## Ollama 未授权访问漏洞（CNVD-2025-04094）研究报告

## 一、引言

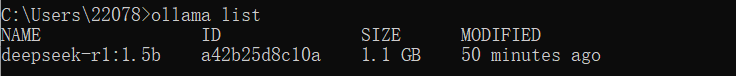
Ollama 作为开源的大语言模型运行环境和工具集，为开发者部署、管理和使用大语言模型提供便利。然而，2025年2月Ollama被监测发现存在未授权访问漏洞（CNVD-2025-04094），且在野利用。攻击者可借此执行恶意操作，对用户数据安全和服务稳定性构成严重威胁。

## 二、Ollama 简介

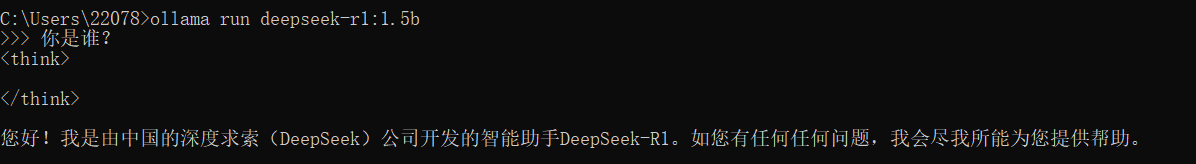
Ollama 用于本地私有化部署大语言模型（如DeepSeek等 ），具备简化部署、轻量级可扩展、API 支持和跨平台等特性，在AI领域应用广泛。它支持模型量化，降低显存要求，可在普通计算机上运行大语言模型，兼容 MacOS、Windows、Linux 及 Docker 容器。

Ollama应用示例（以本地运行Deepseek为例）

1. Ollama 拉取Deepseek模型



1. Ollama调用Deepseek模型，实现模型对话



## 三、漏洞详情

### （一）漏洞基本信息

* **漏洞类型**：未授权访问
* **漏洞等级**：高危
* **漏洞编号**：CNVD-2025-04094
* **影响版本**：Ollama 所有版本（未设置访问认证情况下 ）
* **利用方式**：远程

### （二）漏洞原理

Ollama 默认未设置身份验证和访问控制功能，且大部分开源大模型需部署在公网并开放外网访问。攻击者能够未授权访问服务默认端口 11434，调用敏感功能接口，执行恶意操作。

### **（三）漏洞危害**

* **数据泄露风险**：攻击者可获取已部署模型的相关信息，包括模型版本等。
* **服务滥用**：利用未授权访问，攻击者能够无限制地调用模型计算资源，进行大规模的文本生成、推理等操作，导致服务性能下降，影响正常用户的使用，甚至可能造成服务拒绝。
* **恶意篡改**：攻击者可以尝试上传恶意模型文件或修改现有模型的配置参数，使模型输出恶意或错误的内容，干扰正常的业务逻辑。
* **删除模型**：攻击者可以未授权删除已部署的模型，导致正常的模型业务中断。

## 四、漏洞检测

我们提供漏洞检测工具脚本，工具支持网段扫描。

工具下载链接如下：

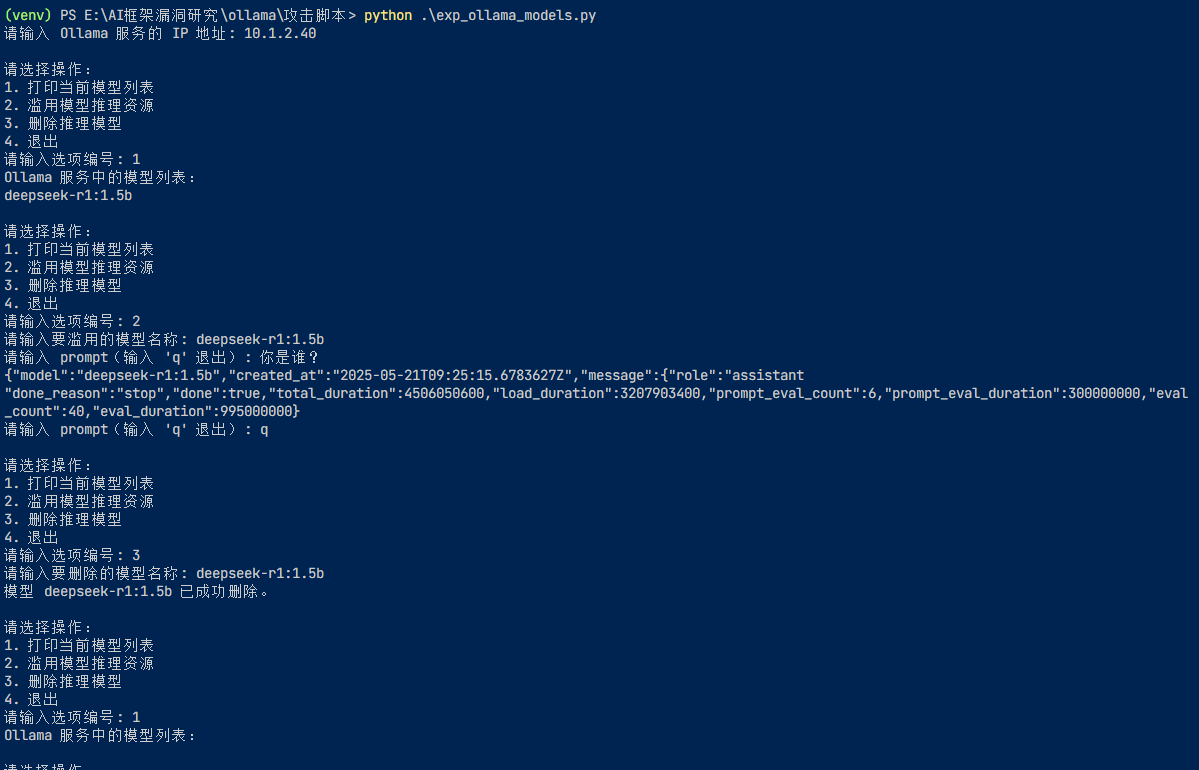
工具检测示例：



## 漏洞利用

我们研发交互式漏洞利用工具脚本，可用于攻击 Ollama 服务的未授权访问漏洞（CNVD-2025-04094）。该脚本提供了三种主要功能：打印当前模型列表、滥用模型推理资源和删除推理模型。

漏洞利用示例：



## 六、漏洞防护

请使用Ollama部署大模型的单位和用户立即采取以下措施进行漏洞修复：

1. 若Ollama只提供本地服务，设置环境变量:Environment="OLLAMA\_HOST=127.0.0.1"，仅允许本地访问。
2. 若Ollama需提供公网服务，选择以下方法添加认证机制：
3. 修改config.yaml、settings.json 配置文件，限定可访问Ollama 服务的IP地址；
4. 通过防火墙等设备配置IP白名单，阻止非授权IP的访问请求；
5. 通过反向代理进行身份验证和授权（如使用OAuth2.0协议），防止未经授权用户访问。