

# 王沛然

电子邮箱: whilebug@gmail.com

电话: +86-17883693551

博客: <https://www.whilebug.com>



## 教育经历

09/2018 – Present      四川大学（985/211/双一流），成都，中国  
· 网络空间安全学院 2018 级网络空间安全卓越人才班（特招班）  
GPA: 3.89/4.00 必修成绩: 90.72（年级排名 2/172）前五学期

## 获奖经历

- ❖ 2018-2019 年度大学生国家奖学金
- ❖ 2018-2019 年度四川大学学年一等奖学金
- ❖ 2019-2020 年度四川大学学年三等奖学金
- ❖ 2020 年度全国大学生数学建模竞赛四川赛区三等奖
- ❖ 2019 年度全国大学生数学竞赛四川赛区三等奖
- ❖ 2020 年度精英百强比赛精英百强奖

## 研究经历

04/2020 - 现在      黄诚教授研究组，四川大学网络空间安全学院  
项目: 针对浏览器 JavaScript 中的恶意挖矿行为的检测  
◆ 提出了一种检测浏览器 JavaScript 的恶意挖矿代码的静态检测方法;  
◆ 论文已投至 *TrustCom2021 (CCF-C)* 一作;

11/2020 - 现在      李贝贝教授研究组，四川大学网络空间安全学院  
项目: 针对联邦学习中的拜占庭问题的解决方法 (proceeding 版本);  
◆ 提出了一种检测和防范联邦学习中的拜占庭节点的方法;  
◆ 论文已完成, 投至 *ISCC 2021 (CCF-C)* 二作 (导师一作);

11/2020 - 现在      李贝贝教授研究组，四川大学网络空间安全学院  
项目: 针对联邦学习中的非独立同分布问题的解决框架;  
◆ 提出了一种针对联邦学习中的非独立同分布数据的个性化问题的解决方法;  
◆ 论文已完成, 投至 *GlobeCom 2021 (CCF-C)* 通讯领域顶会;

11/2020 - 现在      李贝贝教授研究组，四川大学网络空间安全学院  
项目: 针对联邦学习中的拜占庭问题的解决方法 (Journal 版本, proceeding 版本的扩展);  
◆ 提出了一种检测和防范联邦学习中的拜占庭节点的方法;  
◆ 论文已完成, 拟投至 *TIFS (CCF-A)* 二作 (导师一作) 信息安全领域顶刊;

## 项目经历

03/2021 - 现在      李贝贝教授研究组，四川大学网络空间安全学院  
项目: IoT 隐私保护平台  
◆ 开发应对 IoT 环境中的泄露用户隐私和 IoT 环境隐私的隐私保护平台;  
◆ 作为组长带领项目组研究和开发, 提高了项目管理组织能力和表达展示能力;  
◆ 拟参加 2021 年信息安全国赛-作品赛/中国大学生计算机设计大赛/强网杯/互联网+;

11/2019 - 2020/11      黄诚教授研究组，四川大学网络空间安全学院  
项目: 基于机器学习的国产系统终端态势感知平台  
◆ 利用 Osquery 开发基于机器学习的操作系统攻击检测系统;

- ◆ 作为组长带领项目组研究和开发，提高了项目管理组织能力和表达展示能力；
  - ◆ 2020 年精英百强比赛**精英百强奖**；
- 11/2020 - 现在      **徐新建**教授研究组，四川大学文学与新闻学院  
项目：**重建文化记忆——李劫人“大河三部曲”的文学人类学考察研究**
- ◆ 在项目中对项目使用统计数据进行分析；
  - ◆ 2021 年四川大学**国家级大学生创新创业项目**；
- 11/2020 - 现在      **曹麒麟,赵永红**教授研究组，四川大学商学院&四川大学数学学院；  
项目：**智能投顾自动再平衡频率研究——基于沪深数据和用户画像分析**
- ◆ 对智能投顾的再平衡频率进行研究，提出了一种计算智能投顾再平衡频率的方法；
  - ◆ 作为组员负责人工智能模型的构建与实施；

## 出版物

1. 针对浏览器 JavaScript 中的恶意挖矿行为的检测相关论文(论文已投稿至 *TrustCom 2021 CCF-C*)
2. 联邦学习中的拜占庭防御相关论文（论文已投稿至 *ISCC 2021 CCF-C*）
3. 联邦学习的非独立同分布问题的解决框架相关论文（论文已投稿至 *GlobeCom 2021 CCF-C*）
4. 联邦学习中的拜占庭防御相关论文（论文拟投稿至 *TIFS CCF-A*）

## 研究兴趣

- 人工智能安全：联邦学习\联邦学习中的安全问题\联邦学习的非独立同分布问题\成员推断攻击
- 数据驱动安全：恶意代码分析技术\网络犯罪\地下经济分析

## 语言技能

01/2021	IELTS	R: 8.5	L: 8.5	S: 6.5	W: 5.5	<b>Total: 7.5</b>
09/2019	CET-6	<b>Total:540</b>				
01/2019	CET-4	<b>Total:599</b>				

## 掌握技能

**研究技能：**深度学习/论文写作（LaTex）/文献阅读/项目管理(git)/渗透测试/数据库部署(mysql)/PPT 制作/报告撰写

**偏好编程语言：**C/Python/JavaScript/HTML

**专业技能：**SQL 注入/CSRF 攻击/XSS 攻击/流量分析/逆向工程/Pwn

## 自我陈述

进入四川大学后，通过开学选拔进入网络空间安全卓越人才班。在第一学年，获得了国家奖学金和四川大学年度一等奖学金。在平时的课程中，积极回答老师问题，参与课堂互动。同时在专业课程项目中均担任组长，锻炼自己的管理能力和团队协作能力，并且均取得了不错的成绩。在项目的汇报过程中，总是担任上台汇报的职责，很好地锻炼了自己的表达能力和上台演讲能力。

先后参与了黄诚老师与李贝贝老师的课题组研究。在黄诚老师课题组进行恶意代码检测相关研究，一篇论文在投。在李贝贝老师课题组进行联邦学习相关研究，三篇论文在投。在研究过程中，培养了自己的论文阅读技巧和习惯，增强了研究能力。