CWASP认证体系介绍

# CWASP认证体系简介

CWASP，认证Web应用安全专家（Certified Web Application Security Professional）,是一个专注于培养Web安全人才的培训认证体系，同时也是业界首个理论与实践相结合的培训认证体系。CWASP培训认证体系由来自与微软、诺基亚、华为、惠普、互联网安全研究中心等领域的安全专家，根据所在行业的安全经验，结合OWASP最佳安全实践，以S-SDLC为主线设计开发的。

CWASP认证体系全面覆盖了应用安全技术的七大领域，可以帮助安全从业人员从流程、技术、方法上端到端理解和掌握应用安全技术。学员在学习的过程中，可实际操作大量的Web安全实验，更加充分的了解和理解Web应用安全知识。

## CWASP认证说明

|  |  |  |  |
| --- | --- | --- | --- |
| 级别 | 说明 | 具备能力 | 学习方向 |
| CWASP L1 – Foundation | **基础级，应用安全的积极参与者。** | 了解并掌握基于OWASP top 10的应用安全相关技术。 | 应用安全威胁技术及实验 |
| CWASP L2 – Expert （三年相关从业经验） | **专家级，应用安全技术的推动者。** | 深入了解应用安全全生命周期技术、管理方法，并具备综合安全实践能力。 | 应用安全威胁安全架构设计安全运维S-SDLC暨威胁建模安全开发渗透测试安全测试 |
| CWASP L3 – Master | 大师级, 业界认可的，CWASP技术在特定领域的践行者。 | 创新性的将CWASP技术领域与行业业务领域相结合，促进行业应用安全领域的发展，形成基于行业的应用安全流程、技术、方法。 |

## CWASP L2 – Expert课程大纲

|  |  |  |
| --- | --- | --- |
| 培训类别 | 培训主题 | 培训内容 |
| 应用安全威胁 | 行业案例剖析 | 从各行业安全案例剖析，全面理解安全风险点 |
| 业务安全风险剖析 | 全面剖析业务系统涉及的安全风险 |
| OWASP TOP 10介绍 | 全面介绍OWASP TOP的技术原理、检测方式、防护手段；A1-注入A2-跨站脚本A3-失效的身份认证和会话管理 A4-不安全的直接对象引用 A5-跨站请求伪造 A6-安全配置错误A7-不安全的加密存储A8-没有限制的URL访问 A9-传输层保护不足 A10-未验证的重定向和转发 其他 |
| 安全流程 | S-SDLC过程 | 安全软件开发生命周期及威胁建模涉及过程包括：培训和意识需求设计编码测试部署、维护及响应 |
| 安全架构设计 | 业务层架构安全设计 |  |
| 软件层架构安全设计 |  |
| 应用层架构安全设计 |  |
| 安全开发 | 最佳安全开发实践 | 身份验证的开发实践安全提示问题的开发实践加密的开发实践忘记密码的开发实践密码存储的开发实践避免点击劫持的开发实践HTML5安全开发实践输入验证的开发实践安全日志的开发实践OWASP Top 10开发实践Pinning的开发实践未验证的重定向和转发的开发实践会话管理的开发实践传输层保护的开发实践用户隐私的开发实践Web服务安全的开发实践避免SQL注入式攻击的开发实践避免XSS攻击的开发实践避免DOM XSS攻击的开发实践 避免CSRF攻击的开发实践 攻击面分析开发实践 |
| 代码审核 | 熟悉各类代码审核工具解读代码审核报告 |
| 安全测试渗透测试 | 信息收集 | 测试：蜘蛛，机器人和爬虫搜索引擎发现/侦查应用入口识别WEB 应用指纹测试 应用发现错误代码分析 |
| 配置管理测试 | SSL/TLS 测试数据库监听测试基础结构配置管理测试应用配置管理测试文件扩展名处理测试过时的、用于备份的以及未被引用的文件基础结构和应用管理界面HTTP 方法和XST 测试 |
| 认证测试 | 加密信道证书传输用户枚举测试默认或可猜解(遍历)用户帐户暴力破解测试认证模式绕过测试记住密码和密码重置弱点测试注销和浏览器缓存管理测试CAPTCHA 测试多因素认证测试竞争条件测试 |
| 会话管理测试 | 会话管理模式测试COOKIES 属性测试会话固定测试会话变量泄漏测试CSRF 测试 |
| 授权测试 | 路径遍历测试绕过授权模式测试提权测试 |
| 业务逻辑测试 |  |
| 数据验证测试 | 反射式跨站脚本测试存储式跨站脚本测试基于DOM 的跨站脚本检测FLASH 跨站脚本测试SQL注入LDAP 注入ORM 注入XML 注入SSI 注入XPATH 注入IMAP/SMTP 注入代码注入OS 指令执行缓冲区溢出检测潜伏式漏洞检测HTTP SPLITTING/SMUGGLING 测试 |
| 阻断服务测试 | SQL 通配符攻击测试锁定用户账户缓冲区溢出用户指定型对象分配将用户输入作为循环计数器 将用户写入的数据写到磁盘 释放资源失败存储过多会话数据 |
| Web服务测试 | WS 信息收WSDL 测试 XML 结构测试XML 内容级别测试HTTPGET 参数/REST 测试SOAP 附件测试重现攻击测试 |
| AJAX测试 | AJAX 漏洞检测AJAX |
| 浏览器插件测试 | ActiveX Java Applet |
| 安全测试方法论 | 安全测试原理测试技术解释人工检查及复查软件威胁建模代码复查渗透测试方法平衡的需求 |
| 安全需求测试推导 | 功能性安全需求安全需求在使用和误用中的衍生开发者与测试者的安全测试工作流开发者的安全测试功能测试者的安全测试安全测试数据分析和报告应用发现错误代码分析 |
| OWASP测试框架 | 开发开始前进行测试定义和设计过程中进行测试开发过程中进行测试发展过程中进行测试维护和运行 |
| 安全测试风险评估 | 如何评估实际风险如何书写这个测试报告 |
| 安全测试审计报告 | 关于安全测试审计报告安全测试审计报告check list |
| 安全测试工具 |  |
| 安全运维 | 业务需求 | 业务模型数据终端用户第三方管理员管理规则 |
| 基础设施 | 网络系统网络监控虚拟化 |
| 应用需求 | 环境数据处理访问应用监控应用设计 |
| 运维需求 | 日常操作变更管理软件开发企业章程 |

## 课程体系涉及的七大范围包括：

* 应用安全威胁—OWASP TOP 10
* S-SDLC暨威胁建模
* 安全架构设计
* 安全开发
* 渗透测试
* 安全测试
* 安全运维

## 培训对象：

* 所有应用程序设计人员、开发人员、测试人员
* 团队领导和项目经理
* 安全架构师
* 安全从业人员和安全管理人员
* 安全风险管理人员
* 对应用安全程序感兴趣人员
* 对安全测试、渗透测试感兴趣人员
* 安全运维人员
* 其他安全从业人员

## 培训收获：

* 理解从全流程角度分析业务安全
* 理解安全开发流程
* 理解对应用系统进行风险分析和威胁建模
* 如何设计和开发安全的应用程序
* 安全编码最佳实践
* 如何有效进行渗透测试
* 如何对业务系统进行安全运维
* 获取行业认可的安全证书

# CWASP培训认证报名

## 培训时长

|  |  |  |  |
| --- | --- | --- | --- |
| 类别 | 认证 | 培训时间 | 学习方向 |
| 基础级 | CWASP L1 – Foundation | 免费在线自学，在线考试 | 应用安全威胁 |
| 综合认证 | CWASP L2 – Expert  | 5天（含0.5天考试时间） | 应用安全威胁安全架构设计安全运维S-SDLC暨威胁建模安全开发渗透测试安全测试 |
| CWASP L3 – Master | ／ |

## 培训安排

（培训具体时间由各授权培训机构安排）

|  |  |  |  |
| --- | --- | --- | --- |
| 时间安排 | 培训报名时间 | 培训时间 | 考试时间 |
| 2015年第一季度 | 1月1日-1月31日 | 2月1日--3月21日 | 3月22日 |
| 2015年第二季度 | 4月1日-4月30日 | 5月1日—6月20日 | 6月21日 |
| 2015年第三季度 | 7月1日—7月31日 | 8月1日—9月19日 | 9月20日 |
| 2015年第四季度 | 10月1日-10月31日 | 11月1日—12月26日 | 12月27日 |

## 报名方式：

### 所在区域有授权合作伙伴

填写CWASP培训报名表（见附件）到授权合作伙伴处报名。

**北京区培训单位：**

**北京安赛创想科技有限公司 联系方式：http://www.aisec.cn**

### 所在区域暂无授权合作伙伴

* 填写CWASP培训报名表；
* 提交报名表到cwasp(at)seczone.org；

# 培训考试费用

|  |  |  |  |
| --- | --- | --- | --- |
| **认证** | **培训天数(/天)** | **费用（/元）** | **考试费（/元）** |
| CWASP L1–Foundation | / | ／ | 400 |
| CWASP L2 – Expert | 5 | 5200 | 800 |

CWASP L1：高级会员免费考试1次，普通会员可以8折参与考试；