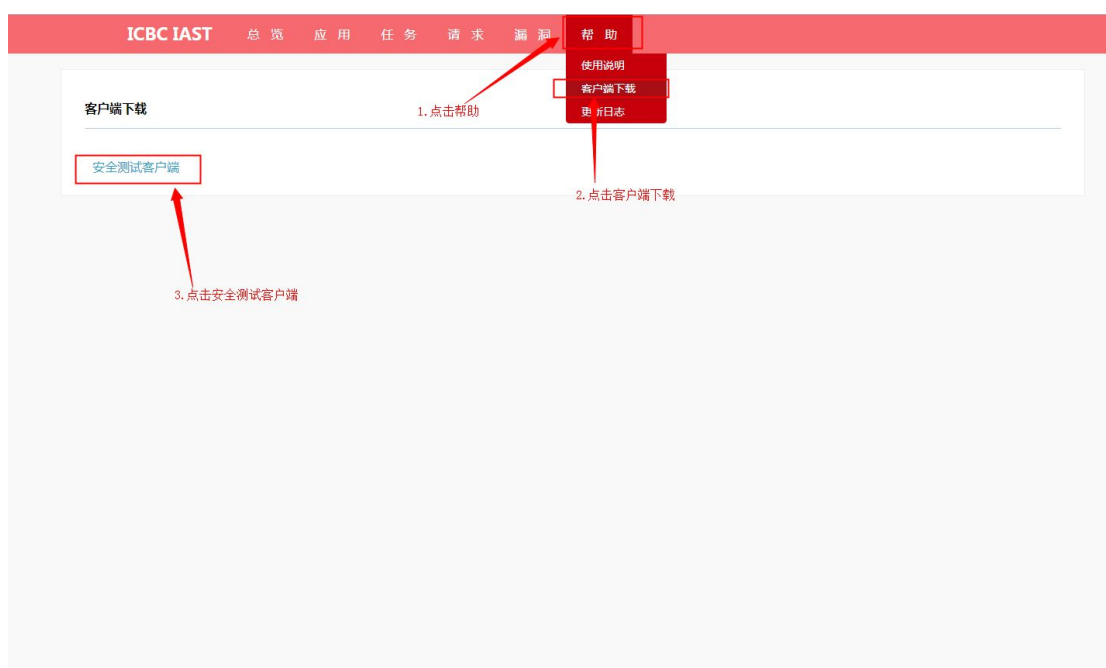


交互试安全测试平台

简介：本项目一个交互式安全测试平台，客户可在进行业务测试的同时，可以自动完成安全测试。

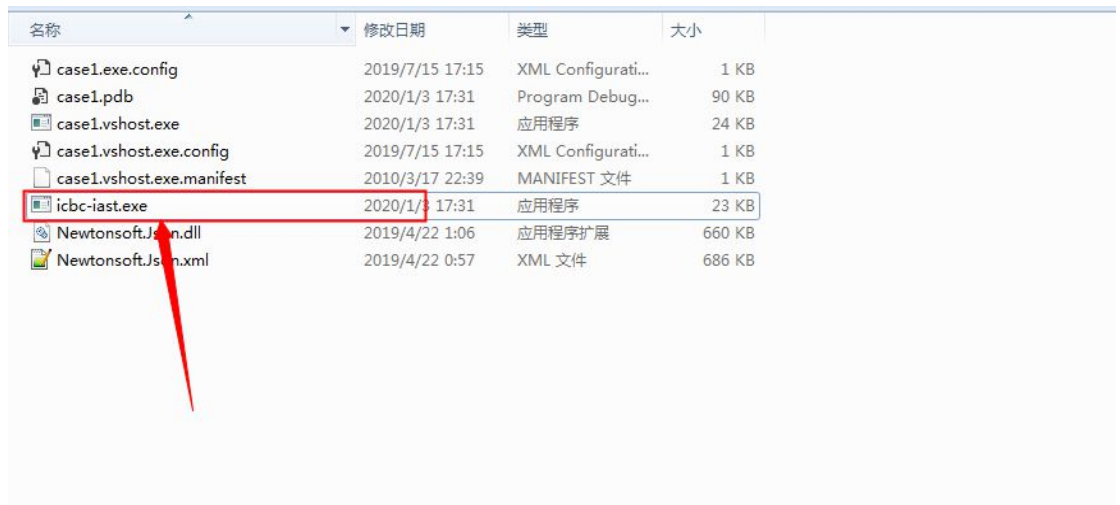
使用手册：

步骤一：如图所示，以下三步下载系统的客户端



步骤二:下载的客户端 icbc-iast.zip。解压 Zip 文件。

**步骤三：解压之后呈现，并且双击打开 IAST.exe 文件，
如图示：**



步骤四：点击*.exe 后，显示如图所示：

客户端

统一认证号: 1. 录入统一认证号

测试账号: 2. 录入测试账号

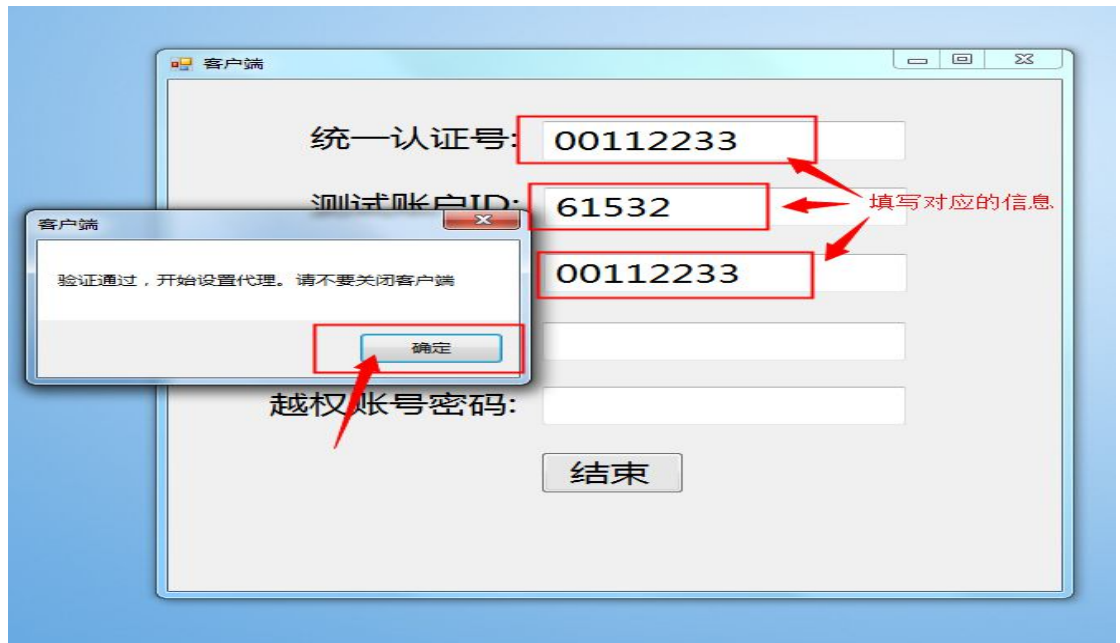
测试账号密码: 3. 录入测试账号的密码

越权账号: 4. 需要测试越权，录入越权账号

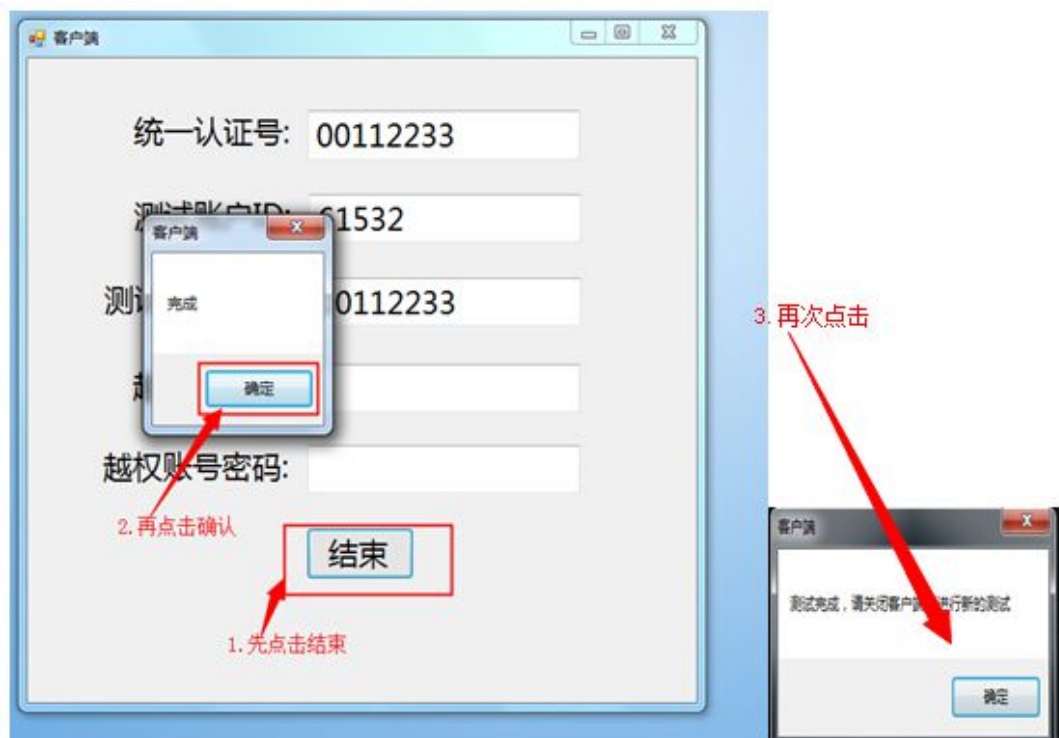
越权账号密码: 5. 越权账号密码

开始

步骤五：点击开始按钮，如图所示，点击确认，默认给浏览器设置代理，打开浏览器，开始录入数据

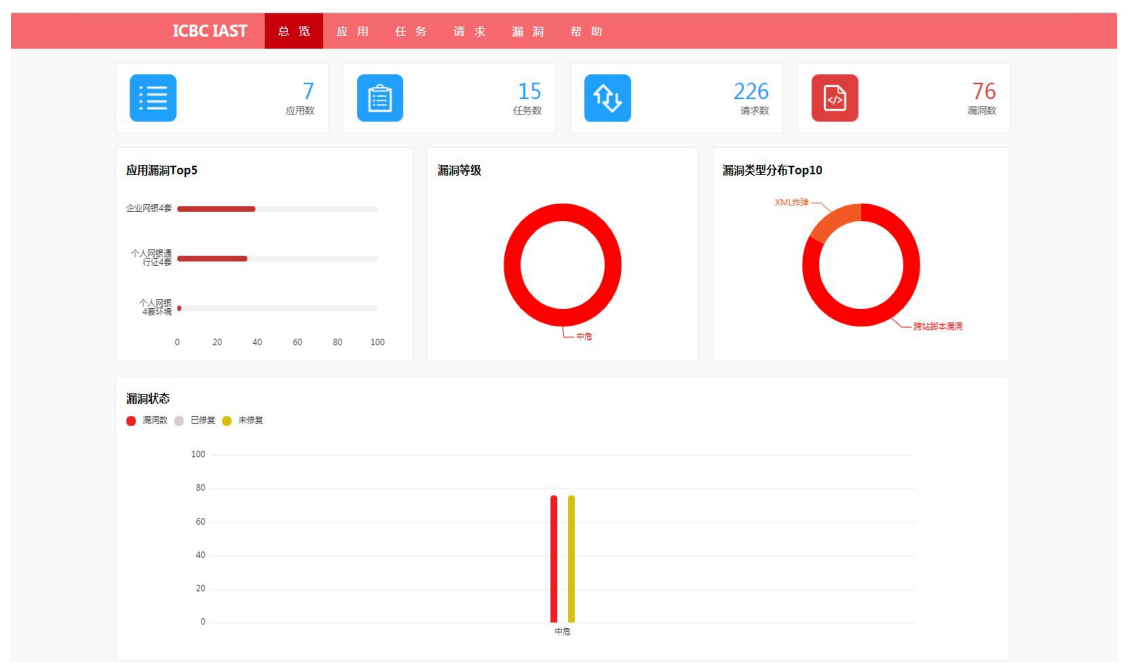


步骤六：录完数据后，点击如图 1，点击如图 2，之后点击如图 3

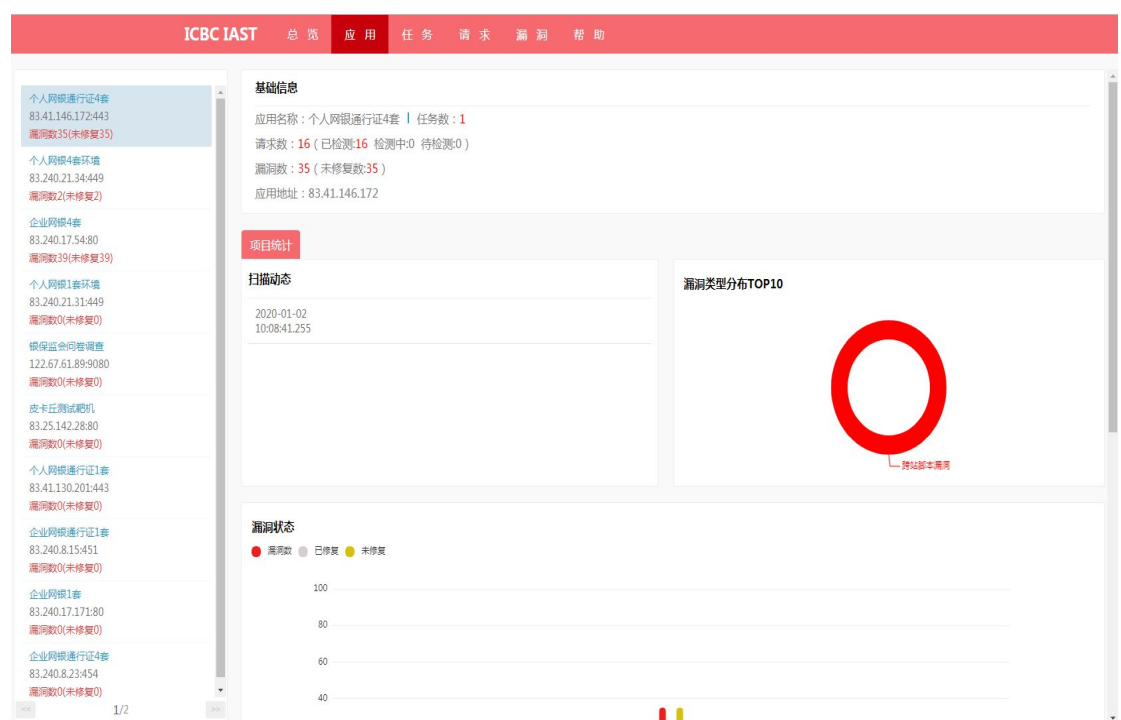


步骤七：数据录入完成，数据会后台自动测试，录入人只需要在页面看数据即可，

7.1 如图所示：显示页面总览的信息



7.2 如图所示：显示应用的信息



ICBC IAST

总 览应 用任 务请 求漏 洞帮 助

请输入用户编号

搜 索

刷 新

任务id	用户编号	客户端ip	开始记录任务时间	结束记录任务时间	任务开始时间	任务结束时间	任务状态
17	00551122	83.10.29.162	2020-01-02 14:54:27	2020-01-02 14:56:28	2020-01-02 14:56:28	2020-01-02 14:56:28	测试完成
16	555034032	83.10.29.163	2020-01-02 14:53:43	2020-01-02 14:55:49			录入结束
15	001187131	83.10.93.33	2020-01-02 14:50:28				录入中
14	555034032	83.10.29.163	2020-01-02 14:43:21	2020-01-02 14:46:31			录入结束
13	001144557	83.10.29.162	2020-01-02 14:39:00	2020-01-02 14:39:13	2020-01-02 14:39:13	2020-01-02 14:39:13	测试完成
12	555034032	83.10.29.163	2020-01-02 13:49:00	2020-01-02 14:00:40	2020-01-02 14:01:38	2020-01-02 14:02:25	测试完成
10	001187131	83.10.93.33	2020-01-02 11:13:20	2020-01-02 11:13:55	2020-01-02 11:13:55	2020-01-02 11:13:55	测试完成
9	001187131	83.10.93.33	2020-01-02 11:12:30	2020-01-02 11:13:05	2020-01-02 11:13:05	2020-01-02 11:13:05	测试完成
8	555034032	83.10.29.163	2020-01-02 11:01:14	2020-01-02 11:03:04	2020-01-02 11:03:56	2020-01-02 11:07:02	测试完成
7	555034032	83.10.29.163	2020-01-02 10:54:44	2020-01-02 10:57:00	2020-01-02 10:57:57	2020-01-02 10:58:32	测试完成

上一页

12

下一页

共2页, 跳至 1 页 确定

[illegible]

ICBC IAST

总览应用任务请求漏洞帮助

		请选择条件 + 请输入关键字		搜索		刷新	
<div>漏洞类型 用户编号</div>							
漏洞类型	用户编号	URL	项目名称	检测时间	状态	操作	备注
跨站脚本漏洞	555034032	https://epass4.dccnet.com.cn/login/hiddenPage1.jsp?forwardUrl=http	个人网银通行证4套	2020-01-02 10:08:41	未修复	详情	发送攻击向量...
跨站脚本漏洞	555034032	https://epass4.dccnet.com.cn/login/hiddenPage1.jsp?forwardUrl=http	个人网银通行证4套	2020-01-02 10:08:41	未修复	详情	发送攻击向量...
跨站脚本漏洞	555034032	https://epass4.dccnet.com.cn/login/hiddenPage1.jsp?forwardUrl=http	个人网银通行证4套	2020-01-02 10:08:41	未修复	详情	发送攻击向量...
跨站脚本漏洞	555034032	https://epass4.dccnet.com.cn/login/hiddenPage1.jsp?forwardUrl=http	个人网银通行证4套	2020-01-02 10:08:41	未修复	详情	发送攻击向量...
跨站脚本漏洞	555034032	https://epass4.dccnet.com.cn/login/hiddenPage1.jsp?forwardUrl=http	个人网银通行证4套	2020-01-02 10:08:41	未修复	详情	发送攻击向量...
跨站脚本漏洞	555034032	https://epass4.dccnet.com.cn/login/hiddenPage1.jsp?forwardUrl=http	个人网银通行证4套	2020-01-02 10:08:45	未修复	详情	发送攻击向量...
跨站脚本漏洞	555034032	https://epass4.dccnet.com.cn/login/hiddenPage1.jsp?forwardUrl=http	个人网银通行证4套	2020-01-02 10:08:45	未修复	详情	发送攻击向量...
跨站脚本漏洞	555034032	https://epass4.dccnet.com.cn/login/hiddenPage1.jsp?forwardUrl=http	个人网银通行证4套	2020-01-02 10:08:45	未修复	详情	发送攻击向量...
跨站脚本漏洞	555034032	https://epass4.dccnet.com.cn/login/hiddenPage1.jsp?forwardUrl=http	个人网银通行证4套	2020-01-02 10:08:45	未修复	详情	发送攻击向量...
跨站脚本漏洞	555034032	https://epass4.dccnet.com.cn/login/hiddenPage1.jsp?forwardUrl=http	个人网银通行证4套	2020-01-02 10:08:45	未修复	详情	发送攻击向量...
跨站脚本漏洞	555034032	https://epass4.dccnet.com.cn/login/hiddenPage1.jsp?forwardUrl=http	个人网银通行证4套	2020-01-02 10:08:45	未修复	详情	发送攻击向量...
跨站脚本漏洞	555034032	https://epass4.dccnet.com.cn/login/hiddenPage1.jsp?forwardUrl=http	个人网银通行证4套	2020-01-02 10:08:45	未修复	详情	发送攻击向量...

上一页

1

2

3

4

5

下一页

共7页, 跳至

1

页 确定

ICBC IAST 总览 应用 任务 请求 漏洞 帮助

漏洞概述

漏洞等级: 中 状态: 未修复

漏洞类型: 跨站脚本漏洞

测试人员: huangl

检测时间: 2020-01-02 10:08:41.255

漏洞地址: https://epass4.dccnet.com.cn/login/hiddenPage1.jsp?forwardUrl=https://vip.dccnet.com.cn:449/servlet/com.icbc.inbs.servlet.ICBCINBSEstablishSessionServlet

漏洞描述

跨站脚本 (Cross-site scripting, 简称XSS)

由于动态网页的Web应用对用户提交的请求中的参数未做充分的检查过滤, 允许攻击者在提交的数据中加入HTML、JS代码, 未加编码地输出到第三方用户的浏览器, 并最终导致攻击者构造的恶意脚本在用户浏览器中执行。跨站脚本攻击危害十分严重, 如可以窃取用户cookie, 伪造用户身份登录、可控制用户浏览器、结合浏览器及其插件漏洞, 下载病毒木马到浏览者的计算机、衍生URL跳转漏洞、键盘攻击、钓鱼欺骗等。

修复建议

- 1 严格校验用户输入的数据, 必须对所有输入中的script、iframe等字样进行严格的检查和html escape转义。这里的输入不仅仅是用户可以直接交互的输入接口, 还包括HTTP请求中的cookie中的变量, HTTP请求头部中的变量等。
- 2 校验数据类型, 验证其格式、长度、范围和内容。
- 3 客户端, 服务端进行双重校验。
- 4 对输出的数据也要检查, 因为数据库里的值有可能会在一个大网站的多处都有输出, 所以即使在输入做了编码等操作, 在各处的输出点时也要进行安全检查。

漏洞演示

原始请求

测试响应

```
GET
https://epass4.dccnet.com.cn/login/hiddenPage1.jsp?forwardUrl=https://vip.dccnet.com.cn:449/servlet/com.icbc.inbs.servlet.ICBCINBSEstablishSessionServlet
Accept:text/html,application/xhtml+xml,*/*
Referer:https://epass4.dccnet.com.cn/login/login.jsp?StructCode=1&orgurl=0&STNO=354&betaFlag=0&encryptedData=iRUtWZtC0R5ev/d5e07Kt7ai5450

GET
https://epass4.dccnet.com.cn:443/login/hiddenPage1.jsp?forwardUrl=%3CIMGSRc%3D%27javascrip%3Awindow.navigate%28%27http%3A%2F%2Fabc.com%27%29%3B%27%3E
Accept:text/html,application/xhtml+xml,*/*
Referer:https://epass4.dccnet.com.cn/login/login.jsp?StructCode=1&orgurl=0&STNO=354&betaFlag=0&encryptedData=iRUtWZtC0R5ev/d5e07Kt7ai5450
```