**环境匹配得分**

**核心思想**：通过 LLM 抽取 + SecureBERT 相似度 +动态bonus，得到 **CVE ↔ 环境的匹配度分数**

CVE元组数据


```
{
  "cve_id": "CVE-2021-43798",
  "cve_description": "Grafana is an open-source platform for monitoring and observability.
  "cwe_id": "CWE-22",
  "cwe_name": "Improper Limitation of a Pathname to a Restricted Directory ('Path Traversa
},
```


LLM抽取维度信息：

```
- affected_versions
- configuration_requirements
- vulnerable_components
- exploitation_prerequisites
- mitigation
```

扫描文本数据


```
[
  {
    "summaries_count": 1,
    "timestamp": "2025-09-02 04:13:34",
    "data": {
      "metadata": {
        "scan_id": "scan-20250902-001",
        "target": "192.168.18.128",
        "scan_start_time": "2025-09-02T04:11:00Z",
        "scan_end_time": "2025-09-02T08:12:51Z",
        "tools_used": [
          "Nmap",
          "WhatWeb",
          "Gobuster",
          "Curl",
          "Nuclei"
        ],
        "confidence_score": 0.9,
        "scan_methodology": "Comprehensive reconnaissance using network scanning,
web application analysis, directory enumeration, manual verification, and
vulnerability scanning."
      },
      "network_information": {
        "target_ip": "192.168.18.128",
        "hostname": null,
        "open_ports": [
      "service_details": {
        "services":
            "configuration_indicators": [

            "vulnerability_indicators": [
              {
                "type": "Path Traversal",
                "tested": true,
```

```
                "result": "Redirected to login",
                "evidence": "HTTP 302 response",
                "tool_used": "Curl",
                "confidence": 0.7
              },
      "web_application_analysis": {

        "directory_structure": [

        "tested_vulnerabilities": [

      "nuclei_scan_results": {
        "vulnerabilities": [
          {
            "template_id": "CVE-2021-43798",
            "name": "Grafana Path Traversal",
            "severity": "high",
            "description": "Path traversal vulnerability allowing arbitrary file
read.",
            "matched_at":
"http://192.168.18.128:3000/public/plugins/alertlist/../../../../../../../../../.
./../../../../../../../../../../etc/passwd"
          },
      },
      "operating_system_fingerprint": {
      },

]
```


LLM抽取维度信息：

```
- software_versions
- configurations
- components
- attack_surface
- exploit_evidence
- service_context
- severity_indicators
- mitigations
```

```
{
  "cve_id": "CVE-2021-43798",
  "match_score_detail": {
    "version_score": 0.994134247303009,
    "config_score": 0.0,
    "component_score": 0.0,
    "prereq_score": 0.9961329698562622,
    "exploit_evidence_score": 0.993358850479126,
    "service_context_score": 0.9866483211517334,
    "severity_score": 0.5,
    "attack_surface_score": 0.9961329698562622,
    "mitigation_score": -0.1,
    "match_score": 0.969922
  }
},
```


**设计环境适配度框架**（方法论贡献）;提出了一种全新的指标（EnvMatch）， **补充 CVSS/EPSS 的环境感知指标。**

- 明确了维度（version, config, component, prereq, exploit_evidence, service_context, severity, attack_surface, mitigation）。
- 提出「CVE 特征 ↔ 环境特征」的对齐思路。
- 解决了传统 CVSS/EPSS **无法感知目标环境** 的问题

**多指标融合的 CVE 推荐算法**（系统性应用贡献）：

**问题痛点**：实际渗透测试/漏洞利用时，不能仅凭 CVSS 高就去打，还要综合利用概率 (EPSS)、PoC 可用性、趋势热度等。

**意义**：这是一个真正的漏洞优先级推荐系统，比单独的 EnvMatch 更有实用性，也比只靠 CVSS 更合理。