FEYU 蜚语安全

安全服务白皮书

上海蜚语信息科技有限公司

www.feysh.com

蜚语安全是一家专注于提供专业信息安全服务的年轻企业。创始团队脱胎于上海交通大学蜚语软件安全研究组，拥有十数年的前沿安全技术研究和一线安全业务攻防经验。

自成立以来，蜚语安全致力于向全社会输出团队在软件和系统安全方面长期积累的安全能力。在进行商业化探索的过程中，蜚语安全逐渐形成了“以定制化服务为切入点，利用成熟的安全产品和前沿的安全技术来对客户整体信息安全能力进行赋能”的业务体系。

目前蜚语安全提供安全咨询、安全审计、安全培训等多种定制化安全服务，旗下安全产品涉及漏洞扫描、代码混淆、密码白盒、应用安全等多个细分领域，为米哈游、星巴克中国、Cobo 钱包、无他相机、果通科技等合作伙伴提供了长期稳定的安全技术支持。

蜚语安全服务体系

在信息安全领域有一个广为流传的观点—“不知攻，焉知防”。发现安全隐患往往是解决安全问题、提升安全水平的第一步。当企业在现实生产中着手进行信息安全建设时，首先需要回答的问题就是“我们的产品究竟有没有安全问题？”。只有先回答了这个问题，才能够基于这个问题的答案去进一步的探讨如何解决现有安全问题，增强现有安全防护机制，最终提升企业及其产品的整体信息安全水平，减少信息安全攻击事件发生的频率。

为了帮助企业回答“知攻”这个问题，进而实现“知防”、“能防”的目标。蜚语安全利用在网络安全领域十数年积累的前沿安全技术研究和一线攻防经验，为企业提供以下 5 大类信息安全服务：

渗透测试	源码审计	基线评估	安全咨询	安全培训
Web 服务	C / C++		业务安全痛点分析	安全开发
内网环境	Java	快速迭代功能	企业安全建设方向	安全测试
移动应用	Java(Android)	业务模块	产品安全设计改进	CTF 竞赛
IoT 设备	Objective-C	域名接口	行业安全水平调研	专项安全技术
智能合约	Swift	…	安全事件应急响应	…
…	…		…	

从产品的研发角度来说，上述安全服务能够覆盖产品整个软件开发生命周期（SDLC，Software Development Life Cycle）。从产品的立项设计开始，直到产品上线运行，在每一个环节去帮助客户评估测试现有产品或代码的安全水平。

除了帮助企业发现产品现有的安全隐患之外，蜚语安全提供的安全服务还能够从隐患中提炼成因，总结最佳安全实践标准，从而反哺企业的技术人员，赋能企业安全团队，提升企业整体安全能力，使得企业能够在未来打造更加安全的产品与服务，减少受到攻击的风险。

渗透测试

渗透测试是一种以攻击者的角度来对被测试对象进行模拟攻击的安全测试方案。在实施渗透测试时，企业无需提供源代码、设计文档等详细信息，仅需向蜚语安全提供一份功能正常的被检测对象样本（测试环境或生产环境均可）。蜚语安全的渗透专家会模拟黑客的攻击方式对被检测对象进行渗透测试，并于测试完毕后提交一份详细的渗透测试报告。

通过在对业务及产品进行渗透测试，企业可以全面的了解被测试对象在面对当下最前沿（state-of-the-art）的攻击技术时，是否存在安全漏洞，能否被攻击者攻击。在蜚语安全专家的帮助下，企业能够了解这些新发现的安全漏洞

可能带来的风险与危害，在攻击者发现并利用漏洞实现攻击之前进行修补，提升产品与业务的安全水平，减少损失。

在渗透测试过程中，蜚语安全将严格遵守事先与企业协商的授权许可范围，在规定的时间内完成对目标的渗透测试任务。基于蜚语安全长期的渗透测试服务经验，控制测试流程与方法，规避风险，避免影响业务的正常运转。

服务流程

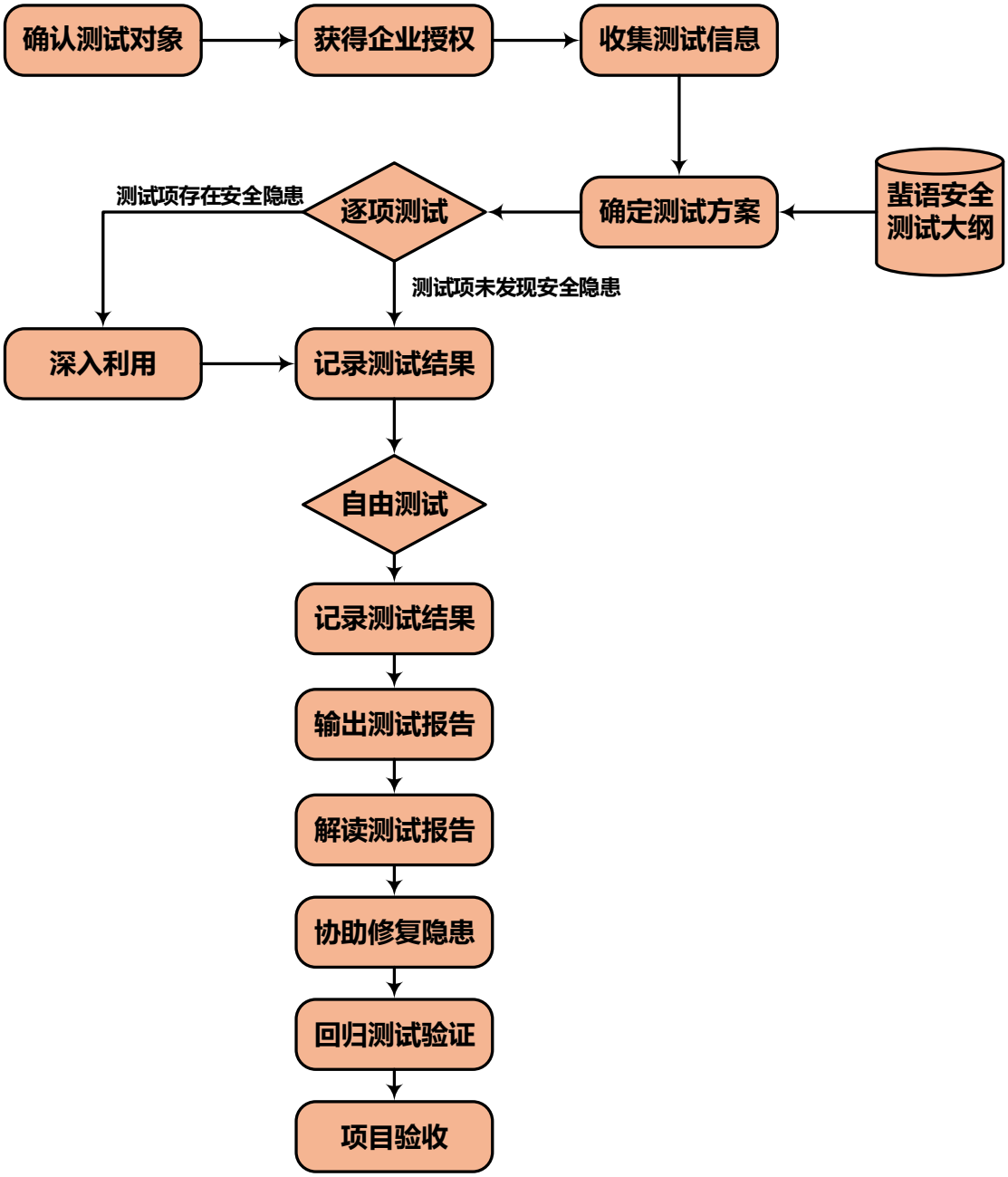

图 1 渗透测试服务流程

服务范围

蜚语安全目前对下列对象提供渗透测试服务：

- **Web 应用渗透测试**

  针对企业开放在公开网络上的网站、应用、业务接口进行渗透测试。测试内容包括但不限于：服务器证书安全、SQL 注入、代码注入、XSS、CSRF、SSRF、XXE、文件包含、文件上传、任意文件读取、密钥爆破、密码学漏洞、业务逻辑漏洞等。

- **内网安全渗透测试**

  通过模拟攻击获取企业内网权限，或在企业提供内网接入权限的情况下，对企业开放在内部网络上的主机、应用、接口等进行安全测试，发现内网中的安全漏洞。测试内容包括但不限于：数据泄露、未授权访问、弱密钥、访问控制失效、密钥爆破等。

- **移动应用渗透测试**

  针对企业旗下的移动平台应用程序进行渗透测试，支持 Android、iOS 多个平台。测试内容包括但不限于：安全配置、组件暴露、数据泄漏、代码安全、权限设置、签名漏洞、动态加载安全、组件安全、密码学误用、native 代码加载、证书安全、通信安全、三方库漏洞等。

- **IoT 设备渗透测试**

  针对企业旗下的 IoT 设备及相关配套组件进行渗透测试。测试内容包括但不

限于：硬件安全、固件安全、OTA 升级安全、操作系统安全、CAN 总线安全（车联网设备）、数据安全、客户端安全、通信安全、身份认证、云端安全等。

- **智能合约渗透测试**

  针对企业发布在常见区块链基础设施上的智能合约进行渗透测试，支持比特币、以太坊等多个常见平台。测试内容包括但不限于：重入漏洞、鉴权安全、变量覆盖问题、逻辑漏洞、数值运算漏洞、拒绝服务攻击安全、密码学误用、短地址攻击等。

服务交付

- **渗透测试报告**

  渗透测试服务的主要交付件为渗透测试报告，渗透测试报告中涵盖了本次渗透测试的基本项目信息和渗透测试细节，报告中会详细描述所有发现漏洞的的成因、影响范围、可能后果，并提供可落地的修复建议。除了发现的漏洞之外，测试报告中还会包括测试过程中所有尝试过的攻击手段和结果。

- **修复指导**

  针对渗透测试中所有暴露出来的安全隐患，蜚语安全均会提供专业的修复指导，帮助企业尽快修复漏洞，抵御攻击。

- **回归测试**

  在企业完成对安全隐患的修复后，蜚语安全负责对渗透目标进行回归测试，

直至所有漏洞确认修复完毕为止。

源码审计

除了渗透测试之外，源码审计也是一种常见的安全测试手段。不同于渗透测试，实施源码审计需要一定的先决条件，其中最为重要的是审计人员需要能够接触到被审计目标的源代码。在能够访问并操作源代码的基础上，审计人员能够实施代码审计、模拟执行、调试、工具扫描等渗透测试时无法执行的操作，这样的优势使得源码审计能够发现那些在渗透测试时难以发现的安全缺陷。

如果说渗透测试的目的是“发现目标系统中确实存在的安全漏洞”的话，那么源码审计的目的则更贴近于“防患于未然”。通过在服务上线前对代码进行源码审计，可以将不安全的因素扼杀在摇篮中，降低服务上线后出现漏洞的概率，同时也能极大的减少后期修复漏洞所带来的成本。

除了挖掘代码中存在的安全漏洞，源码审计还能够发现源代码中不符合安全编码规范的代码片段。这些不符合规范的代码虽然不能直接产生可利用的漏洞，但是会与其他的漏洞组合形成危害更大的组合型漏洞，也有可能会降低系统的整体安全水平从而为其他漏洞的利用带来便利。

服务流程

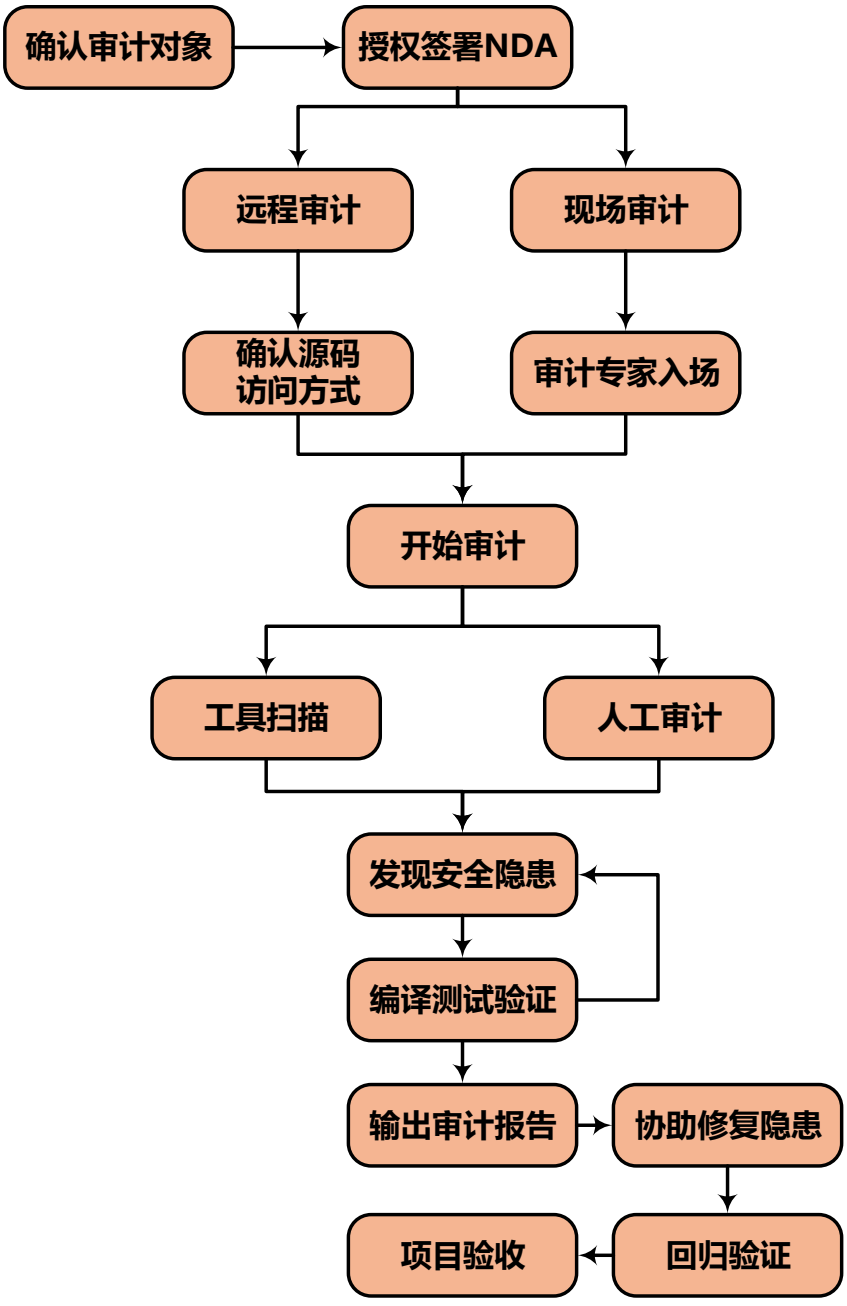

图 2 源码审计服务流程

服务范围

蜚语安全目前对使用以下编程语言编写的业务提供源码审计服务：

C / C++	Java	Java(Android)	Objective-C	Swift
C#	Python	Ruby	PHP	以太坊合约

蜚语安全的源码审计服务参考下列安全编码规范：

1. OWASP 安全开发指南
2. 《软件安全开发标准》（ISO/IEC 27034）
3. 《信息安全技术 应用软件系统安全等级保护通用技术指南》(GAT 711-2007)
4. 《信息安全技术 信息系统安全等级保护测评要求》(GBT 28448-2012)

服务交付

- **源码审计报告**

  源码审计服务的主要交付件为源码审计报告，源码审计报告中会详细描述在该过程中审计专家所使用的技术、工具以及相应的审计结果。

- **修复指导**

  对于审计出来的安全缺陷，源码审计报告会指出安全缺陷的成因和修改建议。帮助企业提升代码的安全质量。

- **回归审计**

  在企业完成对安全隐患的修复后，蜚语安全负责对相关代码进行回归审计，直至所有安全缺陷均得到合理的解决。

基线评估

在现实生产中，有部分企业会面临着旗下业务需要快速迭代的场景，例如电商企业会频繁的推出不同的促销活动，游戏企业会经常性的在游戏内推出新的玩法和活动。这些业务场景的更新频率往往会达到一周一次发版或一周数次发版的程序。对于这些业务场景来说，传统的渗透测试和源码审计服务受限于较长的服务周期（一般规模的业务场景需要 5-10 个工作日来完成测试），无法在业务上线前及时的完成测试工作。而这类业务场景往往与现实生活中的优惠、福利挂钩，会更加受到黑灰产攻击者的重视，更容易受到攻击。

针对这种业务内容高频率变动的场景，蜚语安全专门设计了名为基线评估的快速安全测试服务。通过实现设计的精简测试流程和自动化测试工具，基线评估能够在极短的时间内（1-2 个工作日）完成对目标业务场景的基本安全评估，尽可能的降低发生攻击行为的可能性。

由于基线评估专注于发现常见的、易发的、能够自动化扫描的安全问题，这使得相比起渗透测试和源码审计来说，基线评估具有较低时间和人力成本，适用于对业务内容快速迭代的应用、网站、服务进行定期的安全测试。

服务流程

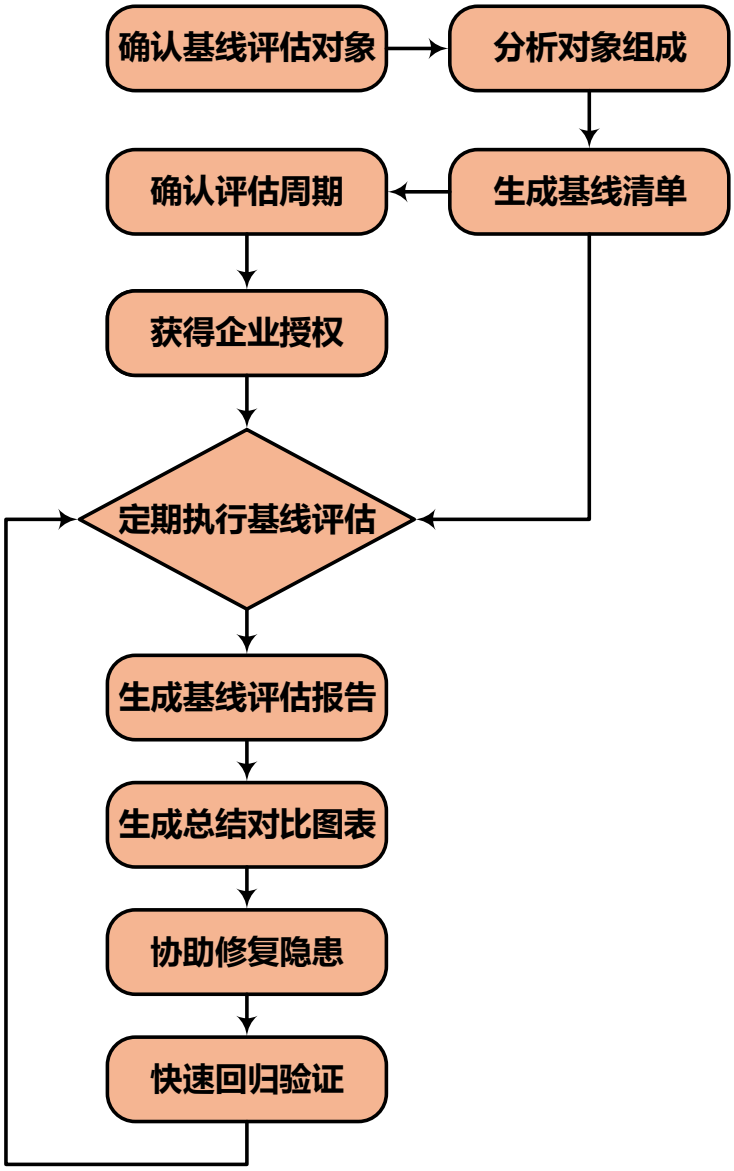

图 3 基线评估服务流程

服务范围

蜚语安全目前对以下场景提供基线评估服务：

- 网站特定页面（活动发布、优惠上新等）

- 特定网络接口
- 移动应用特定模块（如注册登录模块、外卖模块、点单模块等）

服务交付

➢ **基线评估报告**

基线评估服务的主要交付件是基线评估报告，在与企业确定基线评估的范围和频率后，蜚语安全会定期向企业提供评估对象的基线安全评估报告。基线评估报告中会详细阐述蜚语安全为评估对象设计的评估大纲和基线标准，以及评估对象在当期评估中所展现的安全状态。

➢ **总结对比图表**

在每一期的基线评估完成后，蜚语安全会使用精简的图标来展示评估对象在本次评估中的安全状态，并和往期评估结果进行横向对比，帮助企业了解评估对象安全状态的演变和发展。

安全咨询

对于部分刚启动信息安全建设或信息安全能力不足的企业，蜚语安全提供全方位的安全咨询服务。蜚语安全的专家拥有十数年的一线安全研究经验和攻防经验，覆盖 Web 安全、应用安全、系统安全、程序分析、密码学、取证等多个细分领域。能够解决绝大部分场景下企业对于信息安全建设提出的疑问，包括但不

限于业务安全痛点分析、企业安全建设方向、线上产品安全改进、行业安全水平调研、安全事件应急响应等等。

对于所有采购了蜚语安全服务的客户，蜚语安全在服务期内无偿提供基础安全咨询服务。

服务形式

根据企业的需求，蜚语安全提供以下几种安全咨询形式：咨询报告、技术报告、线上答疑、远程会议、线下沟通。

安全培训

为了帮助企业提升自身安全能力，赋能企业自身安全部门，蜚语安全向客户提供全面的信息安全培训服务。

对于缺乏独立安全部门的企业，适合选择基础的安全编码、常见漏洞分析等课程，以提升开发人员的安全意识和安全编码水平，在开发过程中减少漏洞的出现概率。

对于拥有独立安全部门，但是安全部门处于初创时期或能力尚且不足的企业，可以选择常见漏洞检测、安全测试技术、安全开发等课程，以提升安全人员的业务水平，更好的向企业内部输出安全能力。

此外，蜚语安全团队拥有多年的 CTF 参赛经验，团队中多名成员曾是知名

CTF 战队 0ops 的主力选手。蜚语安全也向客户提供 CTF 培训，专项安全技术提升等进阶课程。

服务范围

蜚语安全目前向合作伙伴提供下列培训课程：

信息安全概论	CTF 进阶
安全开发 (C/C++，JavaScript，Java)	软件逆向与程序分析
安全测试 (Android、iOS、Web)	网络协议分析
常见漏洞分析 (Android、iOS、Web)	密码学
CTF 入门	漏洞挖掘与利用

蜚语安全团队荣誉

行业荣誉	
2015	2015 乌云安全峰会主题演讲，有关 Android 自动化脱壳技术
	2015 互联网安全大会主题演讲，有关 Android 系统数据保护技术
2016	发现主流移动支付 SDK（微信、支付宝、银联支付、百度钱包）安全漏洞，获多方致谢
	发现华为、魅族等多款手机 TEE 漏洞
2017	2017 网络安全生态峰会主题演讲，有关移动游戏安全
	2017 腾讯安全探索论坛主题主体演讲，有关 VPN 安全
	2017 互联网安全大会主题演讲，有关智能家居安全
	获蚂蚁金服安全应急响应中心漏洞修复致谢
2018	获京东安全应急响应中心、美团安全应急响应中心、蚂蚁金服安全应急响应中心漏洞修复致
	2018DEFCON 神州安全大会主题演讲，有关智能 Wifi 协议安全
	2018 互联网安全领袖峰会主题演讲，有关智能门锁安全
2019	2019 互联网安全领袖峰会主题演讲，有关内存漏洞扫描
	2019Oppo 大移动安全高峰论坛主题演讲，有关智能电视安全
	小米安全年度最佳守护者团队称号
	2019Real World CTF 技术论坛主题演讲，有关移动设备移机服务安全

团队成员竞赛获奖	
2014	阿里移动安全挑战赛双冠
	参与组建 CTF 战队 0ops，获多个比赛冠军
2015	CodeGate CTF 2015 全球冠军
	Hack.lu CTF 2015 全球亚军
	Defcon CTF 2015 全球季军
	CTFtime 年度排名全球第三
2016	Defcon CTF 2016 全球亚军
2017	H1702 移动安全 CTF 全球季军
	Defcon CTF 2017 全球季军
2018	上海市科技进步一等奖，《互联网软件的安全分析与防护》
	Defcon CTF 2018 第四
	网鼎杯 第四
	全国高校网安联赛 总决赛第一
2019	Defcon CTF 2019 第四
	第一届 sgx 应用创新大赛二等奖-面向 SGX 的程序自动化移植框架