上海电力大学信息安全专业中本贯通

理论基础《Web 应用安全》考试大纲

一、考核目的

基于中本贯通教育考试指导意见，本次考试旨在考核学生是否达到了升入本科继续学习的要求。本课程是以 Web 应用前端编程（HTML 语言、CSS 和 JavaScript 语言）、Web 应用后端编程（以 PHP 语言为例）为基础，要求学生熟悉 HTTP 协议基本原理，能熟练分析 HTTP 协议通信数据，理解 Web 前端、Web 服务器端、HTTP 协议、业务逻辑相关的安全问题。测试考生在理解基本原理的基础上，对于 Web 应用安全渗透、Web 应用安全防护、Web 应用安全运维等方面是否满足本科阶段的学习要求。

二、参考教材

1.《HTML5+CSS3 网页设计与制作案例教程》姬莉霞 清华大学出版社 2020 年 06 月
2.《PHP 从入门到精通》明日科技 清华大学出版社 2022 年 03 月
3.《Web 应用安全与防护 》朱添田 电子工业出版社 2022 年 04 月
4.《Web 安全漏洞原理及实战》田贵辉 人民邮电出版社 2020 年 09 月

三、考试内容及要求

1、 Web 应用安全前端基础

- 掌握HTML语言的基本核心元素
- 理解URL
- 掌握CSS的基本元素
- 熟悉JavaScript语言编程
- 理解浏览器的基本原理
- 理解开发者工具

2、 Web 服务器原理及编程

- 理解Web服务器的工作原理
- 掌握PHP语言基础
- 掌握PHP中文件和目录操作
- 掌握PHP中的数组及应用
- 熟悉PHP中的字符串和正则表达式
- 熟悉PHP中的代码重用和函数
- 熟悉PHP+MySQL编程

3、 HTTP 协议

- 理解HTTP协议的基本原理
- 熟悉HTTP协议的报文格式
- 掌握HTTP协议的会话机制

4、 SQL 注入漏洞原理与防护

- 理解SQL注入的基本原理
- 掌握SQL注入的一般利用方式
- 熟悉SQL注入漏洞探测的一般方法
- 熟悉SQL注入漏洞防护方法

5、 跨站脚本 XSS 攻击原理与防护

- 理解同源策略的基本原理和规则
- 理解XSS的基本原理
- 熟悉XSS的常见利用方式
- 了解XSS的常见类型
- 熟悉XSS的预防方法

6、 文件操作类漏洞原理与防护

- 理解文件上传原理和漏洞形式
- 理解文件下载原理和漏洞形式
- 理解文件包含漏洞的基本原理

7、 命令注入和 XXE 漏洞原理与防护

- 熟悉PHP语言中的命令执行
- 理解命令执行漏洞原理与防护方法
- 了解XML的基本规范
- 掌握XXE漏洞的基本原理和利用方法

8、 代码审计与漏洞扫描

- 了解漏洞的本质属性
- 理解漏洞发现的一般过程
- 理解Web应用的基本形态
- 理解代码审计的一般原理

- 理解污点分析的基本原理
- 理解漏洞扫描的一般原理和典型工具的使用

四、考试形式、题型和分值

1、 考试形式： 闭卷笔试， 考试限定用时为 120 分钟。

2、 题型和分值： 选择题、判断题、填空题、简答题、综合题， 满分为 150 分。