OWASP
Open Web Application Security Project

OWASP应用安全评估标准
OWASP ASVS

郭振新

自我介绍

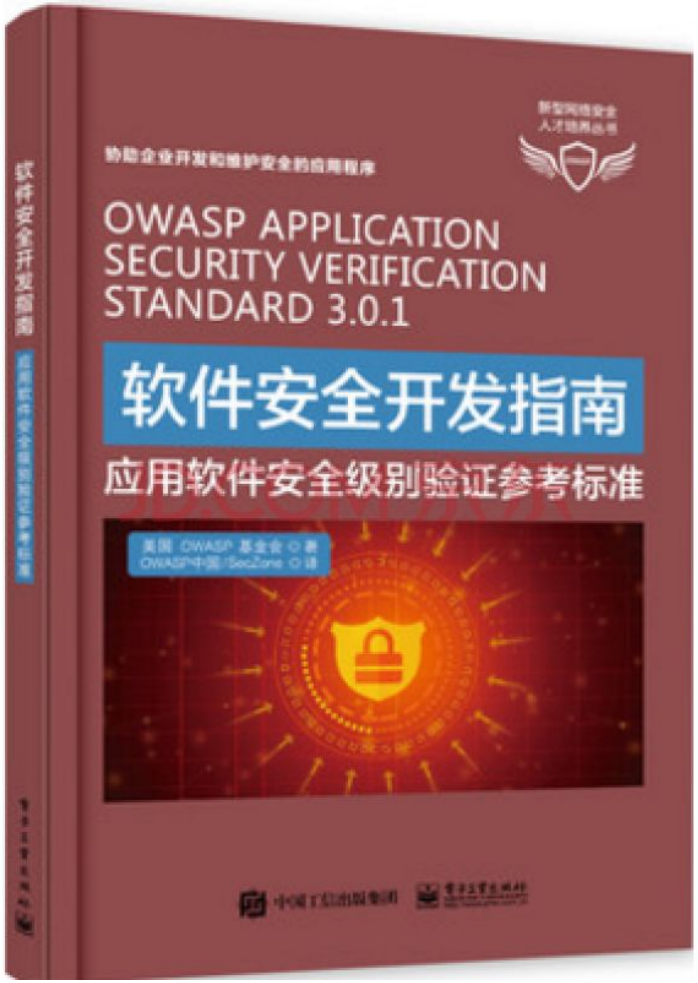
- OWASP ProActive Controls中文项目组成员
- 来自美国径点科技——高级研发工程师
- OSCPer

OWASP
Open Web Application
Security Project

径点科技（ AvePoint, Inc. ）

- 微软金牌合作伙伴。
- 全球26个分公司。
- 产品：全球16000多家企业客户。其中包括众多世界五百强企业。
- 项目：新加坡中央公积金局，新加坡财政部，新加坡金融管理局，新加坡社会及家庭发展部，新加坡共和理工学院，新加坡樟宜机场，新跃社科大学，新加坡科技设计大学等等。

OWASP ASVS



OWASP

Application Security Verification Standard 4.0

Final

March 2019

OWASP
Open Web Application Security Project

OWASP ASVS项目主旨

- **OWASP应用安全评估标准（ASVS）项目**的主旨：为执行Web应用程序 安全验收提供一套可行的标准，以规范应用程序的安全验证覆盖范围和安全级别。
- 该项目不仅为Web应用程序技术安全控制提供了测试参考标准，还为应用程序开发人员提供了一系列安全开发需求建议。

OWASP ASVS发展历程

- 2009年发布1.0版本
- 2014年8月发布2.0版本
- 2016年6月发布3.0.1版本
- 2018年3月中文版3.0.1出版
- 2018年3月发布3.1版本
- 2019年3月发布4.0.1版本
- 原项目地址：https://owasp.org/www-project-application-security-verification-standard/

OWASP ASVS贡献人

- 该项目由Daniel Cuthbert, Andrew Van der Stock, Jim Manico, Mark Burnett, Josh Grossman主导，并由近百名安全专家参与。
- 中文版全书由王颉博士负责总体架构设计和质量控制，由Rip、张家银担任翻译顾问，由包悦忠、李旭勤负责技术指导。内容由王颉博士，王厚奎，吴楠共同翻译。全文由赵学文负责统稿与编排。

OWASP ASVS适用人群

- 网络安全专家
- 渗透测试人员
- 软件安全开发服务咨询
- 软件开发工程师/项目主管
- 网络安全教育工作者/培训讲师
- 软件消费者（甲方）
- 网络安全爱好者

我是怎么开始接触OWASP ASVS

- 新加坡软件研发项目。
- ISO 27001认证。

OWASP ASVS vs OWASP TOP 10

A2 :2017

失效的身份认证

应用程序脆弱吗？

确认用户的身份、身份验证和会话管理非常重要，这些措施可用于将恶意的未经身份验证的攻击者与授权用户进行分离。

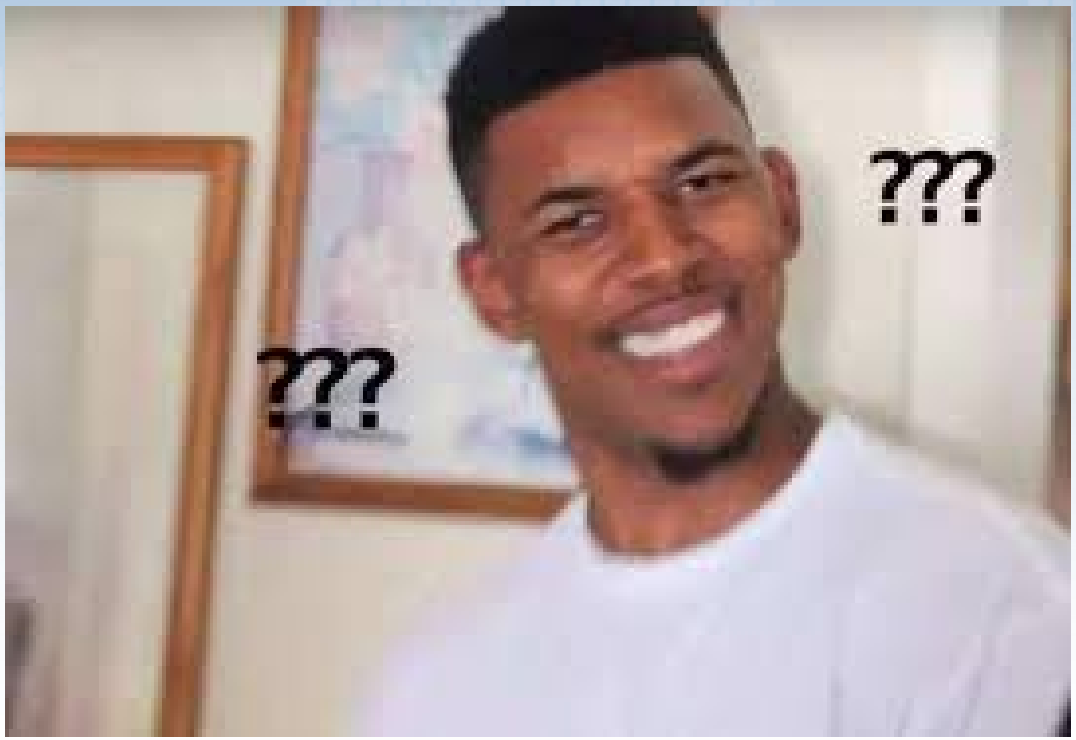
如果您的应用程序存在如下问题，那么可能存在身份验证的脆弱性：

- 允许凭证填充，这使得攻击者获得有效用户名和密码的列表。
- 允许暴力破解或其他自动攻击。
- 允许默认的、弱的或众所周知的密码，例如“Password1”或“admin/admin”。
- 使用弱的或失效的验证凭证，忘记密码程序，例如“基于知识的答案”，这是不安全的。
- 使用明文、加密或弱散列密码（参见：A3:2017-敏感数据泄露）。
- 缺少或失效的多因素身份验证。
- 暴露URL中的会话ID（例如URL重写）。
- 在成功登录后不会更新会话ID。
- 不正确地使会话ID失效。当用户不活跃的时候，用户会话或认证令牌（特别是单点登录（SSO）令牌）没有正确注销或失效。

如何防止？

- 在可能的情况下，实现多因素身份验证，以防止自动、凭证填充、暴力破解和被盗凭据再利用攻击。
- 不要使用发送或部署默认的凭证，特别是管理员用户。
- 执行弱密码检查，例如测试新或变更的密码，以纠正“排名前10000个弱密码”列表。
- 将密码长度、复杂性和循环策略与NIST-800-63 B的指导方针的5.1.1章节-记住秘密，或其他现代的基于证据的密码策略相一致。
- 确认注册、凭据恢复和API路径，通过对所有输出结果使用相同的消息，用以抵御账户枚举攻击。
- 限制或逐渐延迟失败的登录尝试。记录所有失败信息并在凭据填充、暴力破解或其他攻击被检测时提醒管理员。
- 使用服务器端安全的内置会话管理器，在登录后生成高度复杂的新随机会话ID。会话ID不能在URL中，可以安全地存储和当登出、闲置、绝对超时后使其失效。

OWASP ASVS vs OWASP TOP 10



OWASP
Open Web Application Security Project

#	Description	L1	L2	L3	CWE	NIST §
2.1.1	Verify that user set passwords are at least 12 characters in length. (C6)	✓	✓	✓	521	5.1.1.2
2.1.2	Verify that passwords 64 characters or longer are permitted. (C6)	✓	✓	✓	521	5.1.1.2
2.1.3	Verify that passwords can contain spaces and truncation is not performed. Consecutive multiple spaces MAY optionally be coalesced. (C6)	✓	✓	✓	521	5.1.1.2
2.1.4	Verify that Unicode characters are permitted in passwords. A single Unicode code point is considered a character, so 12 emoji or 64 kanji characters should be valid and permitted.	✓	✓	✓	521	5.1.1.2
2.1.5	Verify users can change their password.	✓	✓	✓	620	5.1.1.2
2.1.6	Verify that password change functionality requires the user's current and new password.	✓	✓	✓	620	5.1.1.2
2.1.7	Verify that passwords submitted during account registration, login, and password change are checked against a set of breached passwords either locally (such as the top 1,000 or 10,000 most common passwords which match the system's password policy) or using an external API. If using an API a zero knowledge proof or other mechanism should be used to ensure that the plain text password is not sent or used in verifying the breach status of the password. If the password is breached, the application must require the user to set a new non-breached password. (C6)	✓	✓	✓	521	5.1.1.2
2.1.8	Verify that a password strength meter is provided to help users set a stronger password.	✓	✓	✓	521	5.1.1.2
2.1.9	Verify that there are no password composition rules limiting the type of characters permitted. There should be no requirement for upper or lower case or numbers or special characters. (C6)	✓	✓	✓	521	5.1.1.2

应用安全验证级别 等级1

- 如果应用程序充分防范《OWASP Top 10》和其他类似清单中包含的安全漏洞，它就实现了ASVS 等级1（或取巧级）

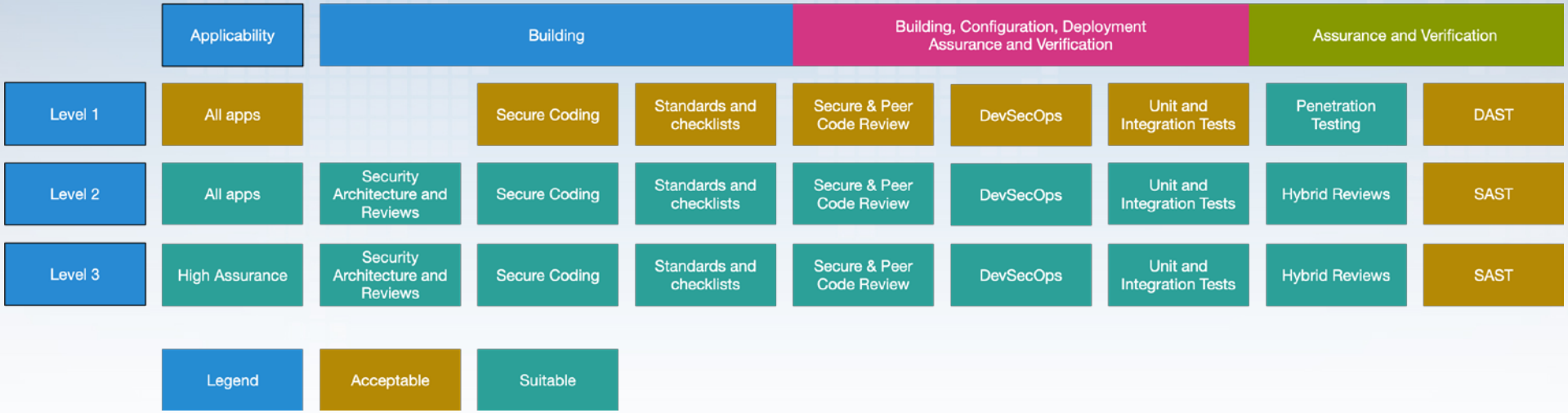
应用安全验证级别 等级2

- 如果应用程序能够充分抵御当前与软件相关的大部分风险，那么应用程序就实现了ASVS 等级2（或标准级）。

应用安全验证级别 等级3

- 如果应用程序充分防范高级的安全漏洞，并且还展示了良好的安全设计原则，它就达到了ASVS 等级3验证标准。
- 这个级别通常保留给需要大量安全验证的应用程序，例如那些在军事、健康、关键基础设施（电力）等领域中的应用程序。

应用安全验证级别



OWASP
Open Web Application Security Project

应用安全验证级别

序号	验证要求描述	1级	2级	3级
8.2.2	验证存储在客户端存储中的数据（如HTML5 local storage、session storage、IndexedDB、常规cookie或flash cookie）不包含敏感数据或个人识别信息。	✓	✓	✓
8.1.2	验证在授权用户访问敏感数据后，保护服务器上存储的敏感数据的所有缓存或临时副本免受未经授权的访问。		✓	✓
8.1.5	验证应用执行了重要数据的定期备份，并执行了数据的恢复测试。			✓

应用安全验证级别

行业	威胁概要	1级建议	2级建议	3级建议
金融和保险	它通常被认为是一个高价值的攻击目标，攻击者通常是出于经济动机。攻击者通常会寻找敏感的数据或帐户凭证，这些数据可以被用来进行欺诈，或者通过利用内置在应用程序中的资金转移功能来直接获利。技术方面通常包括被窃取证书、应用级别的攻击和社会工程学。一些主要的合规事项包括支付卡行业数据安全标准（PCI DSS）、金融现代化法案（Gramm Leech Bliley Act）和萨班斯-奥克斯利法案（SOX）。	所有网络可访问的应用程序。	包含敏感信息的应用程序（例如：信用卡号码、个人信息）可以以有限的方式转移有限的金额。示例包括： （i）在同一机构的账户之间转账； （ii）具有交易限额的较慢形式的货币流动（例如：ACH）； （iii）在一段时间内具有强制转移限制的电汇。	包含大量敏感信息、允许快速转移大量资金（例如：电汇）、以个别交易形式转移大量资金作为一批较小转账的应用程序。

应用安全验证级别

行业	威胁概要	1级建议	2级建议	3级建议
医疗	大多数攻击者正在寻找可用于直接或间接获利的敏感数据，以包括个人身份信息和付款数据。这些数据可用于身份盗用，欺诈付款或各种欺诈计划。 对于美国医疗保健行业，健康保险的便携性和责任法案（HIPAA）规定了隐私、安全、违规通知规则和患者安全规则。	所有网络可访问的应用程序	具有少量或中等数量的敏感医疗信息（受保护的健康信息）、个人身份信息或付款数据的应用程序。	应用程序用来控制医疗设备或可能危及人类生命的设备。支付和销售点系统含有大量的交易数据,可以用来提交欺诈。欺诈通过任何这些应用程序的管理界面进行。

应用安全验证级别

行业	威胁概要	1级建议	2级建议	3级建议
制造、交通运输、技术、公用事业、基础设施和国防	这些行业看起来有很大差异，但是可能在一个阶段，社工威胁更有可能以更多的时间、技能和资源进行集中攻击组织。因为敏感信息或系统不容易定位，需要利用到内部人员和社会工程学技术。攻击可能涉及内部人员，外部人员或两者之间的勾结。他们的目标可能包括获得知识产权的战略或技术优势。我们也不想忽视攻击者滥用应用功能来影响敏感信息系统的行为或中断敏感信息系统。大多数攻击者正在寻找可用于直接或间接获利的敏感数据，包括个人身份信息和付款数据。这些数据可用于身份盗用，欺诈付款或各种欺诈计划。	所有网络可访问的应用程序。	应用程序包含内部信息或员工的可利用在社会工程学攻击方面的信息。应用程序包含非必要的、但重要的知识产权或商业秘密。	包含有价值的知识产权、商业秘密或政府机密（例如：在美国，这可能是秘密或以上的任何分类）的应用程序对于组织的生存或成功至关重要。控制敏感功能的应用（例如：运输、制造设备、控制系统）或有可能威胁生命安全的应用程序。

OWASP ASVS验证规则

分类	等级1	等级2	等级3
V1：架构、设计和威胁建模	0	41	42
V2：认证验证要求	27	52	57
V3：会话管理验证要求	10	18	20
V4：访问控制验证要求	9	10	10
V5：验证、清理和编码验证要求	27	30	30
V6：存储加密验证要求	1	13	16
V7：错误处理和日志记录验证要求	3	13	13
V8：数据保护验证要求	7	15	17
V9：通信安全验证要求	3	7	8
V10：恶意代码验证要求	3	5	10
V11：业务逻辑验证要求	5	8	8
V12：文件和资源验证要求	11	15	15
V13：API和WEB服务验证要求	7	15	15
V14：安全配置验证要求	16	24	25
总计：	129	266	286

V1：架构、设计和威胁建模

- 软件安全开发生命周期。
- 其它13个验证要求从架构设计和威胁建模上的要求。

- 只有第2等级和第3等级。

V2：认证

- V2：身份验证验证要求
  - V2.1密码安全要求
  - V2.2通用身份验证器要求
  - V2.3身份验证器生命周期要求
  - V2.4凭证存储要求
  - V2.5凭证恢复要求
  - V2.6查找密码验证程序要求
  - V2.7带外验证器要求
  - V2.8单因素或多因素一次性验证器要求
  - V2.9加密软件和设备验证程序要求
  - V2.10服务认证要求

V3：会话管理理

- 会话对每一个实体来说是唯一的，不能被猜到或被共享；
- 在非活动周期内，当会话不再被需要或超时时，会话将被无效化。

V4：访问控制

- 访问资源者持有有效身份凭证；
- 用户角色和权限元数据免受重播或篡改。
- 与一组明确定义的角色和特权关联；

V5：验证、清理和编码

- 验证所有输入是正确的，符合预期目的；
- 输入数据是强类型的、经过范围或长度检查验证的，或者在最坏的情况下，应该经过清理或过滤。
- 输出数据根据数据的上下文编码或转义

V6：存储加密

- 所有加密模块均以安全的方式失败，错误被正确处理；
- 当需要随机性时，要使用合适的随机数生成器；
- 使用安全的方式管理密钥的访问。

V7：错误处理和日志记录

- 如无特殊需求，不要收集或记录敏感信息；
- 确保所有记录的信息得到安全处理，并依据它的数据分类 进行合理保护；
- 确保日志不被永远的保存，而是具有尽可能短暂的完整生命周期。

V8：数据保护

- 机密性：保护数据，防止数据传输和储存过程中，有未经授权的查看或披露数据；
- 完整性：保护数据，防止攻击者未经授权的恶意创建，更改或删除数据；
- 可用性：当授权用户需要时，数据是可用的。

V9：通信安全

- 不管传输的数据有多敏感,总是使用TLS和强加密算法。
- 启用最新领先的算法作为首选算法。
- 弱算法或即将被弃用的算法是最后的选择。
- 禁用已弃用或已知的不安全算法。

V10：恶意代码

- 安全和正确地处理恶意行为，以不影响应用程序的其余部分；
- 不要让时间炸弹或其他基于时间的攻击内置于应用程序之中；
- 不要“回拨”到恶意或未经授权的目的地。
- 应用程序不应有后门、“复活节彩蛋”、Salami攻击或遗留可由攻击者控制的逻辑漏洞。

V11：业务逻辑

- 业务逻辑流是连续且有序的；
- 业务逻辑包括对自动化攻击的检测、限制和防治，例如持续的小额资金转移，或一次性添加一百万个朋友等等；
- 高价值业务逻辑流已考虑了滥用案例和恶意行为者，并且具有防止欺骗、篡改、抵赖、信息泄露和提权的保护。

V12：文件和资源

- 不可信文件数据应以安全的方式进行处理；
- 从不受信任源获取的内容存储在webroot之外，并且仅具有有限的权限。

V13：API和WEB服务

- 针对所有Web服务，进行充分的认证，会话管理和授权；
- 从较低信任级别向高信任级别的转换时，需针对所有参数进行输入验证；
- 保证所有API类型的有效安全控制，包括云和无服务器API。

V14：安全配置

- 安全、可重复、可自动化的构建环境。
- 加强第三方库、依赖关系和配置管理，应用程序中不包含过时或不安全的组件。
- 默认使用安全配置。

OWASP ASVS的其它用途

- 作为详细的安全体系结构的指南
- 作为安全编码的清单
- 使用它提供安全开发培训
- 作为自动化单元和集成测试的指南
- 作为指导安全软件采购的框架

OWASP
Open Web Application Security Project