1. 本次实验以web安全工具的使用为主，主要是WebSiteSniffer，用于记录和主机进行通信的文件（好比键盘钩子之于键盘输入）；DirBuster，用于站点资源扫描，针对未知站点可以嗅探其旗下资源。
2. DirBuster的使用需要注意：同时的多线程访问请求会占用目标站点大量的资源，若对服务器中的服务器进行扫描，则可能造成堵塞。注意：对他人的主机进行扫描是违法行为。
3. 一项任务要求使用DirBuster扫描DVWA来获取配置界面，考虑到DirBuster是使用字典进行，若想针对某个站点进行扫描则需要对字典进行相应的修改。
4. 一项任务中要求结合DirBuster确定网站的后端开发技术，课上讲解了查看后缀和查看源码的方法；但这种方法具有其局限性：现在众多网站的后端采用node.js等前后端一体框架，很难从源码直接确定开发使用的技术，也很难从使用的api上看出具体语言。









