|  |
| --- |
| 哈尔滨工业大学(深圳) |
| **《网络与系统安全》 实验报告** |
|  |
| 实验二  SQL注入 实验  学 院:   |  |  | | --- | --- | | 姓 名: |  | | 学 号: |  | | 专 业: |  | | 日 期: | 2024年4月 | |

# 一、实验过程

每个实验步骤（共9个小任务（任务1.1、1.2，任务2.1、2.2、2.3，任务3.1、3.2、3.3，任务4））要求有具体截图和分析说明。

**\*\*任务1.1\*\*** 运行上述命令后，需要使用SQL命令打印员工Alice的所有概要信息。请提供你的结果截图。

**\*\*任务1.2\*\*** 运行上述命令后，可以将credential中的所有信息dump下来。请提供你的结果截图，并根据第一条命令找出可以注入的信息点。

**\*\*任务2.1\*\***:网页SQL注入攻击。利用Admin账户，可以尝试使用其他账户。

**\*\*任务2.2\*\***:命令行SQL注入攻击。利用crul命令进行攻击

**\*\*任务2.3\*\***:追加一条新的SQL语句。请尝试通过登录页面运行两条SQL语句,并说明是否能够获取到信息。

**\*\*任务3.1\*\***:修改自己的工资。

**\*\*任务3.2\*\***:修改其他人的工资。

**\*\*任务3.3\*\***:修改他人密码。

**\*\*任务4\*\***：在这个任务中，我们将使用预处理语句机制来修复SQL注入漏洞。

如果你在任务4中还完善了其他代码，请一并说明。

有余力的同学可以完善下unsafe\_home.php、unsafe\_edit\_frontend.php和unsafe\_edit\_backend.php代码文件，把相关的漏洞修复。

# 二、遇到问题及解决方法

# 三、对本次实验的建议