从应用软件安全角度看待互联网汽车安全

王颉
OWASP中国副主席
SecZone VP

个人简介

王颉

- 英国拉夫堡大学网络安全博士。现任全球顶级安全组织OWASP组织中国区域副主席、深圳开源互联网安全技术有限公司（SecZone）副总经理。
- 主要研究方向包括：软件安全开发全生命周期实时检测防御、威胁分析与建模、网络入侵监测、敏感信息防扩散、企业信息化建设方法等。
- 曾先后在国内外主流学术会议和核心期刊上发表论文15篇、出版联合译著2本、申请发明专利2项，并为超过20个IEEE学术会议担任论文审核专家。
- 曾任英国SZABO软件公司系统架构师、新蛋科技公司信息安全工程师、中石油集团某西南公司信息化建设团队核心成员和信息安全工作负责人。

About OWASP

Every vibrant technology marketplace needs an unbiased source of information on best practices as well as an active body advocating open standards. In the Application Security space, one of those groups is the Open Web Application Security Project (or OWASP for short).

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations are able to make informed decisions. OWASP is in a unique position to provide impartial, practical information about AppSec to individuals, corporations, universities, government agencies and other organizations worldwide. Operating as a community of like-minded professionals, OWASP issues software tools and knowledge-based documentation on application security.

OWASP开源信息

- 应用安全工具和标准；
- 关于应用安全测试、安全代码开发和安全代码审查方面的完整书籍；
- 关于常见风险的Cheat Sheets；
- 标准的安全控制和安全库；
- 全球各地分会；
- 尖端技术研究；
- 专业的全球会议。

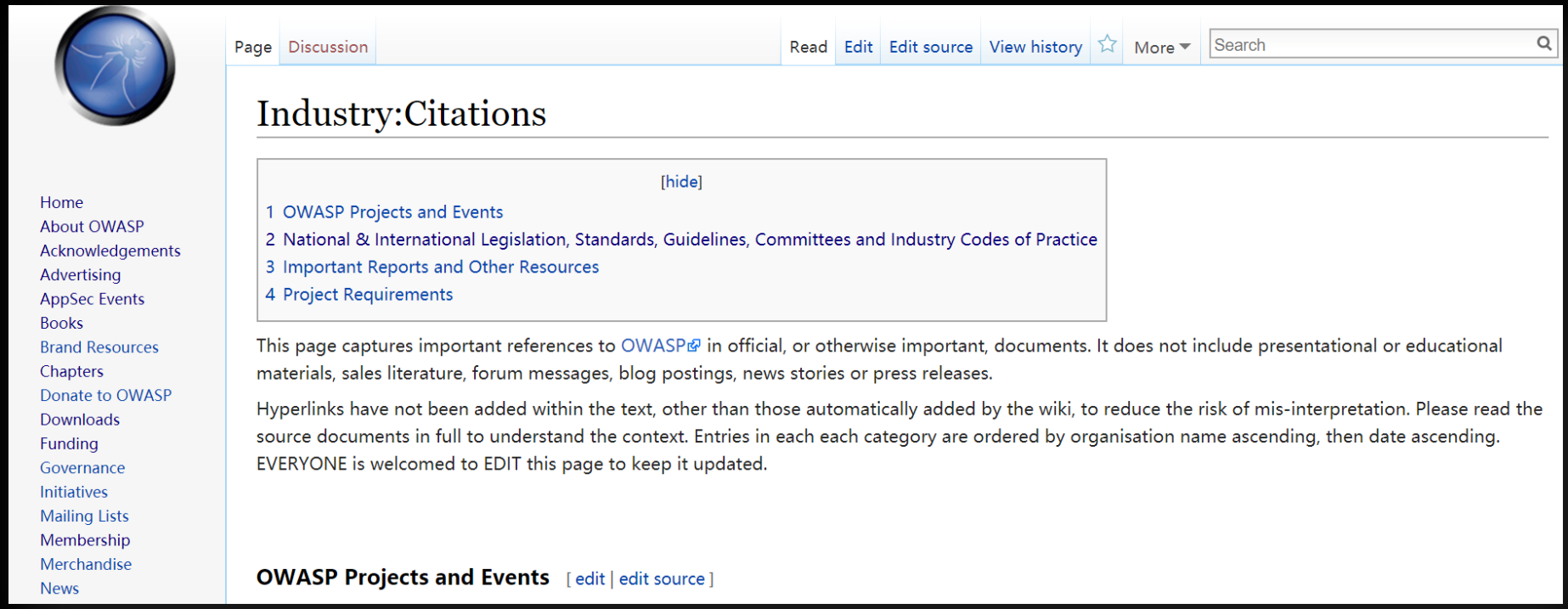

Map
Terrain
Satellite
Suomi
Finland
Iceland
Россия
Russia
Україна
Kazakhstan
Mongolia
China
Korea
Japan
Italia
Italy
Iran
Algeria
Libya
Egypt
Saudi
Arabia
Mauritania
Mali
Chad
Sudan
Nigeria
Ethiopia
Kenya
DR Congo
Tanzania
Angola
Namibia
Botswana
Madagascar
South
Africa
Indonesia
Papua New
Guinea
Australia
New
Zealand
Indian
Ocean
North
Atlantic
Ocean
South
Atlantic
Ocean
South
Pacific
Ocean
Venezuela
Colombia
Perú
Bolivia
Brazil
Argentina

OWASP全球企业会员

OWASP全球学术会员

OWASP权威性

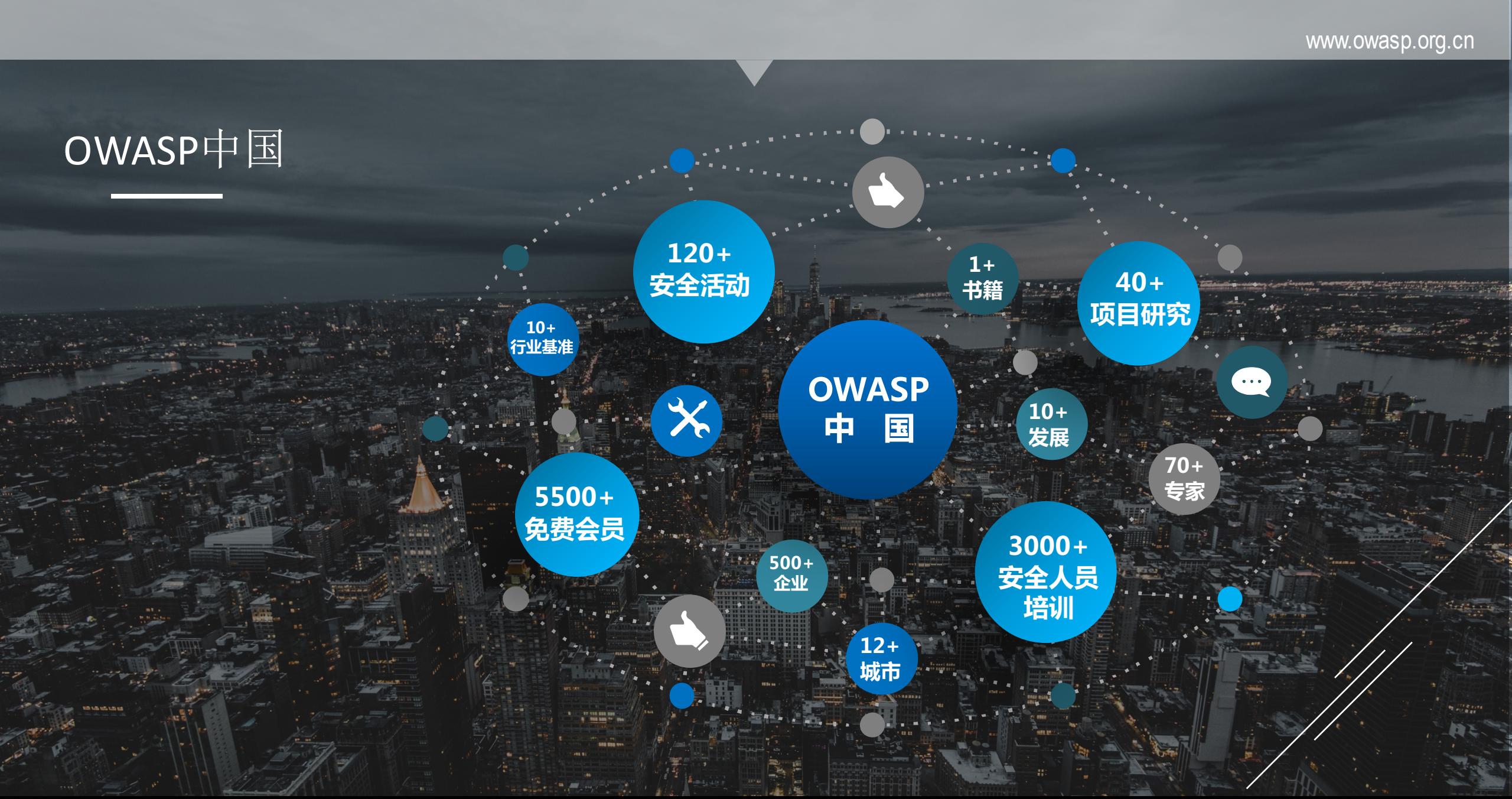
美、欧、日等多个国家的32个政府与行业组织机构引用了OWASP研究成果，形成近百项国际法规、标准、指南和行业行为准则。



目前，OWASP中国正致力于推进我国有关应用软件安全标准的建设。

https://www.owasp.org/index.php/Industry:Citations#National_.26_International_Legislation.2C_Standards.2C_Guidelines.2C_Committees_and_Industry_Codes_of_Practice

OWASP中国


120+
安全活动
1+
书籍
40+
项目研究
10+
行业基准
OWASP
中 国
10+
发展
70+
专家
5500+
免费会员
500+
企业
3000+
安全人员
培训
12+
城市

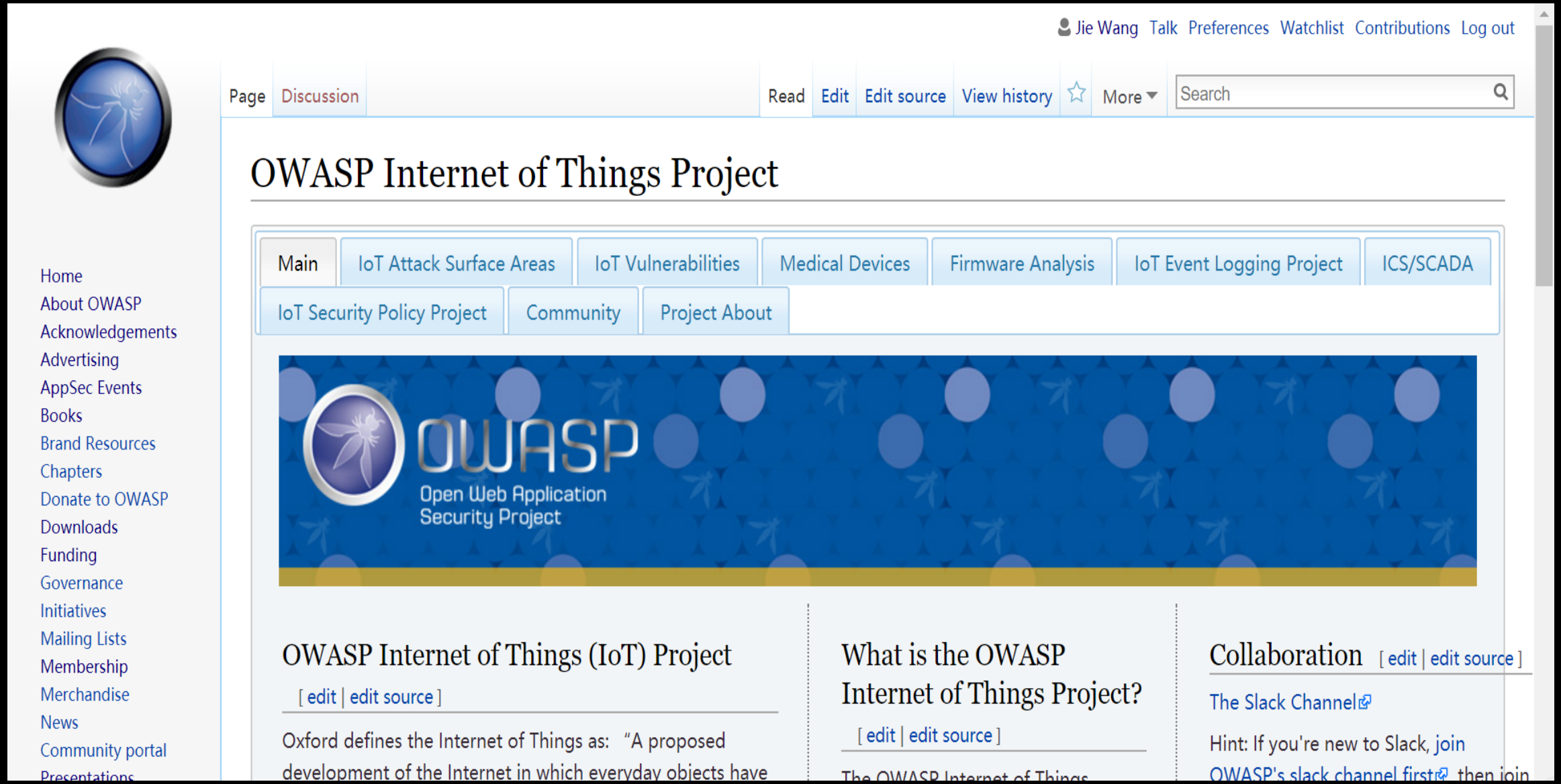
往届峰会照片（2009-2017）

全球十大应用安全风险（2017年版）

全球十大应用安全风险（2017年版）

2017年版《OWASP Top 10》
A1:2017 – 注入
A2:2017 – 失效的身份认证
A3:2017 – 敏感信息泄漏
A4:2017 – XML外部实体（XXE） [新]
A5:2017 – 失效的访问控制
A6:2017 – 安全配置错误
A7:2017 – 跨站脚本（XSS）
A8:2017 – 不安全的反序列化 [新]
A9:2017 – 使用含有已知漏洞的组件
A10:2017 – 不足的日志记录和监控 [新]

全球IoT安全威胁（2017年版）



全球IoT安全威胁（2017年版）

漏洞	概要
用户名枚举	● 能够通过认证交互收集一组有效的用户名。
弱密码	● 如，允许将帐户密码设置为“1234”或“123456”。 ● 使用预先编程的默认密码。
账号锁定	● 能够在3至5次登录尝试失败后，继续发送身份验证尝试。
非加密服务	● 网络服务未作适当加密来防止攻击者窃听或篡改。
双因素认证	● 缺少双因素认证机制，如安全令牌或指纹扫描器。
轻度加密	● 虽然已执行加密，但是该配置不正确或未被能准确更新。例如使用SSL v2 。
非加密更新	● 更新是在没有使用TLS或加密情况下通过网络传输更新文件的。
更新位置为可写	● 更新文件的存储位置为可写，并允许修改固件并分发给所有用户。
拒绝服务	● 服务能够以拒绝该服务或整个设备的服务方式进行攻击。
删除存储介质	● 能够从设备中删除物理存储介质。
无手动更新机制	● 无法手动强制更新检查设备。
缺乏更新机制	● 无法更新设备。
固件版本显示最后更新日期	● 当前固件版本不显示，或者最后更新日期不显示，也有可能两者都不显示。
固件和存储提取	● 固件包含许多有用的信息，例如，运行服务的源代码和二进制文件、预设密码、ssh密钥等。
操纵设备的代码执行流程	● 借助于JTAG适配器和gdb，我们可以修改设备中固件的执行程序，并绕过几乎所有基于软件的安全控制。 ● 侧面通道攻击还可以修改执行流程，或者可以用来获取设备泄漏的有趣信息。
获取控制台访问	● 通过连接到串行接口，我们将获得对设备的完全控制台访问。 ● 通常来说，安全措施包括防止攻击者进入单独用户模式的自定义启动程序，但它也可以绕过攻击者。
不安全的第三方组件	● 使用过期版本的busybox、openssl、ssh、web服务器等。

互联网汽车的安全威胁从哪里来？

X 远距离接入

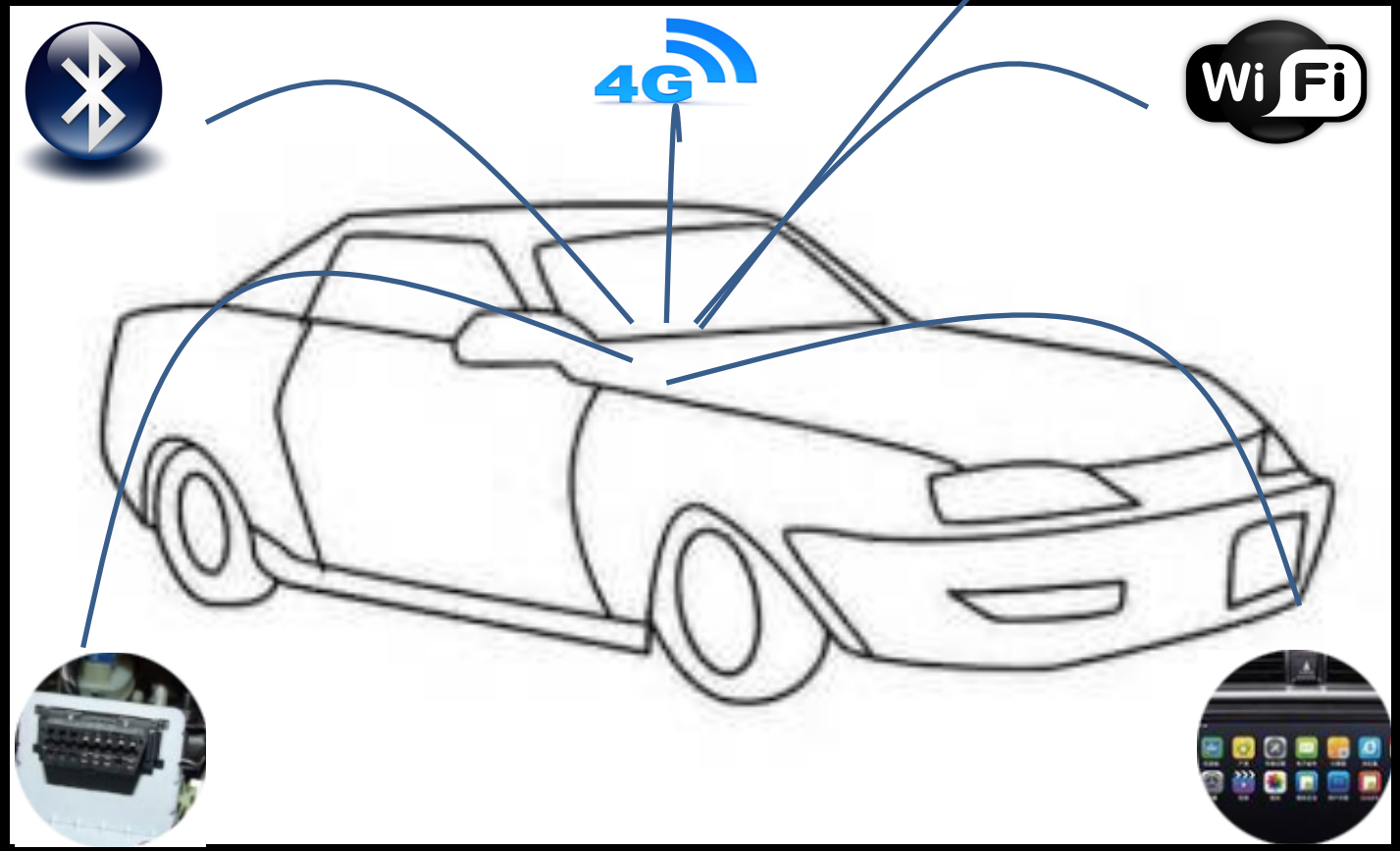
运营商网络

应用和云端TSP

蓝牙

X

近距离接入



Wi-Fi

X

近距离接入

OBD

（车载诊断系统）

X

物理接触

车载应用系统

X

进入汽车总线

对互联网汽车危害的结果

- 干掉引擎
- 控制车辆动力
- 禁用人工介入
- 控制方向盘
- 错误的位置信息
- 系统出错或宕机
- 破解关键技术
- ...

社会危害

想象一下，如果《速度与激情8》中的镜头在现实中真实发生的话....

致命威胁

关键技术被窃取

互联网汽车的应用系统怎么办？

软件安全保障

Software Security Assurance（软件安全保障）

> is the process（流程）of ensuring that software is designed（设计）to operate at a level of security that is consistent with the potential harm that could result from the loss, inaccuracy, alteration, unavailability, or misuse of the data and resources（数据和资源）that it uses, controls, and protects.

------摘自英文Wikipedia网站

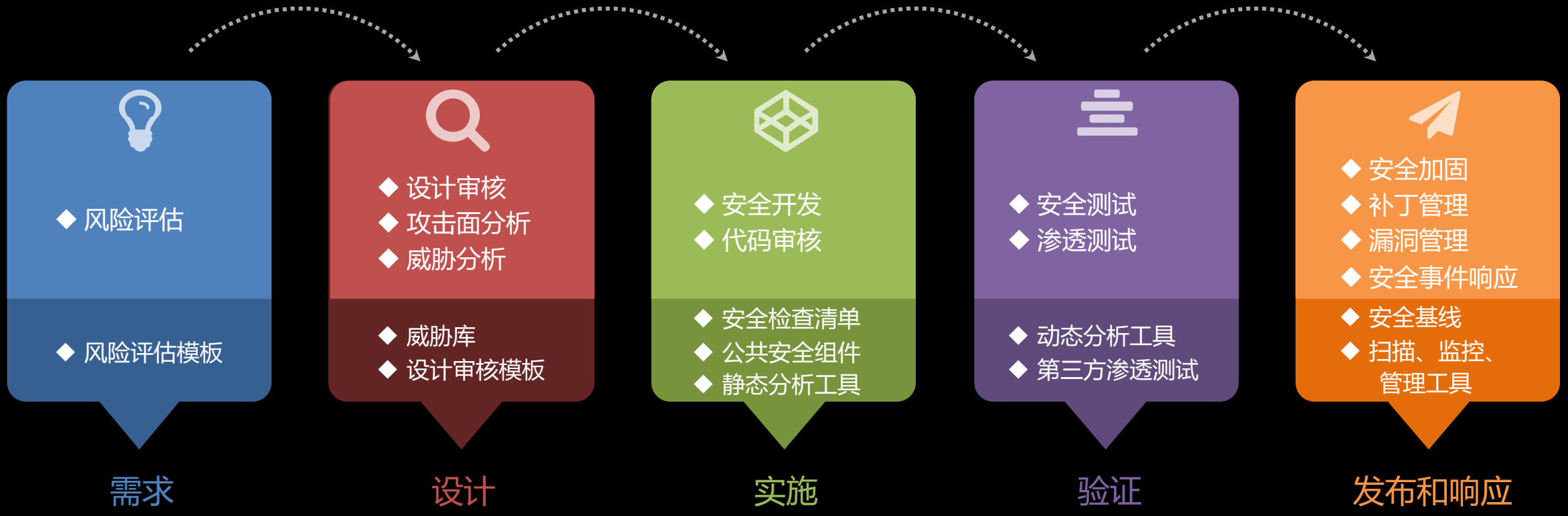
OWASP S-SDLC Project

OWASP S-SDLC Project

- 基本目标：定义一个标准的安全软件开发生命周期，帮助开发人员了解安全软件开发生命周期的每个阶段应该考虑的最佳安全开发实践。

- 最终目标：帮助软件研发类企业在产品研发过程中减少产品的安全问题，并通过方法实践从每个阶段提高产品的整体安全级别。

OWASP S-SDLC Project



培训、政策和组织

https://www.owasp.org/index.php/OWASP_Secure_Software_Development_Lifecycle_Project

提升软件安全开发意识是基本

从互联网汽车应用系统诞生源头维护互联网汽车安全，
是每个应用系统研发者的责任！

致谢

翻译人员：（排名不分先后，按姓氏拼音排列）

- 陈亮（OWASP中国北京地区负责人）
- 王厚奎（OWASP中国广西地区负责人，南宁职业技术学院）
- 王颉（OWASP中国副主席兼成都地区负责人，SecZone）
- 王文君（OWASP中国上海地区负责人，上海观安科技）
- 王晓飞（OWASP中国会员，亚信安全）
- 吴楠（OWASP中国辽宁地区负责人，大连银行）
- 徐瑞祝（OWASP中国会员）
- 夏天泽（OWASP中国安徽地区负责人兼OWASP S-SDLC负责人）
- 杨璐（OWASP中国会员，ThoughtWorks中国）
- 张剑钟（OWASP中国山东地区负责人）
- 赵学文（OWASP中国会员）

审查人员：（排名不分先后，按姓氏拼音排列）

- Rip（OWASP中国主席兼OWASP S-SDLC负责人）
- 包悦忠（OWASP中国副主席）
- 李旭勤（OWASP中国会员）
- 杨天识（OWASP中国会员，中国信息安全测评中心）
- 张家银（OWASP S-SDLC负责人）

汇编人员：赵学文（OWASP中国会员）


软件安全开发指南
协助企业开发和维护安全的应用程序
OWASP APPLICATION SECURITY ASSESSMENT STANDARDS 3.0.1
软件安全开发指南
应用软件安全级别验证参考标准

将于2018年发行

扫一扫

关注OWASP中国


谢谢！