谢远峰

(+86) 186-3089-7985 籍贯:广西； 民族:汉； 年龄:24
xyf20010811@163.com happytraveller3312@gmail.com
happytraveller-alone happy-traveller

教育背景（研二在读）

2019.09 - 2023.06 | **天津大学** · 智能与计算学部 · 网络安全专业 · 全日制 · 本科
2023.09 - 2026.06 | **天津大学** · 智能与计算学部 · 电子信息专业 · 全日制 · 硕士研究生

项目经历

浏览器 JavaScript 引擎的模糊测试改进 **研究课题** 2021.09 – 2022.04

- **对照实验复现：** 基于 SOAT 改进, 完成 V8 引擎测试环境部署, 环境部署文档
- **实验优化与复盘：** 获取测例覆盖率; 复盘已有 V8 引擎 CVE 和模糊测试反馈结果
- **阶段成果：** 输入语料精简优化, 捕获谷歌引擎的逻辑漏洞并获得修复反馈

关系型数据库缺陷的实证研究 **研究课题** 2022.12 – 2023.11

- **关系数据库统一架构：** 综合 Mysql, Sqlite 等框架形成关系数据库完整逻辑框架
- **关系数据库缺陷收集：** 收集缺陷的表征, 代码和问题模块, 构建数据集
- **缺陷实证研究：** 针对 777 个缺陷进行多维度分析, 聚焦 SQL 数据类型缺陷
- **模糊测试框架改进：** 基于缺陷特点，改进 SOTA 方法测试 SQL 数据类型错误
- **阶段成果：** 构建数据集, 构建 SQLT，论文在投（学生二作）

浏览器 JavaScript 引擎 WASM 模块漏洞挖掘 **研究课题** 2023.11 – 2024.4

- **WASM 语法抽取：** 阅读标准, 手动编写文法规则, 用于测试样例生成
- **浏览器引擎调研：** 调研主流 JS 引擎 WASM 支持, 并收集相关 CVE 分析
- **WASM 二进制框架构建：** 利用谷歌 JS 内核 V8 构建简单的 WASM 二进制
- **阶段成果：** 完成语法规则 , 调研报告, WASM 二进制构建框架，捕获特性缺陷并修复

基于 RFC 约束违反的 SSL/TLS 协议模糊测试 **研究课题** 2024.4 – today.

- **相关工作梳理：** 整理 TLS 协议模糊测试，基于状态机的网络协议模糊测测试
- **历史漏洞调研：** 复现历史修复漏洞, 了解 TLS 报文结构, 溯源漏洞代码
- **RFC 文档规则抽取：** 抽取 RFC 文档规则, 构建状态转移范式, 补充有限状态机
- **阶段成果：** 完成相关工作调研, 漏洞复现报告, 状态范式数据集

从安全缺陷到 poc 构造实践 **研究课题** 2024.4 – today.

- **相关工作梳理：** 查找 HTTP 协议相关 RFC 文档，调研相关开源实现
- **历史漏洞调研：** 搜集相关漏洞, 了解 HTTP 报文结构及漏洞问题
- **代码知识库搜索：** 构建开源代码实现与 RFC 文档规则映射
- **阶段成果：** 中选网络安全资助计划, 完成相关工作调研, 映射方法框架

专业技能

- 英语水平：CET6
- 编程语言：C、C++、RUST、WebAssembly
- 科研领域：网络协议，模糊测试，浏览器引擎，编译器