OWASP
Open Web Application Security Project

Web应用安全评估标准
OWASP ASVS

郭振新

自我介绍

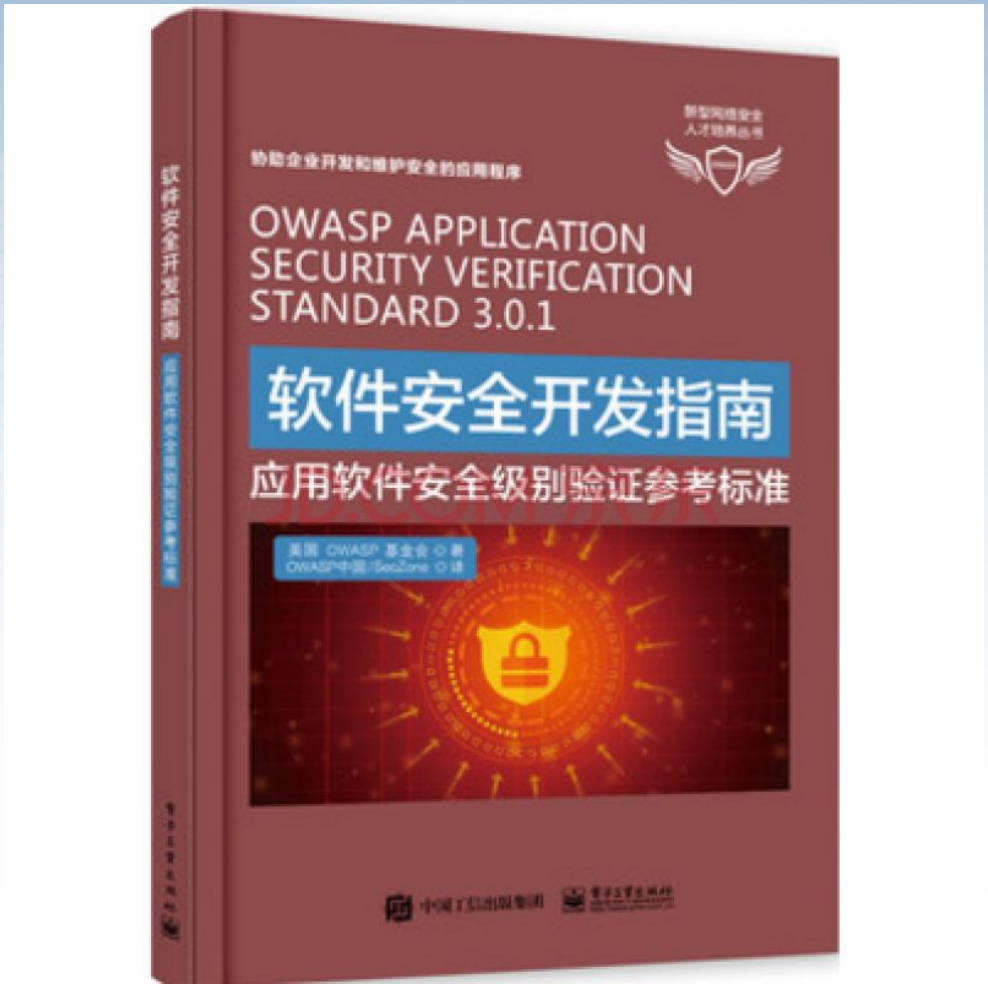
- OWASP ProActive Controls中文项目组成员
- 径点科技——高级研发工程师
- 一个懂安全会渗透的程序员


CONGRATULATIONS!
OFFENSIVE
security
THIS IS TO ACKNOWLEDGE THAT
Zhenxin Guo
IS CERTIFIED AS AN
OSCP
(Offensive Security Certified Professional)
AND HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND CRITERIA FOR SAID CERTIFICATION THROUGH EXAMINATION ADMINISTERED BY OFFENSIVE SECURITY.
THIS CERTIFICATION, EARNED ON
6th of April 2019
Mati Aharoni
This certificate may be verified by contacting orders@offensive-security.com using the certificate holders student ID
OFFENSIVE
security
OSCP
Zhenxin Guo
Certified since 04/2019
OS-101-048163

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，新跃社科大学等等

OWASP ASVS



OWASP
Open Web Application Security Project

OWASP ASVS vs OWASP TOP 10

A2 :2017

失效的身份认证

8

威胁来源 | 攻击向量 | 安全弱点 | 影响

应用描述	可利用性：3	普遍性：2	可检测性：2	技术：3	业务？
攻击者可以获得数百万的有效用户名和密码组合，包括证书填充、默认的管理帐户列表、自动的暴力破解和字典攻击工具，以及高级的GPU破解工具。会话管理攻击很容易被理解，尤其是没有过期的会话密匙。		大多数身份和访问管理系统的设计和实现，普遍存在身份认证失效问题。会话管理是身份验证和访问控制的基础，并且存在于所有有状态应用程序中。 攻击者可以使用指南手册来检测失效的身份验证，但通常会关注密码转储、字典攻击，或者在类似于钓鱼或社会工程攻击之后，发现失效的身份认证。		攻击者只需要访问几个帐户，或者只需要一个管理员帐户就可以破坏我们的系统。根据应用程序领域的不同，可能会导致放任洗钱、社会安全欺诈以及用户身份盗窃、泄露法律高度保护的敏感信息。	

OWASP
Open Web Application Security Project

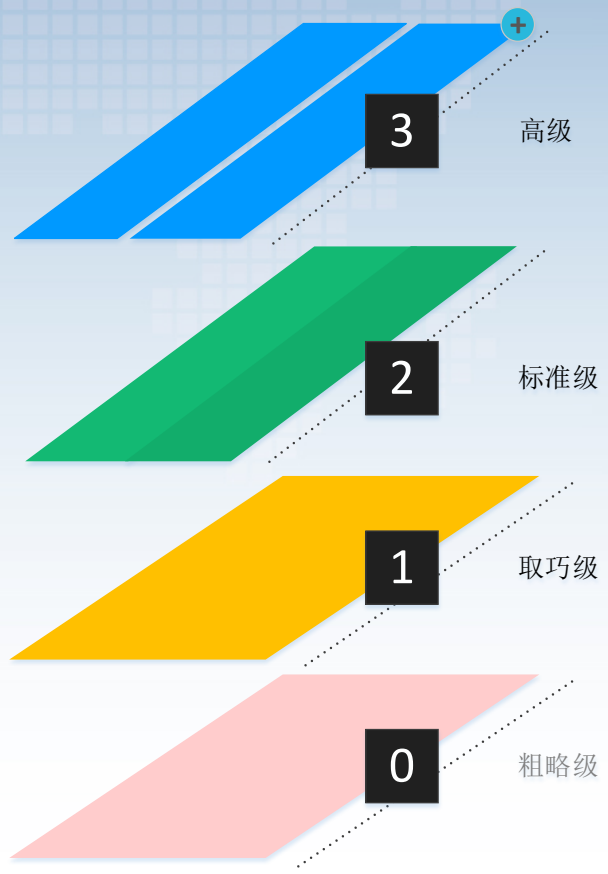
OWASP ASVS vs OWASP TOP 10

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

应用安全验证标准

ASVS为1级及以上验证标准定义了详细的验证要求；而0级验证标准是灵活的、可定制的。



OWASP
Open Web Application Security Project

应用安全验证标准第1等级

- 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 1级（或取巧级）

应用安全验证标准第2等级

- 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 2级（或标准级）。

应用安全验证标准第3等级

- 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 3级验证标准。
- 通常保留给需要大量安全验证的应用程序，例如那些可能在军事、健康和安全、关键基础设施等领域中的应用程序。

应用安全验证标准

行业	威胁概要	1级建议	2级建议	3级建议
金融和保险	尽管这一阶段将经历取巧类型的攻击者的尝试，但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。

应用安全验证标准

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。

应用安全验证标准

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）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（POS）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。

应用安全验证标准

行业	威胁概要	1级建议	2级建议	3级建议
零售、食品、酒店	这一部分的许多攻击者利用投机取巧的“粉碎和抢夺”战术。然而，对于已知含有付款信息，执行金融交易或存储个人身份信息的应用程序，也存在针对特定攻击的常规威胁。虽然不如上述威胁的可能性更大，但也有可能会采取更为先进的威胁来攻击这个行业，窃取知识产权，获得竞争情报，或者与目标组织或商业伙伴在谈判中获得优势。	所有网络可访问的应用程序	适用于商业应用，产品目录信息，内部公司信息和具有有限用户信息（例如：联系信息）的应用程序。具有少量或中等数量的付款数据或结帐功能的应用程序。	支付和销售系统（POS），其中包含可用于提交欺诈的大量交易数据。这包括这些应用程序的任何管理界面。具有大量敏感信息的应用程序，如完整的信用卡号码、姓名、社保号码等。

OWASP ASVS验证要求

V1：架构、设计和威胁建模
V2：认证
V3：会话管理
V4：访问控制
V5：验证、清理和编码
V6：存储加密
V7：错误处理和日志记录
V8：数据保护
V9：通信安全
V10：恶意代码
V11：业务逻辑
V12：文件和资源
V13：API和WEB服务
V14：安全配置

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

- 认证是一种用以建立或者确认某件事物（或者某个人）是否如其所声称的或本身具有的真实行为。

V3：会话管理

- 控制和维护用户与之交互状态的机制，是所有基于Web应用程序的核心组件之一，被称之为会话管理。其被定义为在用户和基于Web的应用程序之间，治理全状态交互的所有控制的集合。
- 确保经验证的应用程序满足如下会话管理的高级别要求：
- 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

- 授权是仅获得许可的实体才被授予资源访问的概念。确保经验证后的应用程序满足如下高级别要求：
- 访问资源者持有有效身份证件；
- 用户与一组明确定义的角色和特权关联；
- 角色和权限元数据免受重播或篡改。

V5：验证、清理和编码

- 最常见的Web应用程序安全性脆弱性是在使用程序输入内容之前，没有正确合理地验证来自客户端或外部环境的输入。这一脆弱性几乎导致了Web应用程序中的所有关键漏洞，如：跨站脚本攻击、SQL注入、解释器注入、locale/Unicode攻击、文件系统攻击和缓冲区溢出。
- 确保经验证后的应用程序满足如下高级别要求：
- 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、经过验证的、范围或长度检查的，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

- 确保经验证的应用程序满足如下高级要求：
- 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，使用合适的随机数生成器；
- 安全的方式管理密钥的访问。

V7：错误处理和日志记录

- 错误处理和日志记录的主要目标是为用户、管理员和事件响应小组提供有用的反应 。其目标不是为了制造大量的冗余日志，而是高质量的日志。
- 高质量的日志通常包含敏感数据，且必须依据当地数据隐私法律或指令进行合理的保护。这应该包括：
- 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。
- 日志中是否包含私有或敏感数据，其界限因国家的不同而不同；日志已成为应用程序所持有的最敏感信息之一，而且它本身对攻击者非常具有吸引力。

V8：数据保护

- 健全的数据保护有三个关键要素：保密性、完整性和可用性（CIA）。本标准假定数据保护在受信的系统上实施（例如服务器），该服务器已被加固并具有充分的保护。
- 应用程序必须假设所有用户设备都以某种方式受到威胁。如果应用程序在诸如共享计算机、电话和平板电脑之类的不安全设备上传输或存储敏感信息，则应用程序负责保证存储在设备上的数据实施了加密，且不能被非法地获取，更改或公开。
- 确保经验证的应用程序满足以下高级数据保护要求：
- 机密性：保护数据，防止数据传输和储存过程中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

- 确保经验证的应用程序满足以下高级别要求：
- 总是使用TLS或强加密，不管传输的数据有多敏感。
- 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

- 确保经验证的应用程序满足以下高级要求：
- 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

- 确保经验证的应用程序满足以下高级要求：
- 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

- 确保经验证的应用程序满足以下高级要求：
- 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

- 确保使用可信服务层api(通常使用JSON、XML或GraphQL)的经过验证的应用程序具有：
- 针对所有Web服务，进行充分的认证，会话管理和授权；
- 从较低信任级向高信任级别的转换时，需针对所有参数进行输入验证；
- 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

- 确保经验证的应用，满足如下要求：
- 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，使过时或不安全的组件不包含在应用程序中。
- 默认安全配置，这样管理员和用户必须弱化默认的安全状态。

OWASP ASVS适用人群

- 安全行业从业者
- 软件测试工程师
- 软件开发工程师
- 架构师
- 教育工作者/培训讲师
- 软件消费者（甲方）
- 软件安全爱好者

OWASP
Open Web Application
Security Project