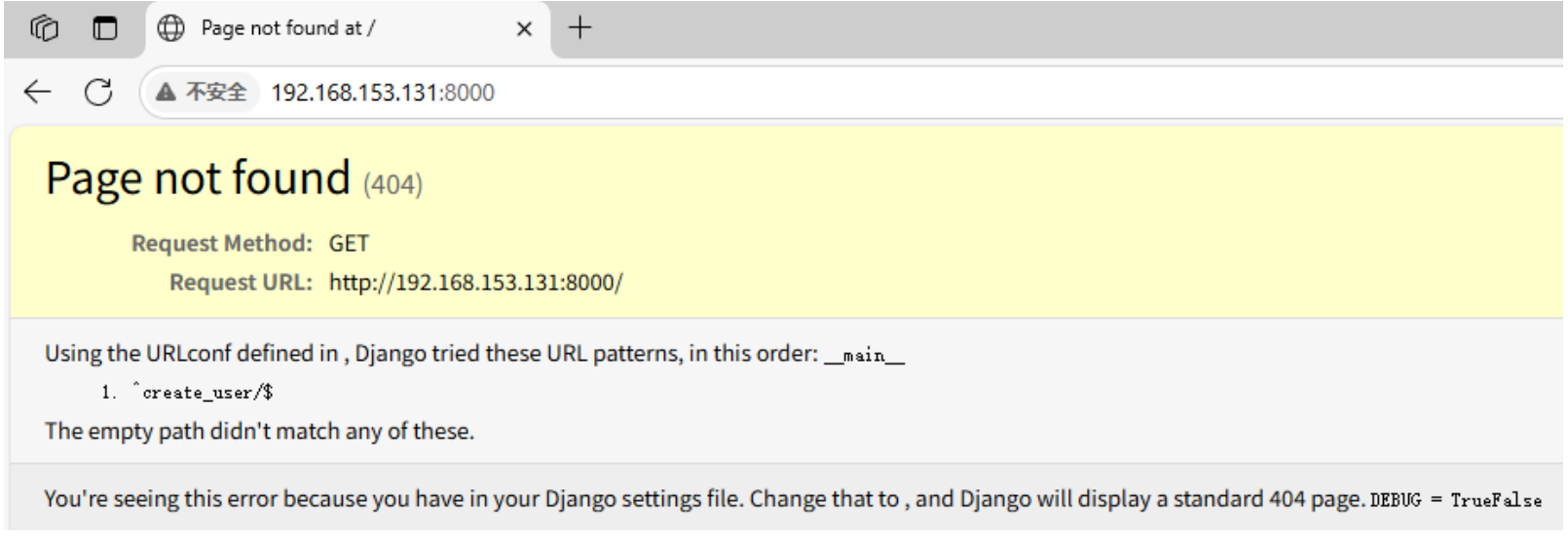
2025-06-26汇报

大模型智能体=>多源扫描日志漏洞信息标准化分析

目标主机Web网页呈现=>CVE-2017-12794

- **Django 1.11.4**： Python Web框架，1.11.5 和 1.10.8 之前的 Django 版本在调试错误页面中包含跨站点脚本(XSS)漏洞，启用 DEBUG 模式后，错误页面可能会通过错误消息中未转义的 HTML 公开敏感信息



智能体扫描呈现

- **扫描特点**：会根据大模型给出的每一步指令进行阶段性扫描，在扫描过程中可能会直接根据服务及版本列出几个潜在漏洞“potential”，且在扫描过程中肯能会直接**测试验证**这几个问题，从而验证出的漏洞特征会被列在“confirmed”中，从而根据这些验证的漏洞特征匹配CVE，例下图服务及版本为Django 1.11.4

- **最终输出表述不固定**：如下图服务及版本为phpMyAdmin 7.2.5，直接列举了这一服务可能存在的CVE，并没有给出主机应该存在的漏洞特征

```
{
    "analysis": {
        "ports": {
            "8080": {
                "accessibility": "open",
                "service": "http-proxy",
                "server": "Apache httpd",
                "server_version": "2.4.25",
                "OS": "Debian",
                "application": "phpMyAdmin",
                "application_version": "4.8.1",
                "backend": "PHP",
                "backend_version": "7.2.5",
                "vulnerabilities": [
                    "CVE-2018-12613 (Local File Inclusion)",
                    "CVE-2018-19968 (XSS)"
                ],
                "interesting_paths": {
                    "/robots.txt": "Disallows all crawlers (User-agent: * Disallow: /)",
                    "/README": "phpMyAdmin 4.8.1 documentation"
                },
                "cookies": "phpMyAdmin session cookie present",
                "headers": {
                    "X-Powered-By": "PHP/7.2.5",
                    "Cache-Control": "private, max-age=10800"
                }
            }
        },
        "OS": "Linux (Debian)",
        "IP": "192.168.18.128",
        "MAC": "00:0C:29:6B:D7:E8 (VMware)",
        "additional_findings": {
            "web_interface": "MySQL/MariaDB administration via phpMyAdmin",
            "security_headers": "Missing security headers like X-Frame-Options, X-XSS-Protection",
            "authentication": "No obvious authentication required (based on initial scans)"
        }
    },
    "next_step": "Proceed with vulnerability assessment and exploitation targeting: 1) phpMyAdmin 4.8.1 vulnerabilities, 2) Apache 2.4.25 potenti
al misconfigurations, 3) PHP 7.2.5 known issues. Consider testing for Local File Inclusion (CVE-2018-12613) first.",
    "executable": "None"
}
```


- **扫描工具特点**：对此我们发现，扫描工具不仅有分阶段性(初期、针对性、深度)的扫描分类，还有侵入式(主动)与非侵入式(被动)的分类
  - 侵入式扫描工具：可能在扫描过程中直接验证了该主机存在的漏洞
    - **Burp Suite**：行业标准Web应用渗透测试工具，主动发送攻击载荷，如：SQL注入/XSS/RCE等
    - **OWASP ZAP**：自动漏洞利用，服务端模板注入检测
  - 非侵入式扫描工具：即不修改系统状态、不尝试漏洞利用，仅发送探测请求，不进行任何渗透测试的验证手段
    - **Nmap**：用于端口扫描和服务识别，提供主机的基本攻击面信息，如：开放端口、运行服务
    - **Nikto**：专门针对Web应用进行漏洞扫描，检测配置错误、敏感文件暴露和常见安全风险
    - **OpenVAS**：用于全面漏洞扫描，识别已知漏洞模式，但不验证或利用，最终生成详细报告
    - **Wappalyzer**：被动识别Web技术栈，包括框架、库、服务器以及相关版本等
    - **curl**：主要发送 HTTP 请求和接收响应，但**不具备主动扫描漏洞或深度探测的能力**，在某些情况下可能被归类为**轻度侵入式**(测试路径遍历)

手动扫描过程呈现

- **核心目标**：扫描出目标主机真实存在的漏洞描述，而非列出各服务版本已有的潜在漏洞或CVE

基础信息收集——nmap

```
┌──(py311env)-(root㉿kali)-[/home/kali]
└─# nmap -sV -p 8000 192.168.153.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-25 01:05 EDT
Nmap scan report for 192.168.153.131
Host is up (0.00063s latency).

PORT     STATE SERVICE VERSION
8000/tcp open  http    WSGIServer 0.2 (Python 3.5.9)
MAC Address: 00:0C:29:39:14:B0 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.45 seconds
```

- **收集信息**：运行了一个基于**Python 3.5.9**的**WSGI HTTP服务**(可能是Django、Flask等Python Web框架开发的应用程序)。MAC地址显示该主机可能是一台VMware虚拟机

curl => 调试和探测目标Web服务 => -v 输出完整的请求头、响应头和网络交互细节

```
┌──(py311env)-(root㉿kali)-[/home/kali/pentest-agent/agents]
└─# curl -v -X OPTIONS http://192.168.153.131:8000
*   Trying 192.168.153.131:8000 ...
* Connected to 192.168.153.131 (192.168.153.131) port 8000
> OPTIONS / HTTP/1.1
> Host: 192.168.153.131:8000
> User-Agent: curl/8.7.1
> Accept: */*
>
* Request completely sent off
* HTTP 1.0, assume close after body
< HTTP/1.0 404 Not Found
< Date: Wed, 25 Jun 2025 08:24:25 GMT
< Server: WSGIServer/0.2 CPython/3.5.9
< Content-Type: text/html
< Content-Length: 1925
```

```
        <li>
            ^create_user/$
        </li>
    </ol>
    <p>
      The empty path didn't match any of these.
    </p>
</div>

<div id="explanation">
  <p>
    You're seeing this error because you have <code>DEBUG = True</code> in
    your Django settings file. Change that to <code>False</code>, and Django
    will display a standard 404 page.
  </p>
</div>
```

- **分析得知**：运行框架为Django[WSGIServer/0.2 CPython/3.5.9]，唯一暴露的URL端点：`/create_user/`，尝试触发错误页面获取更多信息：`curl http://192.168.153.131:8000/create_user/?format=invalid`

```
┌──(py311env)─(root㉿kali)-[/home/kali/pentest-agent/agents]
└─# curl http://192.168.153.131:8000/create_user/?format=invalid

<!DOCTYPE html>
<html lang="en">
<head>
  <meta http-equiv="content-type" content="text/html; charset=utf-8">
  <meta name="robots" content="NONE,NOARCHIVE">
  <title>MultiValueDictKeyError at /create_user/</title>
  <style type="text/css">
```

```
  <form action="http://dpaste.com/" name="pasteform" id="pasteform" method=

  <div id="pastebinTraceback" class="pastebin">
    <input type="hidden" name="language" value="PythonConsole">
    <input type="hidden" name="title"
      value="MultiValueDictKeyError at /create_user/">
    <input type="hidden" name="source" value="Django Dpaste Agent">
    <input type="hidden" name="poster" value="Django">
    <textarea name="content" id="traceback_area" cols="140" rows="25">
Environment:


Request Method: GET
Request URL: http://192.168.153.131:8000/create_user/?format=invalid

Django Version: 1.11.4
Python Version: 3.5.9
Installed Applications:
[&#39;xss&#39;]
Installed Middleware:
[&#39;django.middleware.common.CommonMiddleware&#39;,
 &#39;django.middleware.csrf.CsrfViewMiddleware&#39;]
```

- 捕获到更多的网页信息：得知Django具体的版本号1.11.4，该网页呈现：

Nikto——非侵入式Web服务器轻量漏洞扫描

```
┌──(py311env)-(root㉿kali)-[/home/kali/pentest-agent/agents]
└─# nikto -h http://192.168.153.131:8000/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.153.131
+ Target Hostname:    192.168.153.131
+ Target Port:        8000
+ Start Time:         2025-06-25 03:54:14 (GMT-4)
---------------------------------------------------------------------------
+ Server: WSGIServer/0.2 CPython/3.5.9
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/
Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerab
ilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2025-06-25 03:54:16 (GMT-4) (2 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- **敏感信息泄露**：后端技术栈Python WSGI + Python 3.5.0，可能存在已知漏洞，可针对性搜索该版本的公开漏洞CVE进行利用
- **缺少安全头配置**：
  - **X-Frame-Options**：控制网页是否允许被嵌入到 `<iframe>` 标签中，防止点击劫持(Clickjacking)攻击
  - **X-Content-Type-Options**：强制浏览器遵守服务器声明的 `Content-Type`，阻止 MIME 类型混淆攻击。缺失时，浏览器可能自动将文本/HTML 当作 JS/CSS 执行，导致**XSS**或数据泄露

Web技术识别——WhatWeb(Kali原生工具，代替Wappalyzer)

```
┌──(py311env)-(root㉿kali)-[/home/kali]
└─# whatweb http://192.168.153.131:8000
http://192.168.153.131:8000 [404 Not Found] Country[RESERVED][ZZ], Django, HTML5, HTTPSe
rver[WSGIServer/0.2 CPython/3.5.9], IP[192.168.153.131], Title[Page not found at /]
```

- **确定服务器环境**：WSGIServer (Python 3.5.9) + Django

漏洞精确匹配初步想法

- **扫描文本**：非侵入式扫描=>(主机漏洞描述=0.8、服务可能攻击面描述=0.4)、侵入式扫描=>(已验证攻击面=0.8、服务可能攻击面描述=0.4)
  1. 初步根据扫描文本中所有的攻击面，**语义匹配**所有搜索到的CVE文本，并提取**候选CVE集**
  2. 再根据漏洞描述赋予的相应权重对各CVE可能性进行**优先级评分与排序**