# 大作业题目

**1、题目范畴**

类目1：堆溢出漏洞调试（CVE漏洞为例） 难度：A

类目2：逆向分析与软件破解 难度：C

类目3：web漏洞挖掘或分析 难度：B

类目4：模糊测试工具使用过程分析 难度：A

类目5：面向源码的漏洞扫描工具使用过程分析 难度：B

类目6：android APP的漏洞调试 难度：A

上述题目不限平台，每位同学从6类题中任选一类，**独立**完成实验和大作业报告。**报告重复情况（如效果图重复），两位同学得分均为70以下**。所有分析过程必须包含至少一个实例（如使用源码扫描工具扫描某开源软件）。难度等级从A到C递减，等级越高难度权重越大。

建议参考书目

[1]诸葛建伟等. Metasploit渗透测试魔鬼训练营. 机械工业出版社,2013  
[2]王清. 0day安全：软件漏洞分析技术.电子工业出版社，2011

[3]钱林松，赵海旭. C++反汇编与逆向分析技术揭秘. 机械工业出版社，2011

[4]爱甲健二. 有趣的二进制 软件安全与逆向分析. 人民邮电出版社，2015

[5][邱鹏](http://search.dangdang.com/?key2=%C7%F1%C5%F4&medium=01&category_path=01.00.00.00.00.00)，[陈吉](http://search.dangdang.com/?key2=%B3%C2%BC%AA&medium=01&category_path=01.00.00.00.00.00)，[潘晓明](http://search.dangdang.com/?key2=%C5%CB%CF%FE%C3%F7&medium=01&category_path=01.00.00.00.00.00).移动App测试实战：顶级互联网企业软件测试和质量提升最佳实践. [机械工业出版社](http://search.dangdang.com/?key3=%BB%FA%D0%B5%B9%A4%D2%B5%B3%F6%B0%E6%C9%E7&medium=01&category_path=01.00.00.00.00.00),2015

# B0303051C 安全编程技术

# 评分标准

根据准备情况、功能完成情况、报告撰写情况、验收答辩情况等综合打分，具体如下：

|  |  |  |
| --- | --- | --- |
| **评分内容** | **具 体 要 求** | **比例** |
| **准备情况** | 能独立查阅文献资料及从事其他形式的调研，能较好地理解任务并提出实施方案，有分析整理各类信息并从中获取新知识的能力。 | 10% |
| **功能完成情况** | 论证、分析、设计、实现、实验正确合理。 | 50% |
| **报告撰写质量** | 结构严谨，文字通顺，用语符合技术规范，图表清楚，书写格式规范，符合规定字数要求。 | 20% |
| **答辩** | 内容全面，紧扣课题，突出重点，语言简练准确，演示过程顺利。 | 20% |

大作业占期末成绩的60%，根据：

1. 选题的难度、工作量、完成情况
2. 大作业报告撰写的详实程度和格式
3. 验收答辩情况

综合打分。

要注意大作业的原创性，避免雷同。优秀率不超过25%。