

【密级及编号：公开】

项目用户手册



厚德 明理 慎独 求是

目 录

1	引言.....	3
1.1	编写目的	3
1.2	背景	3
1.3	名词术语	3
1.4	参考资料	4
2	用途.....	4
2.1	功能	4
2.2	性能	6
2.3	安全保密	7
3	运行环境.....	8
3.1	硬件设备	8
3.2	支持软件	8
3.3	数据结构	8
4	使用过程【非本地部署无需此步骤】	10
4.1	系统初始化配置	10
4.2	运行测试	11
4.3	输入数据	12
4.4	输出数据	12
4.5	出错处理	13
5	灵通测系统操作.....	14
5.1	用户端操作	14

1 引言

1.1 编写目的

本文档给出项目的用户指导手册，包括最终实现的程序的功能和性能以及灵通测模糊测试平台操作流程，编写本文档的目的在于：为用户的使用提供指导和帮助；本说明书的预期读者包括：软件维护人员；技术管理人员；执行软件质量保证计划的专门人员；参与本项目开发进程各阶段验证、确认以及负责为最后项目验收、鉴定提供相应报告的有关人员。

1.2 背景

待开发的软件系统名称：灵通测（九尾狐）模糊测试平台

本工程项目的任务提出者：罗森林

本工程项目的开发方：北京理工大学信息系统及安全对抗实验中心

本工程项目的用户为：从事模糊测试与漏洞挖掘的安全技术人员

1.3 名词术语

序号	专门术语	定义或说明
1	测试模板	平台提供的测试基本框架，用于配置测试套
2	测试套	基于测试模板填写相关配置的完整测试组件，可直接进行测试
3	测试任务	一个测试套的一次运行，同一个测试套可生成多个测试任务
4	测试用例	测试任务中一个运行轮次的数据模型，及其所处状态模型和动作序列
5	数据模型	测试过程中所需的全部数据元素的集合类型
6	数据元素	模糊测试中的基本数据单元，如二进制数组、字符串等
7	状态模型	包含测试运行中的完整状态链表，及对应状态下的动作序列
8	变异策略	模糊测试中数据变异的策略，如顺序变异、随机变异等
9	变异权重	数据模型中各数据元素及其字段发生变异的概率
10	变异算子	又称变异器，包含对数据模型和状态模型的变异操作

1.4 参考资料

灵通测模糊测试平台-白皮书

灵通测详细设计说明书

灵通测接口设计文档

2 用途

2.1 功能

2.1.1 功能列表及说明

序号	功能名称	备注（功能指标、性能指标）
1	用户管理	功能指标： 实现普通用户的登录、注册功能；管理员对用户进行增删改查操作。 性能指标： 操作响应时间低于 0.5 秒；可容纳用户量不低于 100,000 个。
2	中英文切换	功能指标： 允许用户在登录时选择中英文版本的系统界面。 性能指标： 版本切换响应时间低于 0.5 秒。
3	数据总览	功能指标： 在主页显示当前测试平台使用情况和测试历史数据总览。 性能指标： 包含 5 种统计信息；10 类测试套占比分析；近 14 天使用详情。
4	新建测试套	功能指标： 支持用户根据提供的标准测试模板新建测试套。 性能指标： 提供的测试模板数不低于 30 个。
5	运行测试套	功能指标： 允许用户重复使用已配置好的测试套，进行运行、复制、编辑和删除。 性能指标： 各功能按键响应时间低于 0.5 秒；可存储 5 类配置信息。
6	配置相关参数	功能指标： 配置测试套的基本参数和系统参数，对于系统参数提供默认值。
7	配置数据监控	功能指标： 设置测试套运行的代理环境和监视器信息，提供监视器的参数配置。 性能指标： 包括本地和远程 2 类代理，提供共 38 种监视器。
8	字段调整	功能指标： 允许用户对测试套中的各字段赋予不同的权重，从而影响突变概率。 性能指标： 权重包含 6 个级别设置。
9	验证测试套	功能指标： 允许用户在模糊测试之前验证测试套是否符合规范，资源加载是否可用。

		性能指标: 实时日志显示延迟低于 0.5 秒。
10	测试运行	功能指标: 设置随机种子和测试轮次, 启动测试任务。 性能指标: 测试轮次上限为 10,000,000。
11	历史记录	功能指标: 允许用户查看并管理历史测试任务。 性能指标: 包含 6 种字段信息和 3 种操作。
12	故障总览	功能指标: 统计并查看测试任务中检测到的故障信息, 支持下载故障详情。 性能指标: 包含 2 大类 15 小类的详细信息。
13	突变因子	功能指标: 记录测试过程中使用的突变算子和对应的测试用例。 性能指标: 包含 5 种记录信息。
14	突变记录	功能指标: 记录测试过程中发生变异的数据元素和状态与动作信息。 性能指标: 包含 8 类字段信息。
15	变异复现	功能指标: 使用与原任务相同的参数设置, 复现数据和状态变异。 性能指标: 提供单轮和多轮 2 种方式。
16	用例解析	功能指标: 记录并显示变异后的具体数据内容。 性能指标: 每个数据元素可显示 32 字节。
17	元素统计	功能指标: 记录发生变异的数据元素。
18	状态统计	功能指标: 记录发生变异的运行状态。
19	数据集	功能指标: 记录模糊测试中使用的外部数据集。
20	存储变化时间轴	功能指标: 记录模糊测试的起止过程时间线及存储空间变化情况。 性能指标: 时间精确至秒级。
21	测试报告	功能指标: 支持生成测试总结报告及 pdf 格式下载功能。 性能指标: 报告包含结果汇总、故障描述、性能指标 3 部分, 其中性能指标包含 5 类信息。
22	日志记录	功能指标: 实现对用户使用行为的日志记录。 性能指标: 包含 4 类字段信息; 记录不低于 20 种用户行为。
23	协议逆向	功能指标: 实现对捕获数据包组的协议分析, 解析网络协议类型, 实现报文分段功能并自动化生成测试套。 性能指标: 支持不低于 30 种类型的协议分析。
24	最小值生成	功能指标: 从原始数据中选择满足目标程序最大代码覆盖率的最小生成子集。 性能指标: 支持不低于 30 种数据类型。
25	风暴攻击	功能指标: 实现对测试目标的风暴攻击, 验证目标是否会发生资源耗尽的故障。 性能指标: 支持 TCP 和 ARP 两种协议类型。
26	分页和搜索	功能指标: 实现在数据显示页面的内容分页以

		及任意字段的查询搜索功能。 性能指标： 在 6 个数据查看前端页面实现。
--	--	--

2.2 性能

2.2.1 服务支持

服务支持指标包括：

- 1) 提供可用的测试模板不低于30个。
- 2) 可进行模糊测试的协议类型不低于30种。
- 3) 可进行分析的数据类型不低于20种。
- 4) 可用的发包器类型不低于40种。
- 5) 提供监视器类型不低于35种。
- 6) 提供3种工具组件：协议逆向、最小集生成、风暴攻击。
- 7) 提供用户行为日志类型不低于20种。

2.2.2 时间特性

- 1) 各页面和按键功能加载响应时间均低于0.5秒。
- 2) 数据搜索响应时间低于1秒。
- 3) 测试运行速度不低于1000个测试用例/小时
- 4) 实时进度条和实时日志显示更新时间低于0.5秒

2.2.3 并发性要求

1. 系统平台基于B/S架构实现，在本地运行灵通测模糊测试平台，支持多用户和应用多开，可保证同时不低于10个用户进行模糊测试。

2.2.4 兼容性

系统的兼容性主要体现在以下几个方面：

1. 兼容主流浏览器

要求在常见的浏览器，如 IE、edge、360、谷歌、火狐等浏览器上正常使用。

2. 兼容主流操作系统

要求在 windows 系统和 Linux 系统上都可以正常使用。

2.2.5 可扩展性

系统的可扩展性针对开发人员进行讨论，主要体现在以下几个方面：

1. 测试模板

开发人员可设计新的测试模板，便捷的添加至系统服务支持中。

2. 监视器

开发人员可设计新的监视器类型，直接通过 json 文件写入可用监视器列表。

3. 变异算子

开发人员可设计新的变异算子，直接在测试模板中进行调用。

4. 数据转换器

开发人员可设计新的加解密或编解码类型，直接在测试模板中进行调用。

5. 发包器

开发人员可设计新的不同协议类型发包器，直接在测试模板中进行调用。

6. 扩展工具

开发人员可设计新的扩展工具，直接集成在前端工具栏中。

2.2.6 其他专门要求

序号	要求	说明
1	可维护性	系统说明文档齐全，模块化设计和清晰的接口设计
2	易读性	系统结构清晰，代码注释充分，遵循一般性的编码的惯例
3	可靠性	系统的可靠性是建立合理的设计和充分测试的基础上的。而目标系统将完成所有的必要的测试。
4	可视化效果	系统具有良好的可视化效果，前端操作步骤简单，逻辑清晰，有丰富的图表说明及详细的日志信息
5	软件形态	应用程序

2.3 安全保密

保密要求主要涉及产品开发代码和测试模板的保密。由于北京理工大学信息系统及安全对抗实验中心对灵通测（九尾狐）模糊测试平台具有独立知识产品，其产品关键技术信息和相关服务组件应受到知识产权保护，且在未公开之前存在保密要求。

3 运行环境

3.1 硬件设备

系统需要至少 1 台服务器，配置要求如下：

服务器		
硬件环境	CPU	处理器个数大于 4, 2.4GHZ
	CPU 位数	64 位
	内存	16GB
	硬盘	512GB
软件环境	操作系统	Windows10 或 Ubuntu 16.04
	软件	Navicat Premium

3.2 支持软件

序号	名称	描述
1	操作系统	Windows10及更高版本
3	开发环境	Visual Studio（c#）
4	软件	.Net 6.0 AngularJS 1.3.20 Python 3.8 Docker Navicat Premium 15

3.3 数据结构

运行本系统平台的数据库结构如图 3-1 所示：

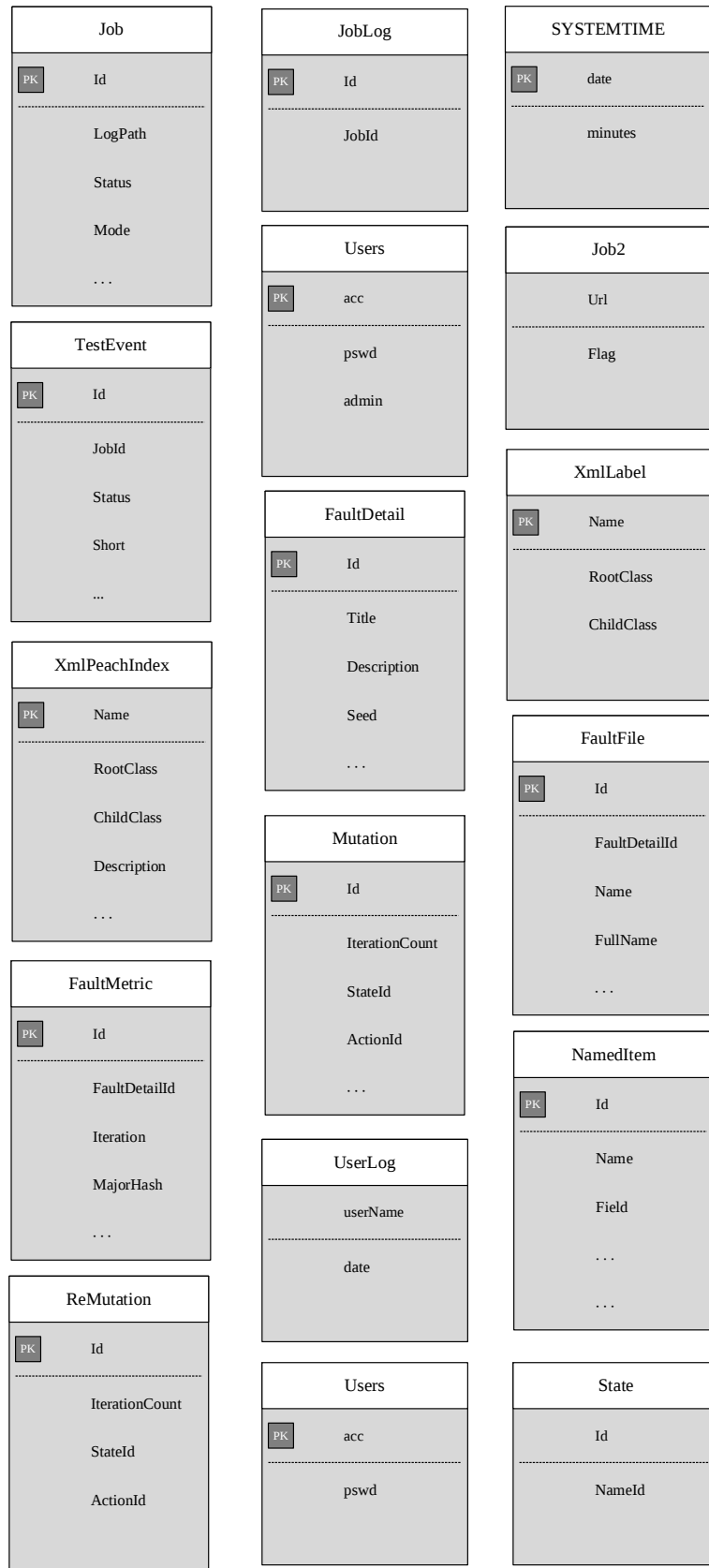


图 3-1 数据库结构示意图

4 使用过程【非本地部署无需此步骤】

4.1 系统初始化配置

以下是保证系统在服务端正常运行的重要条件，请严格按照安装步骤操作，若在安装过程中遇到安装问题，请参考出错处理和恢复章节，解决问题。

4.1.1 模糊测试平台初始化配置

1. 导入完整 bin 目录，确保目录下包含 Gumihho.exe 文件
2. 启动 Gumihho.exe，进入欢迎界面，可进行登录或注册进入平台

4.1.2 扩展工具初始化配置

以下是扩展工具的初始化配置方法，请针对每项扩展工具严格按照安装步骤操作，若在安装过程中遇到安装问题，请参考出错处理和恢复章节，解决问题。

4.1.2.1 协议逆向工具初始化配置

1. 确保当前运行系统支持 Grpc 通信
下载 Google.Protobuf.3.14.0、Grpc.2.31.0、Grpc.Core.2.31.0、Grpc.Core.Api.2.31.0 和 Grpc.Tools.2.31.0
2. 创建 Docker 镜像
打开 powershell
在 powershell 中输入指令“cd 文件夹路径”
输入指令“docker build -t 镜像名称:版本号”
3. 创建 Docker 容器
在 powershell 中输入指令“docker run -e PYTHONIOENCODING=utf-8 -it -p 8090:6001 --name=容器名称 镜像名称:版本号”
4. 进入 Docker 容器
在 powershell 中输入指令“docker start 容器 ID”
5. 运行监听脚本
在 Docker 容器的终端输入指令“python3 NetGumihhoInter.py”进入监听

4.1.2.2 最小集生成初始化配置

1. 打开计算机设置->高级系统设置->高级->环境变量，选择系统变量->Path 进行编辑，新建添加词条..\bin\pin\ia32\bin 于系统环境变量

2. 将要测试的目标应用程序复制到 bin 目录下
3. 将要处理的用例文件复制到 bin\samples\文件目录\下，文件目录为用户自行建立的文件夹，作为在系统中的索引

4.1.2.3 风暴攻击初始化配置

1. 打开计算机设置->高级系统设置->硬件->设备管理器->网络适配器，确保当前网卡可用
2. 确实测试目标已启动，且测试过程中要发送数据的目标端口开放

4.2 运行测试

以下是运行模糊测试或扩展工具的操作流程，若系统运行出现问题，请参考出错处理和恢复章节，解决问题。

4.2.1 模糊测试运行流程

1. 登录/注册账号，进入系统主页
2. 在菜单栏选择测试资源->新建测试套，选择想使用的测试模板点击新建测试套，填写命名和相关描述后进入测试套配置环节
3. 配置测试必需的相关参数，灰色文本框表示系统默认读取的字段，不可更改
4. 点击下一步配置数据监控，点击添加代理增加代理项，需输入名称和代理地址（默认为本地），点击添加监视器可选择监视器，根据监视器中的说明填写相关参数，点击保存按键完成数据监控配置
5. 点击下一步进入字段调整界面，点击‘+’展开数据模型，根据左侧蓝色圆点选择对应字段在突变过程的权重
6. 点击下一步进入验证测试套，点击验证测试套按键验证测试套格式是否符合规定及相关资源是否可以被检索到
7. 点击下一步输入测试终止值开始测试，进入测试运行界面
8. 待进度条结束时完成测试，点击测试详情查看测试详解结果，点击报告导出生成测试报告

4.2.2 扩展工具运行流程

4.2.2.1 协议逆向工具运行流程

1. 点击选择文件从本地导入 Pcap 格式文件数据包

2. 点击解析文件逆向报文中使用到的协议类型并显示在文本框中
3. 输入要解析的协议类型，点击获取协议，读取与目标协议相关的报文并显示在多行文本框中
4. 点击下一步，输入报文序号选择报文，点击报文分段按键，在多行文本框中显示分段结果
5. 点击下一步，输入给文件的命名，点击文件生成按键，自动化生成测试套

4.2.2.2 最小集生成运行流程

1. 点击选择文件夹从 bin\samples 目录下选择存储原数据用例的文件夹
2. 点击选择文件从 bin 目录下选择要测试的可执行文件
3. 点击测试运行执行最小集生成，文本框中显示实时日志信息
4. 点击打开生成子集按键，打开生成的最小集文件夹

4.2.2.3 风暴攻击运行流程

1. 配置数据监控，点击添加代理增加代理项，需输入名称和代理地址（默认为本地），点击添加监视器可选择监视器，根据监视器中的说明填写相关参数，点击保存按键完成数据监控配置
2. 点击下一步输入发包数或截止时间进行测试

4.3 输入数据

输入数据取决于测试所使用的测试套，一般通过前端输入文件路径加载资源

4.4 输出数据

输出数据包含 4 种数据类型，模糊测试和风暴攻击的输出为测试详情和测试报告，协议逆向和最小集生成有独立的输出结果

4.4.1 测试详情

测试详情输出数据包括 8 个详情页：故障总览、突变因子、突变记录、相关元素、状态统计、数据集、存储时间变化轴和 Bucket

4.4.2 测试报告

测试报告按照标准报告格式生成，以 pdf 形式输出

4.4.3 协议逆向

协议逆向工具的输出为基本测试模板，会自动添加至测试模板列表

4.4.4 最小集生成

最小集生成的输出为筛选数据的子集，存入指定文件目录

4.5 出错处理

序号	错误归属	故障描述及含义	处理方式
1	系统	无法启动 Gumih0.exe 或无法进入欢迎页面	检查 bin 目录是否丢失文件，练习开发人员进行处理
2	子系统	协议逆向中无法解析 Pcap 文件	检测 docker 是否正常连接，若相关事项无明显异常请联系管理员解决
3	子系统	最小集生成中测试运行报错	检查应用程序和待筛选数据是否存入正确位置，若相关事项无明显异常请联系管理员解决
4	子系统	风暴攻击中测试异常中止或启动失败	1.检查无线网卡是否可用 2.通过 Ping 指令检查是否可以同测试目标建立连接
5	子系统	最小集生成中无法加载 Pin 文件	检查是否未按教程添加环境变量，若无异常请联系管理员解决
6	系统	提升缺少数据监控	检查是否未保存监控配置，若相关事项无明显异常请联系管理员解决
7	系统	验证测试套失败	1.根据报错信息，查看是否有资源路径无法加载 2.查看设置的数据监控是否缺少必需的参数字段
8	系统	模糊测试中断	1.检查是否与测试目标连接已断开 2.检查是否误关闭模糊测试进程
9	数据库	登录和注册失败	查看是否存在数据库文件丢失或数

			据库连接中断，若相关事项无明显异常请联系管理员解决
10	数据库	主页信息、测试资源、历史记录、日志信息读取为空	查看是否存在数据库文件丢失或数据库连接中断，若相关事项无明显异常请联系管理员解决

5 灵通测系统操作

5.1 用户端操作

5.1.1 操作界面

5.1.1.1 欢迎页面

本系统在未登录时显示欢迎页面，欢迎页面主要包括欢迎窗口以及上方的菜单栏，提供登录与注册功能，欢迎页面包括平台优势，平台简介以及思政教育三个部分。

欢迎窗口仅在用户未登录时显示，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。如下图所示。



图 5-7 欢迎页面

5.1.1.2 注册

本界面主要包括注册窗口以及上方的菜单栏。

注册窗口仅在用户未登录时显示，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行登录或注册操作。如下图所示。

北京理工大学
BEIJING INSTITUTE OF TECHNOLOGY

信息系统及安全对抗实验中心
Information System and Security & Countermeasures Experimental Center

厚德明理，慎独求是

[登录](#) [注册](#)

欢迎注册

用户名:

密码:

确认密码:

语言:

简体中文

注册

北京理工大学信息系统及安全对抗实验中心(ISSCEC) All rights reserved. Beta 0.1

图 5-8 注册页面

5.1.1.3 登录

本界面主要包括登录窗口以及上方的菜单栏。

登录窗口仅在用户未登录时显示，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行登录或注册操作。如下图所示。

北京理工大学
BEIJING INSTITUTE OF TECHNOLOGY

信息系统及安全对抗实验中心
Information System and Security & Countermeasures Experimental Center

厚德明理，慎独求是

[登录](#) [注册](#)

欢迎登录

用户名:

密码:

语言:

简体中文

登录

北京理工大学信息系统及安全对抗实验中心(ISSCEC) All rights reserved. Beta 0.1

图 5-9 登录页面

5.1.1.4 主页

本界面主要包括主页窗口以及上方的菜单栏，主页包括数据总览、测试套占比和测试用例统计三个部分。

首页窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。如下图所示。



图 5-10 主页

5.1.1.5 新建测试套

本界面主要包括新建测试套窗口以及上方的菜单栏，主页面包括分页及搜索、基本测试模板展示、新建测试套三个部分。

新建测试套窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。如下图所示。

灵通测					你好! BFS				
主页 测试资源 历史记录 日志 工具 帮助									
测试套搜索...					首页 上一页 1 下一页 尾页 当前第1页/共4页 转到 页				
序号	测试套名	标签	描述		新建测试套				
1	123	数据模型 系统测试	用于系统测试的测试套		新建测试套				
2	1588v2	应用层协议 有线网络协议	精密时间协议 (PTP) 是一种用于测量和控制系统的高精度同步协议。该协议在 IEEE1588 中定义 (2002 用于 PTPv1, 2008 用于 PTPv2)。		新建测试套				
3	aes128	数据模型 系统测试	用于系统测试的测试套		新建测试套				
4	APS	链路层协议 有线网络协议	APS协议配置中, 将设置一条MPLS Tunnel去保护工作Tunnel, 当工作Tunnel发生故障时, 业务可以切换到保护Tunnel上, 达到保护业务的目的。		新建测试套				
5	AVI	视频文件 文件	AVI视频文件		新建测试套				
6	COPS	应用层协议 有线网络协议	COPS(Common Open Policy Service,公共开放策略服务)是一种简单的使用查询/响应模式的应用层协议, 可用于在策略服务器和客户端之间交互策略信息。		新建测试套				
7	crc	数据模型 系统测试	用于系统测试的测试套		新建测试套				
8	DLDLP	链路层协议 有线网络协议	DLDLP (Device Link Detection Protocol) 设备链路检测协议, 用来监控光纤或铜质双绞线 (例如超五类双绞线) 的链路状态, 如果发现单向链路存在, DLDLP协议会根据用户配置, 自动关闭或通知用户手工关闭相关接口, 以防止网络问题的发生。		新建测试套				
9	Ethernet_Data	链路层协议 有线网络协议	以太网是用于局域网 (LAN) 的常用介质。		新建测试套				

图 5-11 新建测试套

5.1.1.6 运行测试套

本界面主要包括运行测试套窗口以及上方的菜单栏，主页面包括分页及搜索、测试套展示、测试套操作三个部分。

运行测试套窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，

工作时通过切换到不同的视图以进行不同模块的操作。如下图所示。



序号	测试套名	标签	描述	修改时间	运行	复制	编辑	删除
1	zes128x778	数据模型 系统测试	用于系统测试的测试套	2023-04-12 15:35:31	运行	复制	编辑	删除
2	multi-publisher-166	数据模型 系统测试		2023-04-11 19:21:31	运行	复制	编辑	删除
3	aes128xn	数据模型 系统测试	用于系统测试的测试套	2023-04-11 16:15:50	运行	复制	编辑	删除
4	aes128999-1756	数据模型 系统测试	6677用于系统测试的测试套45xn	2023-04-11 16:15:34	运行	复制	编辑	删除
5	aes128999-175	数据模型 系统测试	6677用于系统测试的测试套45xn	2023-04-11 16:12:45	运行	复制	编辑	删除
6	aes128999-17	数据模型 系统测试	6677用于系统测试的测试套45xn	2023-04-11 15:49:55	运行	复制	编辑	删除
7	aes128999-12337	数据模型 系统测试	用于系统测试的测试套457	2023-04-11 15:47:01	运行	复制	编辑	删除
8	aes128999-1233	数据模型 系统测试	用于系统测试的测试套45	2023-04-11 15:32:52	运行	复制	编辑	删除
9	aes128115	数据模型 系统测试	用于系统测试的测试套1	2023-04-11 15:31:15	运行	复制	编辑	删除

图 5-12 运行测试套

5.1.1.7 配置相关参数

本界面主要包括配置相关参数窗口以及上方的菜单栏，主页面包括参数配置列表、参数配置信息两个部分。

配置相关参数窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。

配置相关参数窗口用于查看测试套参数与系统参数或添加自定义参数，其中测试套参数用户可自行修改设置，若不加修改则为默认值，系统参数包括测试任务编号、操作系统、安装目录、工作目录、日志目录、插件目录、脚本目录以及资料库路径等，如下图所示。



Name(参数名)	Key(主函数)	Value(参数值)
Gumiho Job Id(任务编号)	Gumiho.JobId	00000000-0000-0000-0000-000000000000 Job ID for current fuzzing run(当前模糊测试运行的任务ID)
Gumiho OS(操作系统)	Gumiho.OS	windows Operating System that Gumiho is running on(模糊测试运行的操作系统)
Gumiho Installation Directory(安装目录)	Gumiho.Pwd	F:\peach\Gumiho\Gumiho\output\win64\bin Full path to Gumiho installation(模糊测试的完整安装路径)
Gumiho Working Directory(工作目录)	Gumiho.Cwd	F:\peach\Gumiho\Gumiho\output\win64\bin Full path to the current working directory(模糊测试的完整工作路径)

图 5-13 配置相关参数

5.1.1.8 配置数据监控

本界面主要包括配置数据监控窗口以及上方的菜单栏，主页面包括添加代理列表、添加监视器信息两个部分。

配置数据监控窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。

配置数据监控窗口用于为选择的测试套定义一个或多个代理，并可以选择添加一个或多个监视器。其中代理是监视器和发包器的主体。本地代理可以与测试平台处于同一台计算机上，并且可以通过监视器和发包器控制测试环境。远程代理处于测试目标设备上，可以提供远程监视器和发包器信息，如下图所示。

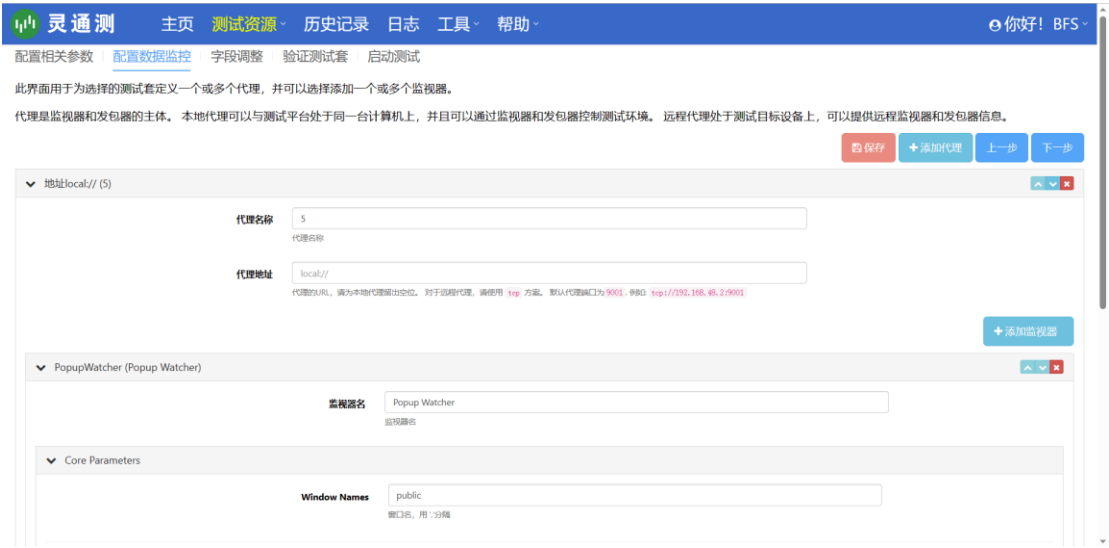


图 5-14 配置数据监控

5.1.1.9 字段调整

本界面主要包括字段调整窗口以及上方的菜单栏，主页面包括字段调整说明、字段调整两个部分。

字段调整窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。

字段调整窗口可使用户逐字段地控制测试进行，如下图所示。



图 5-15 字段调整

5.1.1.10 验证测试套

本界面主要包括验证测试套窗口以及上方的菜单栏，主页面包括验证测试套说明、验证测试套详细信息两个部分。

验证测试套窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。

验证测试套窗口通过执行一个测试用例来验证配置是否存在错误，并陈列出可能对测试任务造成影响的内容，如下图所示。



图 5-16 验证测试套

5.1.1.11 启动测试

本界面主要包括启动测试窗口以及上方的菜单栏，主页面包括测试参数说明、北京理工大学信息系统及安全对抗实验中心

测试参数配置两个部分。

启动测试窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。

启动测试窗口根据用户输入参数进行模糊测试，如下图所示。



图 5-17 启动测试

5.1.1.12 历史记录

本界面主要包括历史记录窗口以及上方的菜单栏，主页面包括分页及搜索、历史记录展示、历史记录操作三个部分。

历史记录窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。如下图所示。



图 5-18 历史记录

5.1.1.13 查看详情

本界面主要包括查看详情窗口以及上方的菜单栏，主页面包括测试操作、测试信息展示、日志显示三个部分。

查看详情窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。如下图所示。



图 5-19 查看详情

5.1.1.14 故障总览

本界面主要包括故障总览窗口以及上方的菜单栏，主页面包括故障总览摘要、故障展示两个部分。

故障总览窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。

故障总览窗口列出了所有故障的信息摘要，如下图所示。



图 5-20 故障总览

5.1.1.15 突变因子

本界面主要包括突变因子窗口以及上方的菜单栏, 主页面包括分页与搜索、突变因子信息展示两个部分。

突变因子窗口是始终存在的窗口, 各视图及其对应工具栏在窗口内显示, 工作时通过切换到不同的视图以进行不同模块的操作。

突变因子窗口列出了所有突变因子的信息, 如下图所示。

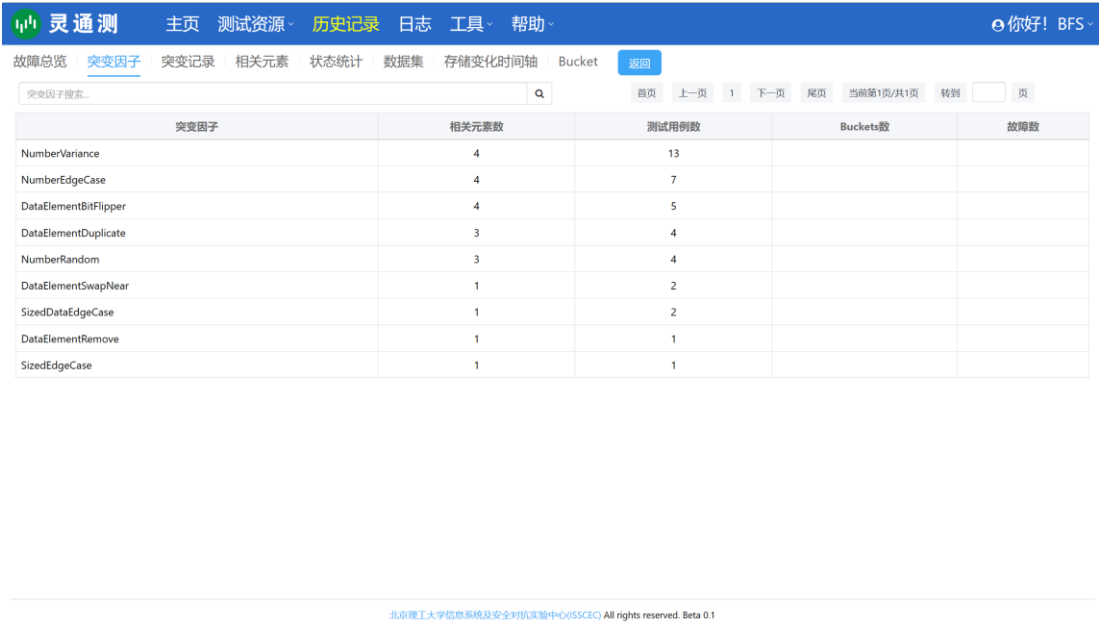


图 5-21 突变因子

5.1.1.16 突变记录

本界面主要包括突变记录窗口以及上方的菜单栏，主页面包括分页与搜索、突变记录信息展示两个部分。

突变记录窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。

突变记录窗口列出了所有突变记录的相关信息，如下图所示。

灵通测

主页 测试资源 历史记录 日志 工具 帮助

你好! BFS

故障总览 突变因子 突变记录 相关元素 状态统计 数据集 存储变化时间轴 Bucket

返回

变异记录搜索...

Q

首页 上一页 1 下一页 尾页

当前第1页/共3页

转到

页

编号	测试轮次	状态编号	动作编号	参数编号	元素编号	变异编号	数据编号	类型	变异复现	用例解析
97	2 rounds	initial	Action		Packet.DestPort	DataElementBitFlipper		0	变异复现	变异解析
99	2 rounds	initial	Action		Packet.Length	DataElementDuplicate		0	变异复现	变异解析
101	2 rounds	initial	Action		Packet.DestPort	NumberRandom		0	变异复现	变异解析
103	2 rounds	initial	Action		Packet.checksum	NumberEdgeCase		0	变异复现	变异解析
105	2 rounds	initial	Action		Packet.Length	NumberEdgeCase		0	变异复现	变异解析
107	2 rounds	initial	Action		Packet.Length	DataElementBitFlipper		0	变异复现	变异解析
109	2 rounds	initial	Action		Packet.SrcPort	DataElementBitFlipper		0	变异复现	变异解析
111	2 rounds	initial	Action		Packet.SrcPort	NumberRandom		0	变异复现	变异解析
113	2 rounds	initial	Action		Packet.Length	NumberVariance		0	变异复现	变异解析
115	2 rounds	initial	Action		Packet.checksum	DataElementRemove		0	变异复现	变异解析

北京理工大学信息系统及安全对抗实验中心(ISSSEC) All rights reserved. Beta 0.1

图 5-22 突变记录

5.1.1.17 相关元素

本界面主要包括相关元素窗口以及上方的菜单栏，主页面包括相关元素说明、相关元素信息展示两个部分。

相关元素窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。

相关元素窗口列出了测试套所有相关元素的统计信息，如下图所示。

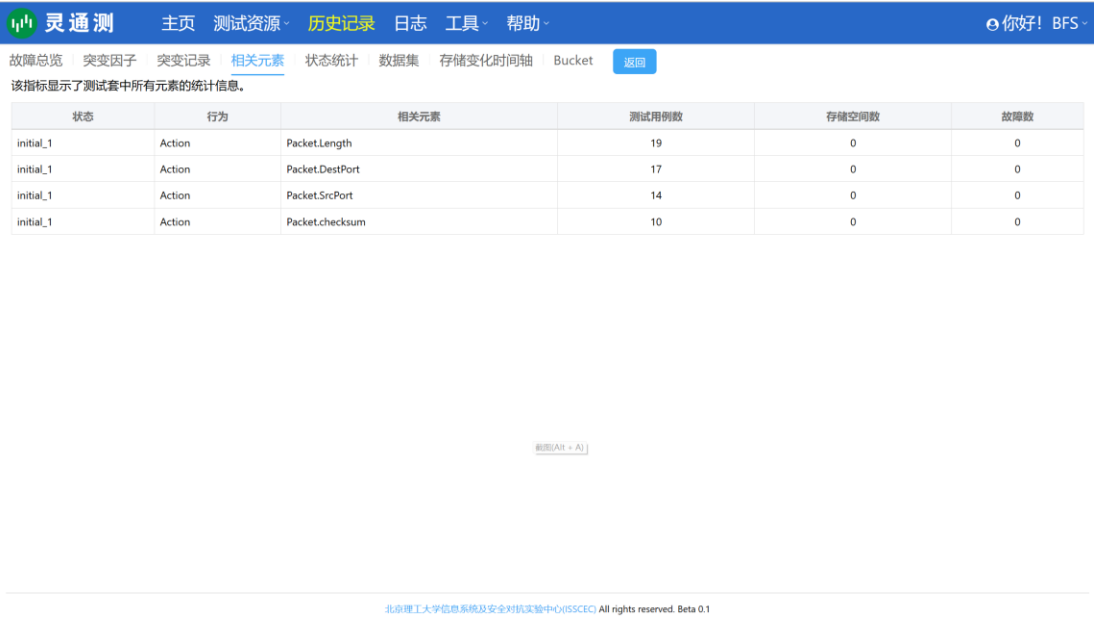


图 5-23 相关元素

5.1.1.18 状态统计

本界面主要包括状态统计窗口以及上方的菜单栏，主页面包括状态统计说明、状态统计信息展示两个部分。

状态统计窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。

状态统计窗口列出了测试套所有状态的统计信息，如下图所示。



图 5-24 状态统计

5.1.1.19 数据集

本界面主要包括数据集窗口以及上方的菜单栏，主页面包括数据集说明、数

数据集信息展示两个部分。

数据集窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。

数据集窗口显示模糊测试过程中使用两个或多个数据集的相关统计信息，这有助于确定唯一 bucket 来源和在变异中使用的数据资源故障，如下图所示。



图 5-25 数据集

5.1.1.20 存储变化时间轴

本界面主要包括存储变化时间轴窗口以及上方的菜单栏，主页面包括存储变化时间轴说明、存储变化时间轴展示两个部分。

存储变化时间轴窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。

存储变化时间轴窗口展示一个时间线，其中列出了新的故障 bucket 以及在模糊测试过程中发现 bucket 的总次数，如下图所示。



图 5-26 存储变化时间轴

5.1.1.21 Bucket

本界面主要包括 Bucket 窗口以及上方的菜单栏，主页面包括 Bucket 说明、Bucket 数据展示两个部分。

Bucket 窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。

Bucket 窗口显示模糊测试过程中遇到的 Bucket，如下图所示。



图 5-27 Bucket

5.1.1.22 故障详细信息

本界面主要包括故障详细信息窗口以及上方的菜单栏，主页面包括故障详细信息、故障数据展示两个部分。

故障详细信息窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。

故障详细信息窗口显示模糊测试过程中遇到故障的详细信息，如下图所示。



图 5-28 故障详细信息

5.1.1.23 变异复现

本界面主要包括变异复现窗口以及上方的菜单栏，主页面包括变异复现操作、变异信息展示、单/多轮参数设置三个部分。

变异复现窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。如下图所示。

本次变异复现选择的测试套件为 crc-4。

返回

开始复现

变异复现

隐藏

"变异复现"用于对已经进行的模糊测试任务进行复现，具体可分为单轮和多轮变异，分别执行选中的单轮或多轮测试用例。

点击"开始变异"按钮开始变异复现工作。

编号	状态编号	动作编号	参数编号	元素编号	变异编号	数据编号	类型	随机种子
97	initial	Action		Packet.DestPort	DataElementBitFlipper		0	13965

单轮

多轮

变异类型

Random

图 5-29 变异复现

5.1.1.24 变异详情

本界面主要包括变异详情窗口以及上方的菜单栏，主页面包括变异操作、变异信息展示、变异日志展示三个部分。

变异详情窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。如下图所示。

灵通测

主页 测试资源 历史记录 日志 工具 帮助

你好! BFS

变异选择

重新测试

2023-05-06 09:54:13

00h 00m 19s

11747

13965

62

1

开始时间

运行时间

每小时测试用例数

随机种子

已执行的测试用例数

总故障数

近期故障

#用例数	日期	监视器	风险	主要Bucket	最小Bucket	下载
1	5/6/23 09:54	PopupWatcher	UNKNOWN	9E290A18	5EC85A7D	下载

日志

2023-05-06 09:54:13.4557 Gmnlho.Pro.Core.MutationStrategies.RandomStrategy Initialized with seed 13965

2023-05-06 09:54:13.4557 Gmnlho.Pro.Core.Engine runTest: context.config.range == true, start: 1, stop: 20

2023-05-06 09:58:34.9746 Gmnlho.Pro.Core.MutationStrategies.RandomStrategy Initialized with seed 13965

2023-05-06 09:58:34.9746 Gmnlho.Pro.Core.Engine runTest: context.config.range == true, start: 1, stop: 5

2023-05-06 10:04:24.8107 Gmnlho.Pro.Core.MutationStrategies.RandomStrategy Initialized with seed 13965

2023-05-06 10:04:24.8107 Gmnlho.Pro.Core.Engine runTest: context.config.range == true, start: 1, stop: 5

2023-05-06 09:54:13.4627 Gmnlho.Pro.Core.Loggers.JobLogger Writing debug log to: F:\pouch\Gmnlho\Gmnlho\output\win64\bin\Logs\crc_ml_20230506095413\debug.log

2023-05-06 09:54:13.5442 Gmnlho.Core.Agent.Channels.AgentLocal StartMonitor: Popup.Watcher.PopupWatcher

2023-05-06 09:54:13.5502 Gmnlho.Core.Agent.Channels.AgentLocal SessionStarting

2023-05-06 09:54:13.5502 Gmnlho.Core.Engine runTest: Iteration Starting: 1. =====

2023-05-06 09:54:13.5502 Gmnlho.Core.Engine runTest: Performing control recording iteration.

2023-05-06 09:54:13.5502 Gmnlho.Core.Dev.StateModel Run(): Changing to state "initial".

2023-05-06 09:54:13.5502 Gmnlho.Core.Dev.Action Run(action): Output

2023-05-06 09:54:13.5502 Gmnlho.Core.Agent.Channels.AgentLocal PublisherStarting

2023-05-06 09:54:13.5502 Gmnlho.Pro.Core.Publishers.ConsolePublisher start()

2023-05-06 09:54:13.5502 Gmnlho.Pro.Core.Publishers.ConsolePublisher open()

2023-05-06 09:54:13.5502 Gmnlho.Pro.Core.Publishers.ConsolePublisher output(8 bytes)

2023-05-06 09:54:13.5502 Gmnlho.Pro.Core.Publishers.ConsolePublisher close()

2023-05-06 09:54:14.4469 Gmnlho.Core.Agent.AgentManager DetectedFault: checking for fault in agent 1

2023-05-06 09:54:14.4469 Gmnlho.Core.Agent.AgentManager Fault detected. Collecting monitor data.

2023-05-06 09:54:14.4469 Gmnlho.Core.Engine runTest: detected fault on iteration 1

2023-05-06 09:54:14.4469 Gmnlho.Pro.Core.Loggers.JobLogger Found core fault: [Closed 1 popup window.]

2023-05-06 09:54:14.4469 Gmnlho.Pro.Core.Loggers.JobLogger Saving data from action: 1.initial.Action.bin

2023-05-06 09:54:14.4469 Gmnlho.Pro.Core.Loggers.JobLogger Saving fault: Closed 1 popup window.

图 5-30 变异详情

5.1.1.25 用户日志

本界面主要包括用户日志窗口以及上方的菜单栏，主页面包括分页及搜索、当前用户日志两个部分。

用户日志窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工

北京理工大学信息系统及安全对抗实验中心

第28页 共60页

作时通过切换到不同的视图以进行不同模块的操作。如下图所示。

灵通测					你好! BFS				
日志搜索					首页 上一页 1 下一页 尾页 当前第1页/共2页 转到 页				
序号	操作用户	操作时间	操作详情		操作类型				
1	BFS	2023-05-06 10:06:53	BFS 查看d3fb0789-5d66-4810-9cea-8f6d9b884a6e crc-4的详情		查看详情				
2	BFS	2023-05-06 10:06:42	BFS 查看63a20f40-da71-4771-918a-6987be49892e crc-4的详情		查看详情				
3	BFS	2023-05-06 10:06:37	BFS 查看cbef845e-2d3e-4f3e-941c-89bf16dc8d05 crc-4的详情		查看详情				
4	BFS	2023-05-06 10:06:35	BFS 查看d3fb0789-5d66-4810-9cea-8f6d9b884a6e crc-4的详情		查看详情				
5	BFS	2023-05-06 10:04:25	BFS 使用3a5441b6-53a5-4478-9f3b-0d48efe8bd6e crc-4进行多轮变异复现		多轮变异复现				
6	BFS	2023-05-06 09:58:34	BFS 使用3a5441b6-53a5-4478-9f3b-0d48efe8bd6e crc-4进行多轮变异复现		多轮变异复现				
7	BFS	2023-05-06 09:54:13	BFS 使用3a5441b6-53a5-4478-9f3b-0d48efe8bd6e crc-4进行测试		用户测试				
8	BFS	2023-05-06 09:53:52	BFS 使用02c721d2-9883-43b1-a510-b0c285b81cfc crc-4进行测试		用户测试				
9	BFS	2023-05-06 09:52:07	BFS登录了系统		登录				
10	BFS	2023-05-06 09:52:04	BFS登出了系统		登出				

图 5-31 用户日志

5.1.1.26 文件上传

本界面主要包括文件上传窗口以及上方的菜单栏，主页面包括文件操作说明、协议解析两个部分。

文件上传窗口是协议逆向的子窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。如下图所示。

灵通测

主页 测试资源 历史记录 日志 工具 帮助

你好! BFS

文件上传

数据处理

文件生成

“文件上传”部分完成的工作是对pcap文件的报文内容进行解析，对不同地址对的报文进行分类，并显示分类结果。

1. 上传待解析的pcap文件，点击“解析文件”按钮，然后根据“解析文件”功能的返回内容，输入要处理的协议类型的名称。

2. 输入协议类型的名称后，点击“获取协议”，得到分类结果。

“文件上传”部分的参数配置说明：

1. 选择文件：选择用于测试的pcap文件。

2. 协议类型：pcap文件中想要处理的报文的协议类型，用于对pcap文件中的报文进行过滤。

选择文件

未解析到文件数据

协议类型

未选择协议类型

解析文件

获取协议

下一步

图 5-32 文件上传

5.1.1.27 数据处理

本界面主要包括数据处理窗口以及上方的菜单栏，主页面包括数据处理操作说明、报文分段两个部分。

数据处理窗口是协议逆向的子窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。如下图所示。



图 5-33 数据处理

5.1.1.28 文件生成

本界面主要包括文件生成窗口以及上方的菜单栏，主页面包括文件生成操作说明、文件生成内容两个部分。

文件生成窗口是协议逆向的子窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。如下图所示。



图 5-34 文件生成

5.1.1.29 最小集生成

本界面主要包括最小集生成窗口以及上方的菜单栏，主页面包括数据选择、数据显示两个部分。

最小集生成窗口是始终存在的窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。如下图所示。



图 5-35 最小集生成

5.1.1.30 风暴攻击数据监控

本界面主要包括风暴攻击数据监控窗口以及上方的菜单栏，主页面包括操作列表、参数设置两个部分。

风暴攻击数据监控窗口是风暴攻击的子窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。如下图所示。



图 5-36 风暴攻击数据监控

5.1.1.31 风暴攻击启动测试

本界面主要包括风暴攻击启动测试窗口以及上方的菜单栏，主页面包括操作列表、参数设置两个部分。

风暴攻击启动测试窗口是风暴攻击的子窗口，各视图及其对应工具栏在窗口内显示，工作时通过切换到不同的视图以进行不同模块的操作。如下图所示。



图 5-37 风暴攻击启动测试

5.1.1.32 故障详细信息

本界面主要包括故障详细信息窗口以及上方的菜单栏，主页面包括错误图片展示一个部分。

故障详细信息窗口告知用户在路由跳转中产生了错误，如下图所示。



出现了未知错误。

北京理工大学信息系统及安全对抗实验中心(ISSSEC) All rights reserved. Beta 0.1

图 5-38 故障详细信息

5.1.1.33 菜单及功能

1. 一级菜单

用户端页面的一级菜单有主页、测试资源、历史记录、日志、工具、帮助等功能，分别对应不同的页面。

2. 二级菜单及其功能

用户端页面一级菜单中的测试资源、工具、帮助均包含二级菜单。

- 1) 测试资源的二级菜单包括新建测试套、运行测试套。
- 2) 工具的二级菜单包括协议逆向、最小集生成、风暴攻击。
- 3) 帮助的二级菜单包括用户指南、开发者指南、编程接口。

从用户端页面的一级菜单进入测试套配置、测试详情、协议逆向、最小集生成、风暴攻击后会出现二级菜单。

1) 测试套配置的二级菜单包括配置相关参数、配置数据监控、字段调整、验证测试套、启动测试。

2) 测试详情的二级菜单包括故障总览、突变因子、突变记录、相关元素、状态统计、数据集、存储变化时间轴、Bucket。

3) 协议逆向的二级菜单包括文件上传、数据处理、文件生成。

4) 最小集生成的二级菜单包括测试运行、打开生成子集。

5) 风暴攻击的二级菜单包括配置数据监控、启动测试。

5.1.2 功能操作

5.1.2.1 登录注册操作说明

1. 用户注册

用户可通过注册页面完成账号注册，若用户名不合法，两次输入不一致系统均会给出相应提示；最下方语言栏可切换系统语言，支持简体中文与 English 两种语言；点击“注册”按钮后，系统对用户名进行判断，不允许注册相同用户名，注册成功后则直接转到系统主页。



图 5-39 用户注册页面

2. 用户登录

用户注册成功后即可使用账号密码登录，系统对用户输入进行判断，若有不一致返回“账号或密码错误”，反之登录成功，转到主页面。



图 5-40 用户登录页面中文版

切换语言为英文后登录页面如下图所示。

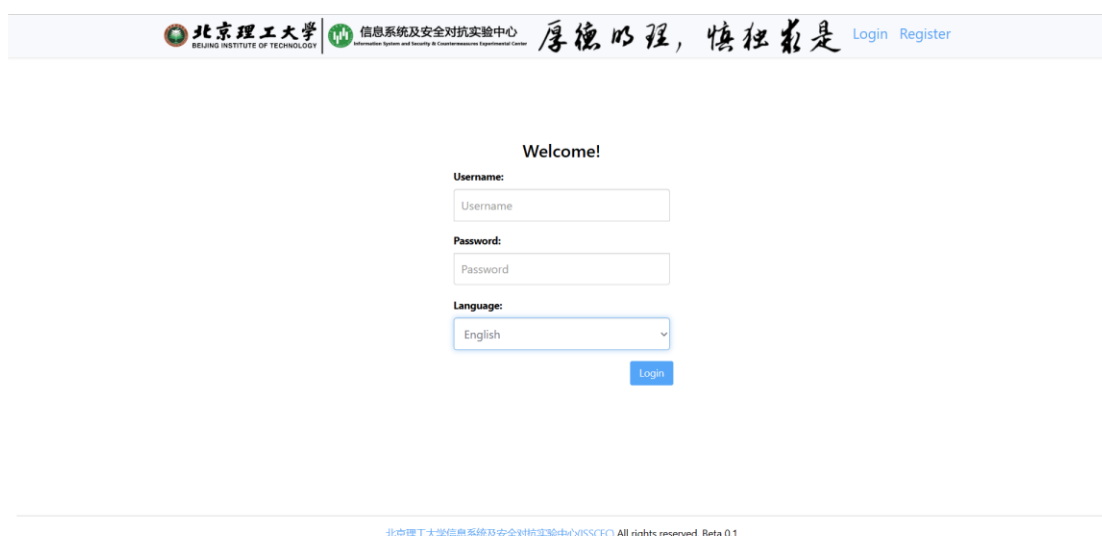


图 5-41 用户登录页面英文版

5.1.2.2 密码修改操作说明

用户登录成功后，将鼠标移至右上角并点击“修改密码”选项即可进行密码修改，“退出登录”将移除用户登录状态，使用户返回至登录界面。



图 5-42 修改密码

点击后用户需在弹窗中输入原密码并确认新密码，若有输入错误则系统弹出提示，当原密码正确时对用户密码进行修改。

用户BFS密码修改

原密码

新密码

确认新密码

图 5-43 修改密码页面

5.1.2.3 模糊测试操作说明

1. 新建测试套

点击测试资源进入新建测试套页面后，点击“新建测试套”在弹窗页面中填写测试套名与自定义描述，测试套的名称不能相同，作为测试套的唯一标识符。建立完相关测试套后即进入测试套配置页面。



图 5-44 新建测试套配置

2. 运行测试套

若之前已经新建过测试套，则可进入运行测试套页面进行选择。

灵通测 主页 测试资源 历史记录 日志 工具 帮助 你好! BFS									
测试套搜索...				Q	首页	上一页	1	下一页	尾页
当前第1页/共9页 转到 页									
序号	测试套名	标签	描述	修改时间	运行	复制	编辑	删除	
1	zes128xn778	数据模型 系统测试	用于系统测试的测试套	2023-04-12 15:35:31	运行	复制	编辑	删除	
2	multi-publisher-166	数据模型 系统测试		2023-04-11 19:21:31	运行	复制	编辑	删除	

图 5-45 运行测试套页面

(1) 运行测试套

点击“运行”即可进入测试套配置页面。

(2) 复制测试套

复制测试套

这将会创建 multi-publisher-166 测试套的一份复制

测试套名

multi-publisher-166

描述

取消

提交

图 5-46 复制测试套页面

点击“复制”按钮后，在弹窗中填写复制后的测试套名与相关描述。填写完毕后点击“提交”即可完成测试套复制。

复制的测试套配置参数、监视器选择、字段调整等属性均与原测试套相同。

(3) 编辑测试套

编辑测试套

测试套名

multi-publisher-166

描述

取消

提交

图 5-47 编辑测试套页面

点击“编辑”可改变当前测试套的名称与描述，测试套参数配置、监视器、字段调整等参数不变，若需对上述参数做出调整，可点击“运行”按钮进入测试套配置页面进行调整。

(4) 删除测试套

点击“删除”按钮即可完成对测试套的删除。

3. 测试套配置

进入测试套配置页面进行参数调整。

灵通测

主页 测试资源 历史记录 日志 工具 帮助

你好! BFS

[配置相关参数](#) [配置数据监控](#) [字段调整](#) [验证测试套](#) [启动测试](#)

此页面用于配置所选测试套的测试所需的相关参数：

- 测试套参数：用户可自行修改设置，若不加修改则为默认值
- 系统参数：包括测试任务编号、操作系统、安装目录、工作目录、日志目录、插件目录、脚本目录以及资料库路径

用户可在此界面设置所选测试套的测试环境，在测试前必须配置这些参数，以确保测试套测试环境的正确。

保存 + 添加参数 下一步

System Defines(系统参数定义)

Name(参数名)	Key(主函数)	Value(参数值)
Gumiho Job Id(任务编号)	Gumiho.JobId	00000000-0000-0000-0000-000000000000 Job ID for current fuzzing run(当前模糊测试运行的任务ID)
Gumiho OS(操作系统)	Gumiho.OS	windows Operating System that Gumiho is running on(模糊测试运行的操作系统)
Gumiho Installation Directory(安装目录)	Gumiho.Pwd	F:\peach\Gumiho\Gumiho\output\win64\bin Full path to Gumiho installation(模糊测试的完整安装路径)
Gumiho Working Directory(工作目录)	Gumiho.Cwd	F:\peach\Gumiho\Gumiho\output\win64\bin Full path to the current working directory(模糊测试的完整工作路径)

图 5-48 测试套配置页面

(1) 配置相关参数

默认参数已完成配置，可直接进入下一步配置数据监控，根据需要可点击添加参数配置自定义测试套需要的参数，添加参数后点击“保存”按钮即可使添加的参数生效，随后点击“下一步”或二级菜单栏配置监视器设置。

添加参数

变量名

变量1

请输入，此处不能为空

密钥

GREATBFS

请输入，此处不能为空

值

BFS

图 5-49 配置相关参数

(2) 配置数据监控

配置数据监控页面用于为选择的测试套定义一个或多个代理，并可以选择添加一个或多个监视器。其中代理是监视器和发包器的主体。本地代理可以与测试平台处于同一台计算机上，并且可以通过监视器和发包器控制测试环境。远程代理处于测试目标设备上，可以提供远程监视器和发包器信息。



图 5-50 配置数据监控

点击“添加代理”后系统在最下方新建代理窗口，设置最下方新添加的代理名称与代理地址后，点击“添加监视器”按钮选择需要的监视器。输入监视器需要的特定参数后点击最上方的“保存”按钮即完成对监视器的配置。

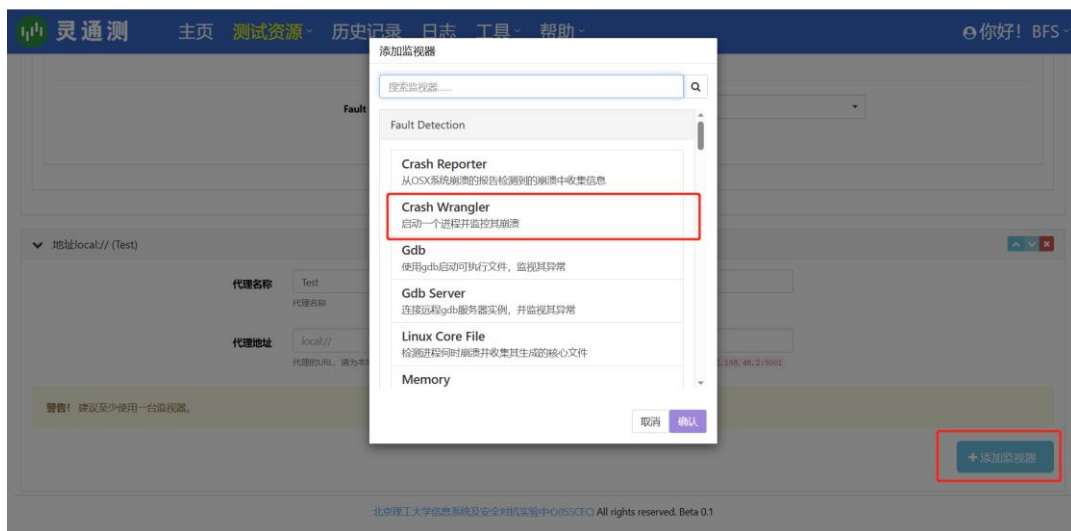


图 5-51 添加监视器

(3) 配置字段调整

配置数据监控页面允许逐字段控制测试进行。可以从测试中排除某个字段或某一组字段，也可以自由调整该字段测试焦点的高低。

左侧所示是字段焦点的分类情况，当字段的焦点调高（“高”或“最高”）时，将更频繁地为该字段生成测试用例。如果某个字段被调低（“低”、“最低”），则将为该字段生成的测试用例更少。其中被排除的字段不会生成任何测试用例。



图 5-52 字段调整

调整完字段后点击“保存”按钮，即可将字段调整应用到测试套中。

(4) 验证测试套

点击“验证测试套”按钮开始对测试套的验证，运行一个测试用例确保配置

测试套后能够成功运行。



图 5-53 验证测试套

开始测试套验证后界面下方将展示测试总览与测试日志，测试总览记录测试流程中记录的相关信息与可能产生的问题；测试日志记录测试过程中的输出细节与可能的报错位置。测试总览与测试日志帮助测试人员更加深入地了解测试过程并快速定位和解决问题

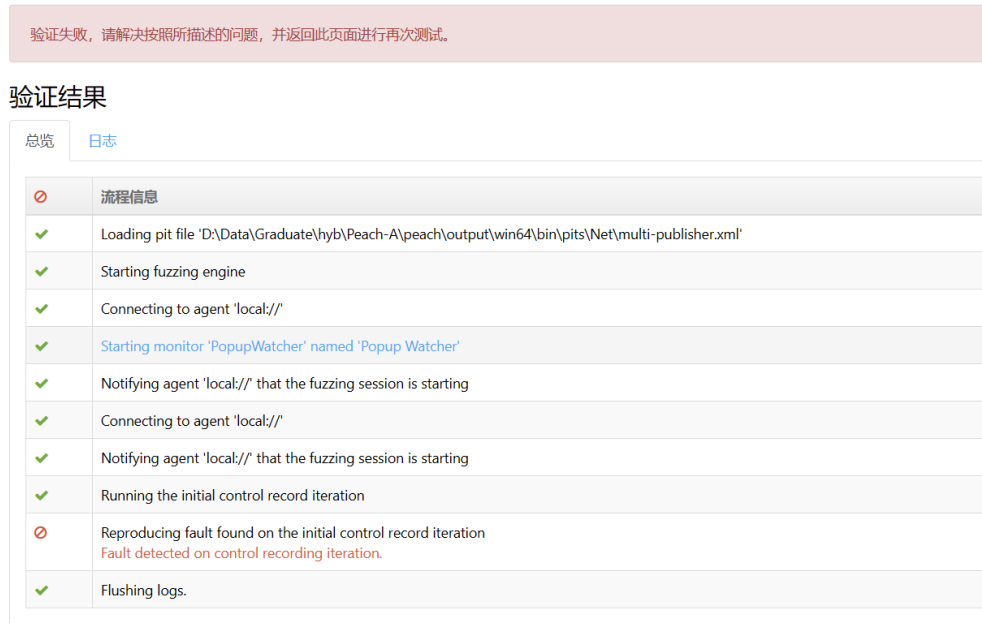


图 5-54 测试套验证失败示例

若测试套验证失败，则需要根据测试总览与测试日志定位出错位置并对测试套配置进行调整，直至测试成功才能启动后续测试。



图 5-55 测试套验证通过示例

(5) 启动测试



图 5-56 启动测试页面

验证测试套通过后即可正式开始测试，可对随机种子和测试终止值进行配置。若未输入随机种子则系统会自动产生，设置相应的随机种子可对历史记录中产生的故障或变异进行复现；若未输入测试终止值则系统会提示输入，测试起始值默认为 1。设置完相关参数后即可点击上方的“开始测试”按钮正式开始测试。

(6) 查看详情

点击“开始测试”后进入查看详情页面，最上方按钮可对模糊测试进程进行控制，根据需要暂停模糊测试，继续模糊测试或停止模糊测试。按钮下方显示实时测试状态的进度条，横轴表示测试用例总数，纵轴表示每小时能完成的测试用例数。进度条下方记录本次测试的开始时间、运行时间、随机种子、总故障数等信息，以及测试过程中产生的故障信息。最下方实时显示测试过程中系统产生的日志信息。



图 5-57 实时测试状态页面

测试完成或停止测试后，可点击上方的操作按钮进行后续操作。点击“测试详情”按钮可查看测试过程中发现的故障及突变等信息；点击“报告导出”按钮可导出并下载当前测试报告；点击“重新测试”按钮将返回到启动测试页面，初始测试参数使用前一轮测试时的随机种子、测试起始值和终止值开展测试；点击“修改参数”将跳转到编辑配置参数页面，用户可对相关参数或监视器进行修改或删除。



图 5-58 实时测试状态页面功能按钮

5.1.2.4 历史记录操作说明

用户完成一轮测试后，进入历史记录页面，该页面提供对历史记录的分页与搜索功能，用户可根据测试套名称对历史记录进行搜索。同时用户可在历史记录

主页 测试资源 历史记录 日志 工具 帮助

你好！BFS-

历史记录搜索...							Q	首页	上一页	1	下一页	末页	当前第1页/共1页	转到	页
序号	名称	状态	开始时间	结束时间	测试用例	错误总数	查看详情	报告下载	删除记录						
1	multi-publisher-11	Stopped	2023-04-19 14:03:53	2023-04-19 14:04:05	200	0	查看详情	报告下载	删除记录						
2	multi-publisher-11	Stopped	2023-04-19 14:03:29	2023-04-19 14:03:43	200	0	查看详情	报告下载	删除记录						
3	multi-publisher-11	Stopped	2023-04-19 12:06:51	2023-04-19 12:07:06	100	0	查看详情	报告下载	删除记录						
4	multi-publisher-11	Stopped	2023-04-19 11:56:30	2023-04-19 11:56:43	200	0	查看详情	报告下载	删除记录						
5	multi-publisher-11	Stopped	2023-04-19 11:56:10	2023-04-19 11:56:24	200	0	查看详情	报告下载	删除记录						
6	multi-publisher-11	Stopped	2023-04-19 11:54:27	2023-04-19 11:54:41	200	0	查看详情	报告下载	删除记录						
7	multi-publisher-11	Stopped	2023-04-19 11:49:17	2023-04-19 11:49:20	50	0	查看详情	报告下载	删除记录						
8	multi-publisher-11	Stopped	2023-04-19 08:58:26	2023-04-19 08:58:41	51	0	查看详情	报告下载	删除记录						
9	xm1 datamodel	Stopped	2023-04-16 20:17:27	2023-04-16 20:17:54	192	0	查看详情	报告下载	删除记录						
10	xm1 datamodel	Stopped	2023-04-16 20:15:54	2023-04-16 20:17:13	409	0	查看详情	报告下载	删除记录						

图 5-59 历史记录页面

灵通测

主页

测试资源

历史记录

日志

工具

帮助

你好! BFS

测试详情

报告导出

重新测试

修改参数

实时测试状态

16116263136414651566166717681869196101106111116121126131136141146151156161166171176181186191196

2023-04-19 14:03:53

开始时间

00h 00m 11s

运行时间

65454

每小时测试用例数

9163

随机种子

200

已执行的测试用例数

0

总故障数

近期故障

#用例数	日期	监视器	风险	主要Bucket	最小Bucket	下载
无可用数据						

日志

测试未开始

图 5-60 实时测试状态页面



图 5-61 历史记录页面故障总览

突变因子页面记录了在本次测试中产生突变用例的突变因子。



图 5-62 历史记录页面突变因子

突变记录页面记录了测试过程中产生所有突变的状态信息，同时该页面提供变异复现功能。

状态统计页面显示了具有两个以上状态的测试套模型的统计数据。下述列表显示了特定状态在模糊测试过程中出现的次数。不常使用的状态可能隐含问题。



图 5-66 历史记录页面状态统计

数据集页面显示模糊测试过程中使用两个或多个数据集的相关统计信息。这有助于确定唯一 bucket 的来源，以及在变异中使用的数据资源方面的故障。



图 5-67 历史记录页面数据集

存储变化时间轴页面展示了一个时间线，其中列出了新的故障 bucket 以及在模糊测试过程中发现 bucket 的总次数。用户可向左或向右拖动移动时间线，并

使用鼠标滚轮放大或缩小。



图 5-68 历史记录页面存储变化时间轴

Bucket 页面显示模糊测试过程中遇到的 Bucket。



图 5-69 历史记录页面 Bucket

5.1.2.5 变异复现操作说明

若需开展变异复现则需在历史记录页面中点击查看详情，跳转到查看详情页面后点击上方“测试详情”按钮，再点击“突变记录”即可查看变异记录。

灵通测

主页测试资源历史记录日志工具帮助

你好! BFS

故障总览

突变因子

突变记录

相关元素

状态统计

数据集

存储变化时间轴

Bucket

返回

变异记录搜索...

Q

首页

上一页

1

下一页

尾页

当前第1页/共4页

转到

页

编号	测试轮次	状态编号	动作编号	参数编号	元素编号	变异编号	数据编号	类型	变异复现	用例解析
1	1 rounds	MiddleState	Two2		Ping.str	StringUtf32BomStatic		0	变异复现	用例解析
7	1 rounds	MiddleState	Three2		Ping.num	DataElementBitFlipper		0	变异复现	用例解析
9	1 rounds	MiddleState	Two2		Ping.str	StringUnicodeFormatCharacters		0	变异复现	用例解析
11	1 rounds	MiddleState	One2		Ping.str	StringUtf8ExtraBytes		0	变异复现	用例解析
13	1 rounds	MiddleState	Two2		Ping.str	StringUtf32BomLength		0	变异复现	用例解析
15	1 rounds	MiddleState	Three2		Ping.str	StringUtf8BomLength		0	变异复现	用例解析
19	1 rounds	MiddleState	Four2		Ping.str	StringUtf16BomStatic		0	变异复现	用例解析
21	1 rounds	MiddleState	Three2		Ping.str	StringUtf8Invalid		0	变异复现	用例解析
25	1 rounds	MiddleState	Three2		Ping.str	StringUnicodePlane1		0	变异复现	用例解析
27	1 rounds	MiddleState	Three2		Ping.num	DataElementDuplicate		0	变异复现	用例解析

北京理工大学信息系统及安全对抗实验中心(CISSCEC) All rights reserved. Beta 0.1

图 5-70 历史记录页面突变记录变异复现操作

点击突变记录后可看到所有突变的相关信息，在最上方可对变异状态进行搜索。当未进行变异复现时，可对测试用例进行解析。

选择需要进行复现的突变记录后，点击“变异复现”按钮后进入变异复现页面，点击“返回”按钮即返回突变记录页面，可重新选择需要复现的突变记录。页面中显示该突变的状态信息与本次测试的随机种子，可选择单轮/多轮模式开展变异复现。其中单轮复现中变异类型固定为测试中产生的变异类型无需修改。

灵通测

主页测试资源历史记录日志工具帮助

你好! BFS

测试套已完成环境配置, 点击“开始复现”按钮进行编辑测试复现。

本次变异复现选择的测试套为 multi-publisher-100。

返回

开始复现

变异复现

帮助

编号	状态编号	动作编号	参数编号	元素编号	变异编号	数据编号	类型	随机种子
1	MiddleState	Two2		Ping.str	StringUtf32BomStatic		0	55939

单轮

多轮

变异类型 Random

北京理工大学信息系统及安全对抗实验中心(CISSCEC) All rights reserved. Beta 0.1

图 5-71 变异复现页面

多轮复现中需要指定复现测试的测试起始值与终止值，若未指定则系统弹出提示，默认值为变异用例所在的测试轮次。

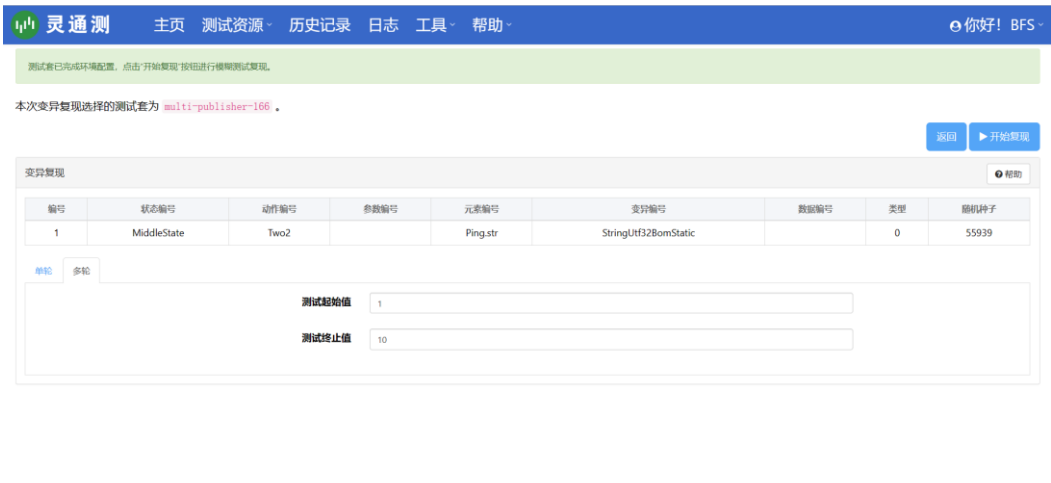


图 5-72 变异复现多轮变异设置

选择多轮变异并点击“开始变异”按钮后，系统检视测试起始与终止轮次间变异，弹窗提示用户变异复现范围内包含的变异轮次和产生的变异用例数，用户若对产生的变异用例不满意可点击“取消”按钮重新选定变异范围。

多轮变异设置

在选定的测试轮次内将进行4轮变异，产生55个变异用例，确定继续吗？

取消

确定

图 5-73 变异复现多轮变异设置

点击“确定”按钮后，系统跳转至变异详情页面，下方日志展示了变异复现的结果。若用户对结果不满意可点击“重新测试”按钮重新开始变异复现，否则点击“变异选择”按钮，返回突变记录页面。

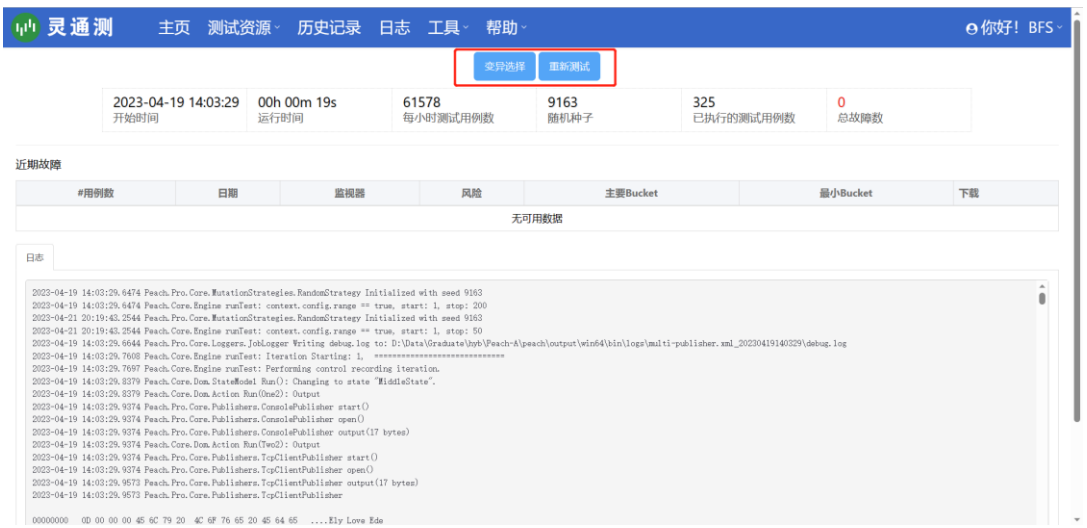


图 5-74 变异复现执行页面

此时在变异复现轮次内的变异用例由于已经进行了变异复现，可以对相应变异进行解析。



北京理工大学信息系统及安全对抗实验中心(CISSCE) All rights reserved. Beta 0.1

图 5-75 历史记录页面突变记录

变异解析后，发现对应值或字符串产生变异发生了变化。

名称	值	长度
num	6475	32
str	Ely Love Eden	

图 5-76 编译解析结果

5.1.2.6 日志查看操作说明

用户仅能查看自己的日志，用户进行登录/退出、新建/使用测试套、添加参数/监视器、进行字段调整/用例测试等操作均会被系统记录。测试套唯一标识符为测试套名，测试任务唯一标识符为其 Guid。



图 5-77 管理员端日志页面

管理员可查看所有人的日志，管理员在用户管理中对用户进行权限更改/密码修改/删除用户等操作均会记录到日志中。



图 5-78 管理员端日志页面

5.1.2.7 协议逆向操作说明

首先进行文件上传，将待解析的 pcap 文件上传，点击“解析文件”按钮，

然后根据“解析文件”功能的返回内容，输入要处理的协议类型的名称。协议类型指 pcap 文件中想要处理的报文的协议类型，用于对 pcap 文件中的报文进行过滤。输入协议类型的名称后，点击“获取协议”，得到分类结果。

灵通测 主页 测试资源 历史记录 日志 工具 帮助 你好! BFS

文件上传 数据处理 文件生成

“文件上传”部分完成的工作是对pcap文件的报文内容进行解析，对不同地址对的报文进行分类，并显示分类结果。

1. 上传待解析的pcap文件，点击“解析文件”按钮，然后根据“解析文件”功能的返回内容，输入要处理的协议类型的名称。
2. 输入协议类型的名称后，点击“获取协议”，得到分类结果。

“文件上传”部分的参数配置说明：

1. 选择文件：选择用于测试的pcap文件。
2. 协议类型：pcap文件中想要处理的报文的协议类型，用于对pcap文件中的报文进行过滤。

选择文件

The protocol include: UDP ADWIN_CONFIG

协议类型

0: endpointsList:('127.0.0.1:57831', '127.0.0.1:4242'), Number of messages:14

解析文件 获取协议 下一步

北京理工大学信息系统及安全对抗实验中心(CISSEC) All rights reserved. Beta 0.1

图 5-79 协议逆向页面文件上传

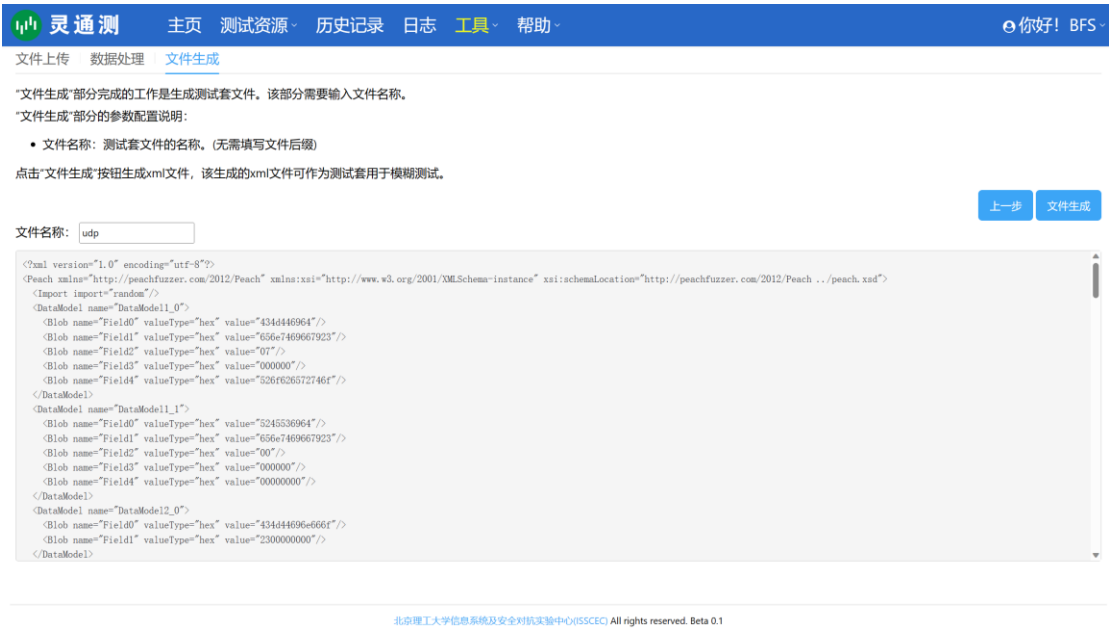
“文件上传”部分完成的工作是对 pcap 文件的报文内容进行解析，对不同地址对的报文进行分类，并显示分类结果。完成文件上传后，进入数据处理部分，该部分需要根据解析结果，输入想处理的报文集序号，以及对协议进行分段的参数。用户输入需要处理的报文集序号后，点击“报文分段”按钮，对所选择的报文集中的报文进行分段，并为报文生成协议状态机链。当数据处理完成后，会将分段的结果将显示于文本框内。



北京理工大学信息系统及安全对抗实验中心(ISSCEC) All rights reserved. Beta 0.1

图 5-80 协议逆向页面数据处理

“数据处理”部分完成的工作是对所选择的报文集中的报文进行分段，并为报文生成协议状态机链。处理完数据后，就可以进行 xml 文件生成。该部分需要输入文件名称。该部分需要根据解析结果，输入想处理的报文集序号，以及对协议进行分段的参数。点击“文件生成”按钮生成 xml 文件，该生成的 xml 文件可作为测试套用于模糊测试。



北京理工大学信息系统及安全对抗实验中心(ISSCEC) All rights reserved. Beta 0.1

图 5-81 协议逆向页面文件生成

“文件生成”部分完成的工作是生成测试套文件，该部分需要用户输入测试套名称。点击“文件生成”按钮后，可以预览测试套文件内容。

当进入新建测试套页面时，可以看到在协议逆向部分生成的测试套（即示例所生成的测试套名为“udp”的测试套）。

灵通测 主页 测试资源 历史记录 日志 工具 帮助 你好! BFS				
测试套搜索		Q	首页 上一页 4 下一页 尾页 当前第4页/共4页 转到 页	
序号	测试套名	标签	描述	新建测试套
31	udp-tst	传输层协议 有线网络协议	UDP协议	新建测试套
32	udp	传输层协议 有线网络协议	UDP协议	新建测试套
33	udp0412	传输层协议 有线网络协议	UDP协议	新建测试套
34	udp0938	传输层协议 有线网络协议	UDP协议	新建测试套
35	xml_datamodel	数据模型 系统测试	用于系统测试的测试套	新建测试套

北京理工大学信息系统及安全对抗实验中心(ISSCEC) All rights reserved. Beta 0.1

图 5-82 测试资源页面

5.1.2.8 最小集生成操作说明

最小集生成模块用于生成给定输入数据中为目标测试程序提供最大代码覆盖率所需的最小示例文件子集。该模块操作流程分为 4 个步骤：选择原数据文件夹、选择目标测试程序、运行日志、生成子集。



图 5-83 最小集生成工具页面

选择原数据文件夹：用于测试的大批量数据所在文件夹路径，测试过程中会新生成 `traces` 和 `minset` 文件夹，将存放于同一目录下。(文件夹需放在：程序安装目录/bin/samples 下)



图 5-84 最小集生成工具页面选择文件夹

选择目标测试程序：要测试的目标程序，应为当前系统下的可执行文件。(测试程序需放在:程序安装目录/bin 下)

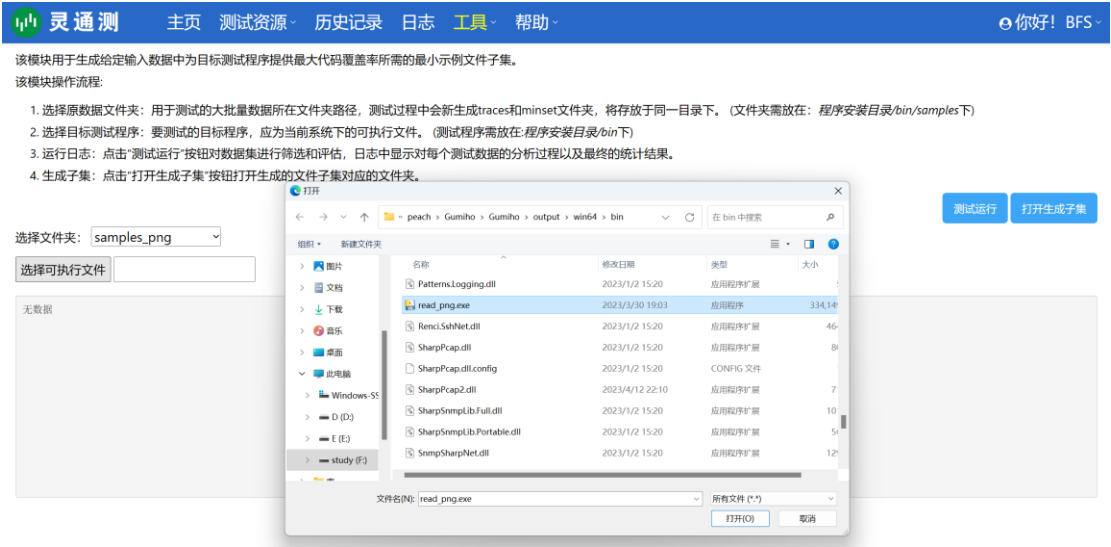


图 5-85 最小集生成工具页面选择文件夹

运行日志：点击“测试运行”按钮对数据集进行筛选和评估，日志中显示对每个测试数据的分析过程以及最终的统计结果。



图 5-86 最小集生成工具页面执行结果

生成子集：点击“打开生成子集”按钮打开生成的文件子集对应的文件夹。



图 5-87 最小集生成工具页面打开生成子集

5.1.2.9 风暴攻击操作说明

风暴攻击模块首先需进行监视器配置。



图 5-88 风暴攻击监视器配置

随后需要配置相关参数，配置好相关参数后即可开展风暴攻击，其中参数配置说明如下：

控制模式：目前该模块只支持 ARP 协议和 TCP 协议，用户可自由选择。

截止发包数、截止时间（ms）：用于控制风暴攻击截止的条件（二选一）。

监视器调用间隔（发包数）、监视器调用间隔（ms）：用于控制监视器调用的条件（二选一）。

注：监视器调用间隔（发包数）应与截止发包数对应，监视器调用间隔（ms）应与截止时间（ms）对应。

IP 地址（TCP）、端口（TCP）：用于 TCP 协议风暴攻击的参数。

注：成功实现 TCP 协议风暴攻击测试需要保证 IP 地址（TCP）的端口（TCP）可以连接访问。两个参数均不可为空！

目标 IP、源 IP、源 MAC、ARP 模型选择：用于 ARP 协议风暴攻击的参数。

注：ARP 模型选择为 1 时，由大量随机源 IP 向目标 IP 发送大量 request 数据包。ARP 模型选择为 2 时，由源 IP 向不同目标 IP 发送大量 reply 数据包。四个参数均不可为空！

灵通测

主页测试资源历史记录日志用户管理工具帮助

你好! admin

配置数据监控启动测试

监视环境已完成配置，点击“开始测试”按钮进行风暴攻击测试。

此界面用于配置攻击需要的参数，用户选择攻击模式并给出攻击所需的信息，即可启动风暴攻击。

上一步

开始测试

测试参数配置

帮助

TCPARP

截止发包数

10000

截止时间(ms)

0

监视器调用间隔(发包数)

3000

监视器调用间隔(ms)

0

目标IP

192.168.0.8

源IP

192.168.0.9

源MAC

1C-1B-85-63-7F-9F

ARP模型选择

1

北京理工大学信息系统及安全对抗实验中心eSSCIC All rights reserved. Beta 0.1

图 5-89 风暴攻击启动测试

点击“开始测试”按钮后，系统开展风暴攻击。

灵通测

主页测试资源历史记录日志用户管理工具帮助

你好! admin

这项工作已完成。

重新测试

修改参数

2023-05-06 11:27:03	00h 00m 00s	0	10000	4	0
开始时间	运行时间	每小时测试轮数	发包数/测试时间 (s)	测试轮数	总故障数

近期故障

#用例数	日期	监视器	风险	主要Bucket	最小Bucket	下载
无可用数据						

日志

2023-05-06 11:27:03.7877 Gmibh.Pro.Core.Loggers.JobLogger Writing debug log to: D:\now_task\peach\peach-zn\Gmibh\output\win64\bin\Logs\Storm Attack.mal_20230506112703\debug.log

2023-05-06 11:27:03.8528 Gmibh.Core.Agent.Channels.AgentLocal StartMonitor: Popup Watcher PopupWatcher

2023-05-06 11:27:03.8528 Gmibh.Core.Agent.Channels.AgentLocal SessionStarting

2023-05-06 11:27:03.8528 Gmibh.Core.Engine.RunProtocol: Iteration Starting: 0, 4

2023-05-06 11:27:04.1196 Gmibh.Core.Agent.AgentManager DetectedFault: checking for fault in agent 1

2023-05-06 11:27:04.1196 Gmibh.Core.Engine.RunProtocol: Iteration Starting: 1, 4

2023-05-06 11:27:04.3701 Gmibh.Core.Agent.AgentManager DetectedFault: checking for fault in agent 1

2023-05-06 11:27:04.3701 Gmibh.Core.Engine.RunProtocol: Iteration Starting: 2, 4

2023-05-06 11:27:04.5108 Gmibh.Core.Agent.AgentManager DetectedFault: checking for fault in agent 1

2023-05-06 11:27:04.5108 Gmibh.Core.Engine.RunProtocol: Iteration Starting: 3, 4

2023-05-06 11:27:04.7474 Gmibh.Core.Agent.AgentManager DetectedFault: checking for fault in agent 1

2023-05-06 11:27:04.7474 Gmibh.Core.Engine all test cases executed, stopping engine.

2023-05-06 11:27:04.7474 Gmibh.Core.Engine EndTest: Stopping all agents and monitors

2023-05-06 11:27:04.7474 Gmibh.Pro.Core.Storage.AsyncDbCache An unexpected error occurred saving the job report. Report can not contain a null job.

2023-05-06 11:27:04.7615 Gmibh.Pro.Core.Runtime.JobRunner Flushing Logs (Version: 0.0.0.0)

北京理工大学信息系统及安全对抗实验中心(CISSCEC) All rights reserved. Beta 0.1

图 5-90 风暴攻击开始测试