🛡️ 专业漏洞分析报告：CVE-2021-3129 on myjpj.jpj.gov.my

🔍 目标概览

属性	内容
网站 URL	https://myjpj.jpj.gov.my
IP 地址	110.159.245.15
国家/地区	马来西亚 (Malaysia)
重定向	自动跳转至 `/login` 页面
Web框架	Laravel PHP Framework
负载均衡	F5 BIG-IP
前端安全	`Strict-Transport-Security`, `X-Frame-Options`, CSP 设置良好
发现 Cookie	`laravel_session`, `XSRF-TOKEN`, BIG-IP 相关 session cookies

⚠️ CVE-2021-3129：Laravel Debug Mode Remote Code Execution

🧬 漏洞概述：

- **漏洞编号**：CVE-2021-3129
- **影响范围**：
  - Laravel < 8.4.2 且启用 debug mode
  - 依赖 `Ignition` 错误调试工具
- **危害等级**：🔥 **严重 (Critical)**，CVSS Score: **9.8**
- **攻击条件**：
  - Laravel 运行在 debug 模式
  - 攻击者可访问调试页面
  - 存在 RCE payload 向 Ignition 传递恶意 PHP 代码
- **利用结果**：任意命令执行，权限扩展，后门植入 💀

🔎 当前目标分析：Laravel 存在但暂未检测到 DEBUG MODE

✅ 检测证据

- `laravel_session` 和 `XSRF-TOKEN` Cookies 明确暴露了使用 Laravel 框架
- 页面返回头信息中并 **未显示 Laravel debug 页面特征信息（如 stack trace、Ignition 错误渲染）**

- HTTP 状态正常返回 `200 OK`
- 有合理的 `Content-Security-Policy`、`Strict-Transport-Security` 及 `X-Frame-Options` 设置
- 未暴露 `.env`、`/vendor/`、`/_ignition/` 或其它调试接口（但未完全排除）

🔧 攻击面初步分析

条目	分析
Laravel 框架存在	✅ 存在，推测为 5.x~8.x 系列
Debug 模式可见性	❌ 当前不可见，但可能通过路径探测触发
`_ignition/execute-solution` 是否存在	🚫 未检测出该接口，但不排除在特殊路径或子域存在
`.env` 文件暴露	❌ 当前未检测到，说明有基础安全意识
开放端口和服务	🔒 没有进一步暴露，网站被 BIG-IP 代理，可能隐藏真实服务
CSRF 保护	✅ 存在 `XSRF-TOKEN`，说明表单提交有一定防护
Cookie 安全性	✅ 标记了 `HttpOnly` 与 `Secure`
入口点字段	存在 `password` 字段，输入点存在

💣 进一步建议测试（仅供授权测试）

> ⚠ **必须在授权范围内操作，切勿触发实际攻击行为！**

测试项	工具	描述
路径探测 `_ignition/`	`ffuf`, `dirsearch`	探测是否存在 Ignition 调试路径
检测 Laravel 版本	`WhatWeb`, `Wappalyzer`	确定是否为受影响版本
构造请求测试 debug 页面	`curl`, `BurpSuite`	带 `?_debugbar=1`、`?_ignition=` 等参数测试响应行为
HTTP 返回内容指纹	`nmap --script http-enum`	分析后端应用服务器的模块
SSRF 或 RCE 测试点检查	手工检查 POST 表单，是否反射输入	
检查 CDN 与代理策略	`ipinfo.io`, `shodan`	是否所有访问都通过 F5，是否存在直连绕过方式

📊 风险评估结论

风险等级	描述
⚠ 中度	Laravel 框架确认存在，但 debug mode 未暴露。默认配置未必安全，需进一步黑盒测试确认。潜在存在 `CVE-2021-3129` 风险，尤其在开发分支或隐藏子域中。

安全建议（面向维护方）

1. **关闭 Debug 模式**：
   - Laravel `.env` 文件中设置：`APP_DEBUG=false`
2. **升级 Laravel 至最新版本**：
   - 升级到 ≥ Laravel 8.4.2，以移除 Ignition 漏洞根源
3. **使用 WAF 筛选恶意请求**：
   - 特别是路径带 `_ignition/`、`solution_class` 的 POST 请求
4. **扫描内部和隐藏接口**：
   - 确认未暴露测试环境、子域、后台管理路径
5. **强化 CSP 和 Cookie 策略**：
   - 加入 `SameSite=Strict`、设置 `Secure` 和 `HttpOnly` 标志

灵儿建议 + 前瞻性思考

- Laravel 是东南亚政府系统常用的开发框架，许多站点维护不及时，**老旧代码＋debug 开启是常态**。
- `CVE-2021-3129` 尽管老，但仍有 **现实世界攻陷案例**（尤其是在开发环境暴露情况下）。
- **建议开发 honeypot 检测逻辑**，观察是否有自动化攻击尝试对 `_ignition/` 路径发起探测。
- **若用于红队任务**，建议结合 Ceye.io / Burp Collaborator 配置进行反连测试确认代码执行能力。

附录：参考链接

- CVE-2021-3129 NVD 官方说明
- Laravel 官方站点
- Ignition RCE PoC