上海市大学生网络安全大赛组委会

沪网安赛函【2016】1 号

关于举办 2016 年全国大学生网络安全邀请赛暨第二届上海市大学生网络安全大赛的通知

各高等学校：

为宣传普及网络安全知识，提高大学生网络安全防护意识和技能，加强大学生实践能力和创新精神，不断提高网络安全人才培养质量，根据《上海市教育委员会关于公布 2016 年上海高校大学生学科竞赛活动入选名单的通知》（沪教委高〔2016〕25 号文）要求，2016 年全国大学生网络安全邀请赛暨第二届上海市大学生网络安全大赛将于 2016 年 11 月在东华大学松江校区举办。

现将大赛有关事项通知如下：

一、组织机构

主办单位：上海市教育委员会

承办单位：东华大学

协办单位：北京永信至诚科技股份有限公司

赞助单位： 上海勋立信息科技有限公司、骇极安全

二、参赛对象

本次大赛面向全国高等院校，以学校为单位组队参赛。各高校选拔本校在校生（含专科生、本科生、研究生）组成参赛团队，每支参赛队伍由 3 名参赛队员组成，其中包括 1 名队长。如有指导教师（限 2 名以内），请注明。另每队必须设置设领队 1 人，负责与组委会进行沟通竞赛事宜。

三、赛程安排

（一）报名

1. 各高校参赛团队首先访问大赛官方网站（http://www.ichunqiu.com/shwas），进入报名页面，下载报名表，填写完成后发送至邮箱：shwas@qq.com

2. 组委会确认各参赛队资格，并在大赛官方网站公布（http://www.ichunqiu.com/shwas）。

(二)赛前学习

各参赛队伍在报名完成后的次日，便可获得 i 春秋学院(www.ichunqiu.com)为期一周的课程免费学习权限。

（三）预赛

此次大赛预赛时间为 2016 年 11 月 13 日 08:00 至 11 月 15 日 8:00 。预赛为 CTF 在线解题比赛，采取网络答题方式进行，各高校参赛队登录大赛官网（http://www.ichunqiu.com/shwas），点击预赛链接，使用网络报名时注册的帐号密码登录预赛网址进行网络预赛，根据预赛成绩由高至低产生 15 支决赛队，于 11 月 16 日前在官网公布。

初赛竞赛规则如下：

- 采用在线解题模式。
- 解题过程需通过离线分析或在线交互克服技术挑战后获取 Flag，提交验证正确后给予相应分数。
- 比赛结束时依据各参赛队完成的积分决定比赛名次，积分高者获胜。
- 不允许频繁提交 FLAG，提交间隔不小于 5 分钟。

- 若在限定时间内没有队伍解出题目，由主办方给出提示。
- 禁止攻击比赛平台，违者取消此次比赛资格，如果发现平台漏洞，请务必联系主办方。

（四）决赛

决赛采取现场攻防对抗赛形式进行，时间为 2016 年 11 月 26 日。决赛的具体形式和规则、报到时间及比赛地点等内容通过大赛官网发布并通知有关参赛队伍。

1、竞赛规则

- 竞赛平台向每个参赛队提供 1 个网络场景，包含 1 台工作服务器和 1 台 flag 服务器。各参赛队之间的网络场景路由可达。
- 每个参赛队互为攻击方和防守方，参赛队要在防守自己服务器的同时，攻击其它参赛队的防守机服务器。
- 在服务器上存在若干漏洞，攻击成功后，可通过应用服务器连接到 flag 服务器，得到特定位置的 Flag，在平台提供的答题界面提交 Flag。
- Flag 每 5 分钟更新一次，参赛选手需尽快修复漏洞，否则其他队会利用此漏洞重复获得 Flag，造成本队持续失分。
- 每个队伍初始 1000 分，提交 Flag 成功后，表示攻击成功，攻击方得 5 分、被攻击方表示防守失败，被扣 10 分。

2、赛题类型

分类为：包括 web 渗透，漏洞挖掘与利用，等方面。

难度等级为高、中、低。难度分布为高（20%）、中（40%）、低（40%）。

赛题实例：

（1）初级难度

题目名称	社会工程学
题目分类	web 安全、社会工程
难易级别	初级人员
考核知识点	暴力猜解、信息收集
知识点描述	社会工程学是一种人为心理学的攻击手段，本类赛题主要考察参赛队员综合实力包含保护技术以及心理素质。
考核目的	个人资料及其他信息的保护。

（2）中级难度

题目名称	代码审计+上传漏洞
题目分类	WEB 安全
难易级别	在代码编写上有一定的基础的进阶人员
考核知识点	抓包改包、解析漏洞、上传漏洞、代码审计
知识点描述	代码审计：检查源代码中的缺点和错误信息，分析并找到这些问题引发的安全漏洞； 上传漏洞：该漏洞的原因在于代码作者没有对访客提交的数据进行检验或者过滤不严，可以直接提交修改过的数据绕过扩展名的检验。
考核目的	1、查找漏洞，通过漏洞进一步提升权限，考察漏洞的修补。 2、利用上传漏洞可以直接得到网站控制权限，考察上传漏洞的防护。

（3）高级难度

题目名称	缓冲区溢出
题目分类	网络安全
难易级别	对程序代码有深入了解的工程师
考核知识点	逆向工程、缓冲区溢出
知识点描述	逆向工程（又称逆向技术），是一种产品设计技术再现过程，即对一项目标产品进行逆向分析及研究，从而演绎并得出该产品的处理流程、组织结构、功能特性及技术规格等设计要素，其主要目的是在不能轻易获得必要的生产信息的情况下，直接从成品分析，推导出产品的设计原理。缓冲区溢出是一种非常普遍、非常危险的漏洞，在各种操作系统、应用软件中广泛存在。利用缓冲区溢出攻击，可以导致程序运行失败、系统宕机、重新启动等后果。更为严重的是，可以利用它执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作。
考核目的	通过缓冲区溢出获取响应权限执行非授权指令的防护

四、奖项设置

1.团体奖：按决赛每支参赛团队 3 人成绩总和进行排名，产生特等奖 1 名（10000 元奖金或等额奖品）、一等奖 2 名（5000 元奖金或

等额奖品)、二等奖 4 名(3000 元奖金或等额奖品)、三等奖 8 名(1000 元奖金或等额奖品)。

比赛结束后，举行颁奖仪式，为获奖团队和个人颁发上海市教委签发的获奖证书及奖金（或奖品）。

五、有关要求

请各高校高度重视，认真做好大赛的宣传发动和组织工作，将大赛举办相关信息发布在学校网站的首页、论坛，并在校园报刊上刊登有关大赛的信息和报名细则，积极动员学生报名参赛，指定专人负责，精心组织好本校参赛团队的选拔、报名及训练工作。

本次大赛食宿自理，不收取团体及个人任何参赛费用。

六、联系方式

1. 邮箱：shwas@qq.com　　QQ 群：515383635

2. 联系电话：021-67792285（赵老师）021-67792809（李老师）

上海市大学生网络安全大赛组委会

2016.10.10

附件1：

2016年全国大学生网络安全邀请赛暨
第二届上海市大学生网络安全大赛赛制

1.预赛赛制

（1）预赛采用在线解题模式(请关注：www.ichunqiu.com/shwas查看相关信息)，题目为CTF在线解题，采取网络答题方式进行。

（2）队伍中参赛队员通过网页在线答题并提交答案。赛题类型为ctf比赛的五大类：杂项、密码学、Web安全、逆向

（3）最终成绩取参赛团队总分由高至低排列，分数相同情况下，按提交时间算，用时短者排名高于用时较长者，产生15支决赛队。

2.决赛赛制

（1）决赛为网络对抗赛，竞赛平台向每支参赛队提供1个网络场景，包含1台工作服务器和1台flag服务器。各参赛队之间的网络场景路由可达。竞赛题目涉及：Web渗透、漏洞挖掘与利用等。

（2）每支参赛队互为攻击方和防守方，参赛队要在防守自己服务器的同时，攻击其它参赛队的防守机服务器。

（3）在服务器上存在若干漏洞，攻击成功后，可通过应用服务器连接到flag服务器，得到特定位置的Flag，在平台提供的答题界面提交Flag。

（4）Flag每5分钟更新一次，参赛选手需尽快修复漏洞，否则其他队会利用此漏洞重复获得Flag，造成本队持续失分。

（5）每支参赛队初始1000分，提交Flag成功后，表示攻击成功，攻击方得5分，被攻击方防守失败，扣10分。

附件 2：

2016 年全国大学生网络安全邀请赛暨第二届上海市大学生网络安全大赛报名表

指导教师：_____

*参赛学校 ：							
*队伍名称：							
参赛人员							
*姓名	*专业	*年级	*学号	*i 春秋账号	*手机号	*电子邮箱	*备注
							领队
							队长
							队员 1
							队员 2
							其他
							其他
							其他

注意事项：

- 每个参赛队伍填报一张表格，多个队伍参赛，须填写多个表格
- 参赛队伍名称请自行命名，如西北狼人队、激流勇进对等
- 参赛队员须保证信息真实性，决赛现场对各参赛队员身份进行一一核对，包括导师和参赛队长。
- 填写完成后，请统一发送至：shwas@qq.com。
- 各参赛队伍请密切关注 www.ichunqiu.com/shwas 和大赛 QQ 官群（515383635），查看本队是否进入决赛。