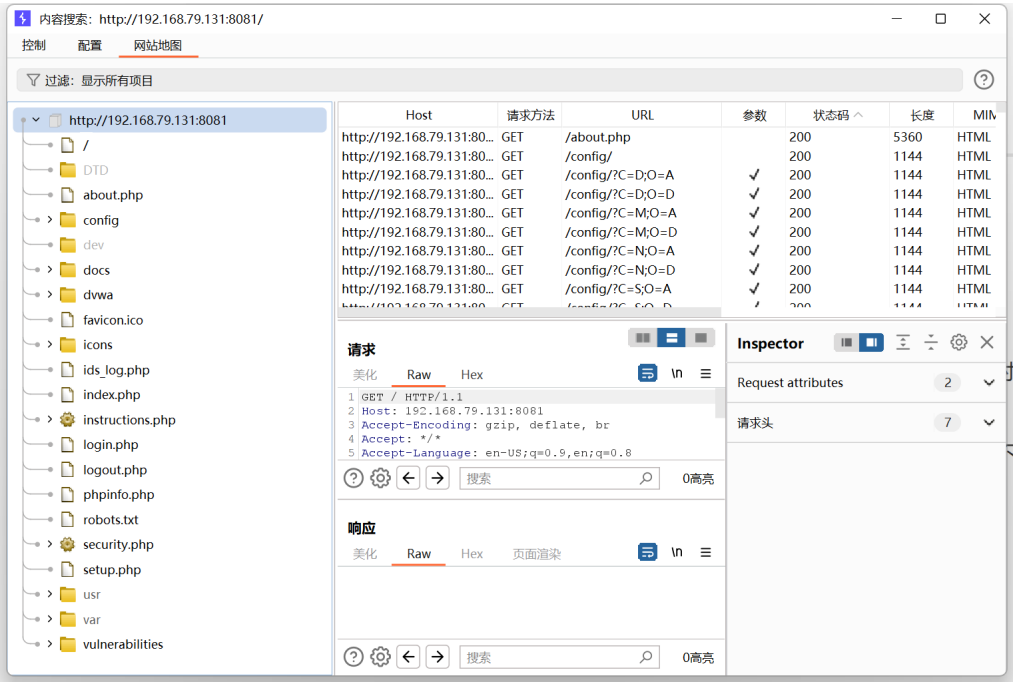
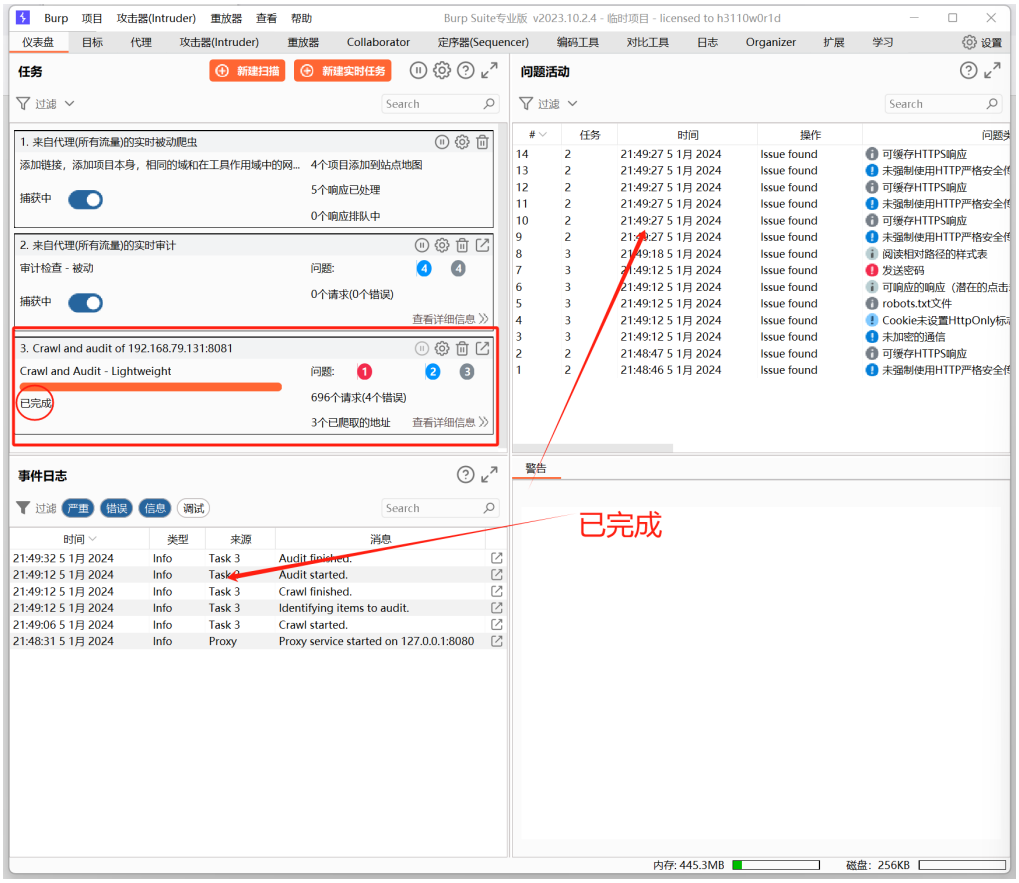
1. 使用 Burp 的 Discover Content 功能爬取任意站点的目录，给出爬取过程的说明文档、站点树截图； burp端口需要打开；DWVS打开；Burp自动爬取站点的目录，可以在设置中设置颗粒度和范围，Discover Content一下会更精细的爬取这个站点的目录，左侧即为站点地图。配置默认即可，记得勾选在找到的文件上测试这些扩展名



2. 分别使用 Burp Scan 的主动扫描和被动扫描功能对 DVWA 站点进行扫描，输出扫描报告；



3. Burp Intruder 爆破题目

靶场地址： http://121.196.62.22:8082/vulnerabilities/brute/

靶场开放时间：2023.9.9 ~ 2023.9.24

管理员账号 / 密码：admin/password

注意事项：爆破成功的同学请勿修改任何账号的密码，以免影响其他同学正常作业。

- 老李今年 52 岁了，他最近也在学习网络安全，为了方便练习，他在 DVWA 靶场中增设了一个自己的账号，密码就是他的生日，请你想办法破解出他的账号密码。
- **laoli 19710728**
- Cookie 老师在 DVWA 靶场中设置了一个账号 Geektime（注意首字母大写），且在靶场中的某处存放了一个文件名为 geekbang.txt 的密码字典，请你想办法找到该字典并尝试爆破，最终获取到账号 Geektime 的正确密码。

- **geektime666**

四、在不依赖于 DVWA 后端数据库的情况，如何通过前端验证的方法判断 DVWA 中的注入点是数字型注入还是字符型注入？（提示：用假设法进行逻辑判断）

假设可以通过输入一系列数字和字符混合的测试数据，并**观察输出结果的长度。**如果注入点的输出长度在数字型数据和字符型数据输入时有明显的不同，那么可以推断注入点是数字型注入还是字符型注入；

逻辑判断

输入 1and 1=1 查询有两种情况

数字型注入能查询到结果 网站本身不对用户的输入做任何处理:能查询到结果 网站本身对用户的输入做了处理: 有隐式转换，还是能查到

查询不到结果那就是字符型注入

输入1 and 1=2 网站本身不对用户的输入做任何处理那就查询不到

如果网站本身对用户的输入做了处理: 会有隐式转换，还是能查到结果