

# 游宇凡

✉ youyf21@mails.tsinghua.edu.cn · 🌐 ouuan · 🏠 2003.1.26

## 🎓 教育经历

🏫 清华大学 致理书院 信息与计算科学 本科 2021.9 — 2025.6 (预期)

## 🔬 科研经历

**ZIP 文件格式解析歧义安全问题** 导师：陈建军 2023.10 — 至今

- 测试发现了不同 ZIP 文件解析器（解压软件）之间的大量解析歧义问题
- 发现了绕过杀毒软件、邮件安全网关检测，绕过扩展市场发布者 ID 认证，造成 Office 文档显示差异绕过审核机制，伪造 Office 文档签名等多个不同场景下的安全漏洞
- 上报漏洞后已得到 Gmail、Coremail、Go 等厂商的确认，获得了漏洞赏金和 CVE 编号
- 研究成果预计将以一作身份发表论文

**基于代码属性图的 PHP 程序污点型漏洞挖掘** 导师：陈建军 2023.7 — 2023.9

- 使用基于代码属性图的 PHP 代码静态分析方法，对一些开源项目进行漏洞挖掘
- 对现有漏洞挖掘工具进行了优化和修复，提升了工具的易用性、效率和准确性
- 在 8 个开源项目中发现了 SSRF、XSS、Path Traversal、SQLi、DoS、CSRF 等类型的多个漏洞
- 对漏洞进行了上报，申请到 4 个 CVE，并获得了漏洞赏金

## 📊 学业成绩

- 计算机专业课 GPA 3.96 / 4.0，其中 8 门课程获得 A+。参与了大量课程项目，在实践中学习巩固了安全、网络、系统、数字逻辑、软件工程等各领域专业知识，并培养了出色的工程开发和团队协作能力。
- 修读了数学分析、高等线性代数、抽象代数、概率论、常微分方程、拓扑学等为数学专业开设的高难度数学课。
- 计算机专业课成绩如下：

计算机网络原理	A+	现代密码学	A+
操作系统	A+	计算机系统概论	A+
程序设计训练	A+	软件工程	A+
数字逻辑设计	A+	数字逻辑实验	A+
网络空间安全导论	A	计算机网络安全技术	A
离散数学(2)	A	离散数学(1)	A-
数据结构	A-	形式语言与自动机	A-
数值分析	A-	计算机组成原理	B+

## </> 课程项目

**路由器安全漏洞验证** 网络空间安全导论 单人（漏洞验证） 2024.5 — 2024.6

- Python (Scapy)
- 搭建测试环境，编写发包脚本，对两款路由器分别进行实验，验证了它们受 *Man-in-the-middle attacks without rogue ap: When wpas meet icmp redirects* 和 *Exploiting Sequence Number Leakage: TCP Hijacking in NAT-Enabled Wi-Fi Networks* 两篇论文所提出的漏洞影响，能被用于实施流量劫持、拒绝服务等攻击
  - 上报了漏洞，申请到 4 个 CVE

**操作系统内存管理组件的形式化验证** 操作系统 单人项目 2024.4 — 2024.6

- Verus / Rust, OS
- 学习了解现有的 OS 形式化验证相关工作，尤其是学习了 Verus 的使用
  - 使用 Verus 工具和 Rust 语言为 ArceOS 编写了经验证的内存分配器组件，并将他人编写的经验证的页表接入 ArceOS，从而构建出了内存相关组件经形式化验证的操作系统

## IPv6 硬件路由器 计算机网络原理 & 计算机组成原理

三人合作（队长） 2023.10 — 2024.1

SystemVerilog / C, Networking / RISC-V CPU

- 在 FPGA 开发板上实现 IPv6 硬件路由器，支持四口 1Gbps 线速转发，并能存下全网路由表（约 20 万条表项）
- 使用硬件描述语言实现邻居发现协议、转发逻辑、树状转发表流水线查询，以及 RISC-V 五级流水线 CPU
- 软件实现 RIPng 路由协议以及路由表数据结构的维护，通过 DMA、MMIO 等软硬件接口与路由器进行通信
- 我的贡献：队长，负责全部的软件部分以及路由器硬件部分的约一半工作量（CPU 硬件实现主要由队友负责）

## Chrome 小恐龙体感游戏 数字逻辑设计

两人合作 2023.4 — 2023.6

SystemVerilog

- 使用硬件描述语言在 FPGA 开发板上实现 Chrome 小恐龙体感游戏
- 使用外置传感器检测玩家动作控制小恐龙，游戏逻辑由硬件执行，画面通过 VGA 显示
- 我的贡献：负责传感器模块组装调试，以及传感器和画面显示部分的代码实现

## GIF 图片搜索网站 软件工程

五人合作 (队长) 2023.3 — 2023.5

Nuxt (Vue / TypeScript) / Python (Django / Flask) / Docker

- 具有图片上传管理、搜索查看、AI 处理等功能，以及订阅、点赞、评论、私信等社交功能
- 前端使用 Nuxt 框架 (Vue) 以及 Naive UI 组件库
- 后端 API server 使用 Django 框架，图片处理使用 Flask 框架
- 使用 Docker 部署了前后端服务以及 PostgreSQL、Elasticsearch
- 我的贡献：和另一位同学一同负责前端开发，并作为队长主管总体设计，协调团队合作，协助队友修复 bug

## Wordle 游戏 & 在线评测系统 程序设计训练

单人项目 2022.8 — 2022.9

Rust (egui / Actix) / Vue

- Wordle 游戏：包括命令行 CLI 界面和原生 GUI 界面（使用 egui 框架），以及基于信息熵算法的自动求解器
- 在线评测系统：后端使用 Rust Actix 框架，前端使用 Vue，支持提交代码查看评测列表、结果、排行榜，使用 SQLite 持久存储数据，采用非阻塞评测任务队列

## 🏆 荣誉奖项

清华大学第七届网络安全技术挑战赛 (THUCTF2023)	特等奖	2023.10
致理书院科技创新优秀奖学金		2022-2023 学年度
清华大学第二十六届智能体大赛	八强	2022.3
第 37 届全国青少年信息学奥林匹克竞赛 (NOI2020)	银牌	2020.8

## 🔗 开源贡献

在 GitHub 上维护了若干项目，并参与贡献了大量项目，历史总计 PR 669 个，issue 442 个，并在科研、学习内外上报了若干安全漏洞，总计获得 11 个 CVE。部分项目如下所示：

**Codle** 🔗 ouuan/codle ★48 Vue / TypeScript 个人项目 2022.3 起

仿照 Wordle 的设计，基于抽象语法树的代码内容猜测游戏

**CP Editor** 🔗 cpeditor/cpeditor ★1.7k C++ / Qt 首席维护者 2019.12 起

为算法竞赛设计的代码编辑器，核心功能包括从网站获取测例、编译代码、运行检查测例、提交代码等

**OI Wiki** 🔗 OI-wiki/OI-wiki ★19.3k 核心贡献者 2019.3 起

算法竞赛知识点教程、百科

## ⚙️ 专业技能

编程语言 C++ / C / Rust / TypeScript / Vue / Python / Shell / SystemVerilog / x86 / RISC-V / MATLAB

工具 Linux（日常桌面主力使用，并有维护个人服务器）/ Git / Docker / Neovim / LaTeX / Typst / .....

语言 全国大学英语六级考试 (CET6) 567 分 / 阅读过大量英文原版计算机教材和论文