实验报告

一、实验内容

内容 1　实验平台搭建

设计并开发一个简单的 web 应用作为实验平台。例如，无人机集群数据采集管理系统、文档在线管理系统、智慧家庭设备管理系统、智慧医疗数据监控和告警系统、多用户图片水印管理系统、区块链金融管理系统等等。该应用需要有简单且必要的页面，除了实现核心业务特性外，还需要包含用户管理模块（包括用户注册/删除、用户登录/登出、用户信息维护、用户操作记录等特性）作为最基本的支撑模块并实现会话管理机制。

内容 2　平台功能要求

该 web 应用能够部署在本地（localhost）或者服务器（有条件的话）正常运行，同时可以使用 chrome/火狐/edge 浏览器通过本机或者局域网主机进行网站页面浏览，并完成用户登录、用户管理及核心业务的运行和操作。另外，该 web 应用的访问协议需要支持 http 和 https 两种协议。该 web 应用系统的源码需要在 github 或者 gitee 等代码管理平台进行托管和发布。

内容 3　平台技术选型

（1）web 前端，使用当前流行的 JS 框架等技术进行开发；
（2）web 后端，使用 Spring MVC/SpringBoot 等 Java 框架、Python 框架以及 Nodejs、PHP 以及 Go 等语言及其框架进行业务逻辑开发；
（3）web 服务器，使用诸如 Nginx/IIS/Apache/Lighttpd 等常用 Web 服务器以及 Weblogic/Tomcat/Jboss 等常见应用服务器进行部署，或者直接使用包含 web 服务器功能的框架；
（4）数据库软件，推荐使用 Mysql、PGSQL、Oracle、sqlserver、MongoDB 等；
（5）数据持久化框架（MyBatis、Hibernate、JDBCTemplate 等）；
（6）其他技术，例如 redis 内存数据库、消息中间件（Kafka、RocketMQ 等）；
（7）操作系统平台，尽量选择 linux，当然 windows 也可以作为部署系统使用。

内容 4　web 漏洞实验

（1）SQL 注入实验

SQL 注入是 web 应用所面临的的最广泛的一种攻击手段，请构造一个 SQL 注入漏洞，同时展示 SQL 注入漏洞利用和如何防范该 SQL 注入，并给出采用防御措施前后的对比。

（2）命令注入实验

类似于 SQL 注入实验，构造一个简单的命令注入漏洞并给出防御手段和相关的对比。

（3）XSS 实验

a. 构造一个简单的反射型 XSS

b. 构造一个简单的存储型 XSS，例如，当增加用户时，设置用户描述时，允许用户从页面输入 XSS 注入代码，观察当这段代码存入数据库，并且在查询该用户信息时的现象

c. 构造 XSS 蠕虫。XSS 蠕虫是指一种具有自我传播能力的 XSS 攻击，杀伤力很大。其最大的危害在于可能在一个系统中的用户间互相感染，以致整个系统的用户沦陷。请构造一个简单的 XSS 蠕虫攻击。

（4）CSRF 实验

使用一个典型场景，例如课堂上展示的例子中的银行场景，模拟一次简单的 CSRF 攻击，并实现防御机制。

内容 5　web 安全测试实验

（1）部署和运行 web 应用后，使用浏览器自带调试工具进行接口 request 和 response 抓取和数据分析，并且通过部署 burpsuite、tcpdump、sniffer、wireshark 等工具进行抓包，对比分析 http 和 https 协议。

（2）部署渗透测试工具（nessus/matasploit 等）和模糊测试工具对所开发 web 应用进行测试，并给出测试结果说明。

二、实验报告

1、输出一个实验报告，报告分四部分：封面、产品描述、实验详情、结尾。

- 封面：需要包含报告名称和小组成员信息。
- 产品描述：完成内容 1、内容 2 和内容 3，对所开发搭建的 web 应用系统所采用的开发技术、用户会话管理技术、部署方法、业务功能和每种功能的使用方法图解以及接口设计（包括接口功能描述、uri、入口参数和输出参数）进行描述。
- 实验详情：完成内容 4 和内容 5，对每个小实验的内容，目标，步骤，过程，结果等进行详细描述。
- 结尾：需要展示每位小组成员的分工和贡献（例如应用设计、前端开发、后端开发、美工设计、uri 接口整理、安全测试、漏洞攻防等），并给出产品源码所在的 github 或者 gitee 链接。