix 直接注入恶意载荷或 Metasploit 框架利用特定漏洞执行命令。此类攻击可导致服务器权限沦陷（从低权用户提权至 root）、敏感信息泄露（如数据库凭据、SSH 密钥）、植入持久化后门（如写入定时任务

或 SSH 授权密钥），甚至以内网主机为跳板进一步渗透企业核心资产（如横向移动攻击数据库、办公系统），最终造成业务停摆、数据窃取或勒索等严重后果。

c）重点关注漏洞

1. Palo Alto Networks Pan-Os 未授权 命令注入漏洞

漏洞编号 LDYVUL-2024-00520293 、 CVE-2024-3400

漏洞等级 严重

漏洞类型 命令注入

漏洞时间 2024-04-13 15:10:45

在野利用 存在

360 漏洞云监测到 Palo Alto Networks PAN-OS 中存在一个命令注入漏洞，未经身份验证的攻击者可利用该漏洞在防火墙上以 root 权限执行任意代码，该漏洞影响启用了 GlobalProtect 网关的 PAN-OS 10.2、PAN-OS 11.0 和 PAN-OS 11.1 防火墙，导致未经身份验证的攻击者可利用该漏洞在防火墙上以 root 权限执行任意代码，Cloud NGFW、Panorama 设备和 Prisma Access 不受此漏洞的影响。漏洞编号：CVE-2024-3400，漏洞威胁等级：严重。

2. Apache Rocketmq 未授权 命令注入漏洞

漏洞编号 LDYVUL-2023-00222303 、 CVE-2023-33246

漏洞等级 严重

漏洞类型 命令注入

漏洞时间 2023-05-30 16:02:14

在野利用 存在

Apache RocketMQ 是美国阿帕奇（Apache）基金会的一款轻量级的数据处理平台和消息传递引擎。360 漏洞云监测到 Apache RocketMQ 5.1.0 及之前版本存在一个命令注入漏洞，攻击者可以利用该漏洞利用更新配置功能以系统用户身份执行命令。

3. CybnerPanel filemanager/upload 未授权 命令注入漏洞

漏洞编号 LDYVUL-2024-00817029 、 CVE-2024-51568

漏洞等级　严重

漏洞类型　命令注入

漏洞时间　2024-11-01 11:17:04

360 漏洞云监测到 CyberPanel filemanager/upload 接口存在命令注入漏洞，可致远程代码执行，该漏洞源于 filemanager/upload 接口未做身份验证和参数过滤，未授权的攻击者可以通过此接口远程加载恶意文件获取服务器权限,从而造成数据泄露、服务器被接管等严重的后果。目前该漏洞技术细节与 EXP 已在互联网上公开，鉴于该漏洞影响范围较大，建议用户尽快做好自查及防护。

4. CyberPanel upgrademysqlstatus 未授权 命令注入漏洞

漏洞编号　LDYVUL-2024-00815896 、 CVE-2024-51567

漏洞等级　严重

漏洞类型　命令注入

漏洞时间　2024-10-29 17:22:43

在野利用　存在

360 漏洞云监测到开源控制面板 CyberPanel 存在一个未授权命令注入漏洞，未经授权的攻击者可以通过该漏洞在服务器上执行任意命令，获取服务器权限。

5. Cyberpanel 未授权 命令注入漏洞

漏洞编号　LDYVUL-2024-00816438 、 CVE-2024-51378

漏洞等级　严重

漏洞类型　命令注入

漏洞时间　2024-10-28 00:00:00

在野利用　存在

CyberPanel 是 Usman Nasir 个人开发者的一款内置了 DNS 和电子邮件服务器的虚拟主机控制面板。360 漏洞云监测到 CyberPanel 存在一个命令注入漏洞，该漏洞允许远程攻击者绕过身份验证并执行任意命令，最终导致服务器失陷。

6. QNAP QTS 未授权 命令注入漏洞

漏洞编号 LDYVUL-2024-00834592 、 CVE-2024-50393

漏洞等级 高危

漏洞类型 命令注入

漏洞时间 2024-10-24 03:41:08

360 漏洞云监测到 QNAP 发布安全公告，修复了多个安全漏洞，其中包括一个影响 QNAP QTS 设备的命令注入漏洞，未授权攻击者可以利用此漏洞执行任意命令。官方已经发布了补丁修复了该漏洞，建议受影响用户及时升级到安全版本。

7. Palo Alto Networks Expedition 未授权 命令注入漏洞

漏洞编号 LDYVUL-2024-00778318 、 CVE-2024-9463

漏洞等级 严重

漏洞类型 命令注入

漏洞时间 2024-10-10 02:53:27

360 漏洞云监测到 Palo Alto 发布安全公告，修复了多个安全漏洞，其中包括一个 Palo Alto Networks Expedition 中存在操作系统命令注入漏洞，未经认证的攻击者可利用该漏洞以根用户身份在 Expedition 中运行任意操作系统命令，从而导致披露 PAN-OS 防火墙的用户名、明文密码、设备配置和设备 API 密钥。

8. Zimbra Collaboration 未授权 命令注入漏洞

漏洞编号 LDYVUL-2024-00546099 、 CVE-2024-45519

漏洞等级 严重

漏洞类型 命令注入

漏洞时间 2024-09-13 12:49:16

在野利用 存在

360 漏洞云监测到 Zimbra Collaboration 发布更新版本，新版本中修复了多个安全漏洞，其中包含 postjournal 服务中的一个命令注入漏洞，在远程 Zimbra 服务器开启了 postjournal 服务时，未经身份验证的攻击者可以利用此漏洞执行系统任意命令，获取服务器

控制权限。

2 代码注入漏洞

a) 漏洞场景

代码注入漏洞是指攻击者通过输入恶意代码片段，篡改程序的执行逻辑或窃取数据的漏洞类型，漏洞根本原因在于开发者未采用安全的编码规范，将用户输入直接作为代码逻辑的一部分，且缺乏输入验证、参数化查询、沙箱隔离等防护机制，一般有以下情况：

1. **未验证的动态代码执行**：应用程序直接拼接用户输入至可执行代码，未实施输入校验或过滤。
2. **危险函数调用**：使用可动态解析代码的接口（如 PHP 的 eval()、Python 的 exec()），或未参数化调用数据库 API（如 JDBC 的 Statement 而非 PreparedStatement）。
3. **上下文逻辑混淆**：在模板引擎（如 XSS 攻击）或 AI 模型（如大模型生成恶意代码）中，未对用户输入内容与代码上下文进行隔离，导致输入被误解析为执行指令。

b) 攻击手段

代码注入漏洞（排除命令执行、SQL 注入及反序列化）主要通过输入数据嵌入恶意逻辑触发非预期代码解析，典型攻击包括：

1. 模板引擎注入（SSTI），如 Thymeleaf 中注入 ${T(java.lang.Runtime).getRuntime().exec('calc')}实现 RCE（某 OA 系统漏洞 CVE-2022-32523）；
2. 表达式语言注入，攻击者篡改 OGNL 表达式参数构造 #_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS,#res=@java.lang.Runtime@getRuntime().exec('id')执行系统命令（Apache Struts S2-045 漏洞）；
3. XPath 注入，输入' or 1=1 or 'a'='a 绕过 XML 查询权限控制，窃取全量数据（某金融系统漏洞致百万用户信息泄露）；
4. 日志注入，通过伪造%0d%0aUser: admin 插入换行符伪造日志条目，干扰审计追踪。

代码注入漏洞攻击可导致敏感数据泄露（XPath/LDAP 注入绕过访问控制）、权限提升（表达式注入调用特权 API）、业务逻辑篡改（模板注入劫持页面渲染）及系统完整性破坏（恶意代码持久化）。

c）重点关注漏洞

1. 亘岩网络 契约锁电子签章系统 template/param/edits 未授权 代码注入漏洞

漏洞编号 LDYVUL-2024-00534914

漏洞等级 严重

漏洞类型 代码注入

漏洞时间 2024-07-31 17:10:02

360 漏洞云监测到亘岩网络契约锁电子签章系统存在代码注入漏洞，未授权攻击者可以利用此漏洞执行任意服务器端代码，获取服务器权限。

2. 北京数字认证 BJCA 电子印章签署系统 需授权 代码注入漏洞

漏洞编号 LDYVUL-2024-00533852

漏洞等级 高危

漏洞类型 代码注入

漏洞时间 2024-07-30 13:16:56

北京数字认证 BJCA 电子印章签署系统存在一个模板注入漏洞，拥有平台账户权限的攻击者可以通过构造恶意请求进行模板注入，导致在服务器上执行任意代码，并且由于平台存在用户注册功能，导致该漏洞实际利用难度较低，请做好安全防护。

3. PHP CGI 代码注入漏洞

漏洞编号 LDYVUL-2024-00270053 、 CVE-2024-4577

漏洞等级 严重

漏洞类型 代码注入

漏洞时间 2024-06-07 14:55:54

在野利用 存在

360 漏洞云监测到 PHP 存在一个代码注入漏洞，当 PHP 的 PHP-CGI 模式运行在 Windows 平台且使用了特定语系时，攻击者可构造恶意请求绕过 CVE-2012-1823 补丁，通过注入恶意的 CGI 模式命令参数，在服务上执行任意 PHP 代码。

4. Atlassian Confluence 未授权 代码注入漏洞

漏洞编号 LDYVUL-2024-00003744 、 CVE-2023-22527

漏洞等级 严重

漏洞类型 代码注入

漏洞时间 2024-01-16 15:15:38

在野利用 存在

360 漏洞云监测到 Atlassian 发布安全公告，其中公开了一个 Confluence 协作平台的代码注入漏洞，允许未经身份验证的攻击者在服务器上执行任意代码，获取服务器控制权限。

5. Pixel&tonic CraftCMS 未授权 代码注入漏洞

漏洞编号 LDYVUL-2024-00840849 、 CVE-2024-56145

漏洞等级 严重

漏洞类型 代码注入

漏洞时间 2024-12-16 18:04:39

Craft 是一个灵活、用户友好的 CMS，用于在网络及其他领域创建自定义数字体验。360 漏洞云监测到 Craft CMS 存在一个代码注入漏洞，在某些特定的环境配置中，攻击者可以发送特殊请求注入恶意代码，在服务器上执行任意代码，导致服务器被攻陷。

6. Rejetto HTTP File Server 未授权 代码注入漏洞

漏洞编号 LDYVUL-2024-00267966 、 CVE-2024-23692

漏洞等级 严重

漏洞类型 代码注入

漏洞时间 2024-06-21 16:27:43

在野利用 存在

Rejetto HTTP 文件服务器在旧版本中（<=2.4.0 RC7）存在一个代码注入漏洞。此漏洞允许远程未经身份验证的攻击者通过发送特制的 HTTP 请求在受影响的系统上执行任意命令。自 CVE 分配日期起，Rejetto HFS 2.x 版本已经不再受支持。

3 访问控制不当漏洞

a) 漏洞场景

访问控制不当漏洞的产生通常源于开发与运营环节的多重失误：

1. **开发阶段**，权限模型设计缺陷（如未遵循最小权限原则或 RBAC 模型），导致功能接口未按角色严格隔离（如某 CMS 系统管理接口/admin/export 未校验用户角色，CVE-2022-33568）；

2. **编码逻辑疏漏**，服务端依赖客户端传入参数（如用户 ID、角色标识）进行权限判断而未与会话身份绑定，引发水平越权（某社交平台漏洞允许通过篡改 userId 参数窃取他人私信）；

3. **测试覆盖不足**，未对边界权限场景（如普通用户访问管理员 API、跨租户数据访问）进行充分验证；运营阶段，安全配置错误，如生产环境误启用测试账号权限（某政务系统因测试账号 admin:test123 未禁用遭攻击者登录），或云存储资源（如 AWS S3、OSS）ACL 策略配置为公开可读写（2019 年 Capital One 数据泄露事件致 1 亿用户信息暴露）。

漏洞根源在于权限校验机制缺失（如未在服务端对 API 请求进行身份与权限关联验证）、业务逻辑与安全逻辑解耦（权限控制未深度集成至业务流程）以及安全开发流程失效（需求评审未纳入权限设计、代码审查未发现鉴权漏洞、渗透测试忽略越权测试用例），最终导致攻击者可绕过权限限制非法操作数据或功能。

b) 攻击手段

访问控制不当漏洞的攻击手段主要通过绕过权限验证机制非法访问受限资源或功能，典型手法包括：

1. **垂直越权**，攻击者伪造管理员身份（如篡改 HTTP 请求头中的 X-User-Role: admin）直接调用管理接口（如用户删除接口/api/admin/delete?userId=123），某开源论坛漏洞（CVE-2022-30115）因此导致任意用户被封禁；

2. **水平越权**，通过枚举或篡改资源 ID 参数（如订单查询接口/api/order?id=1001 修改为 id=1002）窃取他人敏感数据（某银行 App 漏洞致用户交易记录泄露）；

3. **未授权访问**，直接访问无需鉴权的 API 端点（如/api/exportAllUsers）批量导出用户信息（某教育平台漏洞致 50 万学生数据泄露）；

4. **JWT 令牌伪造**，利用弱密钥或算法漏洞（如 HS256 密钥硬编码）篡改令牌 role 字段提升权限（某云服务漏洞 CVE-2023-22973）。

攻击可导致敏感数据大规模泄露（如用户隐私、支付信息）、业务功能滥用（如恶意提现、篡改库存）、系统权限失控（如创建超级管理员账户）及合规风险（如 GDPR 违规罚款）。典型案例为 2022 年 Uber 数据泄露事件，攻击者通过窃取的内部凭证访问 AWS 控制台，因访问控制缺失导致关键数据库被入侵。

c) 重点关注漏洞

1. Jenkins Remote 访问控制不当漏洞 可导致远程代码执行

漏洞编号　LDYVUL-2024-00535405 、 CVE-2024-43044

漏洞等级　严重

漏洞类型　访问控制不当

漏洞时间　2024-08-08 15:04:47

360 漏洞云监测到 Jenkins 发布了安全公告，其中公开了 Jenkins Remote 库的一个任意文件读取漏洞，该漏洞允许代理进程、代理上运行的代码以及具有 Agent/Connect 权限的攻击者从 Jenkins 控制器文件系统读取任意文件。而 Jenkins 官方插件中 bouncycastle API、Groovy、Ivy、TeamConcert 都使用了该依赖库，值得注意 Jenkins 上的任意文件读取漏洞会导致重要敏感数据泄露，最终可能会导致在服务器上执行任意代码。

2.飞致云 DataEase 未授权 访问控制不当漏洞

漏洞编号 LDYVUL-2024-00029297 、 CVE-2024-30269

漏洞等级 中危

漏洞类型 访问控制不当

漏洞时间 2024-03-26 12:52:00

DataEase 是一个开源的数据可视化分析工具。用于帮助用户快速分析数据并洞察业务趋势，从而实现业务的改进与优化。360 漏洞云监测到 DataEase 在 2.5.1 版本之前，DataEase 未能对请求路径进行正确解析，导致攻击者可以通过构造恶意请求获取服务器数据库配置信息。

4 SQL 注入漏洞

a) 漏洞场景

SQL 注入漏洞的产生原因在于应用程序未对用户输入进行严格过滤或参数化处理，直接将外部可控数据（如表单字段、URL 参数、Cookie 值）动态拼接至 SQL 查询语句中，使得攻击者可通过构造包含恶意 SQL 语法结构的输入篡改原查询逻辑；

其漏洞根源在于开发过程中未采用安全的数据库交互方式（如未使用预编译的参数化查询、未对输入进行类型与格式校验）、过度依赖字符串拼接生成动态 SQL 语句、未对特殊字符（如单引号、分号、注释符）进行转义或过滤，同时错误配置数据库权限（如允许应用账户执行高危操作）及开启详细报错信息（如暴露表结构、字段名），导致攻击者可利用注入漏洞执行任意 SQL 指令。

b) 攻击手段

SQL 注入漏洞的利用手法包括攻击者通过构造恶意输入篡改 SQL 逻辑,或利用报错注入(如 AND updatexml(1,concat(0x7e,@@version),1)) 触发数据库错误回显敏感数据；通过布尔盲注或时间盲注逐字符推断信息，甚至利用堆叠查询直接破坏数据。常用工具包括自动化检测工具 sqlmap（支持多种注入类型与数据库类型）、图形化工具 Havij（简化注入流程）、Burp Suite（拦截并构造注入 Payload），以及手工测试辅助工具如 Tamper Data（绕过 WAF 过滤）。攻击者可借此窃取数据库敏感信息（用户凭证、交易记录）、篡改或删除业务数据（伪造订单、清空日志），利用数据库权限执行系统命令（如通过 xp_cmdshell 部署后门），甚至通过内网

横向渗透控制服务器集群。

c）重点关注漏洞

1. 上海建业信息科技 章管家 listUploadIntelligent 未授权 SQL 注入漏洞

漏洞编号 LDYVUL-2024-00539479

漏洞等级 高危

漏洞类型 SQL 注入

漏洞时间 2024-08-14 16:06:14

360 漏洞云监测到上海建业信息科技章管家应用存在一个未授权 SQL 注入漏洞，未经授权的攻击者可以通过该漏洞获取数据库敏感信息。

2. 金斗云 HKMP 智慧商业软件 queryPrintTemplate 未授权 SQL 注入漏洞

漏洞编号 LDYVUL-2024-00539461

漏洞等级 高危

漏洞类型 SQL 注入

漏洞时间 2024-08-14 15:37:46

金斗云 HKMP 智慧商业软件存在一个未授权 SQL 注入漏洞，未经授权的攻击者可以通过该漏洞获取数据库敏感信息。

3. 亿赛通 电子文档安全管理系统 CDGAuthoriseTempletService1 未授权 SQL 注入漏洞

漏洞编号 LDYVUL-2024-00535376

漏洞等级 高危

漏洞类型 SQL 注入

漏洞时间 2024-08-07 14:48:09

亿赛通电子文档安全管理系统存在一个未授权的 SQL 注入漏洞，未经授权的攻击者可以通过该漏洞获取数据库敏感信息。

4. 1Panel search 未授权 SQL 注入漏洞

漏洞编号　LDYVUL-2024-00391562 、 CVE-2024-39907

漏洞等级　严重

漏洞类型　SQL 注入

漏洞时间　2024-07-24 14:45:05

在野利用　存在

1Panel 是中国 1Panel 社区的一个开源的 Linux 服务器运维管理面板。1Panel 1.10.12-tls 以前的版本存在一个 SQL 注入漏洞，该漏洞源于 1Panel 中部分 SQL 注入过滤不善，导致任意文件写入，最终导致远程代码执行。

5. 数字通 指尖云平台智慧办公 DAP PayslipUser 未授权 SQL 注入漏洞

漏洞编号　LDYVUL-2024-00530711

漏洞等级　严重

漏洞类型　SQL 注入

漏洞时间　2024-07-23 16:21:54

360 漏洞云检测到数字通指尖云平台智慧办公 DAP PayslipUser 接口存在 SQL 注入漏洞，未经身份验证的远程攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

6. 亿赛通 电子文档安全管理系统 SaveCDGPermissionFromGFOA 未授权 SQL 注入漏洞

漏洞编号　LDYVUL-2024-00392421

漏洞等级　严重

漏洞类型　SQL 注入

漏洞时间　2024-07-22 18:21:58

亿赛通电子文档安全管理系统存在一个 SQL 注入漏洞，未经身份验证的攻击者通过漏洞注入恶意 SQL 语句，获取敏感信息，甚至可能导致服务器失陷。

7. Showdoc item_id 未授权 SQL 注入漏洞

漏洞编号 LDYVUL-2024-00266778

漏洞等级 高危

漏洞类型 SQL 注入

漏洞时间 2024-05-28 16:26:38

360 漏洞云监测到 Showdoc V3.2.6 之前的版本中存在 SQL 注入漏洞，攻击者可通过此漏洞获取登录登录 token 并进入后台。进入后台后可结合反序列化漏洞，写入 WebShell，从而获取服务器权限。

8. Jeecg JeecgBoot 未授权 SQL 注入漏洞

漏洞编号 LDYVUL-2024-00816915 、 CVE-2024-48307

漏洞等级 严重

漏洞类型 SQL 注入

漏洞时间 2024-10-08 00:00:00

JeecgBoot 是北京国炬软件（Jeecg）公司开发的一个适用于企业 Web 应用程序的 Java 低代码平台。360 漏洞云监测到 JeecgBoot 存在一个 SQL 注入漏洞，未经授权的攻击者可以通过该漏洞获取数据库敏感信息。

9. 数字通 云平台智慧政务 workflow 未授权 SQL 注入漏洞

漏洞编号 LDYVUL-2024-00548584

漏洞等级 高危

漏洞类型 SQL 注入

漏洞时间 2024-09-20 11:28:00

360 漏洞云监测到数字通 云平台智慧政务平台存在一个 SQL 注入漏洞，未经授权的攻击者可以通过该漏洞获取数据库敏感信息。

5 反序列化漏洞

a）漏洞场景

反序列化漏洞常见于应用程序将外部传入的序列化数据（如 JSON、XML、二进制流）直接还原为对象且未进行安全校验的场景，例如远程服务调用（如 Java RMI、HTTP 请求传输序列化对象）、缓存数据处理（Redis 未授权访问时注入恶意序列化数据）、Session 会话管理（PHP 反序列化 Session 文件）或配置文件加载（Apache Dubbo 反序列化攻击链）。其产生的核心条件包括：

1. 应用接收并反序列化不可信的外部输入，如用户可控的 Cookie、网络传输数据或文件内容；
2. 反序列化过程中调用了危险类或方法（如 Java 中重写 readObject()方法未过滤敏感操作、PHP 中魔术方法 destruct()或 wakeup()被恶意触发）
3. 依赖存在缺陷的序列化组件或框架（如 Apache Commons Collections 链、Fastjson 反序列化漏洞）。

反序列化漏洞根源在于开发者未对反序列化过程实施严格的类型白名单校验或数据完整性验证，导致攻击者通过构造包含恶意代码的序列化数据，在反序列化时触发非预期的对象属性赋值、动态类加载或危险方法调用，从而达成远程代码执行（RCE）、服务拒绝（DoS）或权限绕过等攻击效果。

b）攻击手段

反序列化漏洞的利用手法主要包括攻击者构造恶意序列化数据（如篡改 JSON/adze 数据中的类名或属性，植入 Apache Commons Collections、Fastjson 等框架的 Gadget 链），利用目标系统在反序列化过程中自动触发危险方法（如 Java 的 readObject()、PHP 的__destruct()），或通过动态加载恶意类（如 Python 的 pickle 模块）实现代码注入；常用工具涵盖自动化 Payload 生成工具（如 ysoserial、marshalsec）、漏洞利用框架（如 Metasploit）、流量拦截工具（如 Burp Suite）及针对特定框架的利用脚本（如 fastjson-exploit）。此类攻击可导致远程代码执行（RCE，如通过 Runtime.exec()执行系统命令）、敏感信息泄露（如读取数据库凭据）、权限提升（如反序列化后门植入）、服务拒绝（如触发无限循环耗尽资源），甚至利用反序列化漏洞作为跳板进行内网横向渗透（如攻击内网 Redis 或 Hessian 服务），最终造成业务系统沦陷、数据被加密勒索或大规模数据泄露等严重后果。

c）重点关注漏洞

1. 宝兰德软件 BES 管理控制台 ejb 未授权 反序列化漏洞 可致远程代码执行

漏洞编号 LDYVUL-2024-00541423

漏洞等级 严重

漏洞类型 反序列化

漏洞时间 2024-08-15 18:31:14

360 漏洞云监测北京宝兰德软件股份有限公司 BES 管理控制台存在一个未授权反序列化漏洞，未经身份验证的攻击者可以通过该漏洞在服务器上执行任意代码，获取服务器控制权限。

2. 宝兰德 BES 管理控制台 未授权 反序列化漏洞 可致远程代码执行

漏洞编号 LDYVUL-2024-00822901

漏洞等级 严重

漏洞类型 反序列化

漏洞时间 2024-11-18 10:55:16

360 漏洞云监测到宝兰德软件发布安全公告，其中公开披露了一个反序列化漏洞，由于宝兰德 BES 应用服务器产品 Spark 服务存在一个反序列化漏洞，未授权的攻击者可利用该漏洞绕过反序列化黑名单限制，在服务器上执行任意代码，获取服务器权限。

3. 亿赛通 电子文档安全管理系统 UninstallApplicationService1 未授权 反序列化漏洞

漏洞编号 LDYVUL-2024-00779581

漏洞等级 严重

漏洞类型 反序列化

漏洞时间 2024-10-14 14:23:50

亿赛通电子文档安全管理系统（简称：CDG）是一款电子文档安全防护软件，该系统利用驱动层透明加密技术，通过对电子文档的加密保护，防止内部员工泄密和外部人员非法窃取企业核心重要数据资产。360 漏洞云监测到亿赛通电子文档安全管理系统存在一个 xstream 反序列化漏洞，成功利用该漏洞的攻击者可以获取服务器的控制权。

4. Adobe ColdFusion 未授权 反序列化漏洞 可导致代码执行

漏洞编号 LDYVUL-2024-00545745 、 CVE-2024-41874

漏洞等级 严重

漏洞类型 反序列化

漏洞时间 2024-09-12 16:33:12

360 漏洞云监测 Adobe ColdFusion 发布安全公告，修复了 Adobe ColdFusion 中的一个反序列化漏洞，该漏洞允许未授权的攻击者通过恶意反序列化数据在服务器上执行任意代码，获取服务器控制权限。

6 文件上传限制不当漏洞

a) 漏洞场景

文件上传限制不当漏洞通常发生在 Web 应用允许用户上传文件但未对文件类型、内容、路径及权限实施严格管控的场景，例如头像上传、附件提交或文档管理功能模块；其核心产生条件包括：

1. 服务端未对文件扩展名(如.php、.jsp)进行有效过滤或仅依赖前端检查(如 JavaScript 校验 MIME 类型），攻击者可伪造 Content-Type 或修改文件后缀绕过检测；
2. 未校验文件内容合法性（如检测图片文件的幻数头），导致恶意代码（如 Webshell）嵌入图片并通过文件包含漏洞执行；
3. 存储路径可预测或未禁用执行权限，如上传至 Web 可访问目录且服务器配置不当（如 Apache 未设置 php_flag engine off），使恶意文件被直接解析；
4. 未对文件名进行规范化处理，引发路径穿越（如../../../uploads/shell.php）或覆盖系统文件。

漏洞根源在于开发者在设计文件上传功能时缺乏安全思维，未采用白名单机制限制文件类型、未对上传内容进行二次验证、未对存储路径设置隔离与权限控制，且未能及时更新安全策略以应对新型绕过手法（如双扩展名、大小写混淆），导致攻击者可上传恶意文件实施远程代码执行（RCE）、网站篡改、数据窃取或作为跳板进一步渗透内网。

b) 攻击手段

文件上传限制不当漏洞的利用手法包括攻击者通过篡改文件扩展名（如将.php 改为.jpg.php）、伪造 Content-Type 头（如 image/jpeg）、嵌入恶意代码至图片注释或利用文件格式解析差异（如 GIF89a 头部后接 PHP 代码），绕过前端校验与简单服务端检测；通过构造双扩展名（如 test.php.rar）或大小写变形（如.PHp）规避黑名单过滤，或利用服务器解析特性（如 Apache 解析漏洞将 test.php.jpg 视为 PHP 执行）；结合路径穿越（如../../../webroot/shell.php）将恶意文件上传至可执行目录，或利用未授权访问的上传接口实现任意文件覆盖。攻击达成效果包括：植入 Webshell 获取服务器控制权（执行系统命令、数据库操作）、利用恶意文件作为钓鱼载体分发木马、篡改页面内容实施挂马攻击、读取敏感文件（如/etc/passwd）导致数据泄露，或通过上传大文件耗尽存储资源引发服务拒绝（DoS）；此外，攻击者可进一步提权至服务器管理员账户，横向渗透内网服务（如数据库、缓存系统），甚至将受控服务器作为僵尸网络节点发起分布式攻击，形成以文件上传点为入口的完整攻击链，最终造成业务停摆、数据勒索或企业信誉受损等严重后果。

c) 重点关注漏洞

1. 凯京信达 Kkfileview 未授权 文件上传限制不当漏洞

漏洞编号　LDYVUL-2024-00520428

漏洞等级　严重

漏洞类型　文件上传限制不当

漏洞时间　2024-04-17 18:04:09

360 漏洞云监测到 kkFileView 存在一个任意文件上传漏洞，攻击者可利用该漏洞上传恶意文件，获取操作系统权限。

2. Apache Struts2 未授权 文件上传限制不当漏洞

漏洞编号　LDYVUL-2023-00696314 、 CVE-2023-50164

漏洞等级　严重

漏洞类型　文件上传限制不当

漏洞时间　2023-12-07 16:45:43

Apache Struts2 框架是一个用于开发 Java EE 网络应用程序的 Web 框架，它本质上相当于一个 servlet，在 MVC 设计模式中，Struts2 作为控制器(Controller)来建立模型与视图的数据交互。360 漏洞云监测到 Apache Struts2 发布安全公告，其中公开了一个远程代码执行漏洞。由于文件上传逻辑存在缺陷，可能导致上传可用于执行远程代码执行的恶意文件，漏洞编号：CVE-2023-50164(S2-066)，漏洞威胁等级：。该漏洞是由于文件上传逻辑存在缺陷，攻击者可以操纵文件上传参数来启用路径遍历，在某些情况下，这可能导致上传可用于执行远程代码执行的恶意文件。

3. IDocView html2word /html/2word 文件上传限制不当漏洞

漏洞编号　LDYVUL-2024-00268239

漏洞等级　严重

漏洞类型　文件上传限制不当

漏洞时间　2023-08-16 12:00:42

360 漏洞云监测到 iDocView 存在一处文件上传限制不当漏洞，攻击者可以把存在命令执行的 jsp 脚本放到 docview 目录下，利用特殊的方式访问该 jsp 脚本，可以导致远程代码执行。

4. 亘岩网络 契约锁子签章系统 upload 未授权 文件上传限制不当漏洞

漏洞编号　LDYVUL-2024-00268288

漏洞等级　高危

漏洞类型　文件上传限制不当

漏洞时间　2023-08-16 12:00:42

360 漏洞云监测到契约锁电子签章系统/callback/%2E%2E;/code/upload 存在鉴权绕过漏洞，可导致任意文件上传，攻击者可以利用该漏洞上传恶意代码，获取服务器权限。

5. Apache Struts2 文件上传限制不当漏洞 可导致远程代码执行

漏洞编号　LDYVUL-2024-00837193 、 CVE-2024-53677

漏洞等级　严重

漏洞类型　文件上传限制不当

漏洞时间　2024-11-21 17:02:02

360 漏洞云监测到 Apache Struts2 发布安全公告，披露了一个文件上传限制不当漏洞，该漏洞是由于 Struts2 框架使用旧版本的文件上传拦截器来获取上传文件的参数，并自动将相关参数注入到用户实现的 Action 中，由于拦截器存在逻辑缺陷，攻击者可以操纵文件上传参数并启用路径遍历，攻击者可以通过该漏洞上传恶意文件，从而控制服务器。

6. 润乾信息 润乾报表 servlet/dataSphereServlet 未授权 文件上传限制不当漏洞

漏洞编号　LDYVUL-2024-00779554

漏洞等级　严重

漏洞类型　文件上传限制不当

漏洞时间　2024-10-14 11:11:22

360 漏洞云监测到润乾报表存在文件上传限制不当漏洞，未授权的攻击者可以通过该漏洞上传任意恶意文件，从而控制服务器。

7. 浪潮 GS 企业管理软件 UploadListFile 未授权 文件上传限制不当漏洞 可致远程代码执行

漏洞编号　LDYVUL-2024-00541595

漏洞等级　严重

漏洞类型　文件上传限制不当

漏洞时间　2024-09-03 11:34:37

浪潮 GS 企业管理软件 UploadListFile 接口存在文件上传漏洞，未授权攻击者可以利用此漏洞实现远程代码执行。

四、攻防演练需关注的 579 个漏洞

漏洞编号	漏洞标题	漏洞类型
LDYVUL-2024-00544318	Altenergy 电力系统控制软件 set_timezone 未授权 命令注入漏洞	命令注入
LDYVUL-2023-00222303	Apache Rocketmq 未授权 命令注入漏洞	命令注入
LDYVUL-2023-00477085	Apache Spark 需授权 命令注入漏洞	命令注入
LDYVUL-2024-00547786	ArrayNetworks APV 应用交付系统 ping_hosts 未授权 命令注入漏洞	命令注入
LDYVUL-2023-00034438	Atlassian Jira Service Desk 需授权 代码注入漏洞	命令注入
LDYVUL-2024-00815896	CyberPanel upgrademysqlstatus 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00816438	Cyberpanel 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00817029	CybnerPanel filemanager/upload 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00819334	D-Link DNS-X 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00823282	D-Link NAS 设备 sc_mgr.cgi 未授权 命令注入漏洞	命令注入
LDYVUL-2023-00341691	Gitlab Gitlab 未授权 命令注入漏洞	命令注入
LDYVUL-2023-00482642	Gitlab Gitlab 需授权 命令注入漏洞	命令注入
LDYVUL-2023-00044409	Inspur Clusterengine 未授权 命令注入漏洞	命令注入
LDYVUL-2023-00224190	Jeecg Jimureport queryFieldBySql 未授权 命令注入漏洞	命令注入
LDYVUL-2023-00519877	NginxWebUI 团队 Nginx Web 用户界面管理工具 /AdminPage/conf/runCmd 未授权 命令注入漏洞	命令注入
LDYVUL-2023-00006662	Oracle Weblogic Server 未授权 命令注入漏洞	命令注入
LDYVUL-2023-00450144	Oracle Weblogic Server 需授权 LDAP 注入漏洞	命令注入
LDYVUL-2024-00778318	Palo Alto Networks Expedition 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00520293	Palo Alto Networks Pan-Os 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00778322	Paloaltonetworks Expedition 需授权 命令注入漏洞	命令注入
LDYVUL-2024-00834592	QNAP QTS 未授权 命令注入漏洞	命令注入
LDYVUL-2023-00421459	RoxyWi RoxyWi 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00546099	Zimbra Collaboration 未授权 命令注入漏洞	命令注入
LDYVUL-2022-00519452	贝锐信息 向日葵简约版 未授权 命令注入漏洞	命令注入
LDYVUL-2022-00519803	畅捷通信息技术股份有限公司 畅捷通 T+ tplus/ajaxpro 未授权 命令注入漏洞	命令注入

LDYVUL-2022-00519818	顶想信息 Thinkphp public 未授权 命令注入漏洞	命令注入
LDYVUL-2022-00519543	泛微网络 E-Cology 未授权 命令注入漏洞	命令注入
LDYVUL-2023-00253622	泛微网络 E-Office utility_all 需授权 命令注入漏洞	命令注入
LDYVUL-2021-00518963	飞致云 JumpServer 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00530551	海康威视 综合安防管理平台 detection 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00534732	海康威视 综合安防管理平台 licenseExpire 未授权 命令注入漏洞	命令注入
LDYVUL-2021-00519148	金山 V8 终端安全系统 /inter/pdf_maker.php 未授权 命令注入漏洞	命令注入
LDYVUL-2023-00300748	兰德纵横网络 O2OA 翱途办公开发平台 未授权 命令注入漏洞	命令注入
LDYVUL-2022-00519680	蓝凌 OA dataxml.js 未授权 命令注入漏洞	命令注入
LDYVUL-2022-00519686	蓝凌 OA 协同办公 datajson.tmpl 未授权 命令注入漏洞	命令注入
LDYVUL-2022-00519538	蓝凌 OA 协同办公 treexml.tmpl 未授权 命令注入漏洞	命令注入
LDYVUL-2022-00519694	奇安信 新天擎终端管理系统 clientuploadfilejson 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00531801	锐捷 统一上网行为管理与审计系统 static_convert.php 未授权命令注入漏洞	命令注入
LDYVUL-2024-00545236	瑞斯康达多 业务智能网关 list_service_manage.php 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00544411	山石网科 应用防火墙 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00268433	深信服 应用交付报表系统等 /rep/login 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00539958	神州数码云科 DCME 安全网关 ping.php 需授权 命令注入漏洞	命令注入
LDYVUL-2022-00519618	天融信 上网行为管理系统 未授权 命令注入漏洞	命令注入
LDYVUL-2023-00519978	通达信科 网络智能办公系统 update.php 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00539640	统信 uos installDriver 命令注入漏洞 可导致权限提升	命令注入
LDYVUL-2024-00392785	万网博通 全息 AI 网络运维平台 ajax_cloud_router_config.php 未授权 命令注入漏洞	命令注入

LDYVUL-2022-00519489	网康科技 网康下一代防火墙 /directdata/direct/router 需授权 命令注入漏洞	命令注入
LDYVUL-2022-00519797	网康科技 网康下一代防火墙(Ns-Ngfw) NS_Rpc_HeartBeat 未授权 命令注入漏洞	命令注入
LDYVUL-2021-00519014	亿中邮信 亿邮电子邮件系统 webadm 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00545317	银河麒麟 youker-assistant 命令注入漏洞 可导致权限提升	命令注入
LDYVUL-2024-00535453	用友 U8+CRM 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00545776	用友 U8Cloud esnserver 命令注入漏洞	命令注入
LDYVUL-2021-00519089	用友网络 用友NC bsh.servlet.BshServlet 未授权 命令注入漏洞	命令注入
LDYVUL-2022-00519734	宇视科技 Uniview 未授权 命令注入漏洞	命令注入
LDYVUL-2024-00392403	中国电信 电信网关配置管理系统 del_file.php 未授权 命令注入漏洞	命令注入
LDYVUL-2023-00684448	Apache Activemq 未授权 代码注入漏洞	代码注入
LDYVUL-2024-00386625	Apache Apache CloudStack 未授权 代码注入漏洞	代码注入
LDYVUL-2023-00087427	Apache BRPC 未授权 代码注入漏洞	代码注入
LDYVUL-2023-00317451	Apache Commons Configuration 代码注入漏洞	代码注入
LDYVUL-2023-00488578	Apache Commons Text 代码注入漏洞	代码注入
LDYVUL-2023-00063917	Apache Log4j 代码注入漏洞	代码注入
LDYVUL-2024-00535316	Apache OFBiz 未授权 代码注入漏洞	代码注入
LDYVUL-2023-00411512	Apache Solr 未授权 代码执行漏洞	代码注入
LDYVUL-2022-00519705	Array Networks SSL VPN 未授权 代码注入漏洞	代码注入
LDYVUL-2024-00003744	Atlassian Confluence 未授权 代码注入漏洞	代码注入
LDYVUL-2024-00265059	Atlassian Confluence 需授权 代码注入漏洞	代码注入
LDYVUL-2023-00369764	Atlassian Jira Data Center 权限管理不当漏洞	代码注入
LDYVUL-2023-00470767	Atlassian Jira Data Center 需授权 代码注入漏洞	代码注入
LDYVUL-2023-00287144	Atlassian Jira Server 需授权 代码注入漏洞	代码注入
LDYVUL-2023-00198809	Atlassian Jira Server 需授权 代码注入漏洞	代码注入
LDYVUL-2023-00463091	Gitlab Gitlab 需授权 代码注入漏洞	代码注入
LDYVUL-2022-00519587	H3C IMC 智能管理中心 javax.faces.ViewState 未授权 代	代码注入

	码注入漏洞	
LDYVUL-2024-00531287	OpenIdentityPlatform OpenAM 需授权 代码注入漏洞	代码注入
LDYVUL-2023-00221791	Oracle WebLogic Server 访问控制不当漏洞	代码注入
LDYVUL-2024-00520420	Oracle Weblogic Server 未授权 代码注入漏洞	代码注入
LDYVUL-2024-00011935	Oracle Weblogic Server 未授权 代码注入漏洞	代码注入
LDYVUL-2024-00780192	Oracle WebLogic Server 未授权 代码注入漏洞	代码注入
LDYVUL-2024-00391132	Oracle WebLogic Server 未授权 代码注入漏洞	代码注入
LDYVUL-2024-00270053	PHP CGI 代码注入漏洞	代码注入
LDYVUL-2024-00840849	Pixel&tonic CraftCMS 未授权 代码注入漏洞	代码注入
LDYVUL-2024-00267966	Rejetto HTTP File Server 未授权 代码注入漏洞	代码注入
LDYVUL-2023-00210356	Vmware Cloud Foundation 未授权 代码注入漏洞	代码注入
LDYVUL-2024-00536986	Zabbix 需授权 代码注入漏洞	代码注入
LDYVUL-2024-00533852	北京数字认证 BJCA 电子印章签署系统 需授权 代码注入漏洞	代码注入
LDYVUL-2024-00530629	帆软 FineReport 报表 ReportServer 未授权 代码注入漏洞	代码注入
LDYVUL-2020-00518830	泛微 E-Cology BshServlet 未授权 代码注入漏洞	代码注入
LDYVUL-2024-00543322	泛微 E-Cology H2JDBC 需授权 代码注入漏洞	代码注入
LDYVUL-2024-00650569	飞致云 DataEase 需授权 代码注入漏洞	代码注入
LDYVUL-2024-00534914	亘岩网络 契约锁电子签章系统 template/param/edits 未授权 代码注入漏洞	代码注入
LDYVUL-2024-00532359	广联达 OA do.asmx 未授权 代码注入漏洞	代码注入
LDYVUL-2024-00548350	科荣 AIO 系统 UtilServlet 代码注入漏洞	代码注入
LDYVUL-2022-00519639	奇安信 天眼 SkyEye 新一代威胁感知系统 未授权 代码注入漏洞	代码注入
LDYVUL-2023-00519941	通达信科 网络智能办公系统 getdata 未授权 代码注入漏洞	代码注入
LDYVUL-2024-00003169	Gitlab Gitlab 访问控制不当漏洞	访问控制不当
LDYVUL-2024-00535405	Jenkins Remote 访问控制不当漏洞 可导致远程代码执行	访问控制不当
LDYVUL-2023-00381238	Oracle WebLogic Server 访问控制不当漏洞	访问控制不当

LDYVUL-2024-00542689	泛微 E-mobile /client/cdnfile 访问控制不当漏洞	访问控制不当
LDYVUL-2024-00029297	飞致云 DataEase 未授权 访问控制不当漏洞	访问控制不当
LDYVUL-2024-00699872	广联达 OA GetUserXml4GEPS 未授权 访问控制不当漏洞 可导致信息泄露	访问控制不当
LDYVUL-2024-00535309	海康威视 安防综合管理平台 IVMS8700 访问控制不当漏洞	访问控制不当
LDYVUL-2024-00391562	1Panel search 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2022-00519708	Array Networks Array VPN 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00816915	Jeecg JeecgBoot 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00778323	Palo Alto Networks Expedition 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00271035	Salesagility SuiteCRM 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00266778	Showdoc Showdoc item_id 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00541403	WookTeam 在线团队协作工具 Searchinfo 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00267931	堡塔安全 云 WAF get_site_status 需授权 SQL 注入漏洞	SQL 注入
LDYVUL-2020-00518881	北京通达 通达 OA swfupload_new.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00540048	畅捷通 CRM 系统 newleadset.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00268326	畅捷通 TPlus initServerInfo.aspx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00535447	驰骋软件 BPM 系统 Handler.ashx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00837853	大华 DSS 数字监控系统 group_saveGroup 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2023-00520080	大华 智慧园区系统 /portal/services/carQuery/getFaceCapture/searchJson 需授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00545294	点企来 客服系统 getwaitnum 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00543755	顶讯科技 易宝 OA 协同办公 BasicService.asmx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00837851	顶讯网络 易宝 OA GetUDEFStreamID 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00272413	泛微 E-cology BlogService 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00777234	泛微 E-Cology CptInstock1Ajax 未授权 SQL 注入漏洞	SQL 注入

LDYVUL-2024-00820106	泛微 E-Cology FileDownloadLocation 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2021-00519010	泛微 E-Cology getdata.jsp 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00268419	泛微 E-Cology ifNewsCheckOutByCurrentUser.dwr 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00545336	泛微 E-Cology ModeDateService SQL 注入漏洞	SQL 注入
LDYVUL-2024-00818470	泛微 E-Cology QRcodeBuildAction 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00390160	泛微 E-Cology WorkflowServiceXml SQL 注入漏洞	SQL 注入
LDYVUL-2024-00530649	泛微 E-Cology WorkPlanService 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2022-00519738	泛微 E-Office detail.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2022-00519588	泛微 E-Office login.wsdl.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00530732	泛微 E-office10 leave_record.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2022-00519536	泛微 云桥 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2022-00519631	泛微 E-Office /E-mobile/App/System/UserSelect/index.php 需授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00841250	泛微网络 E-Bridge checkMobile 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2023-00519828	泛微网络 E-Cology browser.jsp 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2023-00519844	泛微网络 E-Cology CheckServer.jsp 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2023-00519895	泛微网络 E-Cology getSqlData 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00841322	泛微网络 E-Cology LoginSSOxjsp/x.FileDownloadLocation 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2022-00519550	泛微网络 E-Cology 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00833162	泛微网络 云桥 e-Bridge /taste/addTaste 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00839252	泛微网络 云桥 e-Bridge addTasteJsonp 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2023-00084648	泛微网络科技 E-Cology FileDownloadForOutDoc 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00535419	方天科技 方天云智慧平台系统 GetSalQuatation 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00392398	方正信息 畅享全媒体新闻采编系统 binary.do 未授权 SQL 注入漏洞	SQL 注入

LDYVUL-2024-00392361	飞企互联 FE 企业运营管理平台 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00535243	飞企互联 FE 协作办公平台 apprvaddNew 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00700289	广联达 OA EmailAccountOrgUserService.asmx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00544747	广联达 OA GetDeptByDeptCode 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00542936	杭州三一谦成科技 车辆监控服务平台 platformSql 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2023-00520133	红帆 IOffice 办公自动化系统 net zyy_AttFile.asmx 未授权 SQL 注入	SQL 注入
LDYVUL-2022-00519623	红帆科技 红帆医疗云 OA switch-value/list 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2022-00519756	红帆科技 红帆医疗云 OA udfmrasmx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2022-00519634	红海人力 红海 eHR /RedseaPlatform/NbReport.mc 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00542948	红海云 eHR 系统 pc.mob 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2023-00519849	宏景人力资源管理系统 codesettree 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00539461	金斗云 HKMP 智慧商业软件 queryPrintTemplate 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00545347	金和 OA 协同办公 DBModules.aspx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00721447	金和 OA 协同办公 SignUpload.ashx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00544430	金和 OA 协同办公 UploadFileEditor.aspx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00531461	金和 OA GeneralXmlhttpPage.aspx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00541602	金和 OA jQueryUploadify SQL 注入漏洞	SQL 注入
LDYVUL-2024-00836920	金和网络 OA 协同办公 HomeService.asmx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00819988	金和网络 OA 协同办公 MailTemplates.aspx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00267953	金山 终端安全系统 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00831592	九思科技 OA 协同办公 workflowSync.getUserStatusByRole.dwr 未授权 SQL 注入	SQL 注入

	漏洞	
LDYVUL-2024-00392464	科荣 AIO moffice 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00542938	科荣 AIO moffice_endTime 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00530681	科拓 全智能停车收费系统 DoubtCarNoListFrom.aspx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00531741	科讯 校园一卡通管理系统 dormitoryHealthRanking 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00535248	科讯 一卡通管理系统 get_kq_tj_today 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00822976	蓝凌 OA 协同办公 WechatLoginHelper.do 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00819932	蓝凌软件 EIS 智慧协同平台 ShowUserInfo.aspx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00819927	蓝凌软件 EIS 智慧协同平台 UniformEntry.aspx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2025-00001803	蓝凌软件 EKP 系统 fsscCommonPortlet.do 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00392481	朗新天霁 人力资源管理系统 e-HR GetMessage 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00539760	朗新天霁 智能 eHR GetE01ByDeptCode 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00543753	乐享 智能运维管理平台 getToken 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00841311	灵当 CRM getMyAmbassador 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00667892	灵当 CRM marketing/index.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00535355	普华 PowerPMS APPGetUser 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2022-00519626	启明星辰 天玥网络安全审计系统 index.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00821704	全程云 OA 协同办公 QCPES.asmx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00539473	赛蓝 企业管理系统 GetImportDetailJson 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00822923	上海建业信息科技 章管家 department/list.htm 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00539479	上海建业信息科技 章管家 listUploadIntelligent 未授权	SQL 注入

	SQL 注入漏洞	
LDYVUL-2024-00548584	数字通 云平台智慧政务 workflow 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00530711	数字通 指尖云平台智慧办公 DAP PayslipUser 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2020-00518898	天融信 负载均衡系统 accclsfreportdatasourcephp 需授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00817688	通达 OA submenu.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2023-00519962	通达网络 智能办公系统 /general/document/index.php/recv/register/insert 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00821720	通达信科 OA 协同办公平台 recoverdata 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00532569	通达信科 通达 OA login.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2022-00519664	通达信科 通达 OA query.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2023-00519947	通达信科 通达网络智能办公系统 get_datas.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2023-00519974	通达信科 网络智能办公系统 report_bi.func 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2023-00519944	通达信科 网络智能办公系统 upsharestatus 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00392803	通天星 CMSV6 车载定位监控平台 disable 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00540056	通天星 CMSV6 车载定位监控平台 getAlarmAppealByGuid 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00535349	同享软件 人力资源管理平台 EmployeeInfoService.asmx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00540036	同鑫科技 eHR 人力资源管理系统 GetFlowDropDownListItems 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00547792	万户 ezOFFICE filesendcheck_gd.jsp 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00544437	万户 ezOFFICE receivefile_gd.jsp 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00816546	万户 ezOFFICE SignatureEditFrm.jsp 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00536405	万户 EZOFFICE 系统 graph_include.jsp 未授权 SQL 注入漏	SQL 注入

	洞	
LDYVUL-2024-00535376	亿赛通 电子文档安全管理系统 CDGAuthoriseTempletService1 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00817707	亿赛通 电子文档安全管理系统 HookService SQL 注入漏洞	SQL 注入
LDYVUL-2024-00392421	亿赛通 电子文档安全管理系统 SaveCDGPermissionFromGFOA 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00536989	亿赛通 电子文档安全管理系统 SecretKeyService 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00840042	亿赛通 电子文档安全管理系统 UploadFileToCatalog 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2022-00519497	易软天创 禅道项目管理软件 control.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2023-00519820	易软天创 禅道项目管理软件 misc-captcha-user.html 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2023-00519983	易软天创 禅道项目管理软件 router.class.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00835984	用友 GRP-U8 taskmanager_login 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00540748	用友 NC ActivityNotice 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00545580	用友 NC importPml 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00545625	用友 NC PaWfm SQL 注入漏洞	SQL 注入
LDYVUL-2024-00545564	用友 NC saveProDefServlet 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00545575	用友 NC workflowImageServlet 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00542657	用友 NCCloud TbbOutlineUpateVersionService 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00675362	用友 U8+ U8CRM 未授权 SQL 注入漏洞 可导致 RCE	SQL 注入
LDYVUL-2024-00548438	用友 U8+ U8CRM 未授权 SQL 注入漏洞 可导致 RCE	SQL 注入
LDYVUL-2024-00545155	用友 U8+CRM ajax/chkService.php 未授权 SQL 注入漏洞 可导致命令执行	SQL 注入
LDYVUL-2024-00540128	用友 U8+CRM exportdictionary.php 未授权 SQL 注入漏洞 可导致命令执行	SQL 注入
LDYVUL-2024-00542113	用友 U8Cloud AddTaskDataRightAction 未授权 SQL 注入漏洞	SQL 注入

LDYVUL-2024-00542160	用友 U8Cloud BusinessRefAction 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00542106	用友 U8Cloud CTExecDraftAction 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00543618	用友 U8Cloud IUFO 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00538522	用友 U8Cloud MailApproveServlet 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00542100	用友 U8Cloud MultiRepChooseAction 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00540124	用友 U8Cloud RepAddToTaskAction 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00538496	用友 U8Cloud ThinApproveServlet 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00268314	用友时空 KSOA TaskRequestServlet SQL 注入漏洞	SQL 注入
LDYVUL-2024-00267979	用友网络 GRP-U8 /u8qx/bx_historyDataCheck.jsp 需授权 SQL 注入	SQL 注入
LDYVUL-2024-00837802	用友网络 GRP-U8 bx_dj_check.jsp 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00834228	用友网络 GRP-U8 SelectDMJE.jsp 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00819164	用友网络 NC Cloud OpenAPI SQL 注入漏洞	SQL 注入
LDYVUL-2024-00778942	用友网络 NC 系统 checkekey 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00818535	用友网络 NC 系统 deleteOftenMenu SQL 注入漏洞	SQL 注入
LDYVUL-2024-00818543	用友网络 NC 系统 LfwFileQryServiceImpl SQL 注入漏洞	SQL 注入
LDYVUL-2024-00818518	用友网络 NC 系统 redeploy 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2022-00519557	用友网络 U8 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00830477	用友网络 U8+CRM ajax/getufvouchdata.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00818043	用友网络 U8+CRM getsrvtemplate.php SQL 注入漏洞	SQL 注入
LDYVUL-2024-00818481	用友网络 U8+CRM mysearch.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00839310	用友网络 U8Cloud /attachment/upload 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00545355	用友网络 U8Cloud MeasureQResultAction 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00831329	用友网络 U8CRM reservationcomplete.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2025-00004140	用友网络 U9Cloud /TransWebService.asmx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00830469	用友网络 用友 NC /portal/pt/task/process 未授权 SQL 注入漏洞	SQL 注入

LDYVUL-2024-00842546	用友网络 用友 NC /getMdPropertyJson SQL 注入漏洞	SQL 注入
LDYVUL-2024-00842533	用友网络 用友 NC /MaLoginAction SQL 注入漏洞	SQL 注入
LDYVUL-2024-00821775	用友网络 用友 NC /queryPsnInfo 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00842508	用友网络 用友 NC /queryworkbench SQL 注入漏洞	SQL 注入
LDYVUL-2024-00834254	用友网络 用友 NC /yerfile/down 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00839366	用友网络 用友 NC cartabletimeline 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00268361	用友网络 用友 NC Cloud Smart 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00840568	用友网络 用友 NC infid SQL 注入漏洞	SQL 注入
LDYVUL-2024-00842486	用友网络 用友 NC oacoSchedulerEvents/uncancelEvent SQL 注入漏洞	SQL 注入
LDYVUL-2024-00839378	用友网络 用友 NC portalpage SQL 注入漏洞	SQL 注入
LDYVUL-2024-00839375	用友网络 用友 NC redirect SQL 注入漏洞	SQL 注入
LDYVUL-2024-00839370	用友网络 用友 NC SSOQueryServiceImpl SQL 注入漏洞	SQL 注入
LDYVUL-2024-00831315	用友网络 用友 NC 流程任务查询 task SQL 注入漏洞	SQL 注入
LDYVUL-2024-00840585	用友网络 用友 U8 Cloud ReleaseRepMngAction 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2020-00518896	用友网络 用友 U8 Proxy 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00830385	用友网络 用友 U8+CRM ajaxgetborrowdata.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00268392	用友网络 用友时空 KSOA /servlet/imagefield 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00822950	浙大恩特 客户资源管理系统 Quotegask_editAction 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00530819	智邦国际 ERP GetPersonalSealData.ashx 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2022-00519622	中远麒麟 堡垒机安全运维管理系统 get_luser_by_sshport.php 未授权 SQL 注入漏洞	SQL 注入
LDYVUL-2024-00545745	Adobe ColdFusion 未授权 反序列化漏洞 可导致代码执行	反序列化
LDYVUL-2023-00451405	Alibaba Fastjson 未授权 反序列化漏洞	反序列化
LDYVUL-2023-00519847	Apache Druid 未授权 反序列化漏洞	反序列化
LDYVUL-2023-00487952	Apache Dubbo 未授权 反序列化漏洞	反序列化
LDYVUL-2023-00429849	Apache Kafka Connect 未授权 反序列化漏洞	反序列化

LDYVUL-2024-00545176	Ivanti Endpoint Manager 未授权 反序列化漏洞 可导致远程代码执行	反序列化
LDYVUL-2023-00078973	Metabase 未授权 反序列化漏洞 可致远程代码执行	反序列化
LDYVUL-2023-00325998	Oracle WebLogic Server 未授权 反序列化漏洞	反序列化
LDYVUL-2024-00022521	Progress Software Telerik Report Server 未授权 反序列化漏洞	反序列化
LDYVUL-2022-00519628	Red Hat JBOSS EAPAS 未授权 反序列化漏洞	反序列化
LDYVUL-2024-00779709	Splunk Enterprise 需授权 反序列化漏洞 可导致远程代码执行	反序列化
LDYVUL-2024-00531505	Spring Cloud Data Flow 反序列化漏洞 可导致代码执行	反序列化
LDYVUL-2024-00543390	Veeam Backup & Replication 未授权 反序列化漏洞 可致远程代码执行	反序列化
LDYVUL-2024-00822901	宝兰德 BES 管理控制台 未授权 反序列化漏洞 可致远程代码执行	反序列化
LDYVUL-2024-00541423	宝兰德软件 BES 管理控制台 ejb 未授权 反序列化漏洞 可致远程代码执行	反序列化
LDYVUL-2022-00519752	帆软 FineReport channel 未授权 反序列化漏洞	反序列化
LDYVUL-2024-00840504	海康威视 安防综合管理平台 iSecure Center /applyST 未授权 反序列化漏洞 可导致远程代码执行	反序列化
LDYVUL-2023-00519871	金蝶 云星空 /K3Cloud/Kingdee.BOS.ServiceFacade.ServicesStub.DevReportService.GetBusinessObjectData.common.kdsvc 未授权 反序列化漏洞	反序列化
LDYVUL-2024-00267902	金蝶软件 Apusic 应用服务器等 loadTree 未授权 反序列化漏洞	反序列化
LDYVUL-2022-00519774	金蝶软件 金蝶 EAS appUtil.jsp 未授权 反序列化漏洞	反序列化
LDYVUL-2022-00519723	普元应用开发平台 /default/jmx.jmx 未授权 反序列化漏洞	反序列化
LDYVUL-2024-00268349	瑞友天翼 应用虚拟化系统 session 反序列化漏洞	反序列化
LDYVUL-2024-00535371	苏州梓川信息科技 PEPM 平台 Auth 未授权 反序列化漏洞	反序列化
LDYVUL-2022-00519658	小鱼易连云视讯管理系统 未授权 反序列化漏洞	反序列化
LDYVUL-2024-00536712	亿赛通 电子文档安全管理系统 DecryptionApp 未授权 反	反序列化

	序列化漏洞 可导致远程代码执行	
LDYVUL-2024-00536871	亿赛通 电子文档安全管理系统 docRenewApp 未授权 反序列化漏洞 可导致远程代码执行	反序列化
LDYVUL-2024-00536838	亿赛通 电子文档安全管理系统 SecureUsbConnection 未授权 反序列化漏洞 可导致远程代码执行	反序列化
LDYVUL-2024-00779581	亿赛通 电子文档安全管理系统 UninstallApplicationService1 未授权 反序列化漏洞	反序列化
LDYVUL-2024-00823292	亿赛通 电子文档安全系统 /CDGServer3/TerminalLogService 未授权 反序列化漏洞	反序列化
LDYVUL-2024-00531494	用友 U8Cloud ESBInvokerServlet 未授权 反序列化漏洞	反序列化
LDYVUL-2024-00531491	用友 U8cloud ServiceDispatcher 未授权 反序列化漏洞	反序列化
LDYVUL-2024-00542174	用友 云巡检 未授权 反序列化漏洞 可导致 GetShell	反序列化
LDYVUL-2024-00531144	用友 NC Cloud /service/sprmonitorservlet 未授权 反序列化漏洞	反序列化
LDYVUL-2024-00268367	用友 NC 及 NC Cloud mxservlet 反序列化漏洞	反序列化
LDYVUL-2024-00267905	用友网络 NC registerServlet 未授权 反序列化漏洞	反序列化
LDYVUL-2020-00518845	用友网络 用友 NC ServiceDispatcherServlet 未授权 反序列化漏洞	反序列化
LDYVUL-2021-00519044	用友网络 用友 NC XbrlPersistenceServlet 未授权 反序列化漏洞	反序列化
LDYVUL-2023-00519856	用友网络 用友企业管理软件 NC InvokerServlet 未授权 反序列化漏洞	反序列化
LDYVUL-2023-00519864	用友网络 用友企业管理软件 NC MonitorServlet 未授权 反序列化漏洞	反序列化
LDYVUL-2024-00782257	致远互联 致远 OA loginController.do 未授权 反序列化漏洞	反序列化
LDYVUL-2024-00540863	中科汇联 AiSite 智能内容管理平台 未授权 反序列化漏洞	反序列化
LDYVUL-2023-00696314	Apache Struts2 未授权 文件上传限制不当漏洞 可导致远程代码执行	文件上传限制不当
LDYVUL-2024-00837193	Apache Struts2 文件上传限制不当漏洞 可导致远程代码执行	文件上传限制不当

LDYVUL-2023-00280017	Atlassian Jira Data Center 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2023-00338369	Barangay Management System Project Barangay Management System 需授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00820174	H3C CVM 平台 fileUpload/fd 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00536551	H3C SecPath 下一代防火墙 local_cert_delete_both 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00268239	IDocView html2word /html/2word 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00268340	Jeecg commonController 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2023-00268433	Microsoft Exchange Server 需授权 任意文件写入漏洞	文件上传限制不当
LDYVUL-2024-00379963	Spring Cloud Data Flow 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519542	安恒 明御 WEB 应用防火墙 需授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00544766	奥威亚 云视频平台 UploadFile.aspx 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519545	北京通达 通达 OA /im/upload.php 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2023-00519909	畅捷通 畅捷通 T+Upload.aspx 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2023-00520086	大华 智慧园区系统 /publishing/publishing/material/file/video 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00534298	顶点软件 LiveBos UploadFile.do 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00535276	顶点软件 LiveBos UploadImage.do 未授权 文件上传限制不当漏洞	文件上传限制不当

LDYVUL-2024-00782246	东方通 TongWeb 应用服务器 /sysweb/upload 需授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00778950	东方通 TongWeb 应用服务器 heimdall/deploy/upload 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00535330	泛微 E-Bridge addResume 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00781145	泛微 E-Cology Service_CheckApp 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2020-00518837	泛微 E-Cology WorkflowCenterTreeData 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00392355	泛微 E-Cology 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2021-00519384	泛微 E-Office UploadFile.php 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2023-00023853	泛微 E-Office uploadify.php 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519777	泛微网络 E-Cology Action.jsp 需授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2021-00519049	泛微网络 E-Cology KtreeUploadAction 未授权 文件上传漏洞	文件上传限制不当
LDYVUL-2022-00519660	泛微网络 E-Cology uploaderOperate.jsp 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519718	泛微网络 E-Cology uploadfile 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2021-00518996	泛微网络 E-Cology uploadOperation 未授权 文件上传漏洞	文件上传限制不当
LDYVUL-2024-00267961	泛微网络 E-Office 10 welink-move 需授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519768	泛微网络 E-Office do_excel.php 需授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519649	泛微网络 E-Office Init.php 未授权 文件上传限制不当漏洞	文件上传限制不当

LDYVUL-2022-00519607	泛微网络 E-Office OfficeServer.php 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00821578	泛微网络 e-office webservice 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00543311	方天科技 方天云智慧平台系统 setImg.ashx 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00268288	亘岩网络 契约锁电子签章系统 upload 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00779619	广联达 OA /Js/GWGDWebService.asmx 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2023-00519930	海康威视 安防综合管理平台 Isecure Center /center/api/files 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2023-00519859	海康威视 安防综合管理平台 Ivms-8700 /resourceOperations/upload 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00535291	海康威视 综合安防管理平台 uploadAllPackage/img 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519652	恒锋 信息指挥调度管理平台 testupload.php 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00781193	红帆 IOffice iorepsavexml.aspx 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519661	红海人力 红海 eHR OfficeServer 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519591	华天软件 华天动力 OA ntkoupload 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00535296	建业 章管家 uploadFileByChunks.htm 需授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519685	金蝶 EAS getenvs.jsp 需授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00267947	金蝶软件 Apusic 应用服务器 deployApp 未授权 文件上传限制不当漏洞	文件上传限制不当

LDYVUL-2024-00542963	金和 OA 协同办公 editeprint.aspx 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00542955	金和 OA 协同办公 jcsUploadServlet 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00542946	金和 OA 协同办公 SaveAsOtherFormatServlet 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00520428	凯京信达 Kkfileview 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00392438	科拓 智能停车管理系统 WebService.asmx 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519552	蓝凌 蓝凌 OA treexml 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00378935	蓝凌 OA sysUiComponent.do 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519766	蓝凌软件 OA 协同办公 /sys/attachment/sys_att_main/jg_service.jsp 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00541595	浪潮 GS 企业管理软件 UploadListFile 未授权 文件上传限制不当漏洞 可致远程代码执行	文件上传限制不当
LDYVUL-2024-00815133	联达动力 OA uploadImg.aspx 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00722359	灵当 CRM multipleUpload.php 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00841383	灵当 CRM uploadfile.php 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00779900	灵当 CRM wechatSession/index.php 文件上传限制不当漏洞 可致远程代码执行	文件上传限制不当
LDYVUL-2022-00519712	绿盟 NF 防火墙 bugsInfo/resourse.php 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519776	奇安信 网神 SecGate3600 防火墙 未授权 文件上传限制不当漏洞	文件上传限制不当

LDYVUL-2024-00538506	全程云 OA 协同办公 UploadFile 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00779554	润乾信息 润乾报表 servlet/dataSphereServlet 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00535441	赛蓝 企业管理系统 SubmitUploadify 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00822957	赛普 EAP 企业适配管理平台 Upload 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519728	拓尔思 MAS 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519696	通达信科 通达 OA getdata.php 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2020-00518870	通达信科 通达 OA print.php 未授权 任意文件上传漏洞	文件上传限制不当
LDYVUL-2021-00519114	通达信科 通达 OA upload.php 需授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2023-00519942	通达信科 通达网络智能办公系统 action_upload.php 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2023-00519981	通达信科 网络智能办公系统 api.ali.php 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00535436	同享软件 人力资源管理平台 hdlUploadFile.ashx 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00535301	同享软件 人力资源管理平台 UploadHandler 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00774980	万户 ezOFFICE fileUpload.controller 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00840589	万户 ezoffice wpsservlet 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2023-00519977	万户网络 万户 OA officeserverservlet 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519598	万户网络 万户 OA officeserverservlet 需授权 文件上传限制不当漏洞	文件上传限制不当

LDYVUL-2022-00519562	新华三 CAS 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2023-00520181	亿赛通 电子文档安全管理系统 需授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2020-00518910	易软天创 禅道项目管理软件 需授权 文件上传漏洞	文件上传限制不当
LDYVUL-2024-00541415	银达云创 智慧校园管理系统 FileUpAd.aspx 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00705851	用友 NC importExcelTemplate 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00545169	用友 NC portal/pt/file/upload 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00392370	用友 U8 CRM import.php 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00545617	用友 U8+CRM setting.php 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2023-00520052	用友 移动系统管理平台 uploadApkdo 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00535251	用友 政务 A++ ckeditorUpload 需授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00268309	用友 U8+ CRM 客户关系管理系统 /ajax/getemaildata.php 需授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519600	用友网络 NC accept.jsp 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00819305	用友网络 NC Cloud CA 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519627	用友网络 NC grouptemplet 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00818460	用友网络 NC 系统 saveImageServlet/saveXmlToFIleServlet 文件上传限制不当漏洞	文件上传限制不当

LDYVUL-2022-00519668	用友网络 U8 UploadFileData 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2022-00519640	用友网络 时空 KSOA ImageUpload 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2020-00518926	用友网络 用友 NC FileReceiveServlet 未授权 文件上传漏洞	文件上传限制不当
LDYVUL-2024-00544711	正方软件 移动信息服务管理系统 oaMobile_fjUploadByType 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2021-00518950	致远互联 致远 OA ajax.do 未授权 文件上传漏洞	文件上传限制不当
LDYVUL-2020-00518817	致远互联 致远 OA htmlofficeservlet 未授权 文件上传限制不当	文件上传限制不当
LDYVUL-2024-00268426	致远互联 致远 OA syncConfigManager 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2021-00519030	致远互联 致远 OA thirdpartyController.do 未授权 文件上传漏洞	文件上传限制不当
LDYVUL-2022-00519540	致远互联 致远 OA wpsAssistServlet 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00821548	中国电信 网关配置管理系统 upload_channels.php 未授权 文件上传限制不当漏洞	文件上传限制不当
LDYVUL-2024-00380448	Adobe Commerce 未授权 外部实体注入漏洞	XML 外部实体注入(XXE)
LDYVUL-2023-00519883	泛微 E-Cology deleteUserRequestInfoByXml 未授权 XML 外部实体注入(XXE)漏洞	XML 外部实体注入(XXE)
LDYVUL-2024-00783656	泛微网络 E-Cology ReceiveCCRequestByXml 未授权 XML 外部实体注入漏洞	XML 外部实体注入(XXE)
LDYVUL-2024-00648920	飞致云 DataEase 需授权 XML 外部实体注入漏洞	XML 外部实体注入(XXE)

LDYVUL-2024-00392761	广联达 OA ArchiveWebService 未授权 XML 外部实体注入漏洞	XML 外部实体注入(XXE)
LDYVUL-2024-00817034	金和 OA 协同办公 ApproveRemindSetExec.aspx 未授权 XML 外部实体注入漏洞	XML 外部实体注入(XXE)
LDYVUL-2024-00544420	九思科技 OA 协同办公 WebServiceProxy 未授权 XML 外部实体注入漏洞	XML 外部实体注入(XXE)
LDYVUL-2025-00002031	用友网络 U8Cloud lfw/chart 未授权 XML 外部实体注入漏洞	XML 外部实体注入(XXE)
LDYVUL-2023-00519921	致远 致远 OA SeeyonReportServiceServlet 未授权 XML 外部实体注入(XXE)漏洞	XML 外部实体注入(XXE)
LDYVUL-2024-00268333	致远互联 致远 OA getAjaxDataServlet 未授权 XML 外部实体注入漏洞	XML 外部实体注入(XXE)
LDYVUL-2023-00056219	Apache Hadoop 需授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00537165	Apache OFBiz 未授权 路径遍历漏洞 可导致远程代码执行	路径遍历
LDYVUL-2024-00268476	Apache OFBiz 未授权 路径遍历漏洞 可导致远程代码执行	路径遍历
LDYVUL-2022-00519707	Array Networks Array VPN 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00267040	Check Point Security Gateways 未授权 路径遍历漏洞	路径遍历
LDYVUL-2023-00298814	GitLab CE/EE 未授权 路径遍历漏洞	路径遍历
LDYVUL-2023-00432384	Ignite Realtime 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00548522	Ivanti Cloud Service Appliance 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00269513	SolarWinds ServU 路径遍历漏洞	路径遍历
LDYVUL-2024-00261614	Sonatype Nexus Repository 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00385439	Splunk Enterprise 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00779665	Splunk Enterprise 需授权 路径遍历漏洞 可导致远程代码执行	路径遍历
LDYVUL-2024-00781700	Spring Framework 路径遍历漏洞	路径遍历

LDYVUL-2024-00268284	大华 DSS 综合管理平台 /portal/attachment_downloadByUrlAtt.action 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00835999	大华 DSS 数字监控系统 attachment_downloadAtt.action 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00543305	东华医疗 协同办公系统 templateFile 未授权 路径遍历漏洞	路径遍历
LDYVUL-2023-00519891	泛微 泛微网络 E-Cology Download.jsp 未授权 路径遍历漏洞	路径遍历
LDYVUL-2020-00518902	泛微网络 云桥 e-Bridge saveYZJFile 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00822983	海康威视 综合安防平台 download 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00542975	华平信息 AVCON 系统管理平台 download.action 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00532547	汇智 ERP 未授权 路径遍历漏洞	路径遍历
LDYVUL-2021-00519101	金蝶 EAS /appmonitor/protected/selector/server_file/files 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00267884	金蝶软件 Apusic 应用服务器 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00833255	金蝶软件 金蝶 EAS /pdfViewLocal.jsp 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00392423	金和 OA C6 DownLoadBgImage 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00839286	金和网络 金和 OA 办公平台 /jc6/JHSoft.WCF/login/oaplusrangedownloadfile 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00841248	蓝凌 EKP 系统 sysFormMainDataInsystemWebservice 未授权 路径遍历漏洞	路径遍历
LDYVUL-2021-00519102	蓝凌 OA 协同办公 custom.jsp 未授权 路径遍历漏洞	路径遍历
LDYVUL-2023-00519912	蓝凌 OA 协同办公 kmImeetingRes.do 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00779963	灵当 CRM data/pdf.php 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00535336	启明星辰 天清汉马 VPN download 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00392551	锐明技术 Crocus 系统 Service.do 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00532557	赛蓝 赛蓝企业管理系统 未授权 路径遍历漏洞	路径遍历

LDYVUL-2024-00833686	顺景 ERP TMScmQuote/GetFile 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00532326	天问物业 ERP 系统 docfileDownLoad.aspx 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00533694	天问物业 ERP 系统 VacantDiscountDownLoad.aspx 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00535366	易捷 OA 协同办公软件 ShowPic 未授权路径遍历漏洞	路径遍历
LDYVUL-2022-00519492	用友网络 NC NCFindWeb 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00535178	正奇晟业科技 满客宝智慧食堂系统 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00392826	致远互联 AnalyticsCloud 分析云 未授权 路径遍历漏洞	路径遍历
LDYVUL-2021-00519068	致远互联 致远 A8 协同管理软件 officeservlet 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00543762	智互联科技 SRM 智联云采系统 download 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00840464	卓软信息 IDocView _qJvqhFt.json 未授权 路径遍历漏洞	路径遍历
LDYVUL-2024-00543696	Alibaba Nacos Jraft 未授权 权限管理不当漏洞	权限管理不当
LDYVUL-2023-00517520	Apache Couchdb 权限管理不当漏洞	权限管理不当
LDYVUL-2024-00542189	Apache OFBiz 权限管理不当漏洞 可导致远程代码执行	权限管理不当
LDYVUL-2023-00523641	Atlassian Confluence Data Center 权限管理不当漏洞	权限管理不当
LDYVUL-2023-00389982	Atlassian Jira Align 权限管理不当漏洞	权限管理不当
LDYVUL-2023-00194257	GitLab GitLab 权限管理不当漏洞	权限管理不当
LDYVUL-2023-00287749	Linux Linux Kernel 权限管理不当漏洞	权限管理不当
LDYVUL-2023-00046665	Oracle Coherence 权限管理不当漏洞	权限管理不当
LDYVUL-2023-00476088	Oracle Weblogic Server 权限管理不当漏洞	权限管理不当

LDYVUL-2023-00425928	Redis Redis 权限管理不当漏洞	权限管理不当
LDYVUL-2024-00779707	Splunk Enterprise 需授权 权限管理不当漏洞 可导致敏感信息泄露	权限管理不当
LDYVUL-2023-00371123	Zabbix Zabbix 访问控制不当漏洞	权限管理不当
LDYVUL-2022-00519653	大华 视频管理系统 user_initPasswordRetrieve.action 权限管理不当漏洞	权限管理不当
LDYVUL-2022-00519573	顶想信息 ThinkPHP errfile 权限管理不当漏洞	权限管理不当
LDYVUL-2023-00519885	泛微 E-Office XmlRpcServlet 未授权 权限管理不当漏洞	权限管理不当
LDYVUL-2021-00519072	泛微网络 ECology WorkflowServiceXml 未授权 权限管理不当漏洞	权限管理不当
LDYVUL-2024-00378936	广联达 OA GetUserXml4GEPS 未授权 权限管理不当漏洞	权限管理不当
LDYVUL-2024-00535359	建业 章管家 saveUser.htm 未授权 权限管理不当漏洞	权限管理不当
LDYVUL-2024-00540714	启业云 五指山运维平台 权限管理不当漏洞	权限管理不当
LDYVUL-2022-00519740	拓尔思 MAS 权限管理不当漏洞	权限管理不当
LDYVUL-2022-00519761	信锐网科 交换机 exec_command.cgi 未授权 权限管理不当漏洞	权限管理不当
LDYVUL-2024-00392406	迅饶 sunfull UpdateUser 权限管理不当漏洞	权限管理不当
LDYVUL-2024-00530788	易天智能 eHR 管理平台 CreateUser 权限管理漏洞	权限管理不当
LDYVUL-2024-00617046	用友 U8Cloud UsersComplexRefAction 未授权 权限管理不当漏洞	权限管理不当
LDYVUL-2024-00537012	用友 政务财务云 权限管理不当漏洞	权限管理不当

LDYVUL-2023-00218878	Atlassian Jira Data Center 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2023-00277059	F5 BigIp Policy Enforcement Manager 权限管理不当漏洞	身份验证缺陷
LDYVUL-2024-00836427	Ivanti Cloud Services Application 未授权 身份验证缺陷漏洞 可导致远程代码执行	身份验证缺陷
LDYVUL-2023-00039133	Playsms Playsms 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2024-00267272	Progress Software Telerik Report Server 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2023-00021361	Ruijienetworks RgEw1200g Firmware 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2023-00080196	Vmware Spring Framework 身份认证缺陷漏洞 可导致敏感信息泄露	身份验证缺陷
LDYVUL-2023-00447128	Zabbix Zabbix 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2024-00539442	泛微 E-Cology 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2024-00779452	泛微 E-Office sample.php 身份验证缺陷漏洞 可导致远程代码执行	身份验证缺陷
LDYVUL-2022-00519743	泛微网络 E-Cology VerifyQuickLogin.jsp 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2023-00519852	泛微网络科技股份有限公司 E-Cology ofsLogin.jsp 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2025-00004189	杭州飞致云信息科技有限公司 DataEase 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2024-00542982	华平信息 AVCON 网络视频服务系统 editusercommit.php 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2024-00541394	建业 章管家 updatePwd.htm 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2021-00519020	齐治科技 齐治堡垒机安全运维管理系统 gui_detail_view.php 身份验证缺陷漏洞	身份验证缺陷

LDYVUL-2023-00519904	齐治科技 齐治堡垒机安全运维管理系统 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2020-00518842	通达信科 通达 OA login_code.php 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2023-00519963	通达信科 网络智能办公系统 logincheck_code.php 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2024-00839266	通天星 CMSV6 车载视频监控平台 StandardLoginAction_getAllUser.action 身份验证缺陷漏洞 可导致敏感信息泄露	身份验证缺陷
LDYVUL-2023-00320861	微软公司 Microsoft 365 Apps For Business 等 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2024-00543920	亿赛通 电子文档安全管理系统 getAllUsers 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2024-00527360	易软天创 禅道系统 api.php 需授权 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2024-00539189	用友 NCCloud INtbOBAWebService 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2024-00839318	用友网络 GRP-U8Cloud getAuthorizer/getCzyTableByUnit 身份验证缺陷漏洞 可导致敏感信息泄露	身份验证缺陷
LDYVUL-2024-00535189	正奇晟业科技 满客宝智慧食堂系统 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2021-00519063	致远互联 致远 OA autoinstall.do 未授权 身份验证缺陷	身份验证缺陷
LDYVUL-2021-00519061	致远互联 致远 OA rest.do 未授权 身份验证缺陷漏洞	身份验证缺陷
LDYVUL-2023-00450367	Apache 软件基金会 Apache HTTP 服务器 HTTP 请求走私漏洞	HTTP 请求走私
LDYVUL-2023-00396861	Wps Wps Office UAF 漏洞	UAF
LDYVUL-2024-00391112	Oracle Weblogic Server 未授权 代码注入漏洞	安全缺陷
LDYVUL-2024-00531720	贝锐信息 向日葵企业私有化部署 安全缺陷漏洞	安全缺陷
LDYVUL-2024-00842499	用友网络 U9Cloud kkfileview 安全缺陷漏洞	安全缺陷

LDYVUL-2023-00266361	Atlassian Confluence Data Center 未授权 表达式注入漏洞	表达式注入
LDYVUL-2024-00535428	JeecgBoot JimuReport 积木报表 /jmreport/save 未授权 表达式注入漏洞	表达式注入
LDYVUL-2023-00267629	Apache 软件基金会 Superset 数据可视化平台 初始化不当漏洞	初始化不当
LDYVUL-2024-00822929	Apache OFBiz 服务器端请求伪造(SSRF)漏洞 可致远程代码执行	服务器端请求伪造(SSRF)
LDYVUL-2024-00542181	Apache OFBiz 未授权 服务器端请求伪造漏洞 可导致远程代码执行	服务器端请求伪造(SSRF)
LDYVUL-2023-00519841	Apache 软件基金会 Solr 未授权 服务器端请求伪造(SSRF)漏洞	服务器端请求伪造(SSRF)
LDYVUL-2023-00412022	Atlassian Atlassian Jira 需授权 服务器端请求伪造(SSRF)漏洞	服务器端请求伪造(SSRF)
LDYVUL-2023-00239953	Atlassian Jira Server 需授权 服务器端请求伪造(SSRF)漏洞	服务器端请求伪造(SSRF)
LDYVUL-2023-00354024	Microsoft Exchange Server 未授权 服务器端请求伪造(SSRF)漏洞	服务器端请求伪造(SSRF)
LDYVUL-2024-00822972	泛微 E-Cology getFileViewUrl 未授权 服务器端请求伪造漏洞	服务器端请求伪造(SSRF)
LDYVUL-2022-00519605	安恒 明御 WEB 应用防火墙 代码注入漏洞	固定会话
LDYVUL-2022-00519612	盈世科技 Coremail 缓冲区操作限制不当漏洞	缓冲区操作限制不当

LDYVUL-2023-00191509	H3c Magic B1st Firmware 缓冲区溢出漏洞 可导致拒绝服务	缓冲区溢出
LDYVUL-2023-00483572	Redis Redis 缓冲区溢出漏洞	缓冲区溢出
LDYVUL-2023-00519927	致远互联 致远 OA /seeyonreport/ReportServer 未授权 服务器端请求伪造(SSRF)漏洞	跨站点脚本攻击(XSS)
LDYVUL-2022-00519732	金山软件 WPS Office 未授权 逻辑缺陷漏洞	逻辑缺陷
LDYVUL-2024-00534962	思迈特 Smartbi 未授权 逻辑缺陷漏洞	逻辑缺陷
LDYVUL-2023-00082891	Minio Minio 对象存储服务 敏感信息存储不当漏洞	敏感信息存储不当
LDYVUL-2024-00392407	大华 DSS 数字监控系统 user_edit.action 敏感信息存储不当漏洞	敏感信息存储不当
LDYVUL-2024-00539454	泛微 e-office10 schema_mysql.sql 敏感信息存储不当漏洞	敏感信息存储不当
LDYVUL-2024-00543315	方正信息 畅享全媒体新闻采编系统 syn.do 未授权 敏感信息存储不当漏洞	敏感信息存储不当
LDYVUL-2024-00268320	腾讯 企业微信 agentinfo 敏感信息存储不当漏洞	敏感信息存储不当
LDYVUL-2020-00518875	通达信科 通达 OA get_cal_list.php 敏感信息存储不当漏洞	敏感信息存储不当
LDYVUL-2024-00833696	同享软件 人力资源管理系统 ActiveXConnector 敏感信息存储不当漏洞	敏感信息存储不当
LDYVUL-2023-00353075	Gitlab Gitlab 凭证管理不当漏洞	凭证管理不当
LDYVUL-2023-00362721	Gitlab Gitlab 凭证管理不当漏洞	凭证管理不当
LDYVUL-2020-00518825	Redis Redis 未授权 身份验证缺陷漏洞 可导致远程代码执行	凭证管理不当
LDYVUL-2024-00268301	大华 智慧园区系统 /user_getUserInfoByUserName.action 凭证管理不当漏洞	凭证管理不当

LDYVUL-2024-00269486	思迈特 Smartbi setEngineAddress 凭证管理不当漏洞	凭证管理不当
LDYVUL-2023-00519872	思迈特 Smartbi 商业 BI 平台 /smartbi/vision/RMIServlet 凭证管理不当漏洞	凭证管理不当
LDYVUL-2022-00519645	通达信科 通达 OA header.inc.php 凭证管理不当漏洞	凭证管理不当
LDYVUL-2022-00519565	新华三 SecPath 凭证管理不当漏洞	凭证管理不当
LDYVUL-2021-00519056	致远互联 OA A8 thirdpartyControllerdo 凭证管理不当漏洞	凭证管理不当
LDYVUL-2022-00519637	Elastic NV Elasticsearch 签名验证不当漏洞	签名验证不当
LDYVUL-2024-00526825	CrushFTP 团队 Crushftp 未授权 输入验证不当漏洞	输入验证不当
LDYVUL-2024-00831821	H3C SecCenter SMP 未授权 输入验证不当漏洞 可导致远程代码执行	输入验证不当
LDYVUL-2024-00780326	Oracle WebLogic Server 未授权 输入验证不当漏洞	输入验证不当
LDYVUL-2024-00780287	Oracle WebLogic Server 未授权 输入验证不当漏洞	输入验证不当
LDYVUL-2024-00821749	九思科技 OA 协同办公 dl.jsp 未授权 输入验证不当漏洞	输入验证不当
LDYVUL-2024-00548355	易睦网络 imo 云办公室 Imo_DownLoadUI.php 输入验证不当漏洞	输入验证不当
LDYVUL-2024-00840174	Apache Tomcat 条件竞争漏洞 可导致远程代码执行	条件竞争
LDYVUL-2024-00842130	蓝凌软件 EKP 系统 sysTagWebService 未授权 外部资源引用不当漏洞	外部资源引用不当
LDYVUL-2024-00842142	蓝凌软件 EKP 系统 kmImeetingBookWebService 未授权 外部资源引用不当漏洞	外部资源引用不当
LDYVUL-2024-00842175	蓝凌软件 EKP 系统 kmImeetingResWebService 未授权 外部资源引用不当漏洞	外部资源引用不当

LDYVUL-2024-00842132	蓝凌软件 EKP 系统 sysNotifyTodoWebService 未授权 外部资源引用不当漏洞	外部资源引用不当
LDYVUL-2022-00519488	泛微 E-Office do_excel.php 未授权 文件包含漏洞	文件包含
LDYVUL-2024-00530542	金和 OA UploadFileDownLoadnew 未授权 文件包含漏洞	文件包含
LDYVUL-2024-00530662	赛蓝 企业管理系统 ReadTxtLog 未授权 文件包含漏洞	文件包含
LDYVUL-2022-00519748	新华三 H3C Cloud Application Service 未授权 文件包含漏洞	文件包含
LDYVUL-2022-00519798	信呼安全团队 信呼 Oa indexActionphp 需授权 文件包含漏洞	文件包含
LDYVUL-2023-00520176	亿赛通 电子文档安全管理系统 UploadFileList 未授权 文件包含漏洞	文件包含
LDYVUL-2024-00386392	Apache Tomcat 资源分配控制不当漏洞	异常处理不当
LDYVUL-2023-00006965	Redis Redis 越界读取漏洞	越界读取
LDYVUL-2023-00294520	Redis Redis 整数溢出漏洞	整数溢出
LDYVUL-2023-00269214	Atlassian Jira 项目与问题追踪工具 证书验证不当漏洞	证书验证不当
LDYVUL-2024-00530813	同享软件 人力资源管理平台 DownloadTemplate.asmx 未授权 路径遍历漏洞	资源控制不当

五、专家服务

360 漏洞云漏洞情报服务是依托 360BugCloud 0day 漏洞知识库、安全情报数据库、360 安全卫士安全大数据知识库、360 大网蜜罐威胁攻击知识库中的海量漏洞数据，凭借 360 搜索分布式聚合分析引擎，结合百余名 360 漏洞安全研究专家，打造出的一款实时全网 0-1day 漏洞威胁分析与预警服务。目前已在金融、证券、运营商、大型国企、央企、Top 互联网企业等诸多行业客户中提供 0day 漏洞预警订阅服务。

实时漏洞情报推送，请关注 360 漏洞云公众号（免费推送漏洞情报）

漏洞情报订阅咨询 ：

六、漏洞云情报服务介绍

为响应国家各级监管机构关于各单位对外部的漏洞开展快速响应和处置的工作要求，深化推进行业安全体系建设，360 漏洞云情报平台为客户提供定制化的漏洞情报推送及监测服务，服务特点如下：

多源整合，数据全面：1W+监测点，涵盖 CNVD、CNNVD、NVD 等权威漏洞库，24 小时不间断监测全球网站、博客、Twitter 等信息平台的安全漏洞资讯。自有 360BugCloud 开源漏洞收集平台、360 漏洞研究院可以持续产出高价值独家战略级零日漏洞情报。目前已储备标准化漏洞数量 30W+。

多渠道推送，及时响应：通过大数据、全天候、分布式的漏洞情报智能分发平台，漏洞情报可以通过邮件、微信消息或 API 接口的方式，助力漏洞情报推送极速响应，实现对企业客户多维触达，让企业走在安全的最前沿。

精准检测，方便验证：通过漏洞专家团队赋能，用标准化 POC 脚本实现漏洞的批量检测，快速精准发现企业内部资产存在的漏洞威胁。情报中机读关联信息可与客户业务联动，将企业 IT 资产与漏洞情报进行智能匹配分析，锁定受影响资产，辅助企业快速定位漏洞，确认危害等级。

专业补丁，助力漏洞修复：依托于 360 安全大脑强大的数据支撑，结合 360 漏洞云、漏洞研究院资深专家的漏洞分析研判，第一时间为企业提供漏洞防护策略及相应补丁，为客户抢占漏洞处置时机，消除漏洞隐患。

建议您订阅 360 漏洞云-漏洞情报服务，获取更多漏洞情报详情以及处置建议，让您的企业远离漏洞威胁。

联系电话：010-52447660

邮箱地址：g-ldyvi@360.cn

官网地址：https://vi.loudongyun.360.net

360 数字安全集团(三六零数字安全科技集团有限公司)是数字安全的领导者，以“上山下海助小微”为战略方向，专注为国家、城市、大型企业、中小微企业提供数字安全服务。过去 18 年，360 投入 250 亿，聚集超 2000 名安全专家，积累了 2000PB 安全大数据，为数字经济、数字政府、数字社会的建设提供全方位的安全解决方案，帮助城市、政府、企业规划和建设数字安全体系，形成应对数字安全复杂威胁的完整能力。

https://360.net