API接口深度发现的动态爬虫实现(2. 测试报告)

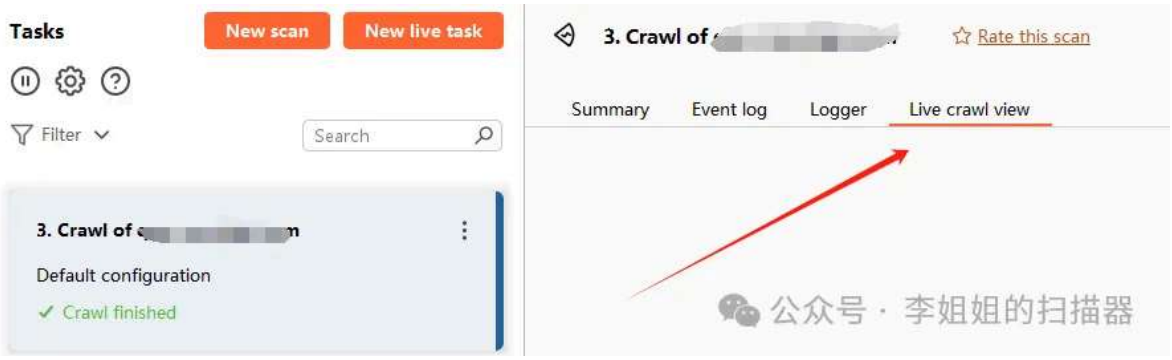
原创 扫到漏洞的 李姐姐的扫描器 2025年05月01日 13:30 北京

Burp测试结果

上一篇中，因Burp不支持配置交互登录，笔者在本地启动一个代理，注入cookie，写入local storage，最终使用该代理完成多个工具的对照测试（**测试环境一致：均在代理环境完成**）。

Burp表现效果不佳，简单web应用爬取超过1个小时。通过Live Crawl View检查其爬取过程，发现Burp在导航页之间反复跳转和交互，产生了大量无效请求，但并没成功抓到接口。

如下图所示，在Burp抓取过程，用户可检视浏览器交互动作：



Katana v1.1.3测试结果

昨天留言中有朋友提到katana，立即下载进行了测试。开启-headless 开关，代理中能看到8个不重复的接口请求。但诡异的现象是，记录中未包含任何API接口。静态文件倒是都给出来了，高价值的API均被丢弃。

API发现测试结果

多个扫描器类型爬虫工具，测试站点扫描效果如下

工具名称	发现接口	主要缺陷
CrawlerGo 0.4.4	11	■ 填表规则简单，偶尔填充失败 ■ 路由拦截有失效情况，页面跳出 ■ 无效URL太多，因打包工具引入
Rad 1.0	6	■ 效率高，但结果不够稳定，丢API ■ 和katana一样引入的leakless，长亭的会报毒
BurpSuite Professional 2025.1.4	5	■ 爬虫不支持交互登录和简单维持身份 ■ 爬取陷入无效交互， ■ 效率低，小型应用超过1个小时
AWVS 24.8	9	
Katana v1.1.3	0	■ 代理能看到8个接口正常请求，但输出结果为0

未公开API扫描工具	59	

可以初步得出结论，大部分扫描器未对API接口的发现做专门优化，错过了发现API接口漏洞的机会。

接下来的文章中，我将继续介绍API发现工具的优化细节。