总编号：_____

网络安全奖学金申请书

申 请 人 姓 名　　邢浩

学　生　类　别　　大学生

推　荐　单　位　　北京航空航天大学

院 系 所 名 称　　计算机学院

填表时间　2016　年　8　月　26　日

中国互联网发展基金会网络安全专项基金办公室制

填 表 说 明

1. 本表用钢笔填写或打印，要求字迹清楚、端正，内容翔实、准确。

2. 封面总编号由中国互联网发展基金会网络安全专项基金办公室统一编写。

3. 申请人所填内容，由推荐单位负责审核。

4. 学生类别是指大学生、硕士研究生或博士研究生，只能选填一种。

5. 如表格篇幅不够，可另附纸。

6. 申请书中所填奖项、专利和论文等须提供支撑材料，作为附件与申请书一并提交。

7. 提供的支撑材料应属于网络安全。

申请人基本情况表

学生类别	大学生	姓名	邢浩	性别	男	身份证号	370523199508114612
政治面貌	共青团员	出生年月	19950811	民族	汉	学校	北京航空航天大学
院系	计算机学院		入学时间	2013.09		学号	13061174
通信地址	北京市海淀区学院路 37 号 北京航空航天大学		Email	634208109@qq.com		电话	13070118897

主要学历和专业技术实习经历

起止年月	学习、实习单位	学历、学位、职务
2013.9-至今	北京航空航天大学	计算机科学与技术，本科生
2015.12-2016.7	国家计算机网络与信息安全管理中心	工控系统安全项目渗透测试实习生
2016.8-至今	北京启明星辰信息安全技术有限公司	ADlab 攻防实验室实习生

个人自述

（字数不超过 500 字）

我从大二就选择网络安全方向，师从李舟军教授。

从高三起就学习 web 安全相关技术。大一开始编写渗透测试框架及工具，大二成功申报**第八届全国大学生创新创业训练计划项目《可扩展的针对 web 漏洞的自动化渗透测试平台》，结题时获得“优秀”的成绩好评**。暑假开始接触 CTF 赛事，大三开始在国家安全管理中心工控实验室实习。具有丰富渗透测试和 web 漏洞挖掘的实战经验，**在国内多个安全平台提交过大厂商的高危漏洞，发表过多篇有关网络安全的技术文章**。

我参与组建了北航第一支 CTF 战队 lancet，并在初始阶段担任队长，参与了十多项全国比赛，**获得多个奖励**。在战队内主攻 web、密码学、杂项。**在 XCTF2015-2016 赛季，战队的积分进入全国前 20，且我的个人成绩曾达到前 20 名**。

目前的研究方向是 **web 安全、渗透测试和工控安全**（主要是施耐德系列的 plc）。曾作为核心骨干，参与过针对**航天科工、松江污水处理厂、南方电网**等多家企业的渗透项目，并参与了**针对郑州市地铁一号线的渗透与安全评估工作，挖掘了 dz、dedecms 等多个知名框架的高危漏洞，并且为 php 开源组贡献 bug，为 msf 开源项目修复错误模块，而且通过流量分析挖掘了多个施耐德 plc 的漏洞**。

除此之外，还获得**网络空间安全人才技能测评认证证书（CCSSA）、信息安全保障人员认证证书（ISCCC）**。

网络安全相关专业课程信息

课程名称	必修/选修	成绩	考试时间
数据结构与算法	必修	100	2015.1
UNIX 程序设计环境	选修	87	2015.1
计算机组成	必修	84	2015.1
算法设计与分析	必修	94	2015.6
操作系统	必修	87	2015.6
密码学课程实践	选修	82	2015.6
软件工程基础	必修	100	2016.1
编译技术课程设计	必修	83	2016.1
计算机网络实验	必修	82	2016.7
专业名称	计算机科学与技术	专业人数及排名	

竞赛信息

竞赛名称	国际/国内赛事	承办单位	排名	获奖等级	时间
安恒信息首届CTF训练营结业赛	国内	杭州安恒信息技术有限公司	1	一等奖	2015.7.31
2015 EICS+工控系统信息安全攻防竞赛	国内	EICS+工控系统信安全攻防竞赛组委会	7	优秀奖	2015.11
第五届信息安全大赛渗透测试个人赛	国内	中国信息安全测评中心	4	鼓励奖	2015.10.25
“西普杯”京津冀信息安全人才选拔挑战赛-初赛	国内	北京西普阳光教育科技股份有限公司	3	三等奖	2016.4
“西普杯”京津冀信息安全人才选拔挑战赛-决赛	国内	北京西普阳光教育科技股份有限公司	3	三等奖	2016.5
2016 年第九届全国大学生信息安全竞赛	国内	教育部高等学校信息安全专业教学指导委员会&中国信息安全认证中心	3	三等奖	2016.8

学术论文				
论文名称	刊物名称	排名	时间，卷（期），起止页码	
标准				
标准名称	标准类型（国际、国家或行业标准）	排名	是否发布	时间
参加科研项目情况				
项目名称	课题种类	说明		时间
1.《可扩展的针对 web 漏洞的自动化渗透测试平台》	第八届全国大学生创新创业训练计划项目	将渗透测试的功能分层解耦为几个独立的模块，形成自动化流水线，提供插件开发框架以云的方式扩展平台		2014.6-2015.11
2.《功能安全和工业信息安全标准研究和验证平台建设》	工业和信息化部智能制造专项	调研常见 PLC 设备及相关漏洞，对工业控制设备，工厂网络，工业企业业务网络进行渗透测试		2015.9-至今
专利				
专利名称	专利类型	排名	是否授权	时间
在网络安全行业的成就（参加众测、漏洞贡献、开源项目贡献等）				
名称	说明			时间

《面向外网开放的 plc 一种新型的后门》	发表于乌云知识库（wooyun drops）。 文章从 black hat 2015 中获得灵感，研究并设计了针对西门子 plc 的一种后门形式。	2015. 6
《 php 内存破坏漏洞的 exp 编写和禁用绕过》	发表于乌云社区。文章对 CVE-2014-8142 和 CVE-2015-0231 php 内存破坏漏洞的 exp 编写与函数绕过进行详细的阐述，获得业界同行的广泛关注。	2016.4
《打造可扩展的针对 web 漏洞的渗透测试平台 - skadi 》	发表于 freebuf（http://www.freebuf.com/sectool/30886.html）。文章提出了一种基于插件式的 web 漏洞渗透测试平台的架构设计。这种具有创新性的架构设计思想，获得网络安全界一些知名黑客的关注，阿里巴巴的云舒、君立华域的副总经理等一系列圈内人士的邮件质询	2014.4.3
腾讯 DZ 3.2X 后台命令执行漏洞	在后台 ImageMagick 处理图片时，命令被无过滤的拼接，所以可以传入恶意命令（并不是 ImageMagick 的漏洞，是 dz 代码的拼接问题）	2016.6
腾讯 DZ 3.2X 后台代码执行漏洞	dz 某反序列函数没有对 gpc 配置项进行判断，结合 mysql 的宽 utf8 字节截断的特性可以进行序列化字符串内容的逃逸，构造任意变量内容，最终在后台某位置可以执行任意代码。	2016.6
腾讯 DZ 3.2X 前台 xss 漏洞	某反序列函数存在问题，在群组帖子分组的位置可以使用畸形的序列化内容构造任意变量，导致前台 xss	2016.6
腾讯 DZ 3.2X 前台 csrf 任意代码执行 getshell	后台某函数的参数不正确，导致从用户输入中得到 xml 数据并实例化为数组，该数组内容最终会拼接为 include 代码，导致了文件包含引发的代码执行。	2016.7
浙江宇视科技的视频监控系统多处代码执行，命令执行，无需登录	某几处命令执行和代码执行的地方没有对用户输入进行有效过滤，并且没有登录验证	2016.5
友宝（滨系集团）由一个邮箱到内网沦陷	友宝集团某邮箱弱口令，从该邮箱得到的信息构建社工字典，最终沦陷内网，并控制多台业务服务器，甚至拿到董事长敏感信息和售货机固件等等。	2016.2
从外网 ihome 黑入三层内网进入北航核心网络控制全校监控系统	北航某社交网络 ihome 的源码在 github 上泄露，最终通过一系列的代码审计和内网渗透，黑入三层内网，到达核心网络，最终控制了全校的监控系统。	2016.5
Wooyun 网	注册有 hoerwing，7 路公交老司机等多个 id，在 zone 中为人解决问题，小有名气	2013.10-至今

开源语言 PHP 的 bug	https://bugs.php.net/bug.php?id=72680 .gdbinit 中变量的不合理引用，和对更新的不及时导致的 bug，我对这两处 bug 提供了可用补丁	2016.8
发现施耐德 plc 多个弱口令后门	通过分析施耐德 plc 固件更新时的流量得到其多个服务的后门	2015.12
发现施耐德 plc ftp 高危指令执行漏洞	发现某些型号的 plc 可以通过存在后门的 ftp 执行高危指令	2015.12
对 msf 中对于施耐德 plc 的组态上传下载的模块进行了修复	发现 msf 中对于施耐德上传下载组态的模块存在错误，对其进行了修复，并且编写了中间脚本可以让下载的 apx 文件和组态项目的转换	2016.1

获奖情况

奖励种类	获奖项目名称	获奖等级	排名	时间
信息安全竞赛（CTF）	安恒信息首届 CTF 训练营结业赛	一等奖	1	2015.7.31
信息安全竞赛（工控系统）	2015 EICS+工控系统信息安全攻防竞赛	优秀奖	7	2015.11
信息安全竞赛（CTF）	第五届信息安全大赛渗透测试个人赛	鼓励奖	4	2015.10.25
信息安全竞赛（CTF）	“西普杯”京津冀信息安全人才选拔挑战赛	三等奖	3	2016.4
信息安全竞赛（CTF）	“西普杯”京津冀信息安全人才选拔挑战赛决赛	三等奖	3	2016.5
信息安全竞赛（CTF）	2016 年第九届全国大学生信息安全竞赛	三等奖	3	2016.8

教师/导师推荐意见

邢浩同学政治立场坚定，思想品德好，对网络安全方向有极大的研究兴趣。

从本科二年级就跟我学习网络安全领域的相关知识，在我的指导下，成功申报第八届全国大学生创新创业训练计划项目《可扩展的针对 web 漏洞的自动化渗透测试平台》，结题时获得“优秀”的成绩好评。同时，并在乌云知识库、乌云社区以及 freebuf 上，发表过多篇有关网络安全的技术文章，获得网络安全界一些知名黑客的关注与好评。

邢浩同学大二开始接触 CTF 赛事，参与组建了北航第一支 CTF 战队 lancet，参与了十多项全国比赛，获得多个奖励。在 XCTF2015-2016 赛季，战队的积分进入全国前 20，且其个人成绩曾达到前 20 名。他具有丰富渗透测试和 web 漏洞挖掘的实战经验，在国内多个安全平台提交过大厂商的高危漏洞。同时，还获得网络空间安全人才技能测评认证证书（CCSSA）、信息安全保障人员认证证书（ISCCC）。

大三开始在国家安全管理中心工控实验室实习，主要从事 web 安全、渗透测试和工控安全（主要是施耐德系列的 plc）。作为核心技术骨干，参与过针对航天科工、松江污水处理厂、南方电网等多家企业的渗透项目，并参与了针对郑州市地铁一号线的渗透与安全评估工作，挖掘了 dz、dedecms 等多个知名框架的高危漏洞，并且为 php 开源组贡献 bug，为 msf 开源项目修复错误模块，而且通过流量分析挖掘了多个施耐德 plc 的漏洞。

综上所述，我认为邢浩同学网络安全专业知识扎实，技术水平高，实战能力强，特此推荐。

签 字：　李舟军
职称/职务：教授/系主任
研究方向：网络空间安全
院系盖章：

年　月　日

推荐单位意见
签 字： 单位盖章： 年　月　日
中国互联网发展基金会网络安全专项基金专家委员会意见
签 字： 年　月　日
中国互联网发展基金会网络安全专项基金管理委员会意见
签 字： 年　月　日