

代码安全审计报告

共发现 4 个安全问题

test.py:5

路径遍历风险 (MEDIUM)

直接使用外部输入的'input.pcap'文件名未做安全校验，可能导致任意文件读取

修复建议：增加输入文件白名单校验或路径合法性检查，限制用户只能读取指定目录文件

test.py:9

敏感信息泄露 (HIGH)

遍历所有数据包

使用二进制追加模式'ab'写入文件可能导致历史数据残留，且未限制文件权限

修复建议：使用'wb'模式覆盖写入，并设置适当文件权限（如0o600），写入前清空文件内容

test.py:5

内存耗尽风险 (MEDIUM)

rdpcap()直接加载大pcap文件可能导致内存耗尽

修复建议：采用流式处理方式（如PcapReader迭代处理），避免全量加载数据包

test.py:2

硬编码凭证 (MEDIUM)

目标字符串硬编码在代码中，增加凭证泄露风险

修复建议：将敏感字符串存储在环境变量或配置文件中，通过运行时读取方式获取