OWASP
Open Web Application
Security Project

OWASP SAMM
软件保障成熟度模型
v2.0

王颉

Open Web Application Security Project

SAMM的背景

发展历程

2009年
V1.0

2016年
V1.1.1

2017年
V1.5

2020年
V2.0

OWASP
Open Web Application
Security Project

OWASP项目的关联关系（S-SDLC的视角）

Requirement | **Design** | **Implementation** | **Verification** | **Deploy**

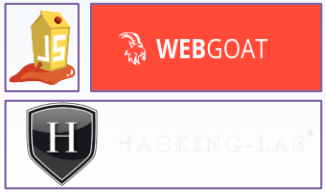
SecurityRAT

DEPENDENCY-CHECK

More...

Training

DevSLOp



More...

OWASP Open Web Application Security Project

原始核心团队

- Sebastien (Seba) Deleersnyder – Project Leader, Belgium
- Chris Cooper – United Kingdom
- Bart DeWin – Belgium
- John DiLeo – New Zealand
- Daniel Kefer – Germany
- Nessim Kisserli – United Kingdom
- Yan Kravchenko – United States

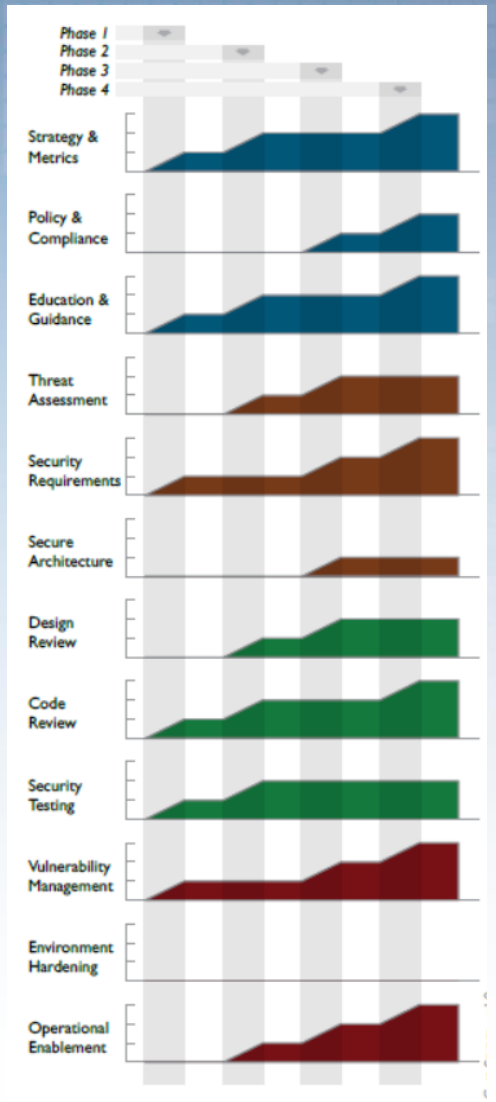
Open Web Application Security Project

什么是“SAMM”?

- SAMM是“Software Assurance Maturity Model”的英文缩写。
- SAMM是一个规范性模型，是一个易于使用、完全定义和可测量的开放框架。

用处

- 评估组织现有的软件安全实践。
- 构建明确定义的、平衡的软件安全保障迭代路线图。
- 展示出对安全保障计划的具体改进。
- 定义和衡量整个组织的安全相关活动。



来源：OWASP SAMM v1.0

OWASP
Open Web Application Security Project

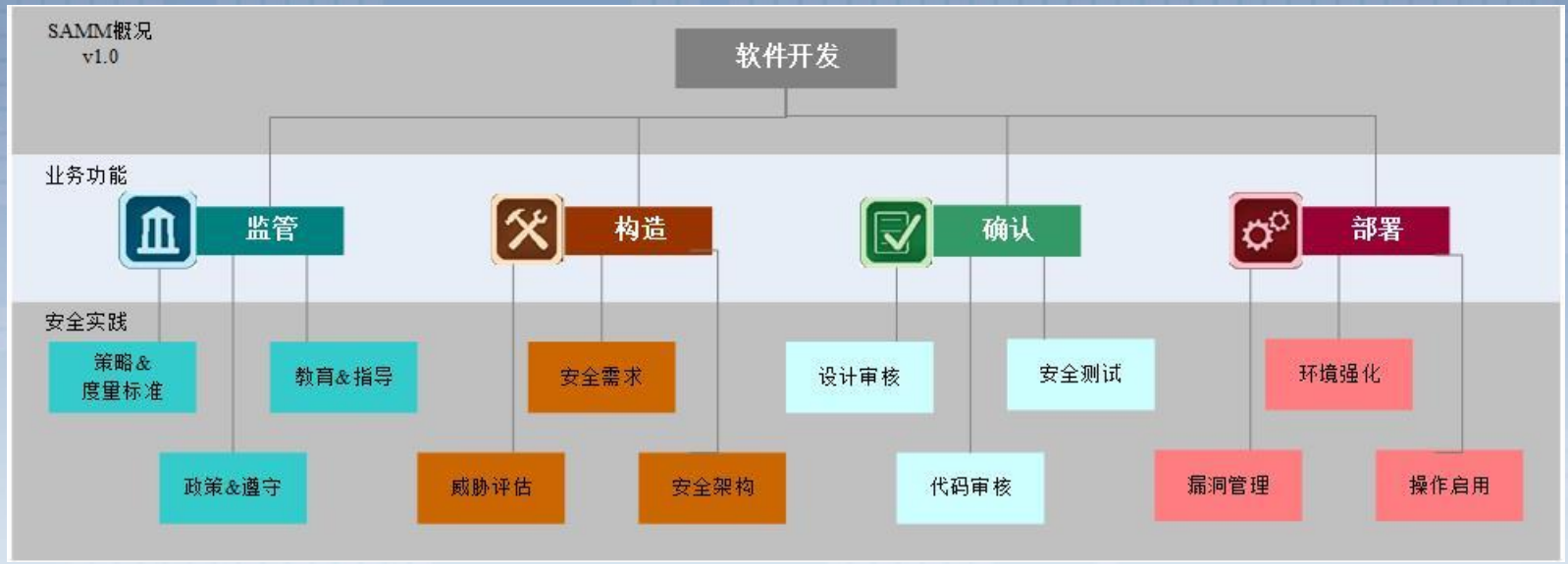
用户评价

Dell uses OWASP's Software Assurance Maturity Model (OWASP SAMM) to help focus our resources and determine which components of our secure application development program to prioritize.

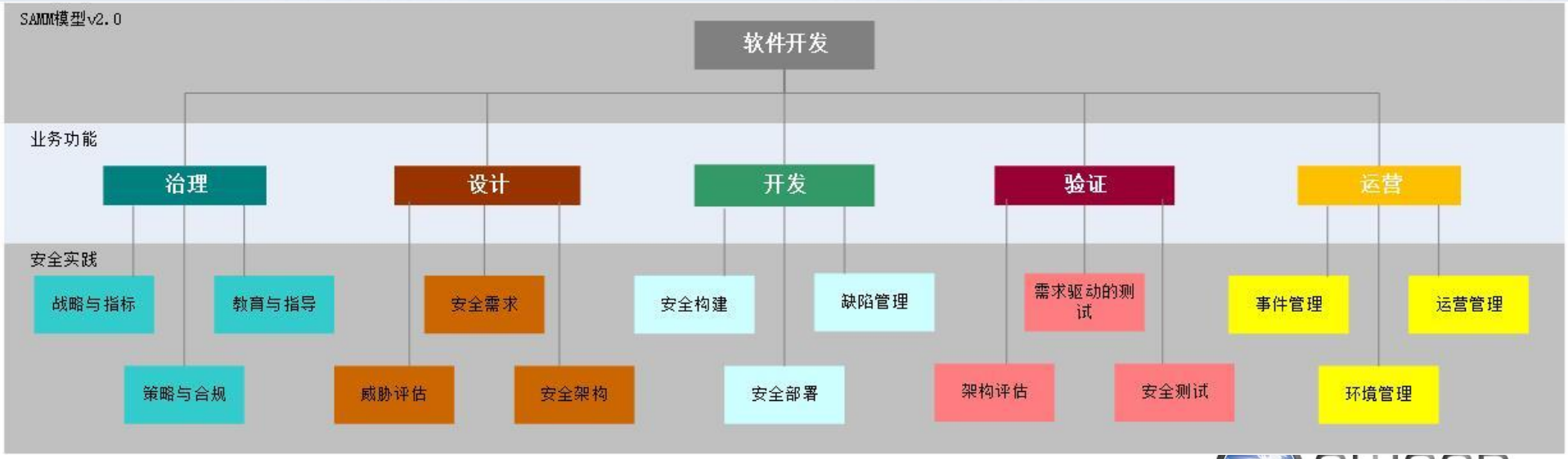
——Michael J. Craigue, Information Security & Compliance, Dell, Inc

Open Web Application Security Project

SAMM核心模型



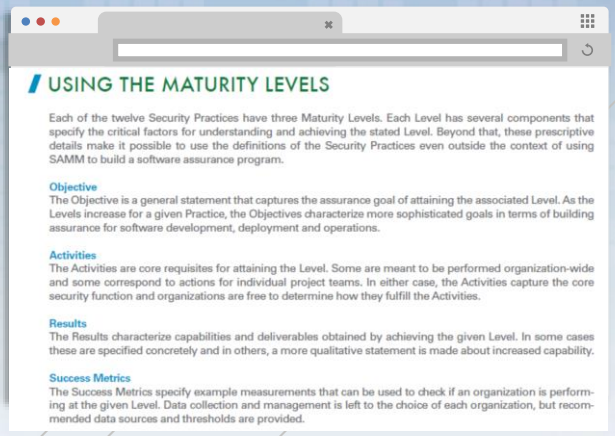
SAMM v1.0



SAMM v2.0

SAMM的成熟度等级

- 设置了3个成熟度等级；并与CMMI的5个级别大致对应



USING THE MATURITY LEVELS

Each of the twelve Security Practices have three Maturity Levels. Each Level has several components that specify the critical factors for understanding and achieving the stated Level. Beyond that, these prescriptive details make it possible to use the definitions of the Security Practices even outside the context of using SAMM to build a software assurance program.

Objective
The Objective is a general statement that captures the assurance goal of attaining the associated Level. As the Levels increase for a given Practice, the Objectives characterize more sophisticated goals in terms of building assurance for software development, deployment and operations.

Activities
The Activities are core requisites for attaining the Level. Some are meant to be performed organization-wide and some correspond to actions for individual project teams. In either case, the Activities capture the core security function and organizations are free to determine how they fulfill the Activities.

Results
The Results characterize capabilities and deliverables obtained by achieving the given Level. In some cases these are specified concretely and in others, a more qualitative statement is made about increased capability.

Success Metrics
The Success Metrics specify example measurements that can be used to check if an organization is performing at the given Level. Data collection and management is left to the choice of each organization, but recommended data sources and thresholds are provided.

0 隐藏起点，即，安全开发实践没有实现时

1 对安全实践有了初步了解并有了一定的执行

2 安全实践的执行被提高了效率和有效性

3 安全实践得到了综合性的全面落地

OWASP SAMM	CMMI
第1级	能力级别1—非正式执行
	能力级别2—计划跟踪（部分）
第2级	能力级别2—计划跟踪（完整）
	能力级别3—充分定义
第3级	能力级别4—量化控制
	能力级别5—持续优化

核心原则

组织的行为随时间逐渐改变

改变必须是迭代的，同时努力实现长期目标

没有适用于所有组织的单一方案

解决方案必须针对企业特定的风险

SAMM的核心原则

必须简单、定义明确且可衡量

与安全活动相关的规定必须具有指导性

解决方案必须为非安全人员提供足够的详细信息

1.3 教育与指导

成熟度等级		活动流A 培训和意识	活动流B 组织和文化
1级	为员工提供有关安全开发和部署主题的可访问资源。	为所有软件开发涉及的人员提供安全意识培训。	在每个开发团队中确定一个“安全专家（Security Champion）”。
2级	对软件生命周期中的所有人员提供有关安全开发技术和针对特定角色指导的教育。	提供技术和特定角色的指导，包括每种语言和平台的安全细微差别。	开发一个安全软件中心，以显著促进开发人员和架构师的思想领导力。
3级	开发由不同团队开发人员共同推动的内部培训计划。	围绕组织的安全软件开发标准形成标准化的内部指导。	建立一个软件安全社区，包含所有参与软件安全的组织内部人员。

培训和意识—成熟度等级1

- **收益**

所有相关员工的基本安全意识。

- **活动**

对当前参与软件管理、开发、测试、审计的所有角色进行安全意识培训。目的是提高人们对应用软件安全威胁和风险、安全最佳实践以及安全软件设计原则的认识。在组织内部创建培训，或从外部购买培训。理想情况下，应提供面对面的培训，以便参与者可以进行小组讨论，但是也可以选择基于计算机的上机培训。

- **问题**

您是否要求涉及应用软件开发的员工接受SDLC培训？

- **质量标准**

① 培训是可重复的、持续的，并且对任何参与软件开发生命周期的人员都可用。
② 培训在适当的情况下包括最新的OWASP Top 10，并包括诸如最低权限、纵深防御、安全故障保护、完全消减、会话管理，开放式设计和心理接受性的概念。
③ 培训需要参加者的签字或确认。
④ 您在最近12个月内更新了培训。
⑤ 在员工入职过程中提供了培训。

- **回答**

① 没有；
② 是的，要求其中一些；
③ 是的，要求至少有一半；
④ 是的，要求大多数或全部。

组织和文化—成熟度等级1

- **收益**

将安全基本嵌入在开发组织中。

- **活动**

实施一个计划，其中，每个软件开发团队都有一个被视为“安全专家（Security Champion）”的成员，该成员是信息安全人员与开发人员之间的联络人。根据团队的规模和结构，“安全专家”可能是软件开发人员、测试人员或产品经理。“安全专家”每周有固定的工作小时数与信息安全相关实践相关。他们参加定期的情况介绍会，以提高对不同安全领域的认识和专业知识。“安全专家”需要接受额外的培训，以帮助他们发展作为软件安全主题专家。出于文化原因，您可能需要自定义创建和支持“安全专家”的方式。

- **问题**

您是否为每个开发团队确定了“安全专家”？

- **质量标准**

① “安全专家”接受了适当的培训；
② 应用软件安全团队和开发团队会定期收到来自“安全专家”的简报，内容涉及安全计划和修复的总体状态；
③ “安全专家”在解决应用软件积压的问题之前，先审查外部测试的结果。

- **回答**

① 没有；
② 是的，对于某些团队；
③ 是的，对于至少一半的团队；
④ 是的，对于大多数或所有团队。

4.3 安全测试

成熟度等级		活动流A 可测量的基线	活动流B 深入理解
1级	执行安全测试（包括人工的和基于工具的）以发现安全缺陷。	利用自动化安全测试工具。	对高风险组件执行人工安全测试。
2级	通过自动化以及常规的手动安全渗透测试，可以使开发过程中的安全测试更加完整和高效。	采用特定于应用软件的自动化安全测试。	执行人工渗透测试。
3级	将安全测试嵌入到开发和部署过程中。	将自动化安全测试集成到构建和部署过程中。	将安全测试集成到开发过程中。

可测量的基线—成熟度等级3

- **收益**
- 在尽可能早的阶段识别可自动识别的漏洞。

- **活动**
- 组织内的项目通常会运行自动化的安全测试，并在开发过程中检查结果。将安全测试工具配置为在构建和部署过程中自动运行，以使其具有较低的开销而可扩展。检查发现的结果。

- **问题**
- 您是否将自动化安全测试集成到构建和部署过程中？

- **质量标准**

① 管理层和业务利益相关者在整个开发周期中跟踪和审查测试结果；
② 您可以将测试结果合并到中央仪表板中，并将其输入到缺陷管理中。

- **回答**

① 没有；
② 是的，集成了其中一些；
③ 是的，集成了至少一半；
④ 是的，集成了大部分或全部。

深刻的理解—成熟度等级3

- **收益**

在尽可能早的阶段里识别可人工识别的安全问题。

- **活动**

与所有其他开发活动（包括：需求分析、软件设计和构建）并行集成安全测试。

由于在开发的每个阶段都运行着多种安全工具，因此，不再适合或不希望在指定的阶段修复安全问题（例如，发布前的测试）。必须对安全问题进行快速分类，并在风险和修复成本之间进行权衡取舍，并制定修复计划。通过将特定的、低摩擦的自动化测试集成到开发工具和构建过程中，以持续在开发生命周期的早期阶段检测问题，从而降低了修复成本、增加了迅速解决问题的可能性。

- **问题**

您是否使用安全测试的结果来改进开发生命周期？

- **质量标准**

① 您使用其他安全活动的结果来改进开发过程中的集成安全测试；
② 您审查测试结果，并将其纳入安全意识培训和安全测试手册中；
③ 利益相关者审查测试结果并根据组织的风险管理进行处理。

- **回答**

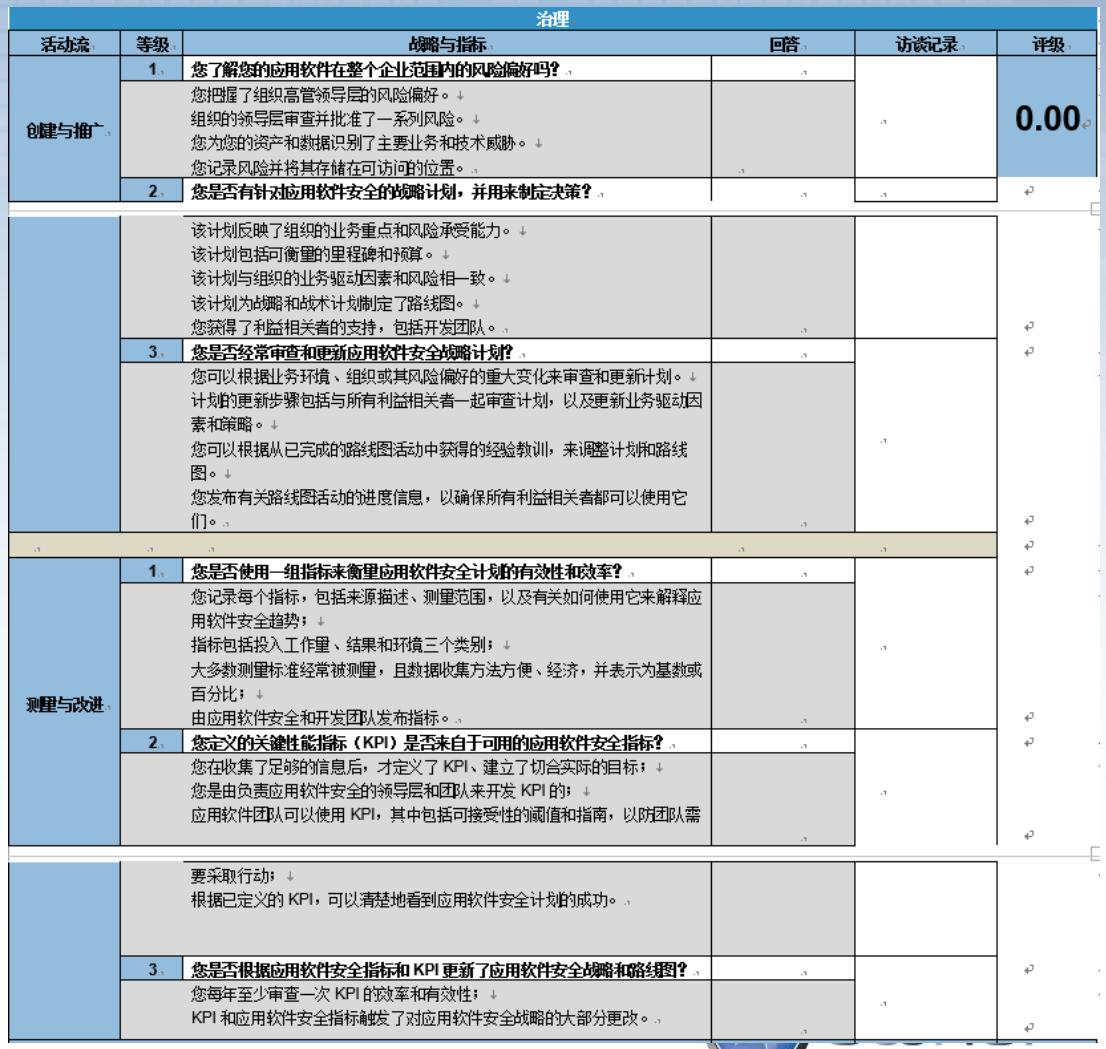
① 没有；
② 是的，但我们会临时改进；
③ 是的，我们会定期改进；
④ 是的，我们至少每年改进一次。

Open Web Application Security Project

使用方法

评估软件开发组织的能力现状

- 根据SAMM业务功能和安全实践组织访谈。
- 从“答案”列中的多项选择下拉选择中选择最佳答案。



治理					
活动流	等级	战略与指标	回答	访谈记录	评级
创建与推广	1	您了解您的应用软件在整个企业范围内的风险偏好吗?			0.00
		您把握了组织高管领导层的风险偏好。 组织的领导层审查并批准了一系列风险。 您为您的资产和数据识别了主要业务和技术威胁。 您记录风险并将其存储在可访问的位置。			
	2	您是否有针对应用软件安全的战略计划，并用来制定决策?			
		该计划反映了组织的业务重点和风险承受能力。 该计划包括可衡量的里程碑和预算。 该计划与组织的业务驱动因素和风险相一致。 该计划为战略和战术计划制定了路线图。 您获得了利益相关者的支持，包括开发团队。			
	3	您是否经常审查和更新应用软件安全战略计划?			
		您可以根据业务环境、组织或其风险偏好的重大变化来审查和更新计划。 计划的更新步骤包括与所有利益相关者一起审查计划，以及更新业务驱动因素和策略。 您可以根据从已完成的路线图活动中获得的经验教训，来调整计划和路线图。 您发布有关路线图活动的进度信息，以确保所有利益相关者都可以使用它们。			
测量与改进	1	您是否使用一组指标来衡量应用软件安全计划的有效性和效率?			
		您记录每个指标，包括来源描述、测量范围，以及有关如何使用它来解释应用软件安全趋势； 指标包括投入工作量、结果和环境三个类别； 大多数测量标准经常被测量，且数据收集方法方便、经济，并表示为基数或百分比； 由应用软件安全和开发团队发布指标。			
	2	您定义的关键性能指标（KPI）是否来自于可用的应用软件安全指标?			
		您在收集了足够的信息后，才定义了 KPI、建立了切合实际的目标； 您是由负责应用软件安全的领导层和团队来开发 KPI 的； 应用软件团队可以使用 KPI，其中包括可接受性的阈值和指南，以防团队需			
		要采取行动； 根据已定义的 KPI，可以清楚地看到应用软件安全计划的成功。			
	3	您是否根据应用软件安全指标和 KPI 更新了应用软件安全战略和路线图?			
		您每年至少审查一次 KPI 的效率和有效性； KPI 和应用软件安全指标触发了对应用软件安全战略的大部分更改。			

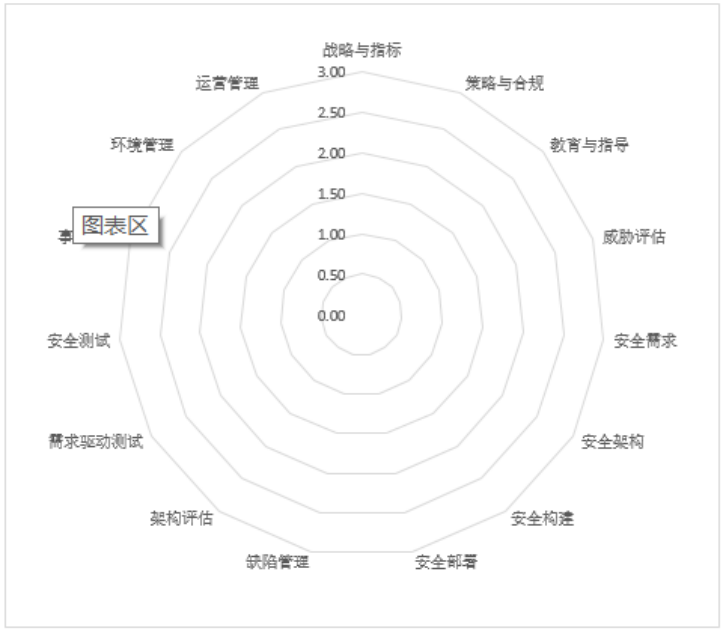
访谈记分卡

成熟度得分

业务功能	安全措施	当前	成熟度 1	2	3
治理	战略与指标	0.00	0.00	0.00	0.00
治理	策略与合规	0.00	0.00	0.00	0.00
治理	教育与指导	0.00	0.00	0.00	0.00
设计	威胁评估	0.00	0.00	0.00	0.00
设计	安全需求	0.00	0.00	0.00	0.00
设计	安全架构	0.00	0.00	0.00	0.00
开发	安全构建	0.00	0.00	0.00	0.00
开发	安全部署	0.00	0.00	0.00	0.00
开发	缺陷管理	0.00	0.00	0.00	0.00
验证	架构评估	0.00	0.00	0.00	0.00
验证	需求驱动测试	0.00	0.00	0.00	0.00
验证	安全测试	0.00	0.00	0.00	0.00
运营	事件管理	0.00	0.00	0.00	0.00
运营	环境管理	0.00	0.00	0.00	0.00
运营	运营管理	0.00	0.00	0.00	0.00

业务功能	当前
治理	0.00
设计	0.00
开发	0.00
验证	0.00
运营	0.00

成熟度得分



OWASP
Open Web Application Security Project

Open Web Application Security Project

价值与意义

对组织的价值与意义

- 提升组织的软件安全开发能力
- 有助于组织开发安全的软件产品
- 有助于组织在开发过程中的安全合规
  - 《网络安全法》
  - 《等级保护2.0》

谢 谢

项目Email: project@owasp.org.cn
个人Email: wangj@owasp.org.cn

OWASP
Open Web Application Security Project