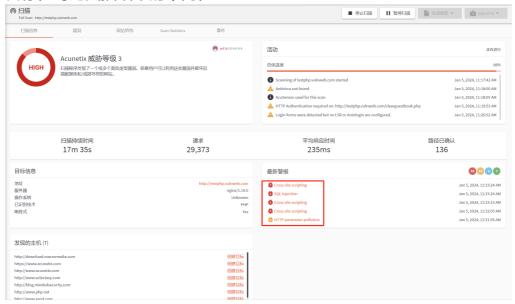
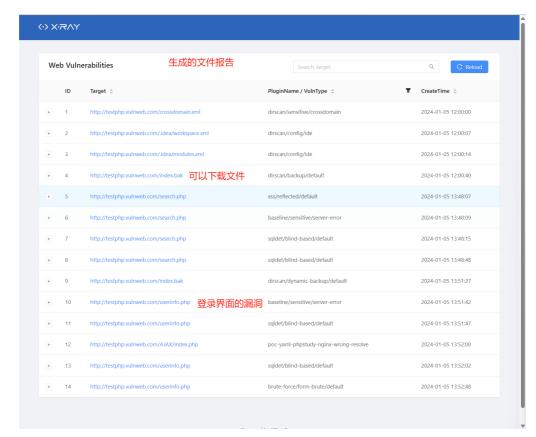
1. 分别使用 AWVS 和 Xray (被动扫描模式) 去扫描任一 SRC 允许测试的目标,对比扫描结果的不同; AWVS



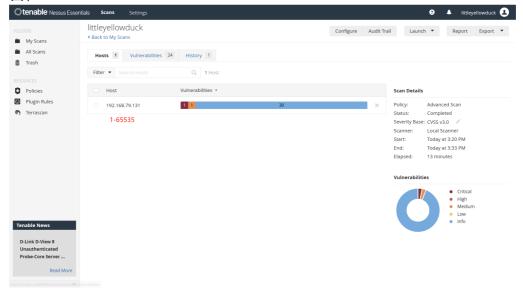
## **Xray**

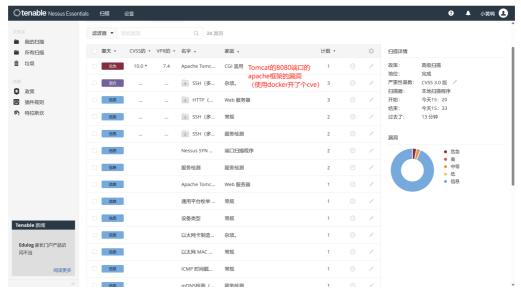
```
[INFO] 2024-01-05 11:59:33 script poc-yaml-gurock-testrail-cve-2021-40875-info-leak run payload req02
[INFO] 2024-01-05 11:59:33 script poc-yaml-bitbucket-unauth run payload path02
[INFO] 2024-01-05 11:59:34 script poc-yaml-bitbucket-unauth run payload path02
[INFO] 2024-01-05 11:59:34 script poc-yaml-bitbucket-unauth run payload path03
[INFO] 2024-01-05 11:59:34 script poc-yaml-bitbucket-unauth run payload path04
[INFO] 2024-01-05 11:59:35 script poc-yaml-bitbucket-unauth run payload path05
[INFO] 2024-01-05 11:59:35 script poc-yaml-bitbucket-unauth run payload path06
[INFO] 2024-01-05 11:59:35 script poc-yaml-bitbucket-unauth run payload path06
[INFO] 2024-01-05 11:59:36 script poc-yaml-bitbucket-unauth run payload path06
[INFO] 2024-01-05 11:59:37 script poc-yaml-bitbucket-unauth run payload path07
[INFO] 2024-01-05 11:59:37 script poc-yaml-bitbucket-unauth run payload path08
[INFO] 2024-01-05 11:59:37 script poc-yaml-adobe-experience-manager-cve-2019-8086-xxe run payload win
[INFO] 2024-01-05 11:59:37 script poc-yaml-adobe-experience-manager-cve-2019-8086-xxe run payload win
[INFO] 2024-01-05 11:59:37 script poc-yaml-adobe-experience-manager-cve-2019-8086-xxe run payload win
[INFO] 2024-01-05 11:59:38 script poc-yaml-adobe-experience-manager-cve-2019-8086-xxe run payload win
[INFO] 2024-01-05 11:59:38 script poc-yaml-adobe-experience-manager-cve-2017-1512-1fi run payload req02
[INFO] 2024-01-05 11:59:38 script poc-yaml-aplpi-telemetry-cve-2021-39211-info-leak run payload req02
[INFO] 2024-01-05 11:59:38 script poc-yaml-managengine-servicedesk-cve-2017-1512-1fi run payload req02
[INFO] 2024-01-05 11:59:38 script poc-yaml-managengine-servicedesk-cve-2017-1512-1fi run payload linux
[*] scanned: 1, pending: 1, requestSent: 2809, latency: 571.76ns, failedRatio: 0.00%
[*] scanned: 1, pending: 1, requestSent: 2821, latency: 578.58ns, failedRatio: 0.00%
[*] scanned: 1, pending: 2, requestSent: 2875, latency: 566.45ns, failedRatio: 0.00%
[*] scanned: 1, pending: 2, requestSent: 2875, latency: 566.45ns, failedRatio:
```



不同:被动扫描相对比比较麻烦,而且扫出来的漏洞较少(因为要模拟用户点击),报告相对简洁,一般只有rul、payload、请求头、响应头,但是命令行执行相对自由;主动扫描相对成熟,图形化界面,AWVS功能较全面

2. 使用 Nessus 扫描任一主机,要求使用全端口扫描,提供主机扫描报告;



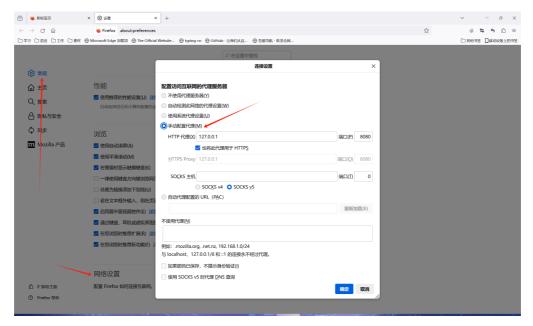


主机扫描报告在第五周作业文件夹

3. 安装 Burp,分别在本机上**实现全局代理和局部代理**,提供设置过程的说明文档;全局代理



设置→网路和Internet→代理→开启编辑代理服务器和设置IP地址 局部代理



火狐浏览器:设置-->网路设置-->手动代理设置-->127.0.0.1:8080

4. 利用 Burp 实现对 HTTPS 站点的抓包。

