大学生互联网安全创新计划

说明文档

目录

概述

安全是互联网的基石、创新是互联网的生命、大学生是创新的源泉！

伴随着互联网的蓬勃发展，日益增多的互联网安全威胁在影响着整个产业的成长，也在挑战现有的人才培养模式。培养优质的互联网安全人才事关重大，不仅是高校的责任，也是互联网企业和安全行业共同的社会责任和义务。

大学生互联网安全创新计划是**国内互联网企业针对高校的首次大型合作**，该计划将为广大学生提供学习与实践的赛场，让他们了解互联网产业对安全的需求；将促进互联网产业和高校间的对话合作，共同培养具有创新和实践能力的人才；将为互联网安全行业挖掘和输送优秀的人才和新鲜的血液。

创新计划由互联网企业安全工作组发起，中国计算机学会计算机安全专委会指导、多家知名安全公司共同参与，通过每期比赛对互联网安全相关的创新作品和想法进行选拔，为优胜者提供多家业界著名公司(微软、腾讯、百度、奇虎 360、58 同城、绿盟科技、安天)的实习机会及现金奖励。

背景

伴随着互联网的蓬勃发展，日益增多的互联网安全威胁在影响着整个产业的成长，也在挑战现有的人才培养模式。培养优质的互联网安全人才事关重大，不仅是高校的责任，也是互联网企业和安全行业共同的社会责任和义务。

由于互联网安全行业在国内发展时间尚短，广大高校在校生对行业的现状、发展前景了解不深，导致企业对人才的技能需求和高校毕业生所具备的技能产生了偏差，即阻碍了互联网安全人才的就业与发展，也减缓了互联网安全企业的成长速度。因此，急需一个能使高校在校生中潜在的互联网安全从业人员能够接触到国内互联网安全领域最新情况的契机。

通过国内互联网企业的合作，本项目将为广大学生提供学习与实践的赛场，让他们了解互联网产业对安全的需求；将促进互联网产业和高校间的对话合作，共同培养具有创新和实践能力的人才；将为互联网安全行业挖掘和输送优秀的人才和新鲜的血液。

目标

- 推动信息安全教育，促进产学研结合
- 提升大学生对互联网安全的创新热情和能力
- 提升大学生互联网安全相关创意的社会价值和应用价值
- 为有志于投身互联网安全的大学生提供实践的平台和机会
- 引导广大学生从事信息安全事业，培养信息安全人才

项目描述

1. 组织机构

1.1. 汇总

发起单位：互联网安全工作组

组织单位：大学生互联网安全创新计划组委会

协办单位：北京邮电大学信息安全中心、西安交通大学信息安全法律研究中心、国家网络信息安全技术研究所、浙江大学计算机系统结构与网络安全研究所

学术指导：互联网企业安全工作组学术委员会

工程技术指导：互联网企业安全工作组工程技术委员会

比赛平台：www.ISWG.cn

企业支持：阿里巴巴集团、新浪、微软、腾讯、百度、网易、奇虎 360、58 同城、绿盟科技、安天

1.2. 详细

互联网企业安全工作组学术委员会

- 杨义先　教授，　北京邮电大学信息安全中心主任
- 马民虎　教授，　西安交通大学信息安全法律研究中心主任
- 严明　研究员，　中国计算机学会计算机安全专委会主任
- 杜跃进　博士，　国家网络技术研究所所长
- 陈焰　教授，　浙江大学特聘教授
- 郭涛　博士，　中国信息安全测评中心副总工程师
- 马兆丰　博士，　北京邮电大学信息安全中心

互联网企业安全工作组工程技术委员会

- 褚诚云　微软　可信赖部安全工程团队负责人
- 陈起儒　腾讯　腾讯电脑管家高级产品总监
- 周晓波　百度　百度资深架构师
- 刘小熊　奇虎 360　安全顾问
- 窦喆　58 同城　运维总监
- 鲍旭华　绿盟科技　战略研究部高级研究员
- 李柏松　安天　副总工程师

2. 参赛资格

高校在校学生（专科生、本科生、硕士研究生、博士研究生），且报名以及比赛时未在创新计划支持企业实习

3. 报名形式

参赛者以不超过三名成员的小组为单位（不包括指导老师在内）进行在线注册，注册后在系统中选择参赛作品方向及题目，独立完成并提交作品。

4. 参赛作品方向

围绕当前互联网安全热点问题展开(不提倡任何形式的网络攻击)。

具体包括但不限于以下方向：

- 百度：
    - 反病毒技术
    - 反网页及邮件钓鱼

- 腾讯：
  - 网购场景下的立体防御体系
  - QQ 安全
- 微软：
  - 漏洞利用技术及防御技术
  - 双因子认证技术
  - 可信计算及其应用
- 360：
  - 移动互联网
    - APP 安全和隐私
  - 云安全
    - 虚拟化安全
  - 软件安全
    - 缓冲区溢出对抗
    - 数据库安全
  - 业务安全
    - 防拒绝服务攻击
    - 验证码
    - 账号安全
- 58：
  - 信息发布系统的防灌水
  - WEB 防火墙
- 绿盟科技
  - 信息安全 OSINT
  - 应用层拒绝服务攻击和防护方法
- 安天
  - 安全事件的可视化
  - 基于海量数据的安全事件分析
  - 格式溢出的静态检测
  - 移动互联网安全
    - APP 行为监控和分析
    - Android 应用安全保护和加固
    - Android 系统内核安全
    - Android 应用漏洞发现和检测
  - 软件相似性研究
  - 恶意代码基因家族分析
  - 移动操作系统安全加固
  - 漏洞利用代码检测（如何检测 Exploit 代码）

以及任何你认为有创新点的作品和想法!

5. 参赛作品要求

作品提交的形式包括但不限于：代码、演示系统、手机或 PC 软件等。提交的作品必须可验证，或具备可执行性。

6. 参赛作品的知识产权

- 提交作品的知识产权归提交者本人所有；
- 作品的提交和论文的发表不冲突；
- 已在任何比赛中获奖的作品不能再参赛；
- 知识产权不属于参赛者本人或已经商业化的作品，不允许参赛；
- 参赛作品，应向大赛提供所有技术细节。不禁止其申请专利，但专利申请人中不应该有公司；

7. 比赛规则及评审机制

- 初赛
    - 成功提交的作品按照作品方向、所选题目进行分类，根据分类结果制定各类别中可晋级复赛的名额数量；
    - 按照所属类别，将初赛作品转交给负责该类别的工程技术委员会负责人（及其团队）进行评审，选出总共 30 个晋级作品；
    - 晋级作品交由学术委员会进行审核；
    - 在官网上公布晋级复赛的名单及作品。
- 复赛
    - 晋级的小组在负责该类别的工程技术委员会负责人（及其团队）的指导下，完善作品；
    - 完善的作品交由学术委员会进行评审，确定晋级决赛的名单；
    - 在官网上公示晋级决赛的名单及作品。
- 决赛
    - 与颁奖仪式前一天进行现场答辩，由技术委员会及学术委员会现场投票决定名次。
    - 在官网上公布决赛获奖名单及作品。

8. 评审标准

- 原创性和创新性
- 应用潜力
- 技术质量
- 社会影响

由互联网企业安全工作组学术委员会和工程技术委员会，以投票方式选出优胜者。

9. 奖项设置

对作品进入复赛的 30 个参赛小组，奖励如下：

- 证书及奖金：
  - 一等奖：一名，奖金 2 万及“大学生互联网安全创新计划一等奖”证书
  - 二等奖：三名，奖金 1 万及“大学生互联网安全创新计划二等奖”证书；
  - 三等奖：四名，奖金 5000 元及“大学生互联网安全创新计划三等奖”证书；
  - 优胜奖：全国三十强均可获得“大学生互联网安全创新计划优胜奖”证书；
- 实习机会 (由参与计划公司提供)：
  - 前二十名均可优先获得实习机会；
  - 如前二十名中有人放弃实习机会，则实习机会顺延。

时间表

时间		环节	描述
2013 年	4 月 11 日	项目提出	宣布计划总体纲要。
	4 月 11 日至 6 月 27 日	项目改进	更新方案，工作组成员间沟通。
	7 月	项目筹备	确定方案，整合资源，分配任务。
	8 月	项目执行	项目各部分由负责企业/人推进，包括： 媒体宣传、形象设计、校园活动、在线系统等。
	9 月 1 日至 15 日	线上宣传	通过媒体平台进行宣传。
	9 月 16 日至 10 月 13 日	线下宣传及在线报名	启动校园宣讲，并开始线上报名。
	10 月 14 日	初赛开始	开始接受提交作品
	12 月 30 日	初赛结束	停止接受作品提交，开始评审作品。
2014 年	1 月 10 日	初赛结果公布	宣布复赛晋级名单
	3 月 10 日	复赛开始	晋级复赛的小组在导师指导下完善作品
	3 月 30 日	复赛结束	开始评审作品
	4 月	复赛结果公布	宣布决赛晋级名单
	4 月	决赛答辩及颁奖仪式	于工作组年会举办