

三、Burp Suite模块详解

- 1、Burp Suite界面布局
- 2、模块总体介绍
- 3、各模块详细功能

01

Burp Suite界面布局

<https://portswigger.net/burp/documentation/contents>

界面总览

⚡

Burp

Project

Intruder

Repeater

Window

Help

菜单栏

Burp Suite Professional v2021.12.1 - Temporary Project - licensed to wuya

标题栏

Dashboards

工具栏

Proxy

Intruder

Repeater

Sequencer

Decoder

Comparer

Logger

Extender

Project options

User options

Learn

Tasks

+

New sc...

+

New live ta...

⏸

⚙

?

↗

Filter

Running

Paused

Finished

Live task

Scan

🔍

Search...

1. Live passive crawl from Proxy (all traffic)

⏸⚙🗑

Add links. Add item itself, same domain and... 0 items added to site map

Capturing:

🔵

0 responses processed

0 responses queued

2. Live audit from Proxy (all traffic)

⏸⚙🗑↗

Audit checks - passive

Issues:

0

0

0

0

Capturing:

🔵

0 requests (0 errors)

Event log

?

↗

Filter

Critical

Error

Info

Debug

🔍

Search...

Time

Type

Source

16:32:36 22 1月 2022

Info

Proxy

Proxy service started on

Issue activity

?

↗

Filter

High

Medium

Low

Info

Certain

Firm

...

🔍

Search...

#

Task

Time

Action

Advisory

状态栏

Memory: 122.1MB

Disk: 32KB

旧版对比

Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Site map Scope

Logging of out-of-scope Proxy traffic is disabled [Re-enable](#)

Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Contents

Host	Method	URL
http://192.168.56.102	GET	/mutillidae/
http://192.168.56.102	GET	/mutillidae/?page=
http://192.168.56.102	GET	/mutillidae/?page=
http://192.168.56.102	GET	/mutillidae/?page=
http://192.168.56.102	GET	/mutillidae/?page=
http://192.168.56.102	GET	/mutillidae/?page=
http://192.168.56.102	GET	/mutillidae/docum
http://192.168.56.102	GET	/mutillidae/docum
http://192.168.56.102	GET	/mutillidae/docum

Issues

- ! Cleartext submission of password
- ! Serialized object in HTTP message [100]
- ! Password submitted using GET method
- ! Password field with autocomplete enabled
- ? Password returned in later response [2]
- ! Cookie without HttpOnly flag set [2]
- ! Content type incorrectly stated [2]
- ? Source code disclosure [34]
- i Cross-domain Referer leakage [8]
- i Email addresses disclosed
- i Private IP addresses disclosed [8]

Request **Response**

Raw **Headers** **Hex**

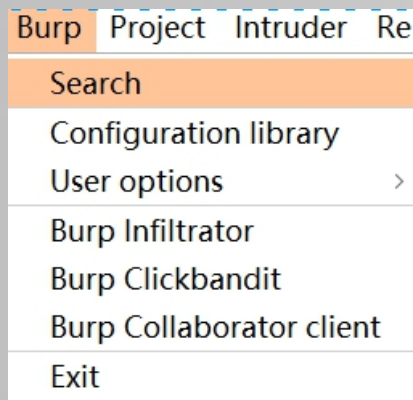
GET /mutillidae/ HTTP/1.1
Host: 192.168.56.102
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3

Advisory **Request** **Response**

! Cleartext submission of p

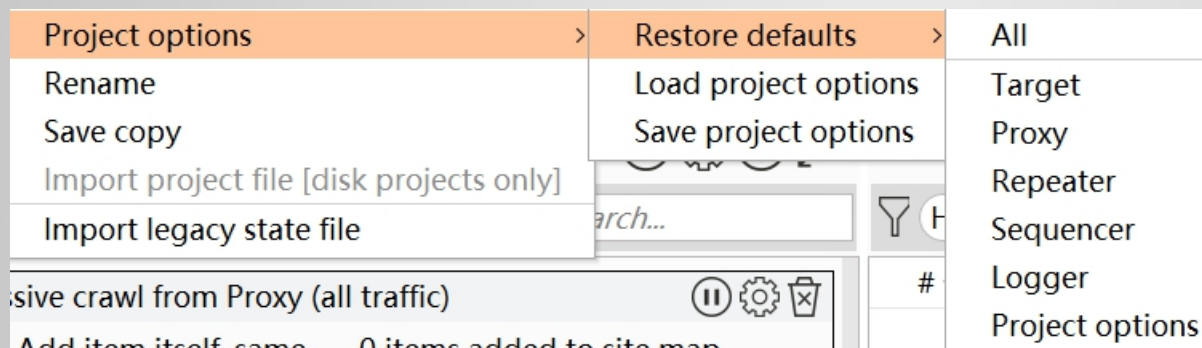
Issue: **Cleartext submission of passw**
Severity: **High**
Confidence: **Certain**
Host: **http://192.168.56.102**
Path: **/mutillidae/index.php**

菜单栏-Burp



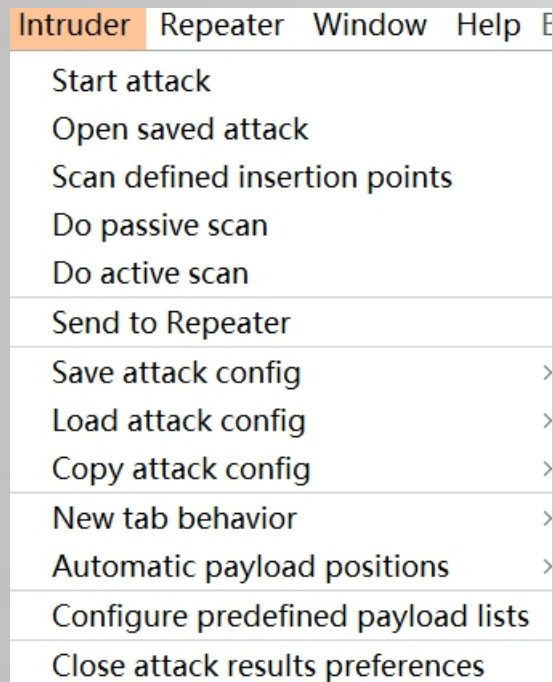
- 1、搜索内容
- 2、配置库
- 3、用户选项
- 4、Infiltrator
- 5、Clickbandit
- 6、Collaborator client

菜单栏-Project



- 1、工程配置
- 2、重命名
- 3、保存备份
- 4、导入配置
- 5、导入遗留状态文件

菜单栏-Intruder



发起攻击

打开工作空间

扫描预定义的插入点

被动扫描

主动扫描

发送到Repeater

保存、加载、复制配置

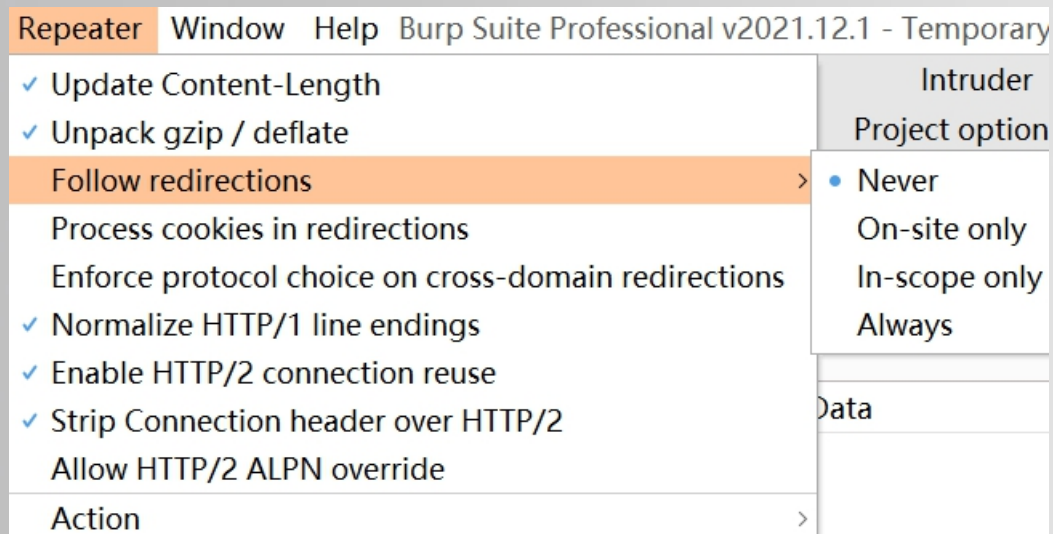
打开新标签时的操作

自动标记payload位置

配置预定义字典

关闭攻击结果时的偏好

菜单栏-Repeater



更新 Content-Length

解压压缩的数据

跟随重定向跳转

重定向的cookie处理

跨域跳转

HTTP1 行结尾

HTTP2 连接重用

剥离 HTTP2 连接头

允许 HTTP2 ALPN 覆盖

<https://portswigger.net/burp/documentation/desktop/tools/repeater/options>

菜单栏-Window



剥离窗口

菜单栏-Help

Help Burp Suite Professional v2021.

Burp Suite documentation

Getting started

Using Burp Suite

Support Center

Release notes

Report bug

Diagnostics

Embedded browser health check

License

Check for updates

Download other installers

Clean Burp from computer

离线文档

上手

用BP做渗透测试

支持中心（在线）

更新记录

上报bug

运行诊断

内置浏览器健康检查

许可证

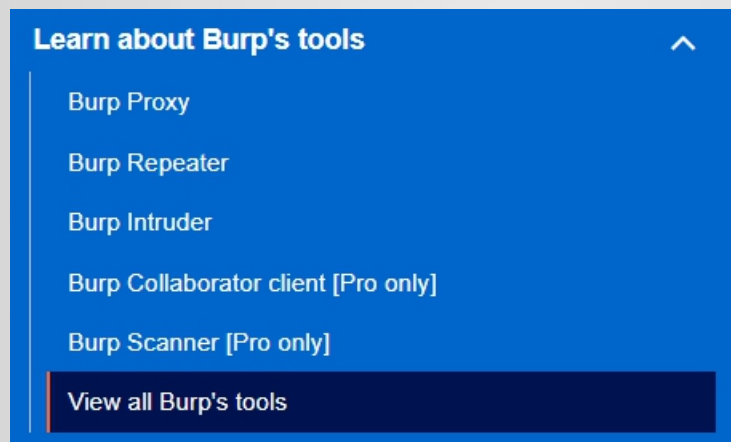
检查更新

下载其他安装器

删除BP

02

模块总体介绍



<https://portswigger.net/burp/documentation/desktop/tools>

Dashboard仪表盘

- 扫描
- 任务 Tasks
- 事件日志 Event Log
- 漏洞问题 Issue activity

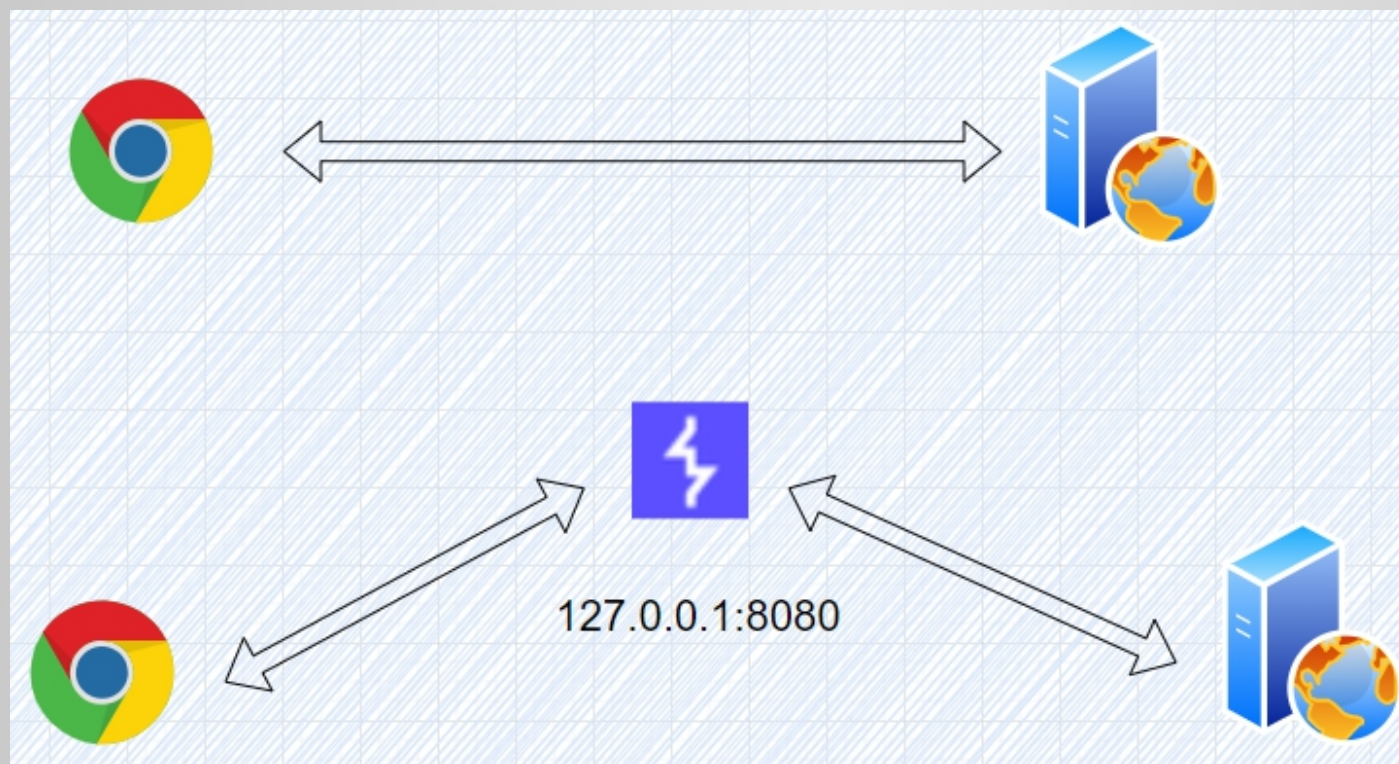
<https://portswigger.net/burp/documentation/desktop/dashboard>

Target 目标模块

- 生成站点地图 (sitemap)
- 设置扫描域 (target scope)
- 生成安全分析

拦截浏览器的HTTP数据包（包括请求和响应）

Proxy 代理模块



对拦截到的请求（地址），设置攻击载荷（payload），利用字典进行渗透测试

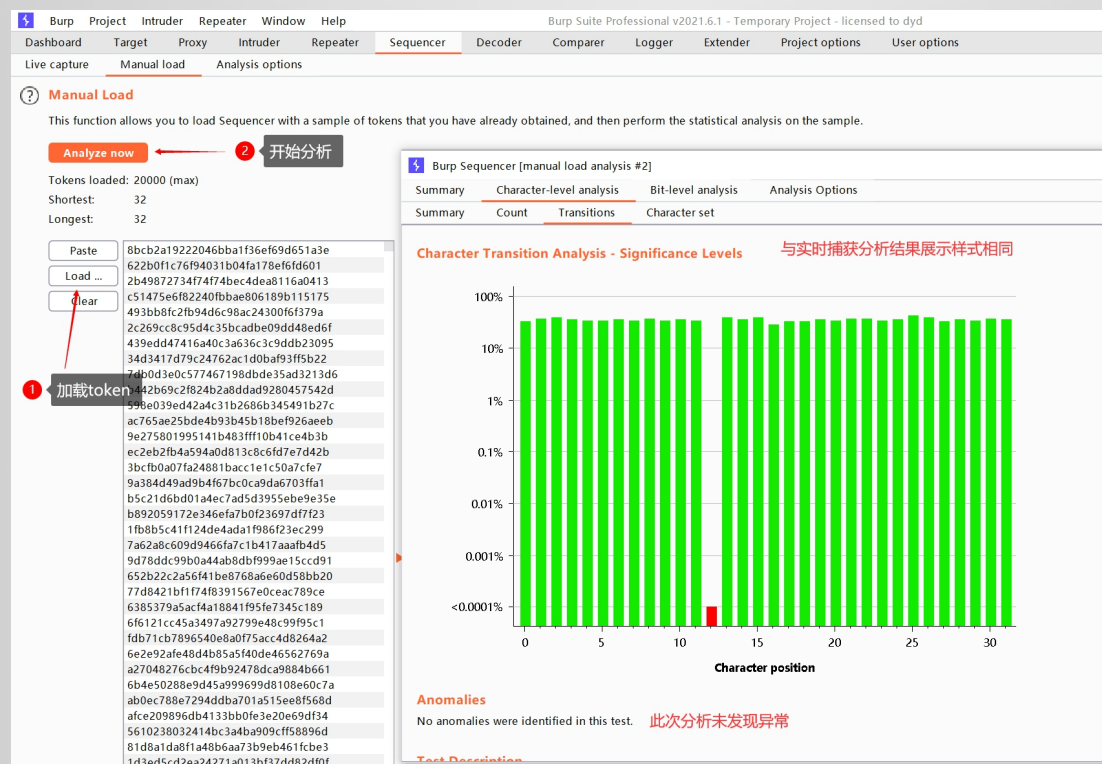
比如：目录扫描、密码暴力破解、压力测试、FUZZ等等

Repeater重放模块

- 1、分析每一步具体的请求和响应内容
- 2、修改请求和响应内容
- 3、重发请求内容

Sequencer 序列器模块

用来评估Token、Session等关键字段
是否可以伪造（是否固定、是否可预测）



The screenshot displays the Burp Suite Professional v2021.6.1 interface, specifically the Sequencer module. The 'Manual Load' tab is active, showing a list of loaded tokens and their statistics (Shortest: 32, Longest: 32). A red arrow points to the 'Analyze now' button, which is labeled '开始分析' (Start Analysis). Another red arrow points to the 'Load' button, which is labeled '加载token' (Load token). The right-hand pane shows the 'Character Transition Analysis - Significance Levels' chart, which is a bar chart with a logarithmic y-axis ranging from <0.0001% to 100%. The chart shows a single red bar at position 11, indicating an anomaly. The text '与实时捕获分析结果展示样式相同' (Same display style as real-time capture analysis results) is present. Below the chart, the 'Anomalies' section states 'No anomalies were identified in this test.' and '此次分析未发现异常' (No anomalies found in this analysis).

Decoder 解码器模块

对请求数据进行编码、解码

URL
HTML
Base64
ASCII hex
Hex
Octal
Binary
Gzip

SHA
SHA-1
SHA-224
SHA-256
SHA-384
SHA-512
SHA-512/224
SHA-512/256
SHA3-224

Comparer比较器模块

对两次请求的结果进行对比

Extender 扩展模块

对插件进行管理

Thank you for watching

无涯老师