第三周：数据库系统表相关学习

1、如何利用数据库的功能读写文件，需要什么样的条件才可以读写

2、学习数据库系统表的功能，如何利用 sql 语句查询库名、表名、字段名、内容以及当前用户等基本信息，将学习过程中关键部分整理成报告

扩展学习：尝试查询出用户的 hash，并使用 hashcat 来对获取的 hash 进行暴力破解

部分解释

1、对于关系型数据库，都会提供文件读写的功能，但是具体如何实现略有不同，文件读写在我们利用数据库注入漏洞获取 webshell 的时候非常有帮助，所以读写文件的基础是必须要学的。

2、任何关系型数据库，在默认安装成功之后会自带一些默认的系统库和表，这些库和表存储了数据库中很多关键的信息，比如用户创建的库相关信息、表相关信息、用户相关信息、权限相关信息、安装配置相关信息等，在我们利用注入漏洞获取更多信息和权限的过程中有很大的帮助，所以熟悉数据库默认的系统库和表也是很必要的。

3、对于关系型数据库，为了安全都会存在用户和密码，但是密码是经过哈希之后存储在系统表中的，当我们通过注入获取数据库的账号和哈希之后，想要知道哈希之前的明文信息，需要进行暴力破解操作，对于跑哈希来说，hashcat 可以利用 GPU 快速破解哈希，支持非常多的哈希格式，在未来的红蓝对抗中帮助很大。