

## 项目课

### 选择 1：模糊测试项目

1. 对现有的模糊测试工具（AFL、libfuzzer）进行安装，并进行软件漏洞挖掘实现；
2. 分析 AFL 现有的源码，找到目前的漏洞挖掘工具存在的缺陷，改进现有的工具，提高漏洞挖掘；
3. 大家可以从 google 学术上，寻找相关的论文，找到现有工具的缺陷；
4. 实现历史 CVE 的挖掘。

### 选择 2：测试用例搜索项目

1. 对该源码进行安装和测试（找我要源码），分析现有方法如何搜索测试用例的。
2. 分析该方法存在的问题。
3. 从测试用例生成的角度触发，提出一种方法，对该工具进行改进，使其更快的找到程序路径。
4. 该项目主要分析现有代码，发现其中的缺陷，并进行改进，实现测试用例的快速搜索。

### 选择 3：AI 安全项目

随着 AIGC 技术的快速发展，AI 生成内容的质量不断提升，但同时也对内容安全带来了新的挑战。虚假信息的泛滥和深度伪造技术的滥用，导致网络谣言和诈骗问题日益严重，提出切实可行的解决方案，以应对这些挑战。

#### 生活娱乐：

智能家庭安全系统：AI 摄像头结合面部识别技术，不仅能实时监控家庭安全，还能根据家庭成员的个性化需求，如外出模式或睡眠模式，自动调整安全设置。

娱乐内容过滤：AI 内容过滤系统利用先进的图像识别和自然语言处理技术，在用户观看视频或玩游戏时，自动识别并过滤掉不适宜的内容。

#### 智能办公：

AI 安全助手：在企业网络中，AI 助手能够学习员工的正常工作行为，及时发现并阻止潜在的网络攻击，保护企业信息安全。

会议内容保密：AI 系统可以对办公会议进行加密记录，并通过访问控制确保只有授权人员能够访问会议内容，防止信息泄露。

**选择 4：**开发一个恶意软件检测程序，保护用户免收病毒的侵害。

**选择 5：**开发自动化漏洞识别与利用工具，至少能够自动识别 5 种类型漏洞。

#### 项目要求：

（1）由于有密码课设，所以该课程的相关项目不能采用之前涉及的密码相关技术，作为该项目的主要内容。

（2）提交内容：代码、项目报告、安装教程

（3）该项目分为 6 人一组，每个人必须参与，并报告中体现工作量。