WordPress前台任意文件读取漏洞复现（CVE-2025-2294）

免责声明：本公众号所发布的全部内容，包括但不限于技术文章、POC脚本、漏洞利用工具及相关测试环境，均仅限于合法的网络安全学习、研究和教学用途。所有人在使用上述内容时，应严格遵守中华人民共和国相关法律法规以及道德伦理要求。未经明确的官方书面授权，严禁将公众号内的任何内容用于未经授权的渗透测试、漏洞利用或攻击行为。 所有人仅可在自己合法拥有或管理的系统环境中进行本地漏洞复现与安全测试，或用于具有明确授权的合法渗透测试项目。所有人不得以任何形式利用公众号内提供的内容从事非法、侵权或其他不当活动。 如因违反上述规定或不当使用本公众号提供的任何内容，造成的一切法律责任、经济损失、纠纷及其他任何形式的不利后果，均由相关成员自行承担，与本公众号无任何关联。

漏洞介绍

WordPress的Kubio AI Page Builder插件在2.5.1及之前所有版本中，存在通过`kubio_hybrid_theme_load_template`函数触发的本地文件包含漏洞。该漏洞允许未经身份验证的攻击者包含并执行服务器上的任意文件，从而运行这些文件中的任何PHP代码。攻击者可利用此漏洞绕过访问控制、获取敏感数据。

该插件目前有10万+的活跃安装次数，可谓**使用范围非常广**；

Kubio AI Page Builder

By Extend Themes

Download

Details | Reviews | Development | Support

Description

Using the power of AI, Kubio gives you a head start by generating a first draft of your website, which you can further customize to your liking.

BUILD AWESOME WORDPRESS SITES FASTER WITH THE HELP OF AI

Version	2.6.1
Last updated	1 week ago
Active installations	100,000+
WordPress version	5.8 or higher
Tested up to	6.8.1
PHP version	7.4 or higher
Languages	See all 3
Tags	blocks gutenberg

该漏洞利用无需任何利用前置条件，可谓**利用条件非常简单**。所以CVE官方也是给出了9.8的CVSS超高评分。

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

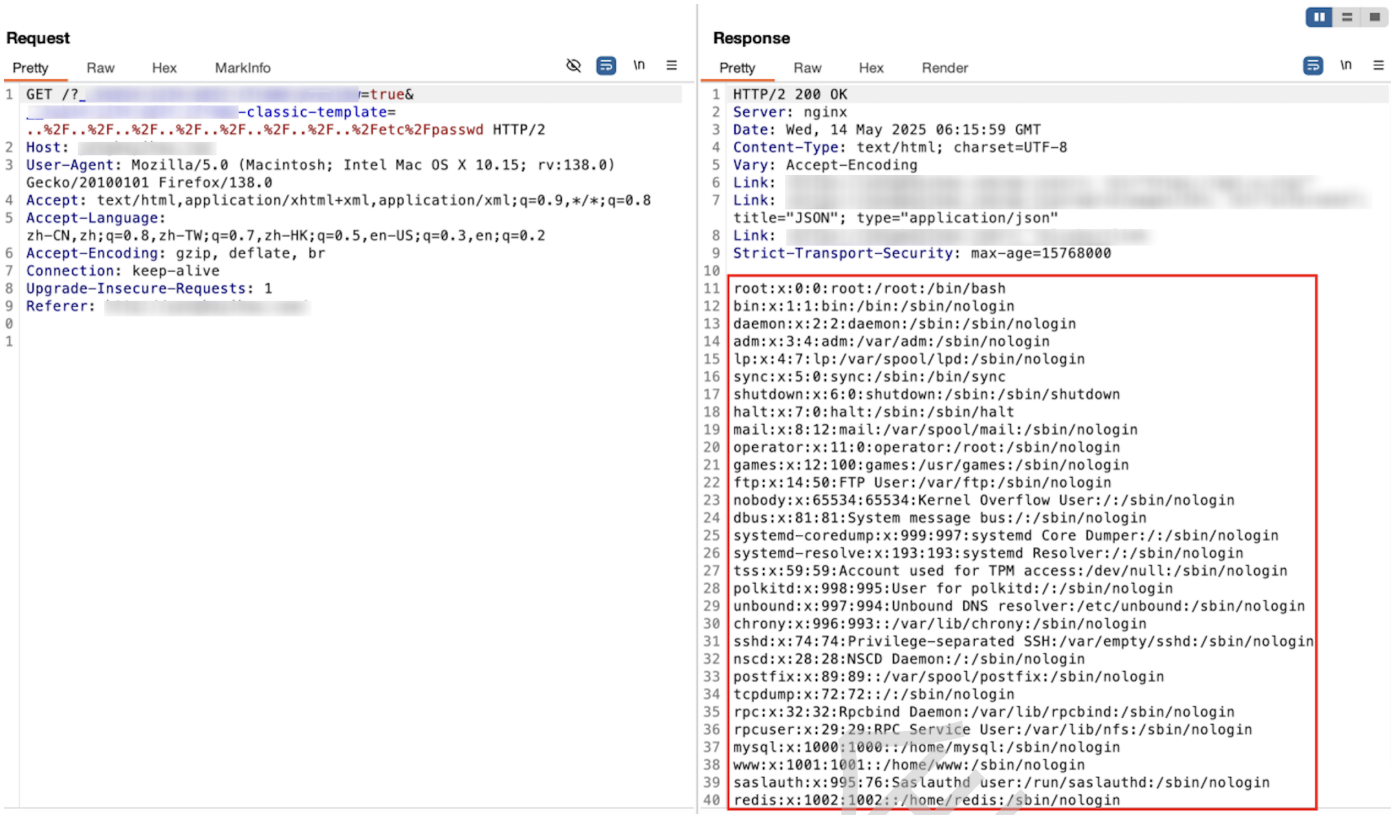
CVE	CVE-2025-2294
CVSS	9.8 (Critical)
Publicly Published	March 27, 2025
Last Updated	March 28, 2025
Researcher	mikemyers

漏洞版本

- Kubio AI Page Builder插件版本 <= 2.5.1

漏洞利用

使用如下POC进行漏洞利用读取到目标`/etc/passwd`文件



批量检测脚本

漏洞修复

- 升级到 2.5.1 以上版本

知识星球

漏洞**利用POC和nuclei检测脚本**可在知识星球内自行领取

> 星球不定期更新市面上最新的热点漏洞及复现环境，欢迎加入交流和学习

亮点一、**市面热点漏洞详细分析**，与**deepseek本地部署**息息相关的：Ollama任意文件读取漏洞（CVE-2024-37032）详细分析

a1batr0ss

仅供星球内部人员学习使用，请勿外传，如有发现，后果自负

《deepseek本地部署工具–ollama 任意文件读取漏洞分析》

当时研究这个漏洞时发现全网所有的资料都只是单纯的POC和复现，想具体了解下原理发现找不到相关文章，于是花了点时间写下了这篇文章。

本质是因为manifest文件中的digest字段过滤规则不严（digest字段类似于md5，用作文件校验，**本身为了安全而创造出的字段却导致了安全漏洞**）导致目录穿越，使得攻击者可以构造一个恶意的服务器读取ollama服务器上任意文件。

#漏洞研究

ollama任意文件读取漏洞详细分析.pdf

漏洞研究

查看详情 >

亮点二、**近日最新披露**漏洞：Erlang/OTP SSH 远程代码执行漏洞（CVE-2025-32433）POC及一键部署环境

a1batr0ss

Erlang/OTP SSH 远程代码执行漏洞（CVE-2025-32433）POC及一键部署环境

#复现环境及POC

CVE-2025-32433复现步骤.pdf

CVE-2025-32433一键部署环境.zip

POC-CVE-2025-32433.py.txt

复现环境及POC

查看详情 >

以及有师傅对该POC提出疑问后也会进行解答：

a1batr0ss

Erlang/OTP SSH 远程代码执行漏洞（CVE-2025-32433）RCE脚本

前段时间有师傅提出问题：之前给的 CVE-2025-32433 利用脚本只能实现写入文件，无法执行任意命令，花了点时间修改了下脚本实现了命令执行的功能（无回显命令执行哦，但可以把shell弹出来）。

使用方法很简单，就是-c参数带你要执行的命令（长命令使用双引号包裹即可）。

#想法&讨论

CVE-2025-32433-cmd.py.txt

想法&讨论

查看详情 >

亮点三、**框架漏洞专题-若依：**

若依某漏洞分析：

a1batr0ss

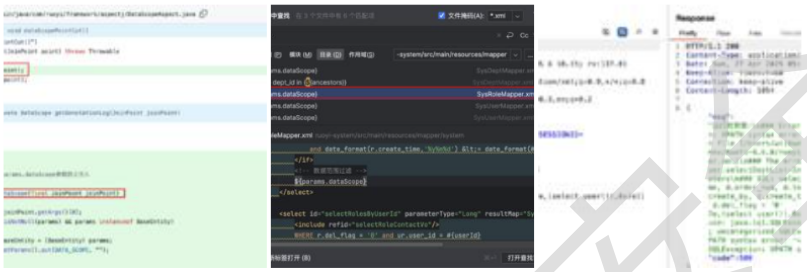
若依框架漏洞03

又是一个sql注入漏洞，漏洞点来源于**${params.dataScope}**，和之前那个漏洞类似，但修复方法却和之前完全不一样，这一次直接在执行方法前添加了一个**clearDataScope**函数清空**params.dataScope**参数的值防止了sql注入。

其次网上基本只讲了**/system/role/list** 和 **/system/role/export** 这两个出发点，但我发现 **/system/dept/list** 也同样能够触发该漏洞。

#框架安全-若依

若依后台SQL注入漏洞分析（DataScope数据权限注解...



框架安全-若依

查看详情 >

a1batr0ss

若依框架漏洞02

这个系列的第一个漏洞分析，先从一个简单的sql注入开始吧，目前市面上讲的较多的sql注入一共有4个，这次挑了**/system/dept/edit** 接口的sql注入来分析，即**CVE-2023-49371**

以及帮助师傅们轻松搭建若依环境的docker的tar包：

a1batr0ss

若依V4.6.0-docker部署环境

近期有师傅提出“本机部署ruoyi环境会出现各种各样的问题”，于是花时间做了这个docker，形式是tar包，两句命令即可部署**V4.6.0版本的若依**：

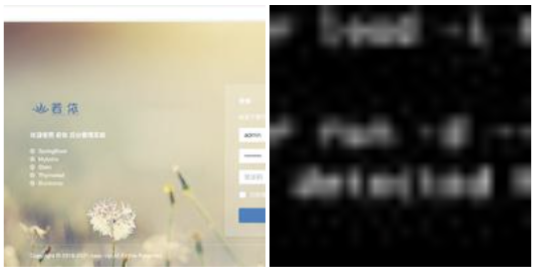
docker load -i ruoyi-v4_6_0.tar

docker run -d --name ruoyi-vuln -p 2222:22 -p 8080:8080 ruoyi-vuln-awd:3.1

具体的tar包放在百度云上了，附件内自行领取

#框架安全-若依

百度云链接&启动命令.txt



框架安全-若依

查看详情 >

亮点四、**实战渗透测试技巧分享&讨论**：某次若依系统渗透测试带来的思考与讨论

a1batr0ss

今天突然想起来，想记录下一些想法，前段时间在某次授权的渗透测试中，遇到了一个若依的系统，默认口令进去，找到swagger API文件里的api测出来个垂直越权；

然后用了若依新的任意文件下载漏洞（CVE-2023-27025）读取了/etc/passwd，接着想着读取一下~/.bash_history看看命令历史，结果发现这个系统是打包成jar包，运维在部署这个系统时使用了命令（java -jar xxx.jar），于是我直接按照命令历史里的路径把xxx.jar包拖出来了，然后扔到JD-GUI反编译。

反编译之后首先找找看有没有shiro的key，找了com.ruoyi.framework.config.ShiroConfig.class和application.xml都没有；如何找

展开全部

想法&讨论

查看详情 >

亮点五、一些比较新奇有趣的漏洞分享：Windows**拖拽图标**而触发的漏洞

a1batr0ss

当时看到就觉得很有意思的一个漏洞，试着复现了一下没有深入研究，有兴趣的可以研究研究

#杂七杂八的漏洞

Zero-day-cve-2024-4351-report.pdf

杂七杂八的漏洞

查看详情