

第一届湖南省研究生网络安全创新大赛校赛推荐汇总表

序号	参赛队名	作品类别	作品名称	级别	备注
1	知行合一	创意作品赛	知忆 EduMemory—面向教育智能体的长期记忆投毒防护与可信更新系统	一等奖	推荐参加省赛
2	智审未来队	创意作品赛	隐枢CipherNexus—隐私成本感知的智能威胁审计与可验证证据链平台	二等奖	推荐参加省赛
3	棱镜戍卫	创意作品赛	契约哨兵-面向银行授信智能体的任务级授权与数据泄露防护平台	二等奖	推荐参加省赛
4	智慧的盾	创意作品赛	智盾先锋-智能体skill审核官	二等奖	推荐参加省赛
5	勾达队	创意作品赛	基于LLM的SSH蜜罐诱捕	三等奖	推荐参加省赛
6	PDCA科研实战队	创意作品赛	VulFix Verify	三等奖	推荐参加省赛
7	羽网先锋队	创意作品赛	RAGShield 知识增强大模型安全防护与持续评测平台	三等奖	推荐参加省赛
8	对勾队	创意作品赛	基于区块链存证功能的数字取证系统	三等奖	推荐参加省赛
9	哈基米米队	创意作品赛	PromptShield • 面向大模型应用的提示词注入攻击级联检测与防御网关	三等奖	推荐参加省赛
10	追光计划	创意作品赛	面向网络安全日志分析与攻击行为溯源的可运行软件系统解决方案	三等奖	推荐参加省赛
11	火烧猪肉干巴队	创意作品赛	盾流 SentinelFlow	三等奖	推荐参加省赛
12	信界卫士	理论创新赛	大模型工具调用链的动态风险控制与闭环评估	一等奖	推荐参加省赛
13	哪都通队	理论创新赛	UTSA：基于样本构造的去中心化联邦遗忘触发攻击	一等奖	推荐参加省赛
14	封神英雄榜	理论创新赛	校准污染与分布漂移下大模型智能体工具授权的条件风险认证	一等奖	推荐参加省赛
15	KSKBL	理论创新赛	面向大模型代码智能体的漏洞发现可信度建模与执行证据验证方法研究	二等奖	推荐参加省赛
16	赤霄智卫	理论创新赛	同源检索投毒的精确鲁棒认证与最小破坏成本	二等奖	推荐参加省赛
17	数盾先锋	理论创新赛	基于LBP-LSB协同优化的动态不可见后门攻击方法	二等奖	推荐参加省赛
18	我要发顶刊	理论创新赛	基于授权见证的多智能体信任洗白约束方法	二等奖	推荐参加省赛
19	漫游队	理论创新赛	后门检测中名义5%误报率的保证语义与校准	二等奖	推荐参加省赛
20	零空间队	理论创新赛	《Adaptation Is Never Free: 深度学习适应机制的后门攻防二重性理论——以可塑性干预与 LoRA 定制化为例》	二等奖	推荐参加省赛
21	码上安全队	理论创新赛	开放集入侵检测的可检出边界与告警队列可用性	二等奖	推荐参加省赛
22	无敌小分队	理论创新赛	差分隐私随机梯度下降的效用损失机制归因与配置依赖性	二等奖	推荐参加省赛
23	泰来	理论创新赛	面向部分可观测多智能体系统的隐式协同安全风险传播与级联抑制方法	二等奖	推荐参加省赛
24	深藏不露	理论创新赛	面向大模型代理的高阶相关失效风险证书与预算约束动态调度	二等奖	推荐参加省赛
25	最吃压力队	理论创新赛	面向受限网络操作的协议约束可逆程序编译与执行语义一致性验证	三等奖	推荐参加省赛
26	智创	理论创新赛	不完整密码资产清单下的鲁棒后量子密码迁移优化理论与方法	三等奖	推荐参加省赛
27	重见天日	理论创新赛	基于检索风险评测与工具调用归因的大模型智能体间接提示注入防护系统	三等奖	推荐参加省赛
28	我超威队	理论创新赛	面向运动想象脑电的身份识别风险评估与任务约束式表征抑制	三等奖	推荐参加省赛
29	你说的都队	理论创新赛	“数”隐之患：上市公司数据隐私违规处罚的前置诱因研究	三等奖	推荐参加省赛
30	网安新卫士	理论创新赛	IndusGurad:工业多采样率时序数据完整性风险的可信修复与任务可靠性评估	三等奖	推荐参加省赛
31	零呀	理论创新赛	面向攻击意图理解的大语言模型提示注入攻击语义-行为联合建模方法研究	三等奖	推荐参加省赛
32	奶蛙	理论创新赛	面向大语言模型智能体工具调用的时序授权一致性机制	三等奖	推荐参加省赛
33	聚力攻坚队	理论创新赛	SDI-RO：基于情境锚定规则与人机协同编码的数据资源安全披露测量框架	三等奖	推荐参加省赛
34	不烧心	理论创新赛	来源误判下多证据投票的最小失效预算与可核验认证	三等奖	推荐参加省赛
35	漏洞捕手队	理论创新赛	网页字段获取成本假设的审计与离线配额分配	三等奖	推荐参加省赛
36	乘风小队	理论创新赛	基于最小必要原则的个人信息分级动态隐私保护方案研究	三等奖	推荐参加省赛
37	XinShell	实网对抗赛			推荐参加省赛
38	WHTT	实网对抗赛			推荐参加省赛