**Burp Suite 官方文档（中文版）【DeepSeek翻译-老祁头整理复现-2025.3.1版本】**

本文档涵盖 Burp Suite 全系列版本及相关组件的功能说明。

法律声明

与所有安全测试工具类似，Burp Suite 的某些功能可能对目标系统造成损害。安全漏洞检测的本质是通过非常规交互方式探测目标，此过程可能导致脆弱系统异常。使用时您必须遵守以下条款：

一、使用前完整阅读所有文档

二、测试前必须对目标系统进行完整备份

三、仅限测试已获得系统所有者明确授权的目标

四、需确保您与系统所有者共同确认并接受潜在风险

任何未经授权的测试行为或未遵循上述安全操作导致的损失，用户需承担全部法律责任。系统所有者保留追究违规使用行为的权利。

1. **Burp Suite 入门指南**

Burp Suite 是一套用于Web应用程序安全测试的综合工具套件。

本互动教程旨在帮助您快速掌握Burp Suite的核心功能。教程通过Web Security Academy中刻意设计存在漏洞的实验环境，让您亲身体验Burp Suite的实际运作方式。

**第一章 Burp Suite系统要求**

Burp Suite 的系统要求主要取决于您的使用场景。虽然大多数任务可以在配置较低的设备上运行，但某些场景（例如同时运行多个扫描任务）可能需要更高的硬件配置以避免性能显著下降。

**一、CPU核心数 / 内存**

**（一）最低要求**：

2核CPU，4GB内存

适用于基本任务，例如代理网页流量和简单的 Intruder 攻击。尽管 Burp Suite 可能在更低配置的设备上运行，但出于性能考虑，不建议这样做。

**（二）推荐配置**：

2核CPU，16GB内存

适合一般用途。

**（三）高级配置**：

4核CPU，32GB内存

适用于高强度任务，例如复杂的 Intruder 攻击或大型自动化扫描。

**二、磁盘空间**

**（一）基础安装**：1GB

**（二）每个项目文件**：2GB

注意

虽然每个项目文件推荐至少预留 2GB 空间，但实际大小可能远超此值（甚至达到数十GB），具体取决于以下因素：

a.代理历史记录的数量

b.运行的扫描任务数量

c.打开的 Repeater 标签页数量

**三、支持的操作系统与架构**

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 芯片）

**四、嵌入式浏览器的额外要求**

Burp 内置浏览器对以下情况不兼容：

**（一）旧版 Windows 系统**：

Windows 7、Windows 8/8.1

Windows Server 2012 和 Windows Server 2012 R2

**（二）特定安装方式**：

在 Apple Silicon 或 ARM 64位 系统上通过 JAR 文件 运行的 Burp Suite。

解决方法：如需在这些设备上使用浏览器功能，请通过 原生平台安装程序 安装 Burp。

重要说明

使用原生平台安装程序时，仍可同时运行多个 Burp 实例，此功能不仅限于通过 JAR 文件运行的实例。

【如需进一步优化性能，请根据任务需求选择硬件配置，并确保操作系统和安装方式符合兼容性要求。】

**第二章 下载与安装**

**步骤1：下载**

通过以下链接下载最新版本的 Burp Suite 专业版 或 社区版：

[专业版](https://portswigger.net/burp/releases/professional/latest)

[社区版](https://portswigger.net/burp/releases/community/latest)

**步骤2：安装**

1、运行安装程序并启动 Burp Suite。

2、当提示选择项目文件和配置时，直接点击 Next[下一步]，然后点击 Start Burp[启动 Burp] 暂时跳过此步骤。

注意

若使用 Burp Suite 专业版，请在提示时输入许可证密钥。若无密钥，可[订阅](https://portswigger.net/buy/pro)或申请[免费试用](https://portswigger.net/burp/pro/trial)。

### 步骤3：开始探索 Burp Suite

### 若您首次接触 Burp Suite，请继续跟随本教程完成 交互式核心功能导览。

**【**如需进一步帮助，请参考官方文档或社区支持资源。**】**

**第三章 使用 Burp Proxy 拦截 HTTP 流量**

在本教程中，您将通过一个实时漏洞测试网站，学习如何使用 Burp Proxy[代理] 拦截 HTTP 请求。

**一、拦截请求的原理**

Burp Proxy[代理] 允许您拦截 Burp 内置浏览器与目标服务器之间发送的 HTTP 请求和响应。通过拦截，您可以观察网站在不同操作下的行为逻辑。

**二、操作步骤**

**步骤1**：启动 Burp 内置浏览器

（1）进入 Proxy[代理] > Intercept[拦截] 标签页。

（2）将拦截开关设为 Intercept is on[开启拦截]。

（3）点击 Open Browser[打开浏览器]，启动 Burp 预配置的内置浏览器。

（4）调整窗口位置，确保同时看到 Burp 和其内置浏览器。

**步骤2：拦截请求**

（1）在 Burp 浏览器中尝试访问 https://portswigger.net，此时页面会卡住。

（2）原因：HTTP 请求已被 Burp Proxy[代理] 拦截，您可以在 Proxy[代理] > Intercept[拦截] 标签页 查看被拦截的请求。

**步骤3：放行请求**

（1）点击 Forward[放行] 按钮，将请求发送到目标服务器。

（2）重复点击 Forward[放行] ，直到页面完全加载（浏览器可能触发多个请求）。

**步骤4：关闭拦截模式**

（1）由于浏览器通常会发送大量请求，建议关闭持续拦截，将拦截开关设为 Intercept is off[关闭拦截]。

（2）返回浏览器，确认可正常与网站交互。

**步骤5：查看 HTTP 历史记录**

（1）进入 Proxy[代理] > HTTP history[历史记录] 标签页。

（2）此处记录了所有通过 Burp Proxy[代理] 的流量（包括拦截关闭时的请求）。

（3）点击任意条目，查看原始 HTTP 请求及服务器的响应内容。

**三、关键功能说明**

**（一）拦截后修改请求**：在 Intercept[拦截] 标签页 中可直接编辑请求内容（如参数、Header），再点击 Forward[放行] 发送修改后的请求。

**（二）过滤历史记录**：在 HTTP history[历史记录] 中右键请求，使用 Filter[过滤] 功能按域名、状态码等快速定位目标流量。

**四、总结**

通过拦截和分析 HTTP 流量，您可以深入理解网站的工作原理，并为后续漏洞测试（如 SQL 注入、XSS）奠定基础。接下来，尝试使用 Repeater 模块 重放修改后的请求，观察服务器响应变化！

**第四章 使用 Burp Proxy 修改 HTTP 请求**

在本教程中，您将学习如何通过 Burp Proxy[代理] 修改被拦截的 HTTP 请求。通过操纵网站未预期的请求参数，观察其响应行为，进而识别并利用真实漏洞。您将使用 PortSwigger 提供的漏洞实验环境（实验室），完成一次实战演练。

**一、准备工作**

[注册](https://portswigger.net/users/register) portswigger.net 免费账户，以访问 Web Security Academy 的漏洞实验室。

**二、操作步骤**

**步骤1**：在 Burp 浏览器中访问漏洞网站

（1）进入 Burp 的 Proxy [代理]> Intercept[拦截] 标签页，确保拦截开关为 Intercept is off[[关闭拦截](https://portswigger.net/burp/documentation/desktop/tools/proxy/intercept-messages" \l "controls)]。

（2）启动 Burp 内置浏览器，访问以下实验室链接：<https://portswigger.net/web-security/logic-flaws/examples/lab-logic-flaws-excessive-trust-in-client-side-controls>

（3）点击 Access the lab，登录 PortSwigger 账户后，进入一个模拟的电商网站。

**步骤2：登录购物账户**

（1）在电商网站点击 My account，使用以下凭证登录：

用户名: wiener

密码: peter

1. 登录后，账户显示有 $100 余额。

**步骤3：选择商品**

返回首页，选择 Lightweight "l33t" leather jacket（轻量级“l33t”皮夹克）查看商品详情。

**步骤4：拦截“加入购物车”请求**

（1）进入 Proxy [代理]> Intercept[拦截] 标签页，开启拦截开关 Intercept is on。

（2）在浏览器中将皮夹克加入购物车，此时会拦截到 POST /cart 请求。

关键观察

请求正文中包含 price 参数，值为商品价格（单位：美分）。

若有多个请求被拦截，请选择 POST /cart 请求。

**步骤5：修改请求参数**

（1）将 price 参数值改为 1（即 1 美分）。

（2）点击 Forward[放行] → Forward all[放行全部] 放行所有拦截的请求。

（3）关闭拦截开关 Intercept is off[拦截已关闭]，确保后续请求正常通过。

**步骤6：利用漏洞完成购买**

（1）在浏览器中点击右上角购物车图标，查看修改后的价格（皮夹克已变为 1 美分）。

（2）点击 Place order[下单]，以极低价格完成购买。

恭喜！ 您已成功解决首个 Web Security Academy 实验室，并掌握了以下技能：

a.拦截并分析 HTTP 请求

b.修改关键参数以利用逻辑漏洞

**三、漏洞原理说明**

该实验室模拟了过度信任客户端输入的逻辑漏洞。网站未对客户端提交的 price 参数进行服务端验证，导致攻击者可通过 Burp Proxy[代理] 篡改价格。实际开发中，应始终在服务端校验关键业务参数（如价格、库存等）。

**四、下一步建议**：

尝试使用 Repeater 模块 重放修改后的请求，观察不同参数对服务器响应的影响，进一步理解漏洞利用链。

**第五章 设置目标范围**

在本教程中，您将学习如何为 Burp Suite 设置目标范围（Target Scope）。目标范围用于明确指定需要测试的 URL 和主机，从而过滤浏览器和其他无关站点产生的干扰流量，让您专注于目标业务逻辑的安全测试。

**一、准备工作**

（一）[注册](https://portswigger.net/users/register) portswigger.net 免费账户以访问 Web Security Academy 的漏洞实验室。

（二）建议先完成前序教程：[使用 Burp Proxy 修改 HTTP 请求](https://portswigger.net/burp/documentation/desktop/getting-started/modifying-http-requests)。

**二、操作步骤**

**步骤1**：启动 Burp 内置浏览器并访问实验室：

（1）启动 Burp 内置浏览器，访问以下实验室链接：

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

（2）点击 Access the lab，登录 PortSwigger 账户后，进入模拟的电商网站。

**步骤2：浏览目标网站**

在电商网站中点击几个商品页面，生成测试流量。

**步骤3：查看 HTTP 历史记录**

进入 Proxy[代理] > HTTP history[历史记录] 标签页。

点击最左侧列标题 #，按降序排列请求，确保最新请求显示在顶部。

关键观察

HTTP 历史记录中混杂了第三方站点的请求（如 YouTube、Google Analytics），需过滤以聚焦目标流量。

**步骤4：设置目标作用域**

进入 Target[目标] > Site map（站点地图）。

在左侧面板中找到目标网站的节点（如 https://\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*.web-security-academy.net/，以实际为准）。

右键点击该节点 → Add to scope[添加到范围] → 弹出窗口中点击 Yes，确认排除范围外流量。

**步骤5：过滤 HTTP 历史记录**

在 Proxy > HTTP history 顶部，点击显示过滤器 → 选择 Show only in-scope items[仅显示范围内条目]。

滚动查看历史记录，此时仅显示目标网站的请求，其他流量已被隐藏。

**三、验证效果**

（一）继续浏览目标网站，观察 Site map[站点地图] 和 HTTP history[历史记录] 中不再记录第三方流量。

（二）范围设置成功后，后续测试将更高效。

**四、下一步：完成实验室挑战**

通过设置目标范围，您已简化流量分析流程。接下来，可基于过滤后的 HTTP 历史记录，继续完成实验室任务（如利用错误信息泄露漏洞）。

**五、关键技巧**：

（一）动态调整范围：在 Target[目标] > Scope[范围] 标签页 中可手动添加/删除范围规则。

（二）正则表达式支持：使用通配符（如 \*）匹配多个子域名或路径（例如 https://\*.example.com/api/\*）。

【通过合理配置目标范围，您能更精准地定位漏洞，避免在无关流量中消耗精力。】

**第六章 Burp Repeater实战：重放请求探测漏洞**

本教程将指导您使用Burp Repeater重复发送请求，通过观察服务器响应分析潜在漏洞。该工具可免去每次拦截请求的繁琐，是验证Burp Scanner发现或手动探测漏洞的利器。

**一、准备工作**

（一）Web Security Academy账号

访问 [portswigger.net](https://portswigger.net/users/register) 免费注册（若尚未拥有账号）

（二）目标范围设置

确保已完成[设置目标范围](https://portswigger.net/burp/documentation/desktop/getting-started/setting-target-scope)教程

**二、发送请求到Repeater**

**步骤1：定位关键请求**

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

在浏览模拟购物网站时，访问商品页会触发携带productId参数的GET /product请求。

**步骤2：转交请求**

在Burp Proxy[代理]的HTTP历史中，右键点击任意GET /product?productId=...请求 → 选择「Send to Repeater」。

发送请求至 Repeater。

**步骤3：发送并观察响应**

切换至Repeater标签页 → 点击「Send」查看实时响应（200，OK）（支持无限次重发）。

Repeater重放请求

**三、输入变异测试**

**步骤1：修改参数值**

将productId参数值更改为不同数字（如123→456→99999），多次点击「Send」观察响应变化（404，未找到）。

**步骤2：历史记录回溯**

使用箭头按钮或下拉菜单，查看已发送请求及对应响应，便于对比分析。

请求历史回溯

**步骤3：注入非常规输入**

将productId改为字符串（如productId=test），发送异常请求。（500，错误）

**步骤4：解析错误响应**

服务器返回包含堆栈跟踪的详细错误，暴露框架信息（如Apache Struts 2.3.31）。

错误响应分析

漏洞启示

此类信息泄露可能帮助攻击者利用已知框架漏洞，需及时修复。

**四、提交实验成果**

返回Web Security Academy实验页面：

（一）点击「Submit solution」

（二）输入发现的Struts版本号：2.3.31

提交解决方案（回到实验室描述）

【恭喜！ 您已掌握通过Burp Repeater发现信息泄露漏洞的核心技能。】

**第七章 执行首次漏洞扫描**

Burp Scanner[扫描仪] 既可作为全自动化扫描工具，也可辅助手动测试流程。其漏洞检测能力持续扩展，涵盖经典漏洞与新兴威胁。

注意

仅限专业版：Burp Scanner 仅在 Burp Suite Professional[专业版] 和 Burp Suite DAST 中可用，社区版无法使用。

环境警告：扫描可能对目标系统产生意外影响。**仅限非生产环境使用，且需获得授权后方可扫描第三方网站**。

**一、扫描流程说明**

Burp Scanner 分两阶段工作：

**（一）爬取内容与功能**：模拟真实用户行为，遍历目标站点，构建完整的站点地图。

**（二）审计漏洞**：分析站点行为，识别安全漏洞。

**二、操作步骤**

**步骤1：启动扫描配置**

（1）进入 Dashboard[仪表盘]标签页 → 点击 New scan[新建扫描]。

（2）弹出 Scan launcher[扫描启动器] 对话框。

**步骤2：输入目标URL**

（1）在 URLs to scan[扫描目标URL] 字段输入 ginandjuice.shop。

（2）若需清除前序教程设置的作用域URL，请手动删除。

（3）其他设置暂保持默认。

**步骤3：配置扫描模式**

点击 Scan configuration[扫描配置] → 选择 Use a preset scan mode[使用预设模式] → 点击 Lightweight[轻量级]。

轻量级模式：快速扫描（最长15分钟），提供目标的高层概览。

**步骤4：启动扫描**

（1）点击 OK 启动扫描。

（2）Dashboard[仪表盘] 中新增扫描任务，可实时查看状态与进度。

**步骤5：观察爬取过程**

进入 Target [目标]> Site map[站点地图]标签页，展开 ginandjuice.shop 节点，观察实时更新的站点结构。

**步骤6：查看漏洞结果**

（1）扫描完成后，在 Dashboard[仪表盘] 中选择任务 → 进入 Issues[问题]标签页。

（2）关键信息：

①Advisory[建议]：漏洞描述与修复方案。

②Request/Response[请求/响应]：漏洞证据（具体内容因漏洞类型而异）。

**三、总结**

您已完成首次自动化漏洞扫描！通过此流程，可快速定位目标站点的潜在风险。下一步建议：

**（1）深入分析**：针对高危漏洞，使用 Repeater 或 Intruder 手动验证。

**（2）调整配置**：在 Scan configuration[扫描配置] 中切换 Crawl[爬取] 和 Audit[审计] 策略，适应不同场景需求。

**第八章 生成扫描报告**

本教程将指导您如何基于扫描结果生成 HTML 格式的漏洞报告。

**一、操作步骤**

**步骤1：选择目标主机的漏洞**

（1）进入 Target [目标]> Site map[站点地图]标签页。

（2）右键点击目标主机 https://ginandjuice.shop → Issues[问题]→ Report issues for this host[该主机的问题报告]。

**步骤2：配置报告选项**

（1）弹出报告向导，按默认配置逐步点击 Next（下一步）。

（2）选项包括：

①报告详细程度（如漏洞描述、修复建议、请求/响应证据）。

②漏洞筛选（按严重级别、类型过滤）。

**步骤3：保存报告文件**

（1）点击 Select file[选择文件]，指定保存路径。

（2）输入文件名（必须包含 .html 扩展名，如 scan\_report\_2025.html）。

（3）点击 Save[保存] → Next[下一步] 生成报告。

**步骤4：查看与分享报告**

（1）报告生成后，使用浏览器打开 HTML 文件，预览内容。

（2）报告内容示例：

①漏洞列表（按严重性排序）。

②每个漏洞的详细描述、复现步骤、修复建议。

③关联的请求与响应数据（用于验证）。

**二、关键提示**

**（一）定制报告**：在向导中可调整包含的漏洞类型或描述详略，适应不同受众（如开发团队、管理层）。

（二）批量导出：支持导出多个主机的报告，或按项目聚合扫描结果。

【通过生成专业报告，您能清晰展示安全测试成果，助力团队高效修复漏洞！】

**第九章 激活Burp Suite许可证**

首次启动Burp Suite Professional时，系统将提示您输入Burp许可证密钥。您可在[账户页面](https://portswigger.net/users/youraccount)下载许可证密钥。大多数用户可通过以下标准流程激活：

当出现输入许可证密钥的提示时，您可以直接在文本框粘贴密钥，或点击「选择许可证密钥文件...」按钮从文件加载，随后点击「下一步」。

若需通过代理服务器访问互联网，请在对应字段输入代理配置信息。

点击「下一步」激活许可证，并继续完成启动向导。

特殊情况下，您可能需要手动激活许可证。此时请勿点击「下一步」，而是选择「手动激活」并按以下步骤操作：

**手动激活流程**

注意

若当前计算机无网络连接，需先在联网设备完成本流程，再将激活响应手动输入至离线设备。

**一、复制URL**

点击「复制URL」按钮获取激活链接。

复制许可证激活URL

**二、访问激活页面**

将复制的URL粘贴至浏览器地址栏并访问。

在浏览器打开激活链接

**三、获取激活请求码**

返回Burp激活向导，点击「复制请求」按钮。

复制许可证激活请求

**四、提交激活请求**

在浏览器打开的激活页面中，将请求码粘贴至「Activation request」字段，点击「发送」。此时「Activation response」字段将生成响应码，请完整复制。

提交许可证激活请求

**五、完成激活**

返回激活向导：

点击「粘贴响应」按钮自动填充响应码

若为离线设备，请手动确保输入无误

粘贴许可证激活响应

六、点击「下一步」，成功激活后将显示确认界面。点击「完成」即可启动Burp配置向导。

**第十章 如何选择Burp Suite Mac安装包？**

自2020年起，苹果公司开始为Mac设备搭载新型处理器。您需根据设备芯片类型选择对应的Burp Suite安装包：

**一、操作步骤**

**（一）查看处理器类型**

1、点击屏幕左上角 苹果图标 → 选择 「关于本机」。

2、在弹出的窗口中，查看 「芯片」 或 「处理器」 项：

（1）显示 Apple M1/M2/M3等 → Apple芯片

（2）显示 Intel Core i5/i7等 → Intel处理器

**（二）下载对应安装包**

访问 [Burp Suite官方下载页](https://portswigger.net/burp/releases)，根据您的芯片类型选择：

1、Apple芯片 → 下载 Apple Silicon版本

2、Intel处理器 → 下载 Intel版本

**二、提示**

若安装错误版本可能导致性能问题或无法运行。若不确定设备芯片类型，可通过终端执行 uname -m 命令验证：

（一）返回 arm64 → Apple芯片

（二）返回 x86\_64 → Intel处理器

**第十一章 接下来做什么？**

恭喜！您已经在掌握Burp Suite的道路上取得了长足进步。现在您已学会如何：

一、使用Burp Proxy拦截和修改HTTP流量。

二、设置目标范围以专注于关键内容。

三、通过Burp Repeater重发请求进行漏洞探测。

四、运行自动化漏洞扫描并使用Burp Scanner生成报告。

五、通过Web Security Academy精进技能。

但以上只是Burp Suite所有功能的冰山一角。既然您已熟悉基础操作，何不尝试更多来自[网络安全学院](https://portswigger.net/web-security)的实验室？