|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 任务 | 子任务名称与提交目录 | 提交文件名 | 文件路径(/root/2024buildup目录下 | 提交要求 |
| 新手任务 | 背景应用了解  commit/task\_1\_1 | engineer\_login.msg | instance/engineer/user | 正确填写工程师用户名与口令 |
| code\_upload.msg | instance/engineer/user | 正确填写代码文件名 |
| bin\_upload.msg | instance/engineer/user | 正确填写二进制逻辑文件名和类型 |
| operator\_login.msg | instance/operator/user | 正确填写操作员用户名与口令 |
| plc\_start.msg | instance/operator/user | 正确填写action\_desc项的名称（寄存器的名称） |
| plc\_read\_t.msg | instance/operator/user | 正确填写action类型和action\_desc项的名称 |
| plc\_set\_t.msg | instance/operator/user | 正确填写action类型、action\_desc项名称和value取值 |
| 重放攻击  commit/task\_1\_2 | plugin\_config.cfg.task\_1\_2 | instance/login\_hacker | 用重放攻击模块替换echo\_plugin模块 |
| engineer\_login\_nopass.msg | instance/engineer/user | 使用预设秘密值触发重放攻击，仿照合法用户登录 |
| 挑战-应答模式  commit/task\_1\_3 | plugin\_config.cfg.task\_1\_3 | instance/engineer/station | login\_user模式设置为挑战-应答模式 |
| aspect\_policy.cfg.task\_1\_3 | instance/engineer/station | 在原有登录过程中插入挑战-应答过程 |
| 攻击模拟任务 | 越权访问  commit/task\_2\_1 | attack\_login1.msg,  attack\_cmd1.msg,  attack\_login2.msg,  attack\_cmd2.msg | instance/engineer/user | 在工程师站违规操作的用户登录与命令执行的组合 |
| attack\_login3.msg,  attack\_cmd3.msg,  attack\_login4.msg,  attack\_cmd4.msg | instance/operator/user | 在操作员站违规操作的用户登录与命令执行的组合 |
| attack\_login5.msg,  attack\_cmd5.msg,  attack\_login6.msg,  attack\_cmd6.msg | instance/monitor/user | 在管理中心违规操作的用户登录与命令执行的组合 |
| 恶意逻辑  commit/task\_2\_2 | file\_replace.c | src/logic/file\_replace | 在收到二进制逻辑传输命令后，将正常逻辑替换成hack\_logic目录下的恶意逻辑 |
| plugin\_config.cfg.task\_2\_2 | instance/engineer/station | 在配置文件中添加file\_replace模块 |
| aspect\_policy.cfg.task\_2\_2 | instance/engineer/station | 在bin\_upload传输过程中插入file\_replace模块，使其可以在上传代码时用hack\_logic中恶意逻辑替换合法逻辑 |
| modbus监听与篡改  commit/task\_2\_3 | modbus\_monitor.c | src/security/modbus\_monitor | 执行modbus协议数据窃听modbus协议温度数值并进行篡改攻击 |
| 访问控制模拟任务 | 角色验证  commit/task\_3\_1 | role\_verify.c | src/system/role\_verify | 增加对用户登录时角色和设备一致性的检查 |
| Plugin\_config.cfg.task\_3\_1 | instance/monitor/center | 添加role\_verify模块 |
| aspect\_policy.cfg.task\_3\_1 | instance/monitor/center | 将role\_verify机制添加到登录过程中 |
| 角色权限限制  commit/task\_3\_2 | aspect\_policy.cfg.task\_3\_2 | instance/monitor/center | 将角色权限检查机制添加到monitor\_ctrl流程和code\_upload流程中 |
| plugin\_config.cfg.task\_3\_2 | instance/monitor/center | 在系统中添加role\_access模块 |
| role\_access.c | src/security/role\_access | 在角色执行命令过程中添加与环境与角色相关的访问控制要求 |
| 自动逻辑屏蔽  commit/task\_3\_3 | operator\_shield.c | src/security/operator\_shield | 在设备端，当操作员设置温度时，屏蔽PLC自动逻辑的访问行为 |
| monitor\_shield.c | src/security/monitor\_shield | 在操作员站，当监视员设置温度时，屏蔽操作员的访问行为 |
| plugin\_config.cfg.task\_3\_3\_1 | instance/plc/device | 启用operator\_shield模块的模块配置文件 |
| plugin\_config.cfg.task\_3\_3\_2 | instance/operator/station | 启用monitor\_shield模块的模块配置文件 |
| aspect\_policy.cfg.task\_3\_3\_1 | instance/plc/device | 将operator\_shield模块接入到正确的路由过程中。 |
| aspect\_policy.cfg.task\_3\_3\_2 | instance/operator/station | 将monitor\_shield模块接入到正确的路由过程中。 |
| 密码保护模拟任务 | 工程师签名上传  commit/task\_4\_1 | sm2sign.c | src/security/sm2sign | 提供密钥初始化、加密、签名等功能 |
| plugin\_config.cfg.task\_4\_1\_1 | instance/engineer/station | 启用签名模块的模块配置文件 |
| aspect\_policy.cfg.task\_4\_1\_1 | Instance/engineer/station | 提供sm2密钥签名过程路由 |
| plugin\_config.cfg.task\_4\_1\_2 | instance/plc/plc\_loader | 启用验证模块的模块配置文件 |
| aspect\_policy.cfg.task\_4\_1\_2 | instance/plc/plc\_loader | 提供sm2密钥验证过程路由 |
| modbus数据加密  commit/task\_4\_2 | modbus\_zuc\_crypt.c | src/security/modbus\_zuc\_crypt | 提供modbus协议的祖冲之算法加密功能，并  要求算法具备防已知明文攻击，且在发生丢包时仍可正常加解密 |
| plugin\_config.cfg.task\_4\_2\_2 | instance/plc/device | 启用加密模块的模块配置文件 |
| aspect\_policy.cfg.task\_4\_2\_2 | instance/plc/device | 提供祖冲之算法加密过程路由 |
| plugin\_config.cfg.task\_4\_2\_1 | instance/operator/station | 启用解密模块的模块配置文件 |
| aspect\_policy.cfg.task\_4\_2\_1 | instance/operator/stationr | 提供祖冲之算法解密过程路由 |