0. 建议在 Linux 环境下完成实验（推荐顺序是 Fedora>Ubuntu>其他 Linux 发行版>Kali or BT )。windows 下如果能搞定配置也是可以接受的。

1. 在实验 1（SQL 注入）的环境中，前置 apache 或者 nginx。

2. 安装并配置 ModSecurity 模块，搭建 WAF。

3. 根据文档自行编写，或者在 OWASP ModSecurity CRS 规则库的基础上修改，对 SQL 注入攻击进行阻断并报警。

4. 尝试对特定扫描器或发包工具（paros、w3af 等）的 User-Agent 进行检测和报警，并在单个 IP 访问数量超过一定门限后对来源 IP 进行封禁。

5. 提交过程文档、配置文件和相关的告警日志。