llama_Index SQL注入漏洞（CVE-2025-1750）POC及一键部署环境

漏洞背景

昨天晚上刷到了“微步在线研究响应中心”发布了了一则漏洞通告，通告了一个llama_Index SQL注入漏洞

> 漏洞通告 | llama_Index SQL注入漏洞
>
> 原创 微步情报局 微步在线研究响应中心 2025年06月03日 16:49 北京

漏洞简介显示漏洞**利用难度低**，造成伤害大，而且技术细节已经公开了，于是想花点时间来研究看看。

> **漏洞概况**
>
> llama_Index是一个用于构建基于数据的LLM驱动代理的领先框架。
>
> 微步情报局获取到llama_Index SQL注入漏洞（CVE-2025-1750）。该漏洞由于llama_Index的DuckDBVectorStore组件中的ref_doc_id参数直接执行攻击者传递的恶意SQL语句，导致任意文件读取和写入漏洞。
>
> 该漏洞利用难度低，且技术细节已公开，建议受影响用户尽快修复。

漏洞介绍

LlamaIndex（原名 GPT Index）是一个开源的数据框架，旨在帮助用户将本地或外部的数据（如文档、数据库、API 等）与大语言模型（LLM）高效集成。它提供了灵活的数据加载、索引构建和查询接口，使开发者可以快速构建基于 LLM 的问答系统、聊天机器人或语义搜索应用。LlamaIndex 常用于构建“私有知识库问答”场景，是 LangChain 等 LLM 应用生态中的重要组成部分。

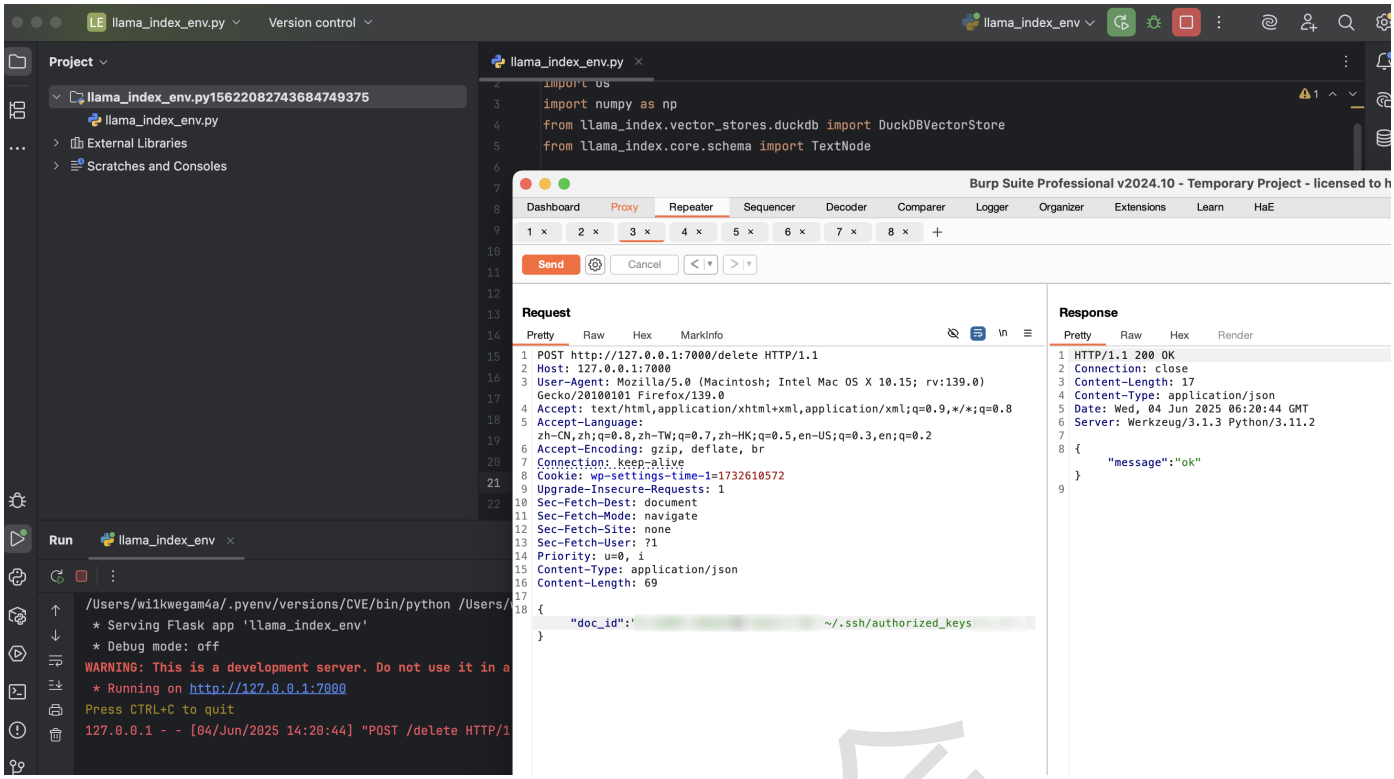
在 run-llama/llama_index v0.12.19 版本中的 `DuckDBVectorStore` 的删除功能存在 SQL 注入漏洞。该漏洞允许攻击者操纵 `ref_doc_id` 参数，从而能够读取和写入服务器上的任意文件，可能导致远程代码执行（RCE）。

漏洞版本

- Llama_index <= 0.12.20
- llama-index-vector-stores-duckdb <= 0.3.0

漏洞利用

首先使用Python开启一个简单的引用了`DuckDBVectorStore库`的web服务器，接着利用如下脚本向`~/.ssh/authorized_keys`写入内容



发现成功写入`~/.ssh/authorized_keys`

```
a1batr0ss@MacBookAir ~ % ls ~/.ssh
id_rsa          id_rsa.pub      id_rsa01.pub    known_hosts     known_hosts.old
a1batr0ss@MacBookAir ~ % ls ~/.ssh
authorized_keys id_rsa.pub      known_hosts
id_rsa          id_rsa01.pub    known_hosts.old
```

漏洞修复

这个更新到**Llama_index >= 0.12.21**的版本即可，官方使用了参数化查询机制来避免SQL注入

```
@@ -321,25 +318,26 @@ def delete(self, ref_doc_id: str, **delete_kwargs: Any) -> None:
+        """
         _ddb_query = f"""
             DELETE FROM {self.table_name}
-            WHERE json_extract_string(metadata_, '$.ref_doc_id') = '{ref_doc_id}';
+            WHERE json_extract_string(metadata_, '$.ref_doc_id') = ?;
             """
         if self.database_name == ":memory:":
-            self._conn.execute(_ddb_query)
-        else:
+            self._conn.execute(_ddb_query, [ref_doc_id])
```