**实操笔记（Burp Suite教程）[DeepSeek翻译-老祁头整理-软件版本:2025.3.1]**

**版权与责任声明**

**▲内容性质**

о本文档技术要点基于 PortSwigger 官方文档（2025-05-23版）核心逻辑重构

о实操笔记均为自主测试验证结论，**与 PortSwigger Ltd. 无任何关联**  
▲**侵权处理**  
若内容引用方式存争议，请24小时内邮件至 [slqxd@163.com](https://mailto:slqxd@163.com" \t "https://chat.deepseek.com/a/chat/s/_blank)，我们将：  
 ✓立即下架涉嫌内容  
 ✓提供修改记录供核查  
▲**用户责任**  
使用者应自行确保：  
 ✓已获目标系统书面授权  
 ✓充分理解测试可能引发的服务中断、数据损坏等风险

**Burp Suite 使用注意事项**  
Burp Suite 作为安全测试工具，**部分功能可能对目标系统造成损害**。安全漏洞检测本质上涉及非常规的交互操作，某些存在漏洞的目标系统可能因此出现异常。使用时请务必：

**充分阅读官方文档**

**测试前备份目标系统**

**严格限制测试范围**（仅限拥有书面授权或明确接受风险的系统）

[译者注：实际测试中曾遇老旧系统因基础扫描崩溃，务必评估目标健壮性！]

**Burp Suite** 是 Web 应用程序安全测试领域事实上的**行业标准工具**。它本质上是一个**集成化的渗透测试平台**，核心功能在于拦截、查看和修改浏览器与目标 Web 应用之间的 **HTTP/S 流量（抓包与改包）**。其强大之处在于将一系列专门的安全测试工具（如代理服务器、扫描器、爬虫、中继器、入侵器、编码器等）无缝整合在一个界面中，极大地提升了安全测试人员发现、分析和利用 Web 漏洞（如 SQL 注入、XSS、CSRF、逻辑缺陷等）的效率。无论是手动安全测试、自动化扫描还是漏洞验证，Burp Suite 都是安全研究人员、渗透测试工程师和漏洞赏金猎人的**必备利器**。本笔记将记录使用 Burp Suite 进行各项安全测试的**关键操作与实战细节**。

**第一篇 Burp Suite 入门指南**

Burp Suite 是一套功能全面的 Web 应用程序安全测试工具集。

本交互式教程旨在帮助您**快速上手掌握 Burp Suite 的核心功能**。教程将引导您使用来自 **Web安全学院 (Web Security Academy)** [译者注：Web Security Academy 是 PortSwigger 官方提供的免费网络安全学习平台] 特意设计的存在漏洞的实验环境（Labs），让您通过实际操作来亲身体验 Burp Suite 的工作方式。 [译者注：强烈建议初学者从这里开始实践，实验环境安全且目标明确。]

**第一章 Burp Suite 系统要求**

Burp Suite 的系统要求在很大程度上取决于您使用该软件的预期目的。虽然通常在配置较低的机器上也能执行大多数任务，但某些使用场景（例如，并行运行多个扫描任务）可能需要显著更强的硬件性能，才能保证运行流畅，避免出现明显的性能下降。

**一、CPU 核心数 / 内存**

**（一）最低要求：** 双核 CPU，4GB 内存 - 此配置适用于基本任务，例如代理 Web 流量和简单的入侵攻击（Intruder attacks）。虽然 Burp Suite 可能在低于此规格的机器上运行，但出于性能考虑，我们不建议这样做。 [译者注：实际体验中，4GB内存运行基础功能尚可，但多开标签或处理稍大项目会明显卡顿，强烈建议至少8GB起步。]

**（二）推荐配置：** 双核 CPU，16GB 内存 - 这是一个良好的通用型配置。 [译者注：16GB内存是当前比较流畅运行Burp进行常规渗透测试的甜点配置。]

**（三）高级配置：** 四核 CPU，32GB 内存 - 此配置适用于更密集的任务，例如复杂的入侵攻击（Intruder attacks）或大型自动化扫描。 [译者注：进行大型应用扫描、高频Intruder攻击或同时处理多个复杂项目时，高内存和多核CPU能极大提升效率，减少卡死。]

**二、可用磁盘空间**

**（一）基础安装：** 约需 1GB

**（二）每个项目文件：** 建议预留至少 2GB

**注意：**

虽然建议为每个项目预留 2GB 的可用磁盘空间作为最低要求，但请注意，项目文件的实际大小可能远超此值（甚至可能达到数十GB）。其大小取决于多种因素，例如包含的代理历史记录数量、运行的扫描次数以及打开的重放器（Repeater）标签页数量。 [译者注：务必定期清理不需要的代理历史（Proxy History）和临时项目文件，否则磁盘占用会飞速增长。建议将项目保存在空间充足的磁盘分区。]

**三、操作系统与架构**

Burp Suite 支持以下操作系统的最新版本：

**（一）Windows** (Intel 64位)

**（二）Linux** (Intel 和 ARM 64位)

**（三）macOS** (Intel 64位 和 Apple M1/M系列) [译者注：更新了Apple Silicon的通用称呼]

**四、内置浏览器**

Burp Suite 的内置浏览器对操作系统和架构有额外的要求，与以下环境**不兼容**：

**（一）较旧版本的 Windows**，包括 Windows 7, Windows 8/8.1, Windows Server 2012 以及 Windows Server 2012 R2。

**（二）**在 **Apple Silicon (M系列)** 或 **ARM 64位** 系统上**通过 JAR 文件运行**的 Burp Suite 实例。若您想在这些芯片架构的系统上使用 Burp 的内置浏览器，请确保使用**对应平台的原生安装程序**来安装 Burp Suite。 [译者注：在M芯片Mac上，务必下载dmg/pkg安装包安装，而非直接运行JAR，否则内置浏览器不可用。]

**重要提示：**

即使您使用的是平台原生安装程序版本（而非JAR文件），也**仍然可以同时运行多个 Burp Suite 实例**。此功能并不仅限于通过 JAR 文件运行的实例。 [译者注：这对于需要同时处理多个独立项目或测试场景非常有用。]

**第二章 Burp Suite 下载与安装**

**步骤 1：下载**

请通过以下链接下载最新版本的 Burp Suite Professional（专业版）或 Community Edition（社区版）：

**选择您需要的版本：**

1、[Burp Suite Professional](https://portswigger.net/burp/releases/professional-community/latest" \t "https://chat.deepseek.com/a/chat/s/_blank) [译者注：国内访问官方下载服务器有时较慢，可尝试寻找可靠的国内镜像源或使用网络加速工具。]

2、[Burp Suite Community Edition](https://portswigger.net/burp/releases/professional-community/latest" \t "https://chat.deepseek.com/a/chat/s/_blank) [译者注：社区版功能受限，但完全免费，是初学者入门的最佳选择。]

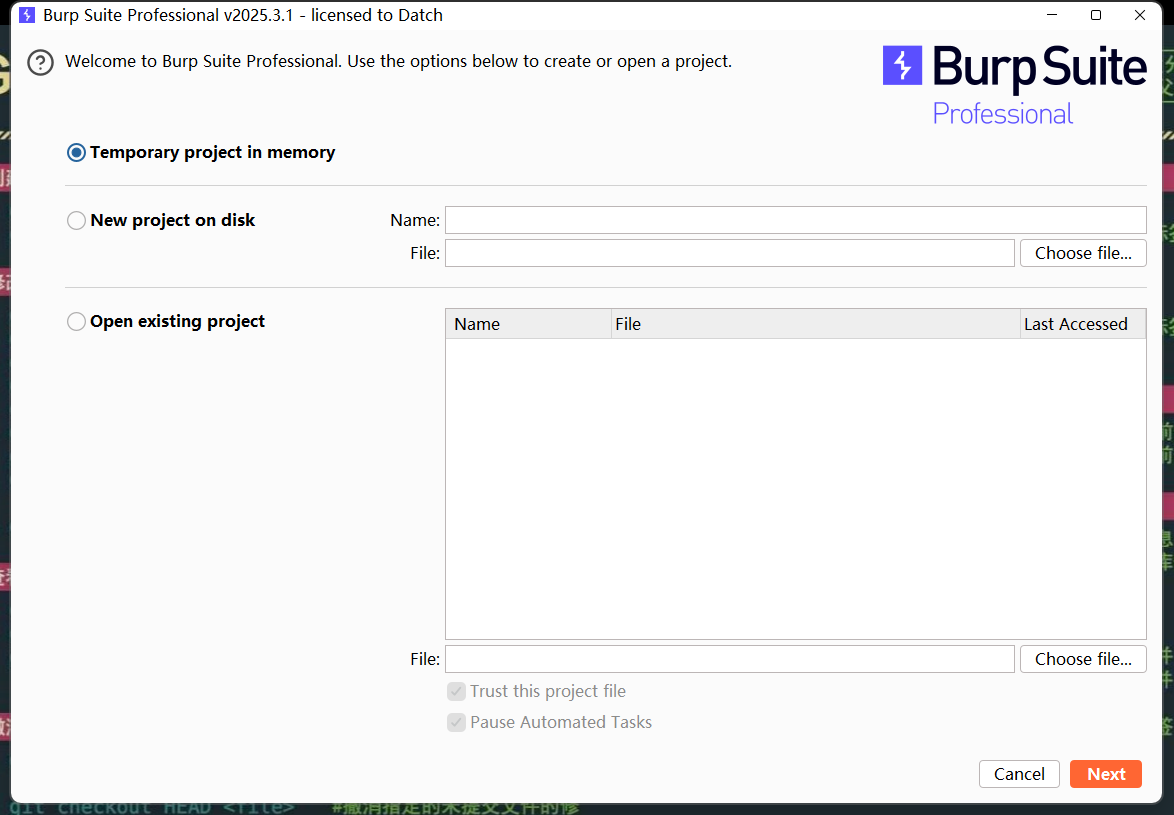
**步骤 2：安装**

****1、**运行安装程序：** 双击下载好的安装文件开始安装过程，一路默认就好。

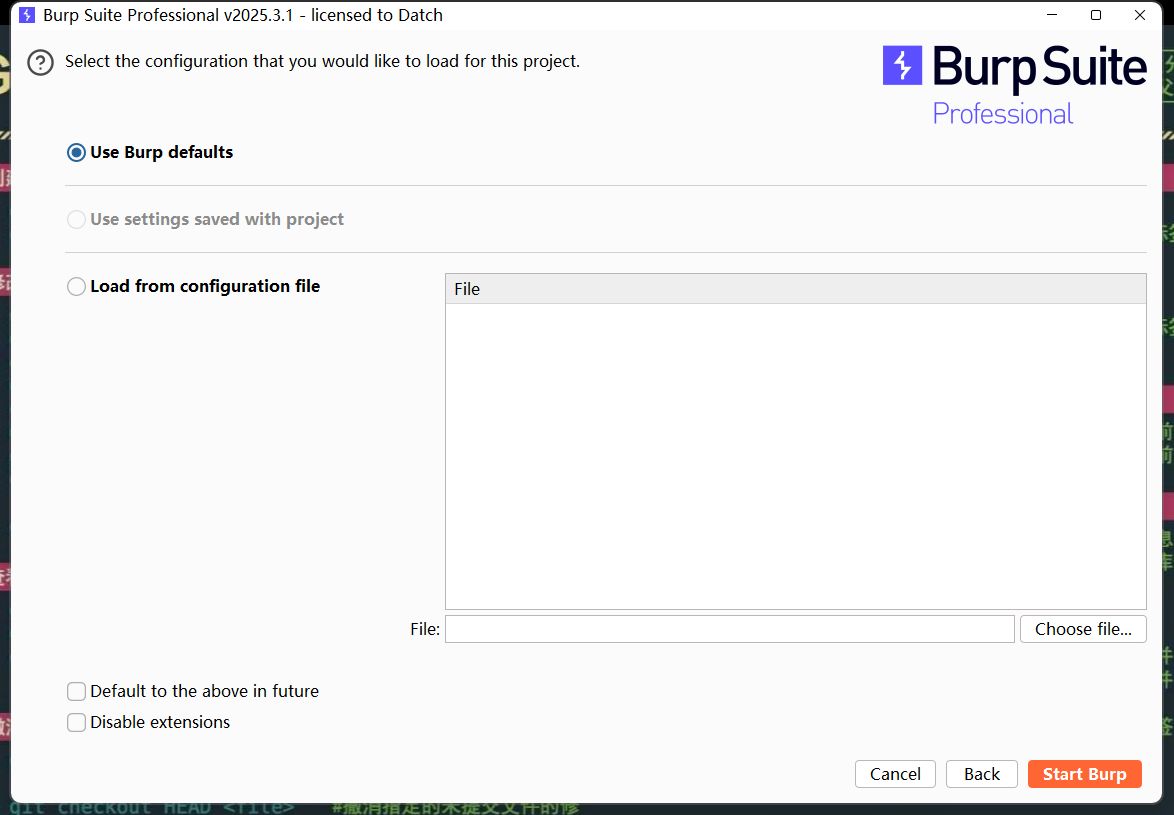
****2、**启动 Burp Suite：** 安装完成后，通常会自动启动 Burp Suite。如果没有，请在开始菜单（Windows）或应用程序文件夹（macOS/Linux）中找到并启动它。

****3、**初始设置：** 首次启动时，程序会提示您**选择项目文件和配置**。作为初次使用，您可以直接：

****（1）**点击** 下一步 **(Next)**



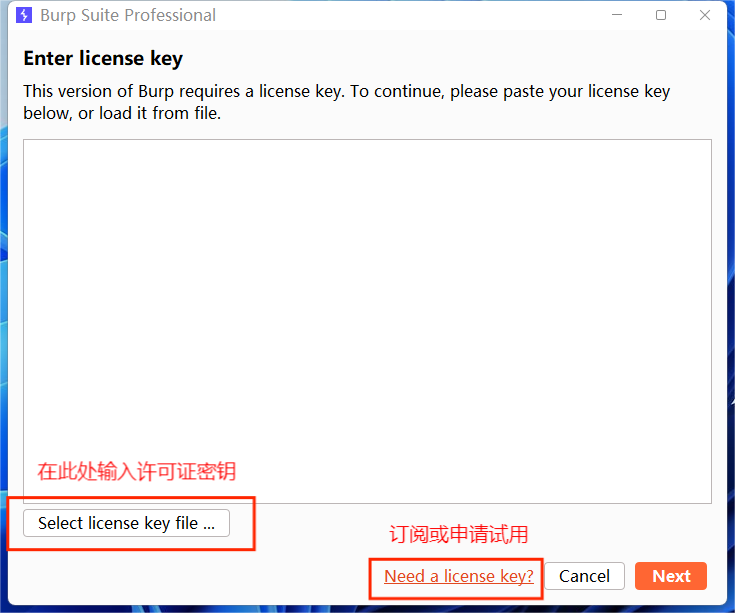
1. **然后点击** 启动 Burp **(Start Burp)**



（3）这样即可暂时跳过此步骤。 [译者注：初次启动建议直接跳过配置创建空项目，熟悉后再创建正式项目文件。安装路径建议保持默认或选择空间充足的磁盘分区。]

**重要提示：**

如果您使用的是 **Burp Suite Professional**，在启动过程中程序会**提示您输入许可证密钥**。如果您还没有密钥，可以访问 PortSwigger 官网[购买订阅](https://portswigger.net/buy" \t "https://chat.deepseek.com/a/chat/s/_blank)或[申请免费试用](https://portswigger.net/burp/pro" \t "https://chat.deepseek.com/a/chat/s/_blank)。 [译者注：试用期通常为14天，建议先熟悉基础功能再决定是否购买专业版。务必保管好许可证密钥。]



**步骤 3：开始探索 Burp Suite**

如果您是 **Burp Suite 的完全新手**，强烈建议您继续**跟随本教程的后续指引**。它提供了一个**交互式的导览**，带您逐步了解 Burp Suite 的**核心功能**和基本操作。 [译者注：官方交互教程是最高效的学习路径，务必动手操作！遇到问题可查阅文档或社区论坛。]

### Burp Proxy 流量拦截实战指南

**一、实验目标**  
通过预设漏洞的在线实验环境，掌握使用 Burp Proxy 拦截 HTTP 流量的核心方法。  
[注：实验平台来自 PortSwigger Web Security Academy]

### ****二、HTTP 请求拦截原理****

Burp Proxy 可捕获浏览器与目标服务器间的 HTTP 请求/响应，使您能够：  
✓ 分析网站对不同操作的反馈机制  
✓ 实时修改通信内容  
[译者注：实际渗透测试中常用于绕过客户端验证、篡改参数等]

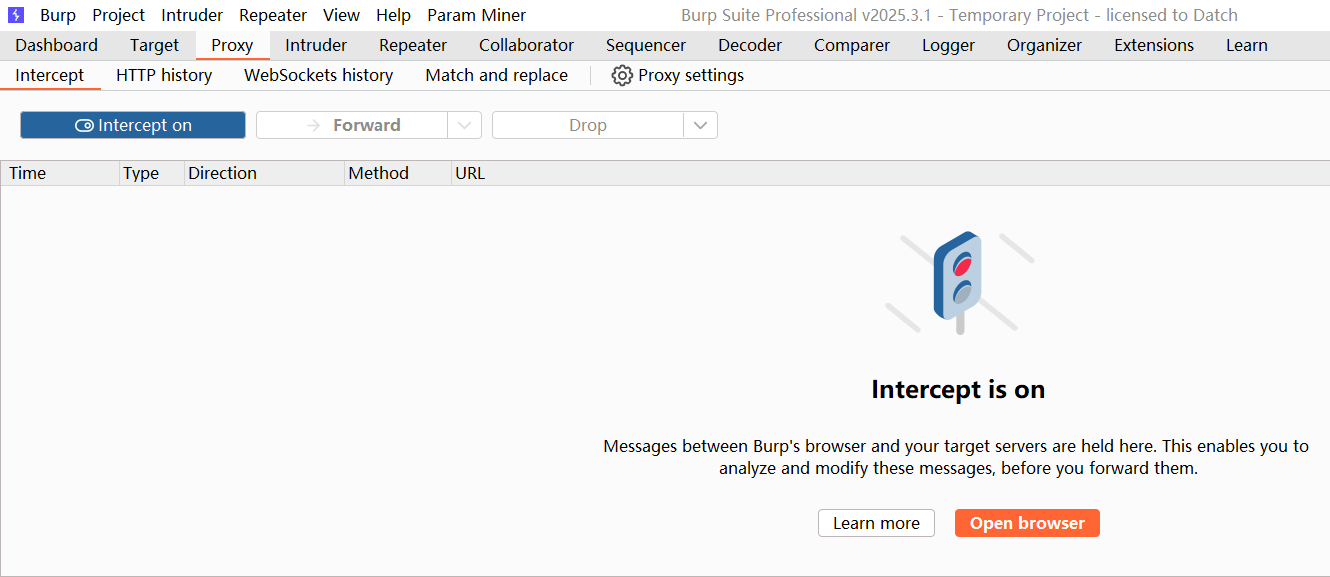
### ****三、操作流程****

**步骤1：启动内置浏览器**

1、进入 Proxy > Intercept 标签页

2、将拦截开关设为 Intercept is on

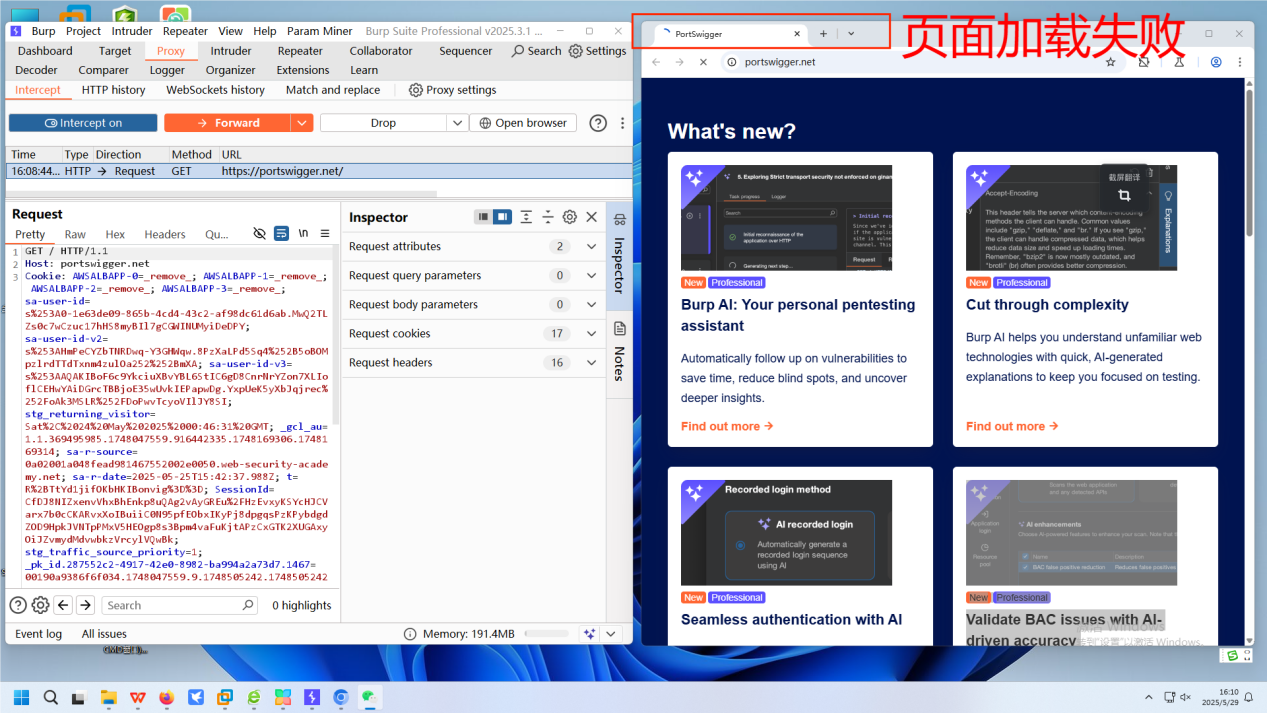
3、点击 Open Browser 启动预配置浏览器

  
[关键提示] 调整窗口布局确保同时可见 Burp 界面与浏览器

**步骤2：触发请求拦截**

1、在内置浏览器访问 https://portswigger.net

2、页面将**停止加载**（请求已被拦截）



3、此时可在 Proxy > Intercept 查看被冻结的原始请求  
[故障排查] 若未拦截成功：检查浏览器代理设置是否为127.0.0.1:8080

**步骤3：放行请求**

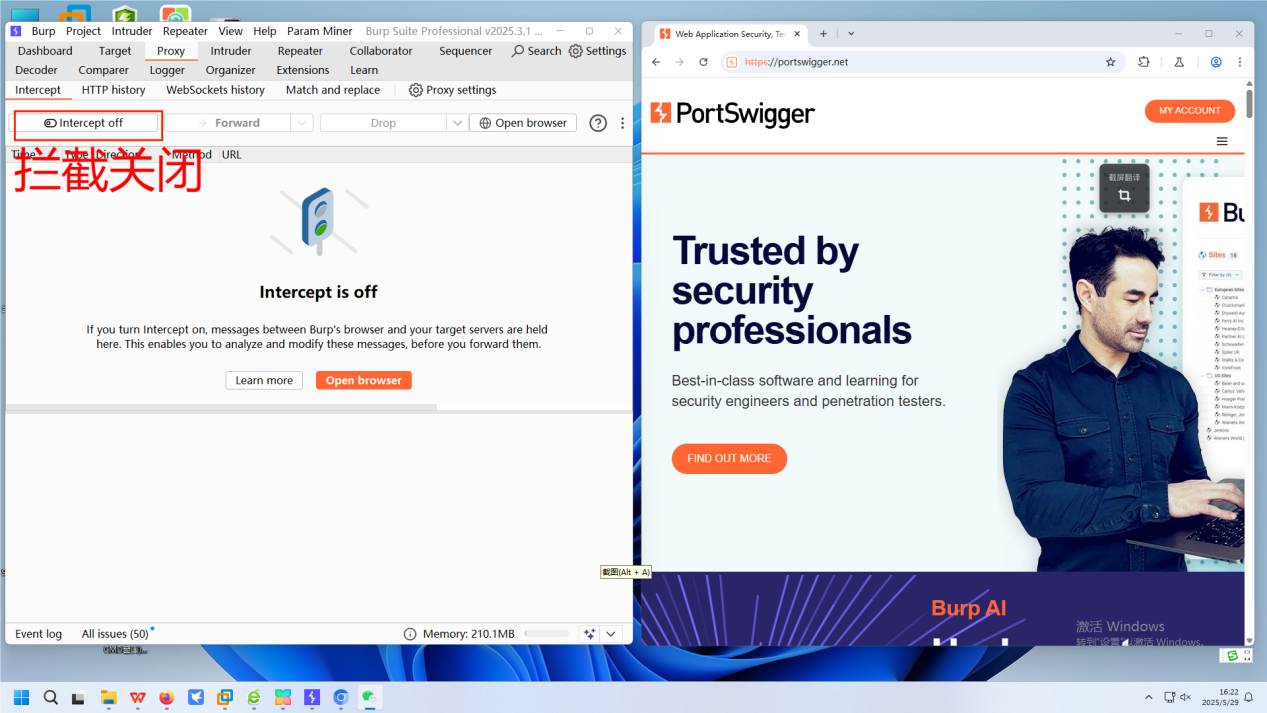
1、点击 Forward 发送当前请求

**2、重复点击**直至页面完成加载（通常需放行多个关联请求）  
[实战技巧] 按住Ctrl多选请求可批量放行

**步骤4：关闭拦截模式**

1、将开关设为 Intercept is off

2、返回浏览器验证网站功能是否恢复正常  
[原理说明] 禁用拦截可避免处理非关键请求（如图片/CSS等）



**步骤5：查看历史流量**

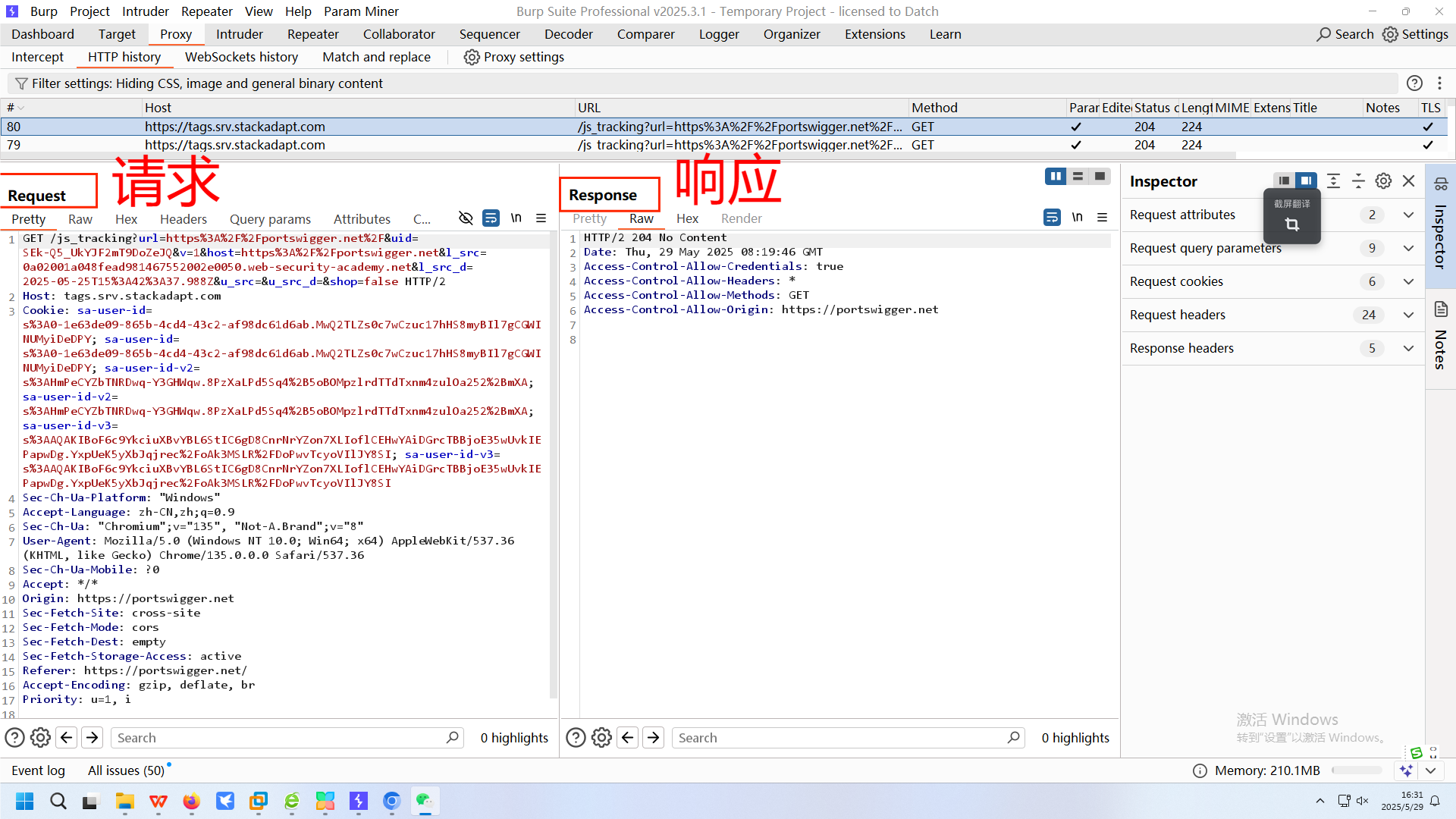
1、切换至 Proxy > HTTP history 标签页

**2、所有过往流量**按时间倒序排列（含拦截关闭期间的记录）

3、点击任意条目可查看：

（1）原始 HTTP 请求

（2）服务器返回的完整响应  
[分析技巧] 使用过滤器（Filter）快速定位关键请求



### 第四章 Burp Proxy 请求篡改实战指南

**一、实验目标**  
通过预置漏洞的在线训练平台，掌握拦截请求的实时修改技术，观察目标系统的异常响应行为。  
[注：实验环境来自 PortSwigger Web Security Academy]

### ****二、前置准备****

（一）拥有 **portswigger.net** 免费账户（[注册入口](https://portswigger.net/users/register" \t "https://chat.deepseek.com/a/chat/s/_blank)）

（二）确保 Burp Proxy 拦截功能处于关闭状态（Proxy > Intercept → Intercept is off）

### ****三、漏洞利用五步法****

**步骤1：启动实验环境**

1、在 Burp 内置浏览器访问训练平台 URL：

<https://portswigger.net/web-security/logic-flaws/examples/lab-logic-flaws-excessive-trust-in-client-side-controls>

2、点击 启动实验环境（需登录 PortSwigger 账户）

3、进入模拟电商网站界面  
[注意] 此环境专为安全训练设计，禁止用于真实系统

**步骤2：登录测试账户**

1、点击 我的账户

2、使用凭证登录：

用户名： wiener

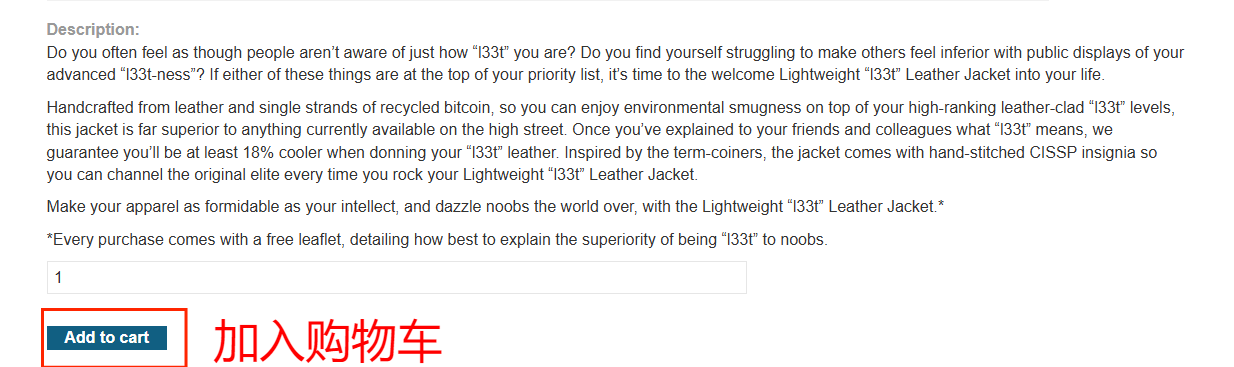
密码： peter

1. 确认账户余额 **$100**

**步骤3：定位目标商品**

1、返回首页

2、选择 **轻量级"l33t"皮质夹克** 查看详情



**步骤4：拦截购买请求**

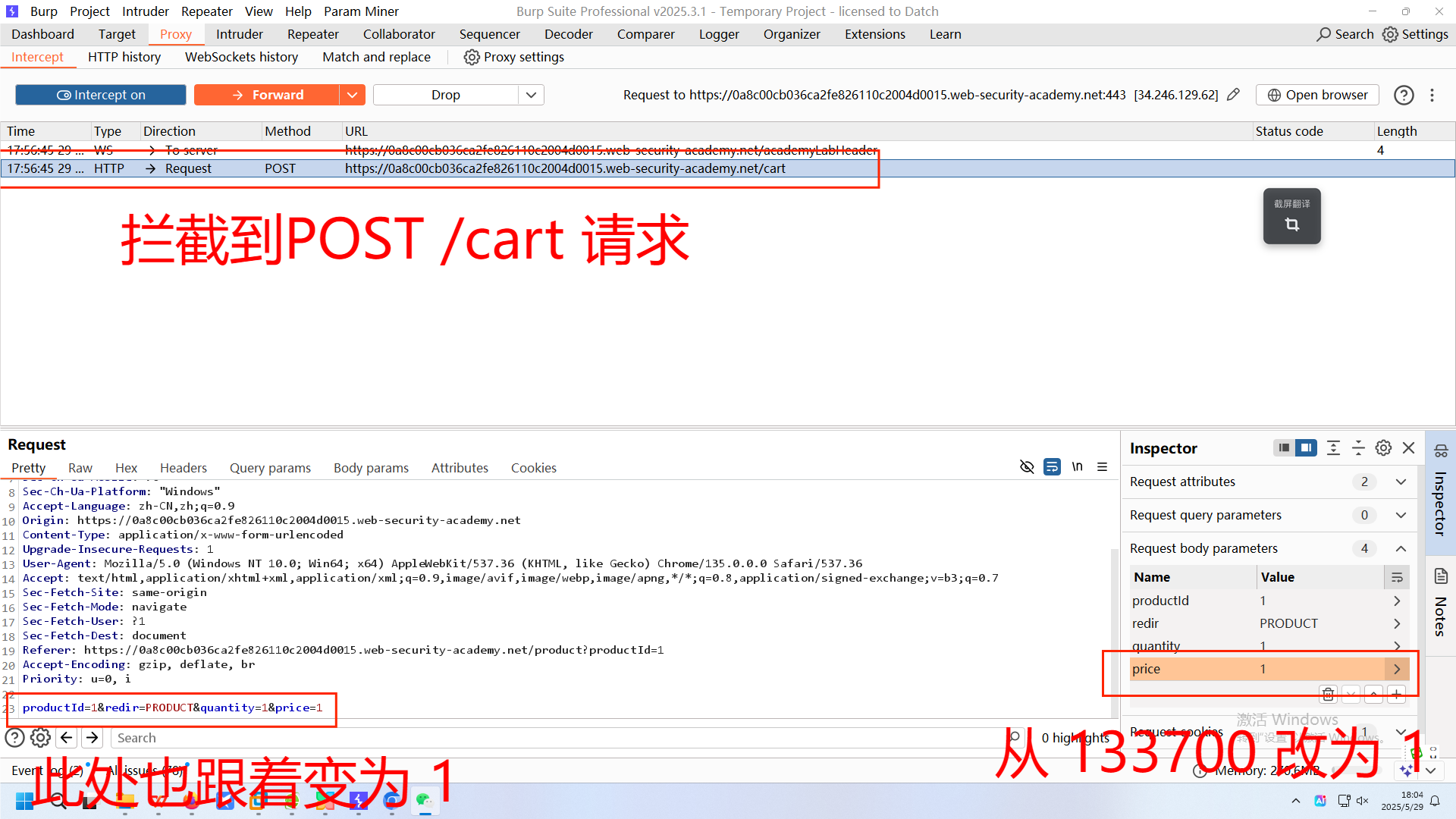
1、开启拦截（Intercept is on）

2、在浏览器点击 加入购物车

3、在 Proxy > Intercept 定位 POST /cart 请求  
[技术要点] 重点观察 **price** 参数（单位：美分）

**步骤5：实施参数篡改**

1. 修改 price 值为 **1**（原价的1/100）

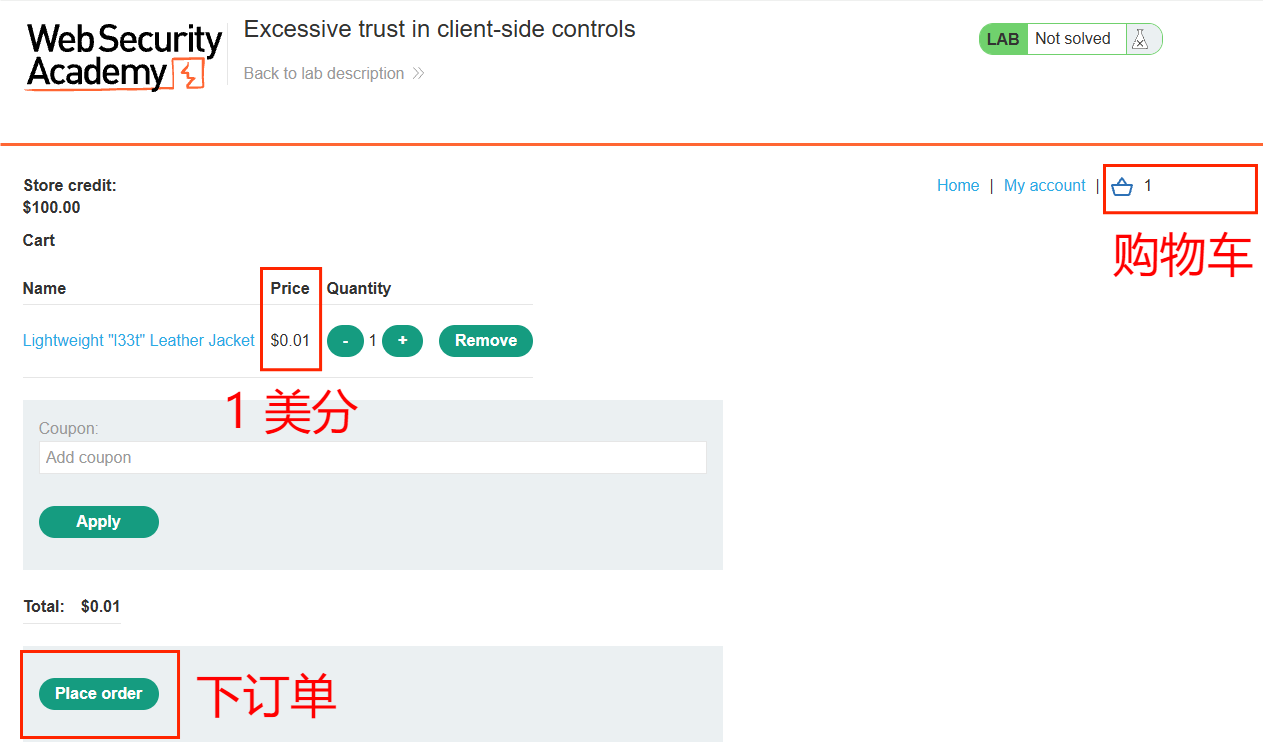


2、点击 Forward all 发送篡改后请求

**3、立即关闭拦截**（避免影响后续请求）  
[风险警示] 真实环境中此操作可能构成犯罪！

**步骤6：验证漏洞利用**

1. 查看购物车 → 夹克价格变为 **$0.01**



1. 点击 提交订单 完成异常交易  
   [实验成果] 您已成功利用客户端信任漏洞！

### 第五章 Burp Suite 目标范围设置指南

**一、技术价值**  
通过定义目标范围（Target Scope）：  
✓ 精准过滤非目标流量（广告/第三方资源）  
✓ 聚焦核心测试站点流量  
✓ 提升历史记录分析效率  
[注：此功能在大型应用测试中可节省70%分析时间]

### ****二、前置准备****

（一）拥有 **portswigger.net** 免费账户（[注册入口](https://portswigger.net/users/register" \t "https://chat.deepseek.com/a/chat/s/_blank)）

（二）已完成《请求篡改》实验（推荐但不强制）

### ****五步配置流程****

**步骤1：启动实验环境**

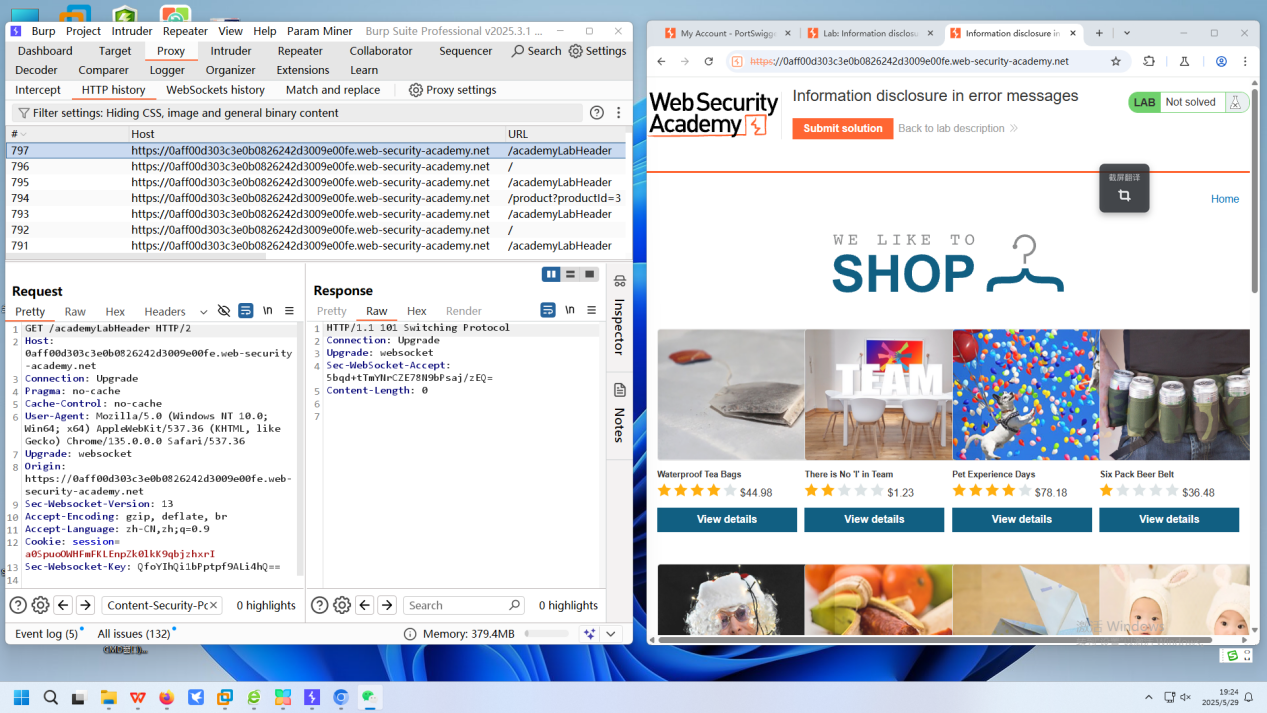
1、在 Burp 内置浏览器访问：

<https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-in-error-messages>

1. 点击 启动实验 → 登录账户 → 进入模拟电商站  
   [注意] 实验环境会话有效期2小时，超时需重新加载

**步骤2：探索目标站点**

点击任意**产品详情页**（生成基础流量）



**步骤3：分析历史流量**

1、进入 Proxy > HTTP history

**2、连续点击 # 列标题**（按时间倒序排列）

3、观察混杂的第三方请求：  
✓ 广告跟踪脚本  
✓ 统计分析服务  
[痛点分析] 无关流量占比常超60%

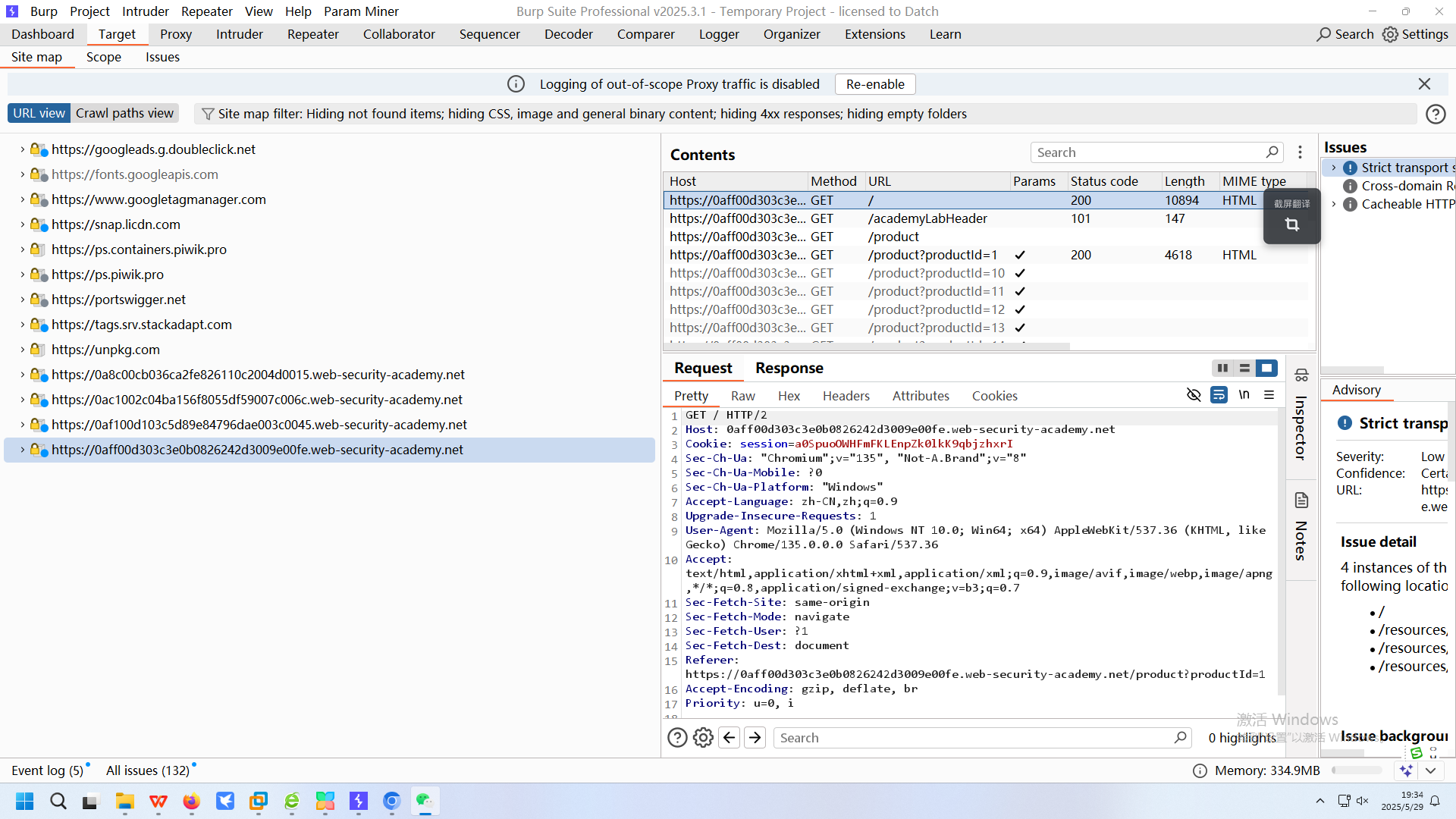
**步骤4：设置目标范围**

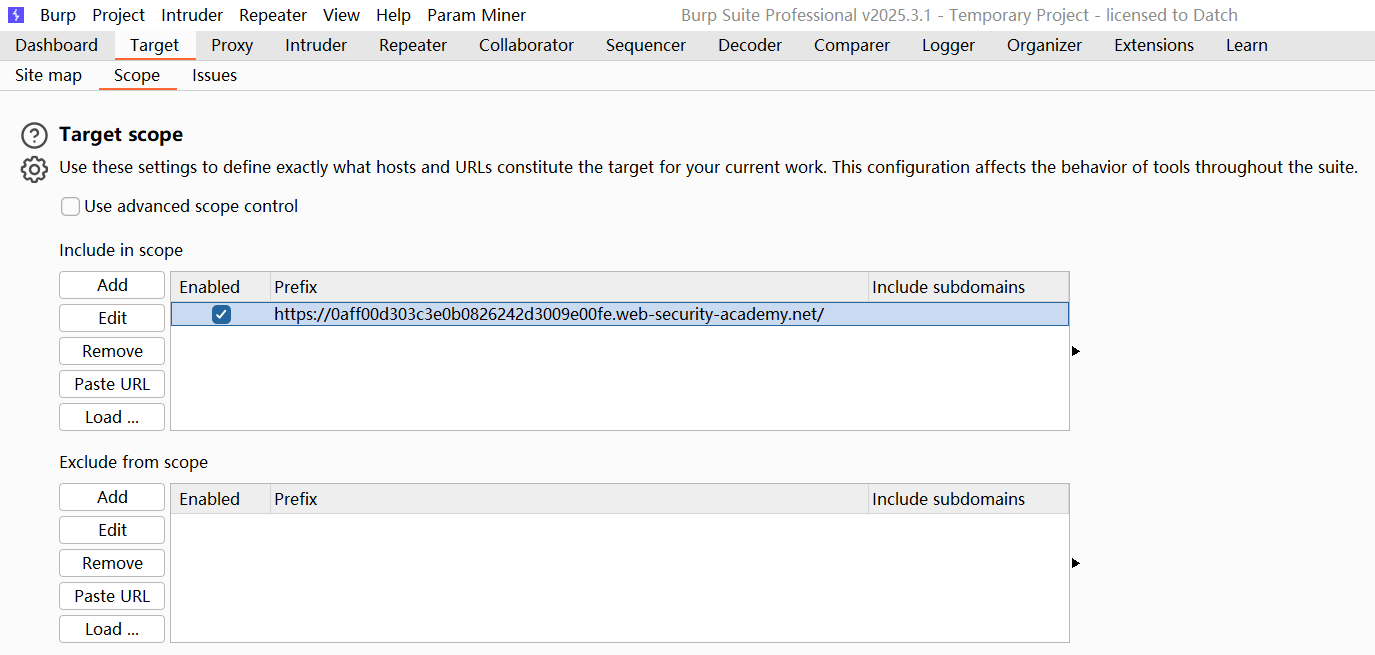
1、转至 Target > Site map

2、在**主机列表**右键目标域名

https://0a77000803a38056a1f275b5001a00a4.web-security-academy.net/[译者注：以实际为准]

3、选择 Add to scope（纳入范围）



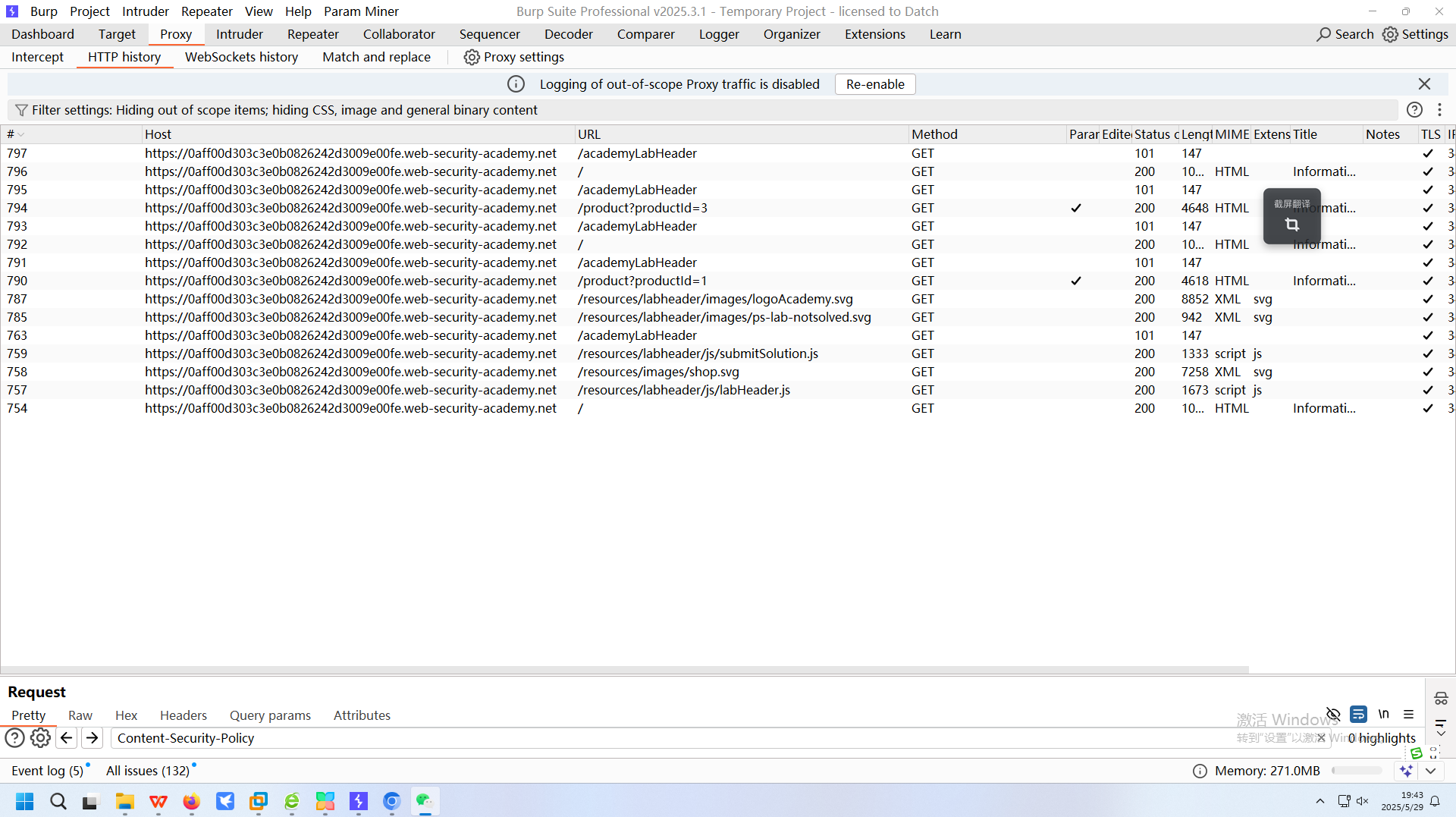
1. 弹窗确认 Yes（自动过滤域外流量）  
   

**步骤5：应用范围过滤**

1、返回 Proxy > HTTP history

2、点击显示过滤器（Display filter）

3、勾选 Show only in-scope items  
[效果验证] 历史记录仅保留目标站点流量



### 第六章 Burp Repeater 请求重放实战

### ****一、核心价值****

通过重复发送请求：  
✓ 无需拦截即可**多次测试不同参数** [译者注：尤其适合需要反复调整Cookie/Token的场景]  
✓ 快速验证漏洞特征  
✓ 对比分析服务器差异响应 [译者注：重点关注响应码/长度/时间变化]

### ****二、前置准备****

✅ PortSwigger 免费账户   
✅ 已完成目标范围设置 [译者注：未设范围会导致第三方请求干扰分析]

### ****三、操作流程****

**阶段1：定位关键请求**

在历史流量中筛选含动态参数的请求：

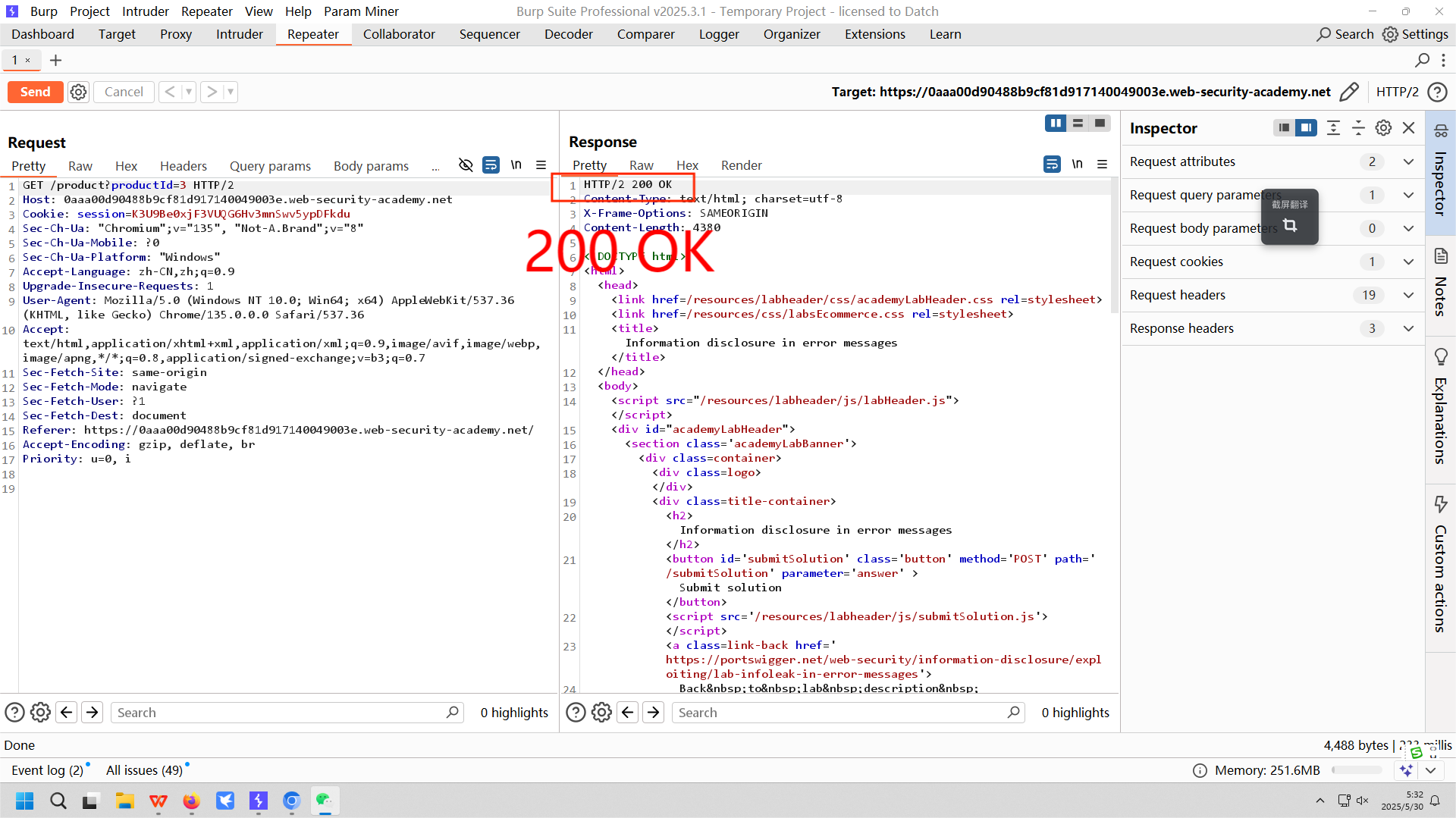
GET /product?productId=1 [译者注：优先选择影响业务逻辑的参数如ID/金额，参数值以实际可见为准]

**阶段2：发送至重放模块**

1、右键请求 → Send to Repeater [译者注：Ctrl+Shift+R 可快速发送]

2、切换至 Repeater **标签页** [译者注：最多支持20个并行标签页]

3、点击「Send」查看实时响应（200，OK）（支持无限次重发）。



**阶段3：参数模糊测试**

测试模式参考

1. 数值边界测试：

- 修改 productId=123 [译者注：检测整数溢出漏洞]

- 修改 productId=999999 [译者注：检测整数溢出漏洞]

- 修改 productId=0 [译者注：检测除零错误]

! 高危操作：生产环境慎用高频请求

1. 类型混淆测试：

- 修改 productId="abc" [译者注：重点观察错误信息泄露]

- 修改 productId=test [译者注：检测类型转换缺陷]

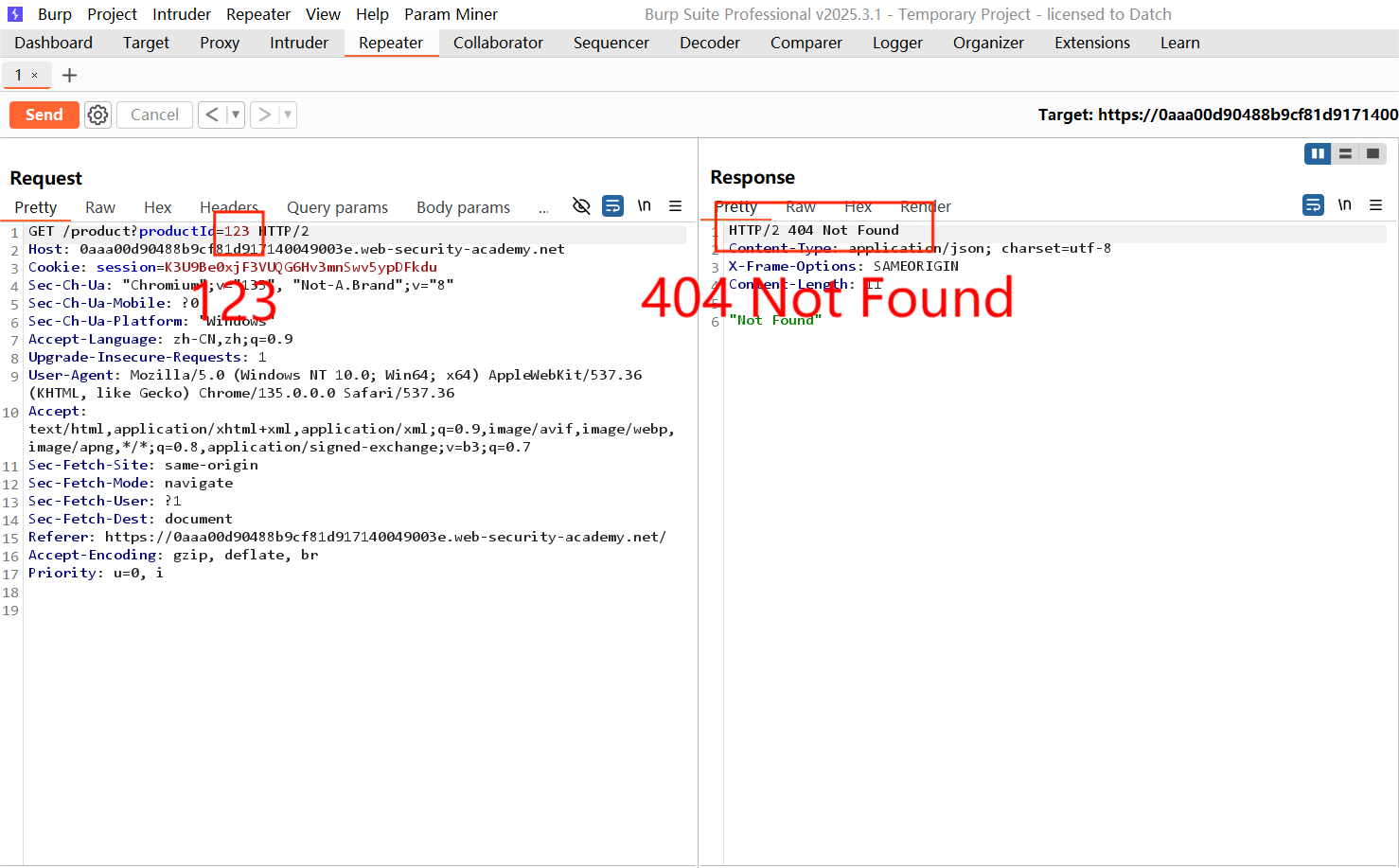
1. 特殊字符测试：

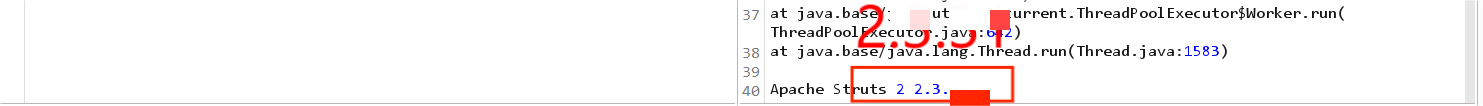
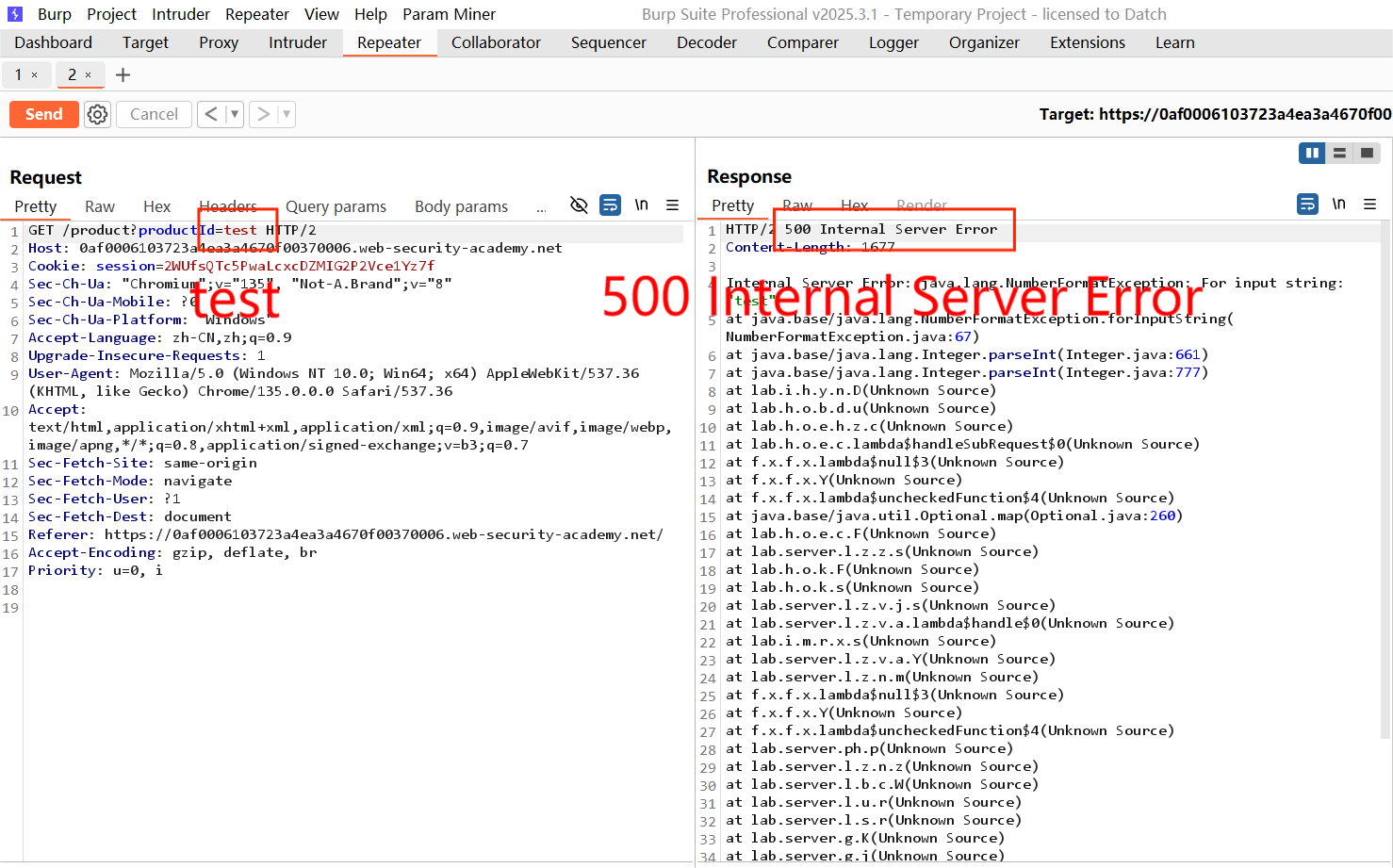
- 修改 productId='">< [译者注：XSS探测基础字符]

- 修改 productId=../../etc/passwd [译者注：路径遍历检测]

**阶段4：响应分析技巧**

1. 使用 **◀ ▶ 箭头**回溯历史请求 [译者注：支持跨标签页对比]





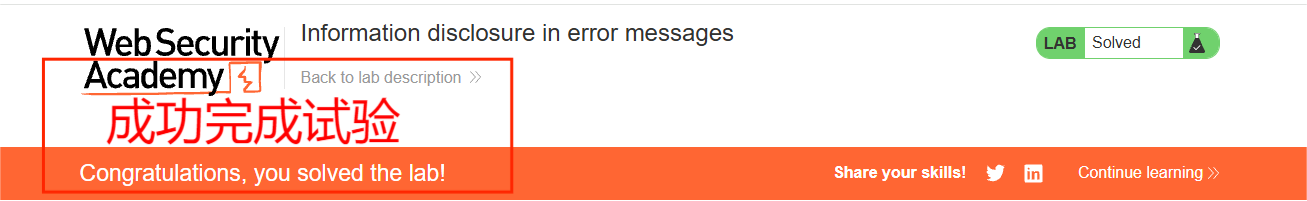
2、异常响应特征分析：

► 堆栈跟踪 → 提取框架类型 [译者注：如Apache Struts/Spring]

► 版本泄露 → 记录特征值 [译者注：严禁公开具体版本号！]

► 路径泄露 → 标记敏感目录

1. 实验平台提交漏洞特征



### Burp Scanner 首次扫描实战指南

### ****一、核心价值****

（一）Burp Scanner 提供两种扫描模式：  
✓ **全自动扫描**：快速覆盖基础漏洞 [译者注：适合周期性巡检]  
✓ **辅助手动测试**：深度验证复杂业务逻辑 [译者注：需配合手动验证结果]

（二）扫描双阶段原理

1. 内容爬取：模拟用户行为绘制站点地图 [译者注：自动处理JS渲染页面]
2. 安全审计：80+漏洞检测策略动态组合 [译者注：含OWASP Top 10漏洞]

### ****版本限制说明****

❗ 仅 **Professional/DAST 版本** 支持扫描功能  
❌ Community Edition 用户无法使用 [译者注：可试用14天专业版]

### ****六步扫描流程****

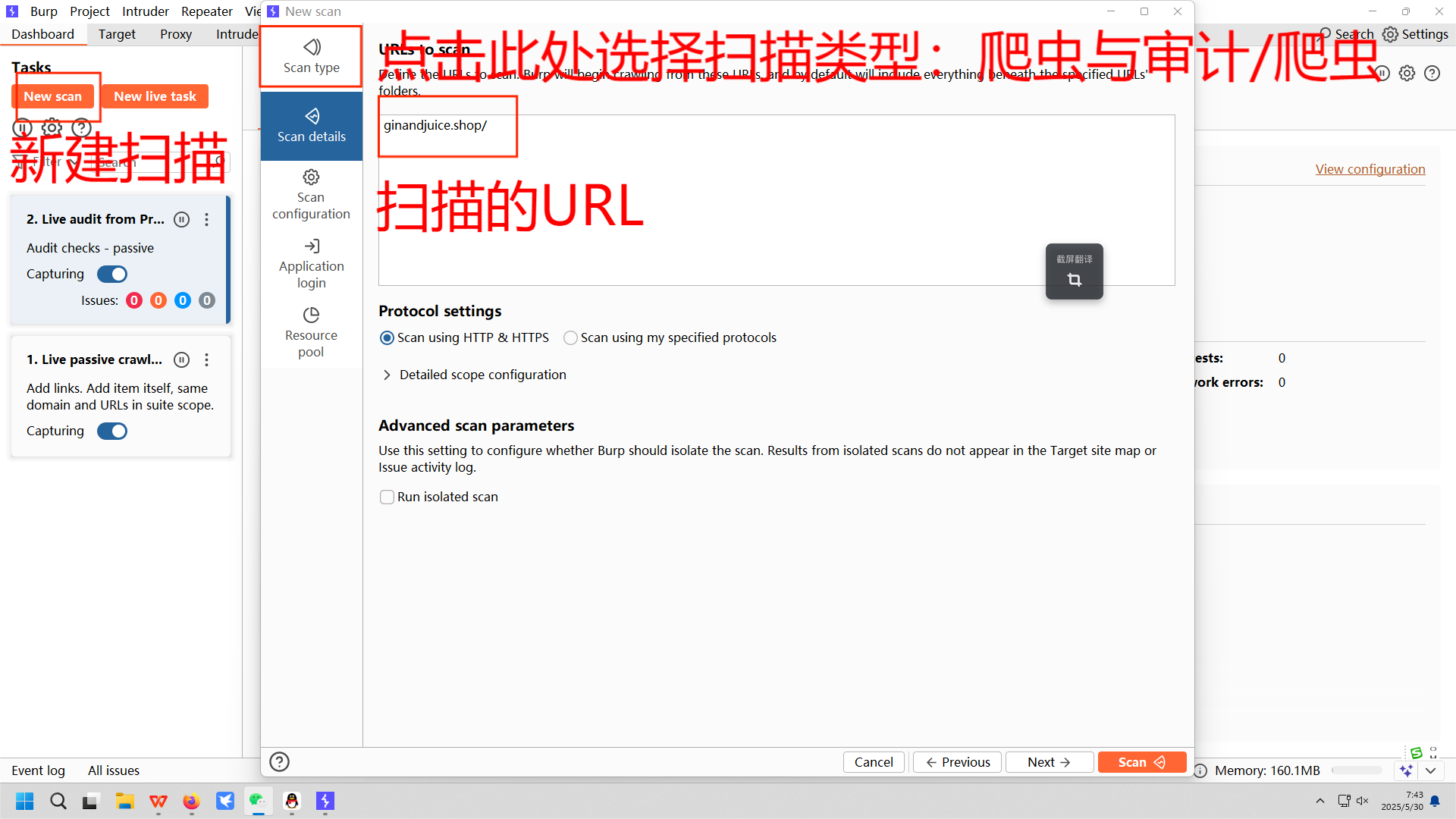
**阶段1：启动扫描器**

进入 Dashboard → New scan [译者注：快捷键 Ctrl+Shift+N]

**阶段2：配置目标地址**

- 在 \*\*URLs to scan\*\* 输入：ginandjuice.shop

- 删除历史测试地址 [译者注：避免扫描范围污染]



! 高危警示：

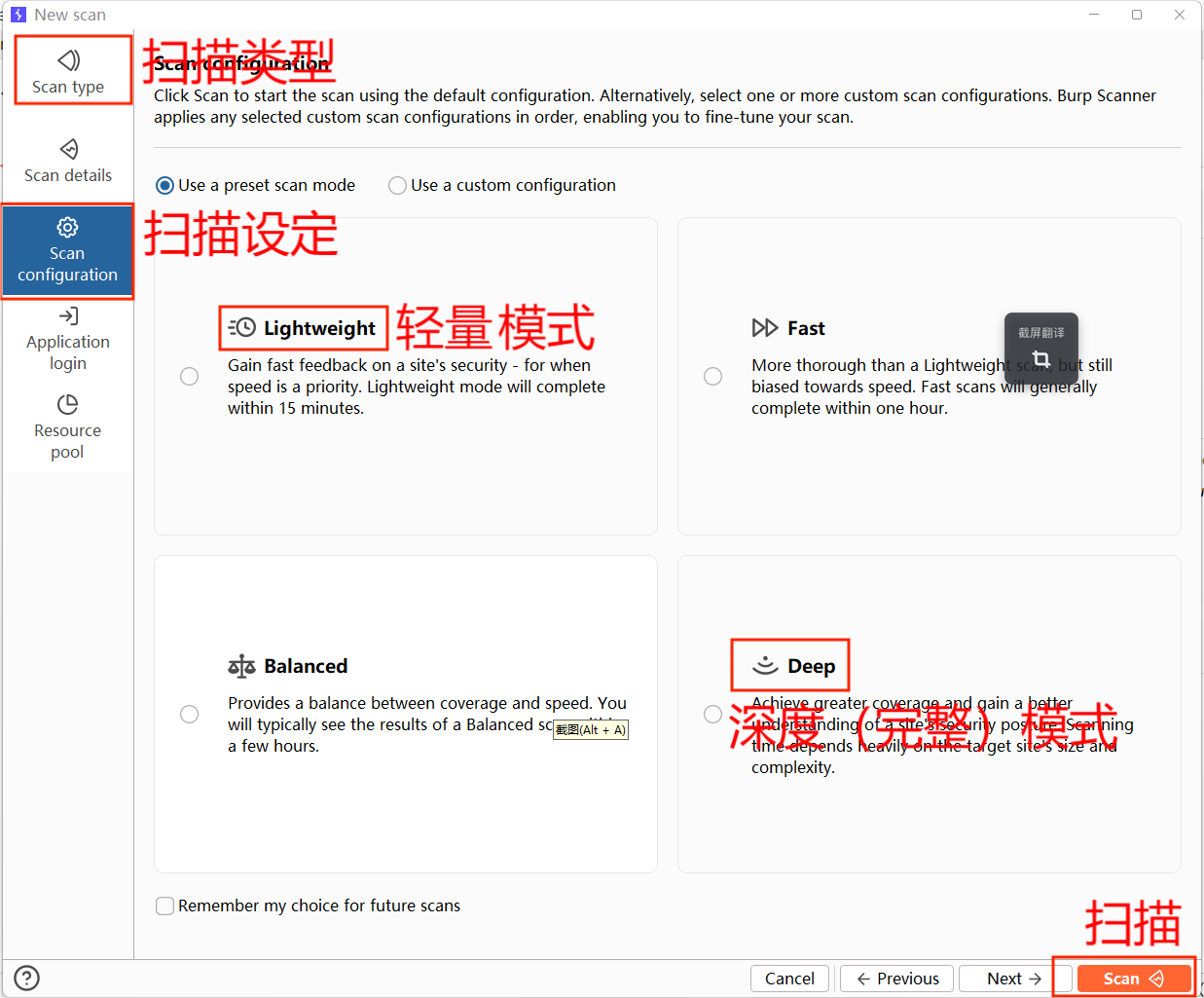
► 严禁扫描生产环境！

► 第三方站点需书面授权！ [译者注：留存《渗透授权书》样本]

**阶段3：模式选择**

1、选择 Scan configuration

2、预设模式 → 勾选 Lightweight [译者注：特点：  
✓ 最大时长15分钟  
✓ 基础漏洞快速筛查  
✓ 适合训练环境使用]



**阶段4：执行扫描**

1、点击 OK 启动 [译者注：首次扫描约消耗300MB内存]

2、在 Dashboard 监控任务进度 [译者注：重点观察：  
► 已爬取URL数量  
► 漏洞检测进度条]

**阶段5：实时监控**

1、转至 Target > Site map

2、展开 **ginandjuice.shop** 节点 [译者注：动态显示：  
✓ 新增API接口  
✓ 隐藏管理路径  
✓ 敏感文件列表]

**阶段6：漏洞分析**

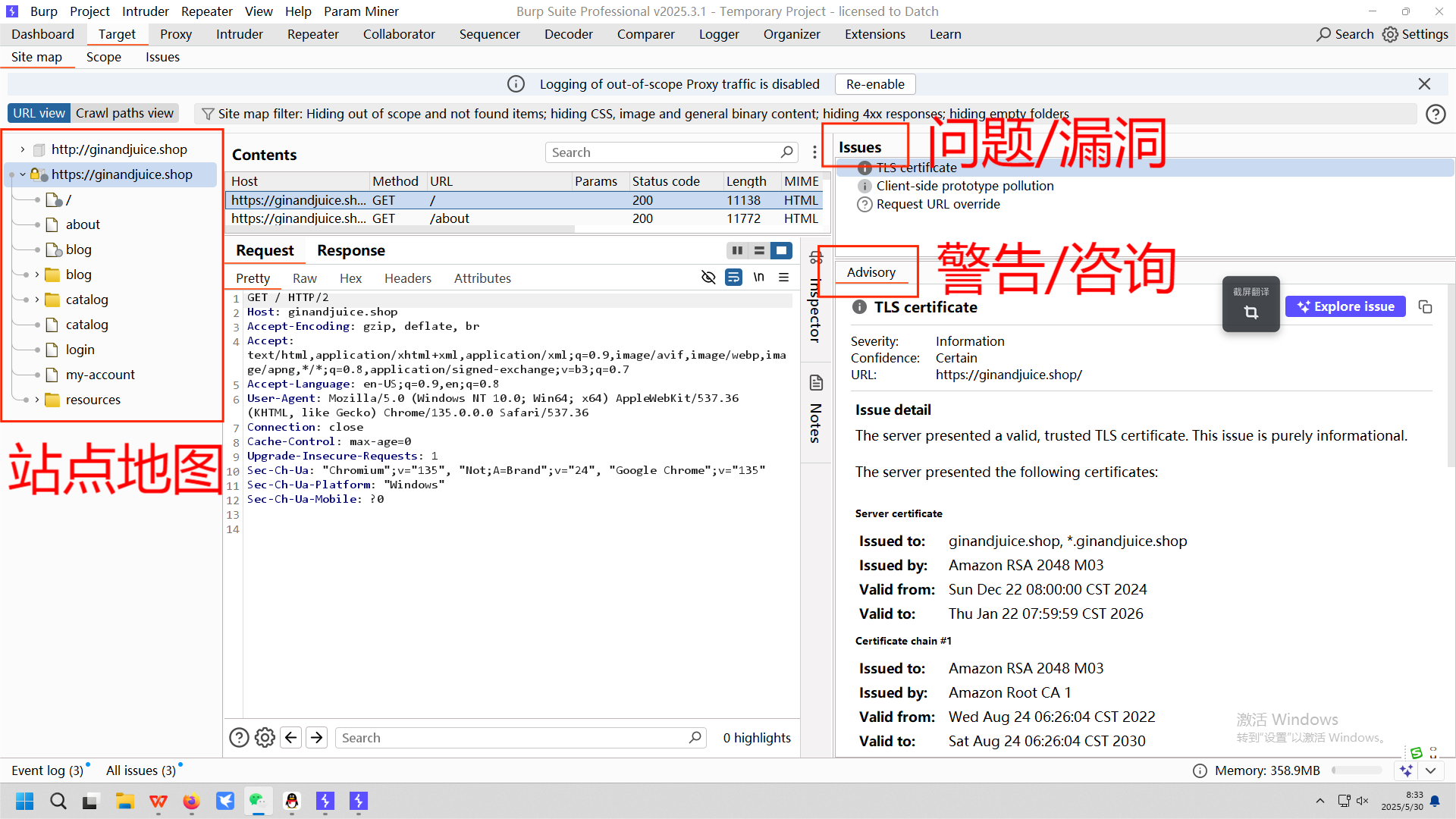
1. 在 `Dashboard` 选择扫描任务 → \*\*`Issues`\*\* 标签页

2. 漏洞报告解读：

► 严重等级：Critical/High/Medium/Low

► 定位证据：Request-Response 对 [译者注：重点保存POC]

► 修复建议：Advisory 选项卡 [译者注：需二次验证误报]



### 第八章 Burp Scanner 报告生成指南

### ****四步生成专业报告****

**步骤1：选择目标漏洞**

1、进入 Target > Site map

2、右键目标域名 https://ginandjuice.shop →  
Issues > Report issues for this host [译者注：支持多选漏洞生成定制报告]

**步骤2：配置报告参数**

1. 向导界面保持默认 → \*\*`Next`\*\*

2. 文件类型选择 \*\*HTML格式\*\* [译者注：PDF需专业版插件]

**步骤3：保存报告文件**

1、点击 Select file 选择存储路径

2、文件名必须包含扩展名：

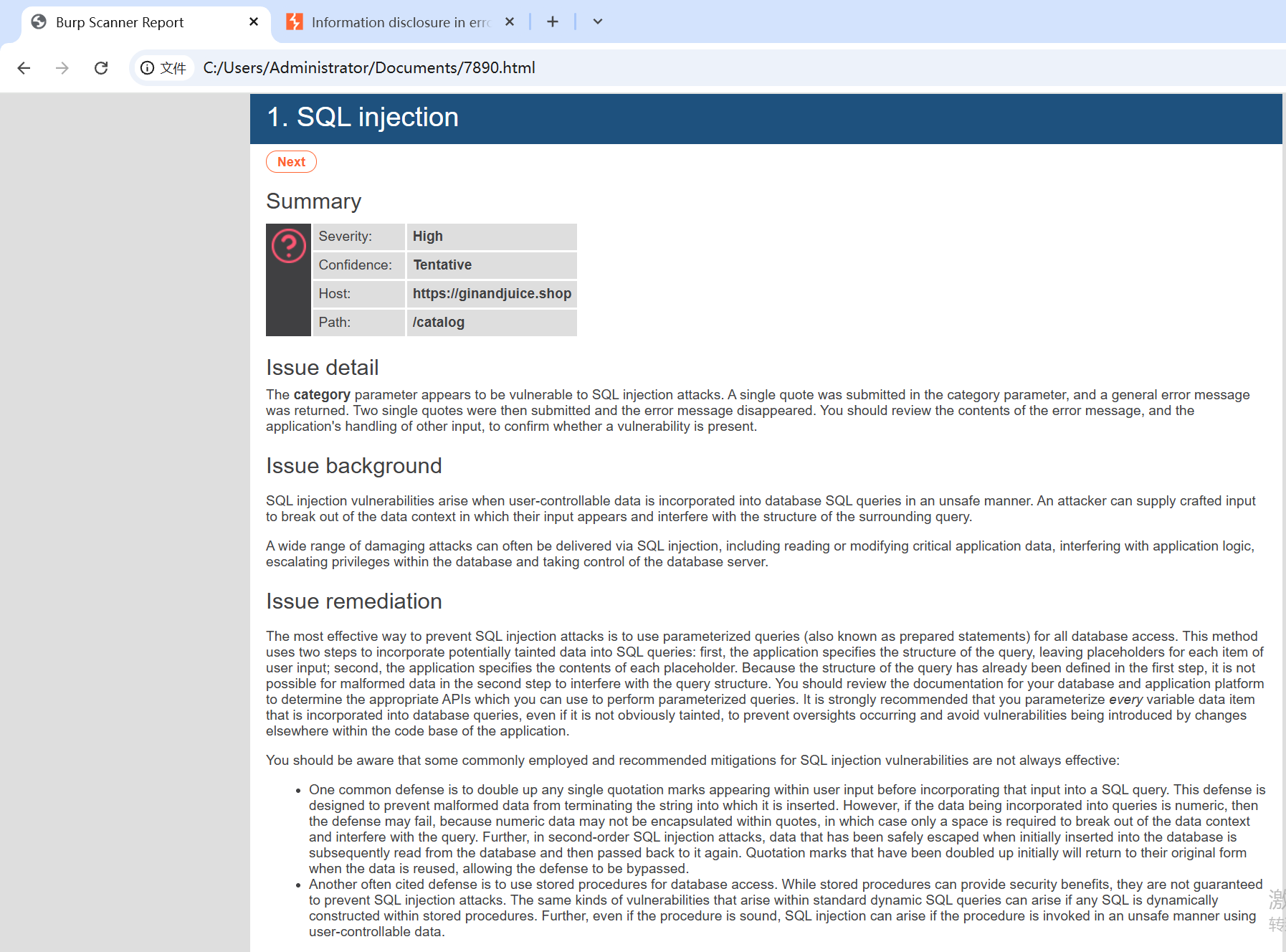
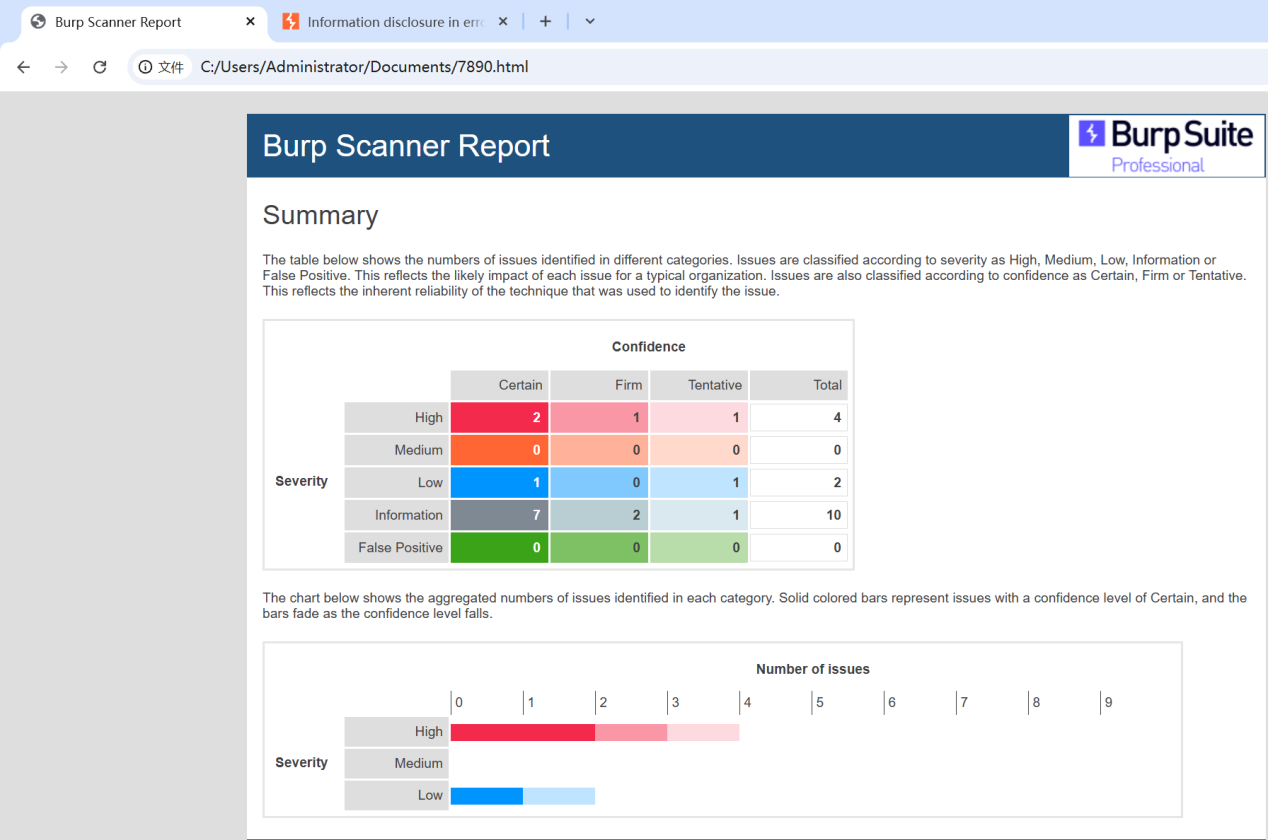
+ 正确：report\_2025.html

- 错误：report\_2025 [！缺失扩展名将导致生成失败]

3、点击 Save → Next 生成报告 [译者注：千条漏洞记录耗时约3秒]

**步骤4：查看与分发**

1. 在Burp浏览器中打开报告 [译者注：按漏洞等级自动分类]



2、核心内容包含：

► 漏洞分布热力图

► 详细复现步骤（含Request/Response）

► 修复建议（附官方参考链接）

[译者注：向客户交付前需人工脱敏处理]