基于 WEB 应用扫描测试

被动式扫描 x-ray

https://xray.cool/xray/#/tutorial/introduce

Github: https://github.com/chaitin/xray/releases （国外速度快）
网盘: https://yunpan.360.cn/surl_y3Gu6cugi8u （国内速度快）

主动式扫描 awvs netsparker appscan

注意验证后扫描

无验证码：模拟登陆

有验证码：带入 cookie

基于操作系统扫描测试

Nessus

Openvas

Goby

基于 NMAP 使用扫描测试

https://blog.csdn.net/qq_29277155/article/details/50977143

其他安全漏洞扫描补充

未授权访问

中间件安全

逻辑越权问题

Commented [t1]: 注：当使用 burpsuite 来抓模拟器的 app 报文时，抓到数据包里的网址，用浏览器访问时，可能会出现某些问题，这时可以参考正确的报文（可以在浏览器的 network 里查看正确的报文结构）进行修改。当我们使用 burpsuite 抓到 app 的地址时，使用 awvs 来进行扫描，要用到自定义扫描，添加信息（可能是头部，类似于上面需要构造正确的报文才能进行访问），才能进行正确扫描

更多安全扫描见：https://www.uedbox.com/tools/type/scanner/

注意：部分漏洞（越权）利用工具无法探针，只能手工