# 注册软件安全专业人员（CWASP CSSP）

# 学员培训手册

发布日期 2017 年 3 月


版本：1.0

中国信息安全测评中心

深圳开源互联网安全技术有限公司

# CWASP CSSP 学员培训指南

**咨询及索取**

关于中国信息安全测评中心 CWASP CSSP 培训相关的更多信息，请与 CWASP CSSP 运营中心联系。

CWASP CSSP 运营中心联系方式：
【联系地址】深圳市龙华清祥路宝能科技园 7 栋 B 座 6J-2
【邮政编码】518000
【电 话】0755-32880880
【传 真】0755-32880880
【电子邮件】cwasp@seczone.cn
【官方网站】www.seczone.cn

深圳开源互联网安全技术有限公司（简称 SecZone），致力于软件安全开发生命周期（S-SDLC：Secure Software Development Life Cycle）的技术研究、推广等。公司是中国信息安全测评中心授权的注册软件安全专业人员（CWASP CSSP）及注册软件安全开发人员（CWASP CSSD）运营机构，负责注册软件安全专业人员（CWASP CSSP）业务的推广、市场宣传、授权培训机构管理及持证人员的服务。 CWASP CSSP 专注于培养高级应用安全人才，是业界首个理论与实践相结合的认证培训体系。

# 目 录

目 录 II
第 1 章 CWASP CSSP 介绍 1
1.1 引言 1
1.2 谁管理 CWASP CSSP 1
1.3 什么是 CWASP CSSP 1
1.4 成为 CWASP CSSP 的基本要求 2
1.5 CWASP CSSP 专业培训 2
1.5.1 CWASP CSSP 专业培训适用人员 2
1.5.2 CWASP CSSP 培训特点 3
1.5.3 CWASP CSSD 培训考试范围 3
1.5.4 CWASP CSSP 培训考试范围 3
1.5.5 CWASP CSSD 培训课程安排 4
1.5.6 CWASP CSSP 培训课程安排 5
1.6 CWASP CSSP 注册流程 6
1.7 CWASP CSSP 职业准则 6
第 2 章 CWASP CSSP 培训 8
2.1 学员申请资料要求 8
2.2 培训报名 8
2.3 学员培训纪律要求 8
第 3 章 考试应考人员考场守则及考试违纪、作弊处罚规则 9
3.1 考试应考人员考场守则 9
3.2 考试违纪、作弊处罚规则 9
附录 1 CWASP CSSP 培训报名表 12
1.个人信息 12
2.工作经历 13
3.CWASP CSSP 运营中心联系方式： 13

# 第 1 章 CWASP CSSP 介绍

## 1.1 引言

随着信息技术的快速发展，软件为人们的日常工作与生活带来了便利，并成为日常工作与生活中不可或缺的部分。而随着信息安全意识的普及，国家和公众也意识到软件同样面临着越来越多的安全威胁。因此，保证软件在其开发生命周期中的开发安全，对于提高软件的安全性有着积极意义。

为了进一步提升国内软件行业的安全竞争力，加强国内软件开发领域从业人员的安全意识及专业水平，中国信息安全测评中心与深圳开源互联网安全技术有限公司（以下简称“SecZone”）共建软件安全专业人员认证体系。该体系基于软件安全开发生命周期（S-SDLC：Secure Software Development Life Cycle），整理出一套适用于广大软件开发人员的知识体系,从 2017 年开始启动注册软件安全专业人员（CWASP CSSP）资质。

此项认证的目的在于提高我国软件开发人员的整体安全意识及安全开发技能，加快我国软件安全专业人员的系统性培养；并通过不断开拓创新，为广大软件开发人员提供优质、专业的软件安全服务。

## 1.2 谁管理 CWASP CSSP

中国信息安全测评中心负责 CWASP CSSP 的咨询和管理工作， 包括负责 CWASP CSSP 的培训管理、考试、注册，深圳开源互联网安全技术有限公司（简称“SecZone”）负责 CWASP CSSP 的教材编写、市场宣传与推广等工作。

## 1.3 什么是 CWASP CSSP

CWASP CSSP （Certified Secure Software Professional）系经中国信息安全测评中心认定的软件安全专业人员，是对我国网络信息系统软件开发人员安全开发能力实施的一种资质评定。

CWASP CSSP 主要从事网络信息系统软件开发的相关工作，其具备一定的软件安全开发知识和技术，能在软件开发生命周期中提供必要的安全保障。

根据认证者的基础不同， CWASP CSSP 共分为两种：

- 注册软件安全开发人员（Certified Secure Software Developer，简称 CWASP CSSD）。证书持有人员主要从事软件开发领域的工作。
- 注册软件安全专业人员（Certified Secure Software Professional，简称 CWASP CSSP）。证书持有人员主要从事软件开发领域的技术与管理工作。

## 1.4 成为 CWASP CSSP 的基本要求

1.申请成为注册软件安全开发人员（CWASP CSSD），具备一定软件开发基础，或有意向从事软件开发的人员，包含软件开发相关专业高校生；申请成为注册软件安全专业人员（CWASP CSSP）应该具备 3 年从事软件安全开发有关的工作经历;

2.参加并完成由中国信息安全测评中心授权培训机构组织的 CWASP CSSP 专业培训；

3.通过中国信息安全测评中心组织的 CWASP CSSP 考试；

4.同意并遵守 CWASP CSSP 职业准则；

5.满足 CWASP CSSP 注册要求并成功通过 CWASP CSSP 审核；

6.获得注册软件安全专业人员资质证书后，遵守和满足 CWASP CSSP 注册维持要求，并缴付年费；

7.不满足 CWASP CSSP 工作经验要求的人员，也可以先参加 CWASP CSSP 培训和考试,在完成培训并通过考试后,获得 CWASP CSSP 培训结业证书;在获得 CWASP CSSP 培训结业证书后的 3 年内累积并满足注 CWASP CSSP 的教育和工作经验要求，经过注册软件安 CWASP CSSP 注册审核后获得 CWASP CSSP 注册资质。

## 1.5 CWASP CSSP 专业培训

### 1.5.1 CWASP CSSP 专业培训适用人员

CWASP CSSP 专业培训是由中国信息安全测评中心统一管理和规范并授权培训机构组织实施的信息安全专业培训。

CWASP CSSP 专业培训适用于以下人员：

- 所有软件开发人员；
- 团队领导和项目经理、信息安全经理、软件项目经理、IT 总监/经理；
- 软件架构师、软件工程师、软件开发工程师；
- 应用程序安全专家、渗透测试人员；
- 软件采购分析员、质量保证测试员；
- 其他从事软件安全开发工作的有关人员。

CWASP CSSD 和 CWASP CSSP 两者之间无认证先后顺序。CWASP CSSD 是 CWASP CSSP 的基础，适合于软件开发基础人员。

### 1.5.2 CWASP CSSP 培训特点

1.体系完善、视野开阔

CWASP CSSP 认证体系涵盖安全威胁、S-SDLC、软件安全架构设计、软件安全开发、软件安全测试和软件安全部署等知识领域，并注重实践，能有效拓宽参培者的视野与技能。

2.贴近实际，案例详实

CWASP CSSP 结合了软件开发全生命周期中软件安全保障工作的实际需要，构建了一个全面实用的软件安全开发人员知识体系。同时重视不同行业的软件开发安全实践经验传承，并不断创新，达到与时俱进。

3.知识全面，技能并重

CWASP CSSP 不仅有全面的知识体系，更加重视学员的技能训练，使之成为能满足软件开发机构实际需要的专业技术型人才。

4.目标明确，持续发展

通过科学严格的考试和认证，为用人单位选拔软件安全高端人才提供权威依据；通过证后服务持续提升获证人员的知识和技能，使之适应软件安全工作不断发展的要求。

### 1.5.3 CWASP CSSD 培训考试范围

在整个“注册软件安全开发人员（CWASP CSSD）”的知识体系结构中，共包括应用安全威胁、S-SDLC 流程和安全开发基本知识这三个知识体，每个知识体根据其逻辑划分为多个知识域，每个知识域由一个或多个知识子域组成。

CWASP CSSD 知识体系结构共包含三个知识体，分别为：

- 应用安全威胁：主要介绍以“OWASP Top 10”为核心的应用安全威胁及应用安全威胁实例。
- S-SDLC 流程：主要介绍软件安全开发全生命周期的主要流程及安全管控措施。
- 软件安全开发：主要介绍软件开发过程中参数化查询、输出编码、输入验证、身份验证、访问控制等方面的技术知识和实践。这些是注册软件安全专业人员需要掌握的核心知识。

### 1.5.4 CWASP CSSP 培训考试范围

在整个“注册软件安全专业人员（CWASP CSSP）”的知识体系结构中，共包括应用安全威胁、S-SDLC、软件安全架构设计、软件安全开发、软件安全测试和软件安全部署这六个知识体，每个知识体根据其逻辑划分为多个知识域，每个知识域由一个或多个知识子域组成。

CWASP CSSP 知识体系结构共包含六个知识体，分别为：

- 应用安全威胁：主要介绍以“OWASP Top 10”为核心的应用安全威胁及应用安全威胁实例。
- S-SDLC：主要介绍软件开发过程中有关 S-SDLC 流程、实施和成熟的模型的知识。
- 软件安全架构设计：主要介绍软件架构设计过程中有关设计安全和威胁分析的安全知识。
- 软件安全开发：主要介绍软件开发过程中有关参数化查询、输出编码、输入验证、身份验证、访问控制等方面的安全知识。
- 软件安全测试：主要介绍软件测试过程中的有关安全测试的基本知识、流程和渗透测试的知识。
- 软件安全部署：主要介绍软件安全部署过程中有关软件部署过程、软件自身安全和基础环境安全的知识。

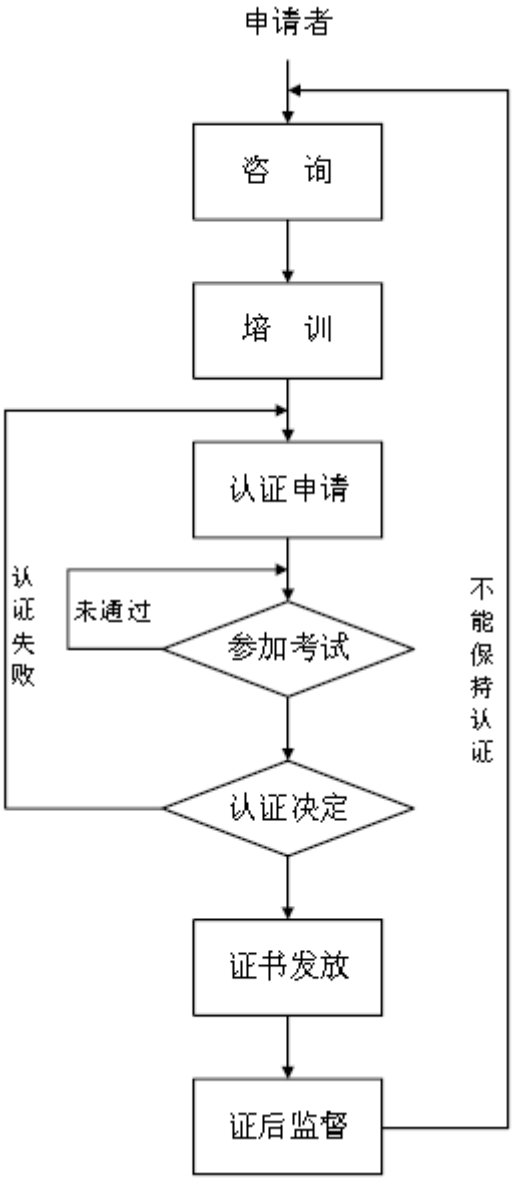
### 1.5.5 CWASP CSSD 培训课程安排

| 知识体 | 知识域 | 天数 |
|---|---|---|
| **应用安全威胁** | OWASP TOP 10 | 1 |
| | 应用安全威胁实例剖析 | |
| **S-SDLC 流程** | S-SDLC 需求阶段关键要素 | 0.5 |
| | S-SDLC 设计阶段关键要素 | |
| | S-SDLC 实施阶段关键要素 | |
| | S-SDLC 验证阶段关键要素 | |
| | S-SDLC 发布与响应阶段关键要素 | |
| **软件安全开发** | 输入验证 | 0.5 |
| | 输出编码 | |
| | 正确的实现访问控制 | |
| | 建立身份验证机制 | |
| | 保护数据和隐私 | |
| | 实现正确的日志和错误处理 | |
| | 利用框架的安全性和安全类库 | |

## 1.5.6 CWASP CSSP 培训课程安排

| 知识体 | 知识域 | 天数 |
|---|---|---|
| **应用安全威胁** | OWASP TOP 10 | 1 |
| | 应用安全威胁实例剖析 | |
| **S-SDLC** | S-SDLC 流程 | 1 |
| | S-SDLC 流程与敏捷开发 | |
| | S-SDLC 流程实施与成熟度模型 | |
| **软件安全架构设计** | 设计安全 | 0.5 |
| | 威胁分析 | |
| **软件安全开发** | 输入验证 | 0.5 |
| | 输出编码 | |
| | 正确的实现访问控制 | |
| | 建立身份验证机制 | |
| | 保护数据和隐私 | |
| | 实现正确的日志和错误处理 | |
| | 利用框架的安全性和安全类库 | |
| **软件安全测试** | 安全测试基本知识 | 0.5 |
| | 安全测试流程 | |
| | 渗透测试 | |
| **软件安全部署** | 软件部署过程 | 0.5 |
| | 软件自身安全 | |
| | 基础环境安全 | |

## 1.6 CWASP CSSP 注册流程




## 1.7 CWASP CSSP 职业准则

在中国信息安全测评中心注册的 CWASP CSSP 必须保证严格履行职责并承诺完全遵守以下道德准则：

1. 必须诚实，公正，负责，守法；
2. 必须勤奋和胜任工作，提高专业能力和水平；

3. 必须保护信息系统、应用程序和系统的价值。

4. 必须接受中国信息安全测评中心的监督，在任何情况下，不损坏中国信息安全测评中心或注册过程的声誉，对中国信息安全测评中心针对 CWASP CSSP 而进行的调查应给予充分的合作；

5. 必须按规定向中国信息安全测评中心交纳费用。

# 第 2 章 CWASP CSSP 培训

## 2.1 学员申请资料要求

1.学员需要填写如下申请资料：

《注册软件安全专业人员（CWASP CSSP）考试及注册申请表》

填写申请表格时应注意：申请表格可采用电子模版录入填写，也可手写，填写过程中应确保内容的真实准确，手写申请表格应用正楷字体，字迹要求清晰可辨。

**注：**填写注册申请表第二部分时，需要由申请人所在单位（部门）领导签字并加盖本单位公章。

2.申请（CWASP CSSP）注册资质除了填写申请书外，还需要准备以下资料：

- 个人近期免冠 2 寸彩色白底证件照片 3 张
- 身份证复印件 1 份
- 申请人专业工作证明文件；需单位证明；

3.学员应在报名同时将所有资料全部提交。

## 2.2 培训报名

**学员报名：**学员可以通过电话、传真与 CWASP CSSP 运营中心确认报名，可登录中国信息安全测评中心网站查询开班信息。培训报名表见附录 1

## 2.3 学员培训纪律要求

1. 上课期间共同维护教学工作的顺利进行，专心学习；
   - 学员上课时间应关闭手机或将手机等设置于无声状态，以免干扰其他学员的学习；
   - 学员上课时间内应认真听讲，不得从事于听课无关的其他事宜。
2. 学习期间不得迟到、请假，旷课，如学员迟到三次或无故旷课半天以上，取消该学员注册考试资格。

# 第 3 章 考试应考人员考场守则及考试违纪、作弊处罚规则

## 3.1 考试应考人员考场守则

第一条 为规范 CWASP CSSP 资质认定考试工作，制定本守则。

第二条 应试人员将身份证件放在考桌桌面的右上角。

第三条 应考人员应提前 20 分钟入场，在每期考试开始后迟到 30 分钟的应考人员不得进入考场考试。考试开始 30 分钟后，应考人员可以交卷退出考场。

第四条 应考人员不得携带任何书籍、笔记、纸张、具备文字储存和音响功能的计算器、具上网功能的平板电脑、各类通讯工具等进入考场座位。

第五条 开考之前，应考人员应在答题卡和答题卷指定的位置用正楷正确填写（填涂）姓名、身份证件号、准考证号。凡因错填或错涂姓名、身份证件号、准考证号或损坏答题卡造成评卷期间不能登统成绩或出现差错的，责任由应考人员自负。

第六条 应考人员在考试中，要严格遵守考场纪律，保持考场肃静，不得相互交谈，不得看他人试卷或相互对答题内容，不得夹带换卷，不得在考场内吸烟、随意站立及走动。

第七条 考试结束时间到，应考人员应立即停止答卷，将试卷翻放在桌面上，等候监考人员当众清点回收。待监考人员宣布退场时，应考人员应立即退出考场。不得将试题卷、答题卷、答题卡及草稿纸带出考场。

## 3.2 考试违纪、作弊处罚规则

为了确保考试的质量，严肃考试纪律，维护考试信誉和应考人员的合法权益，公开、公平、公正地举办考试，特制定本规则。

第一条 本规则所指的违纪、作弊行为人包括应考人员和考试监考工作人员，及与违纪、作弊行为有关的其他人员。

第二条 对违纪、作弊行为人处罚的基本原则是事实清楚，证据确凿，处罚得当。

第三条 中国信息安全测评中心依照本规则对违纪、作弊行为人进行处罚。

第四条 违纪、严重违纪及作弊：

一、 应考人员在考试期间有下列行为之一，为违纪：

1. 将书籍、笔记、带有文字的纸张、具备文字储存和音响功能的计算器、具上网功能的平板电脑、各种通讯工具等夹带至考场座位；
2. 考试开始 30 分钟内仍未在答题卡和答题卷规定的位置填写（填涂）姓名、身份证件号。

二、 应考人员在考试期间有下列行为之一，为严重违纪：

1. 有第四条第一款所列行为，经监考人员 3 次明确警告后仍不改正；
2. 考试开始后，手机及平板电脑出现在身边，发生震动或铃声等行为；
3. 考试开始 30 分钟后仍未在试卷和答题卡规定的位置填写（填涂）姓名、身份证件号，经监考人员警告后仍不填写（填涂）。

三、 应考人员在考试期间有下列行为之一，为作弊：

1. 偷看、抄袭他人答案或其他资料；
2. 由他人在考场外协助答题；
3. 互相交换试题卷、答题卡、答题卷；
4. 协助他人答题，传递有关考试内容的信息，或让他人抄袭答案；
5. 由他人冒名代考或代替他人参加考试；
6. 不服从监考人员管理，故意扰乱考场秩序。

四、 在考试试卷评阅期间由评阅人员发现的异常答卷，经专家鉴定为互相抄袭的，按作弊处理。

第五条 处理办法及程序：

凡应考人员或监考人员出现涉及第五条、第六条及第八条所列行为时，应当按照以下程序对其提出警告并责令当事人立即改正；

1. 凡应考人员出现严重违纪行为的人员，应停止当事人继续参加考试，并取消当事人的考试资格及成绩；
2. 凡应考人员出现作弊行为，应停止当事人继续参加考试，并取消当事人的考试资格及成绩，且自培训之日起半年内不能参加考试。
3. 监考人员应在其答题卷得分栏和答题卡页首空白处签注"严重违纪"或"作弊"字样，并在《注册软件安全专业人员考试监考及评卷记录》中记录当事人的严重违纪、作弊情况。
4. 当试卷评阅期间评阅人员确认答卷异常时，应当填写《注册软件安全专业人员考试监考及评卷记录》，按试卷评阅工作规程核实。经中国信息安全测评中心委派的专家鉴定为互相抄袭的，提交有关证据，并按本规则以予处罚。
5. 凡应考人员出现作弊行为，除按前款规定进行处罚外，还将作弊情况向其所在工作单位通报。

第六条 应考人员违纪、作弊有下列情节之一者，应加重处罚直至移交司法机关处理：

1. 销毁、藏匿作弊证据或伪造虚假证据；
2. 包庇、串通作弊人员；
3. 强迫、唆使他人违纪、作弊或串通作弊；
4. 阻止他人揭发检举、提供证据资料；

5. 对揭发检举人打击报复；

6. 干扰、妨碍考试组织机构调查核实。

第七条 应考人员对违纪、作弊行为的处罚有异议的，可向中国信息安全测评中心提出书面复审申请，收到应考人复审申请后，中国信息安全测评中心应对严重违纪、作弊事实进一步予以核实，将复核结果通知至应考人员。

第八条 本规则自公布之日起执行。

# 附录 1 CWASP CSSP 培训报名表

## 1.个人信息

<table>
<tr><td>姓　　名</td><td colspan="2"></td><td>性　　别</td><td></td><td rowspan="4">正面免冠彩色照片（2 寸）</td></tr>
<tr><td>姓名拼音</td><td colspan="2"></td><td>民　　族</td><td></td></tr>
<tr><td>出生日期</td><td colspan="2">年　　月　　日</td><td>政治面貌</td><td></td></tr>
<tr><td>籍　　贯</td><td colspan="2"></td><td>专　　业</td><td></td></tr>
<tr><td>最高学历</td><td colspan="2"></td><td>身份证号</td><td colspan="2"></td></tr>
<tr><td>工作单位</td><td colspan="5"></td></tr>
<tr><td colspan="6">联系方式</td></tr>
<tr><td>通信地址</td><td colspan="3"></td><td>邮　编</td><td></td></tr>
<tr><td>联系电话</td><td colspan="3"></td><td>手机号码</td><td></td></tr>
<tr><td>电子邮箱</td><td colspan="5"></td></tr>
<tr><td rowspan="5">文化程度</td><td>时　间</td><td colspan="2">毕业学校</td><td>学　历</td><td>专　业</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td rowspan="3">相关培训证书情况（附培训证书复印件）</td><td>证书名称</td><td colspan="2">发证机构</td><td>证书编号</td><td>获证日期</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
</table>

## 2.工作经历

| 起止日期 | 工作单位 | 职务 | 主要职责 | 证明人 | 是否与软件安全领域相关 |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| 小计：<br>工作经验　　年，其中软件安全领域工作经验　　年。 | | | | | |

## 3.CWASP CSSP 运营中心联系方式：

【联系地址】深圳市龙华清祥路宝能科技园 7 栋 B 座 6J-2
【邮政编码】518000
【电　　话】0755-32880880
【传　　真】0755-32880880
【电子邮件】cwasp@seczone.cn
【官方网站】www.seczone.cn