

# burpsuite 之 intruder

## 1、简介

Burp Intruder 是一个强大的工具，用于自动对 Web 应用程序自定义的攻击，Burp Intruder 是高度可配置的，并被用来在广范围内进行自动化攻击。你可以使用 Burp Intruder 方便地执行许多任务，包括枚举标识符，获取有用数据，漏洞模糊测试。合适的攻击类型取决于应用程序的情况，可能包括：缺陷测试：SQL 注入，跨站点脚本，缓冲区溢出，路径遍历；暴力攻击认证系统；枚举；操纵参数；拖出隐藏的内容和功能；会话令牌测序和会话劫持；数据挖掘；并发攻击；应用层的拒绝服务式攻击。

## 2、模块说明

Burp Intruder 主要有四个模块组成：

- 1: Target 用于配置目标服务器进行攻击的详细信息。
- 2: Positions 设置 Payloads 的插入点以及攻击类型（攻击模式）。
- 3: Payloads 设置 payload，配置字典
- 4: Options 此选项卡包含了 request headers, request engine, attack results , grep match, grep\_extract, grep payloads 和 redirections。你可以发动攻击之前，在主要 Intruder 的 UI 上编辑这些选项，大部分设置也可以在攻击时对已在运行的窗口进行修改。

**Target 目标选项(Target tab)**

Burp Suite Professional v1.7.11 - 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

1 ... Target Positions Payloads Options

2 Attack Target 攻击目标

Configure the details of the target for the attack.

Host:

Port:

☒ Use HTTPS

Start attack...

配置攻击的目标的详细信息

**Host:** 这是目标服务器的IP地址或主机名。

**Port:** 这是目标服务的端口号。

**Use HTTPS:** 这指定的SSL是否应该被使用

这个选项是用来配置在攻击里产生的所有 HTTP 请求的模板:

配置有效载荷将插入基本请求的位置攻击类型确定有效载荷分配给有效载荷位置的方式 - 请参阅帮助获取完整详细信息

**Payload Positions 有效载荷位置**

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: **Sniper**

**attack type: 攻击模式设置**

- sniper:** 对变量依次进行破解。多个标记依次进行。
- battering ram:** 对变量同时进行破解。多个标记同时进行。
- pitchfork:** 每一个变量标记对应一个字典，取每个字典的对应项。
- cluster bomb:** 每个变量对应一个字典，并且进行交集破解，尝试各种组合。适用于用户名+密码的破解。

**add:** 插入一个新的标记

**clear:** 清除所有的标记

**auto:** 自动设置标记，一个请求发到该模块后burpsuite会自动标记cookie URL等参数

**refresh:** 如果必要的话，这可以要求模板编辑器的语法高亮。

使用一对\$字符来标记出有效负荷的位置，在这两个符号直接包含了模板文本的内容。当把一个有效负荷放置到一个给出的请求的特殊位置上时，就把这\$

符号放到这个位置,然后在两个符号之间的出现的文本都会被有效负荷替换。当有个特殊位置没有为一个给出的请求安排有效负荷时(这只适用"sniper"攻击类型),那个位置的\$字符会被删除,出现在它们之间的文本不会变化。

当使用 Burp Suite 发送一个其他地方的请求时, Burp Intruder 会对你最想放置有效负荷的位置做一个最好的猜测,并且它把这些放置在每个 URL 和主体参数的值里,以及每个 cookie 里。每个标记和它中间的文本都会被加亮以显得更清晰。你可以使用 Intruder 菜单上的选项标记的位置是要替换还是附加现有的参数值。在上面的请求编辑器里,指出了定义位置的数量和文本模板的大小。

你可以使用选项上的按钮来控制位置上的标记:

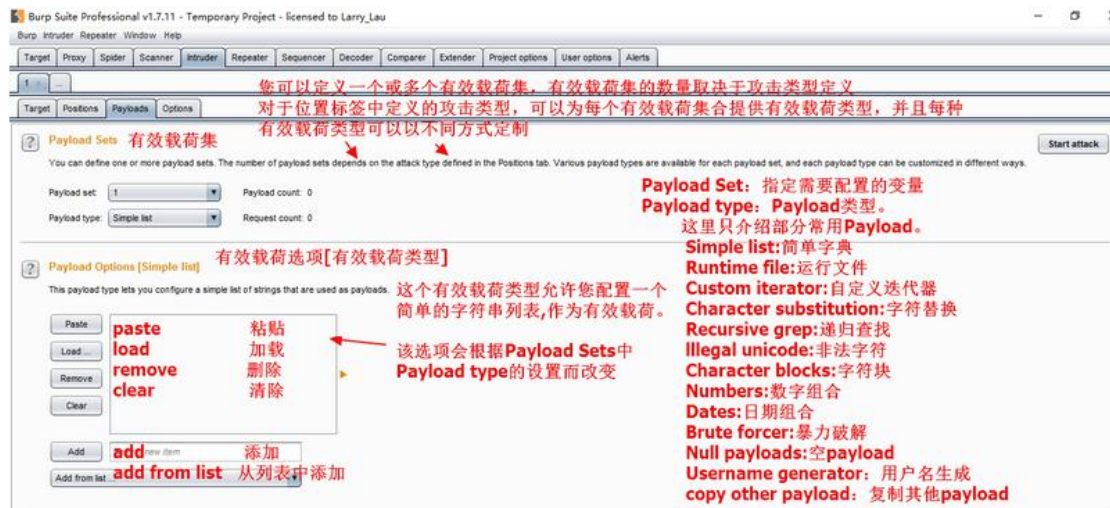
1. add \$ — 在当前光标位置插入一个位置标记。
2. clear \$ — 删除整个模板或选中的部分模板里的位置标记。
3. auto \$ — 这会对放置标记的位置做一个猜测,放哪里会有用,然后就把标记放到相应位置。这是一个为攻击常规漏洞(SQL 注入)快速标记出合适位置的有用的功能,然后人工标记是为自定义攻击的。
4. refresh — 如果需要,可以刷新编辑器里有颜色的代码。
5. clear — 删除整个编辑器内容。

### **Payloads 有效负荷选项(Payloads tab)**

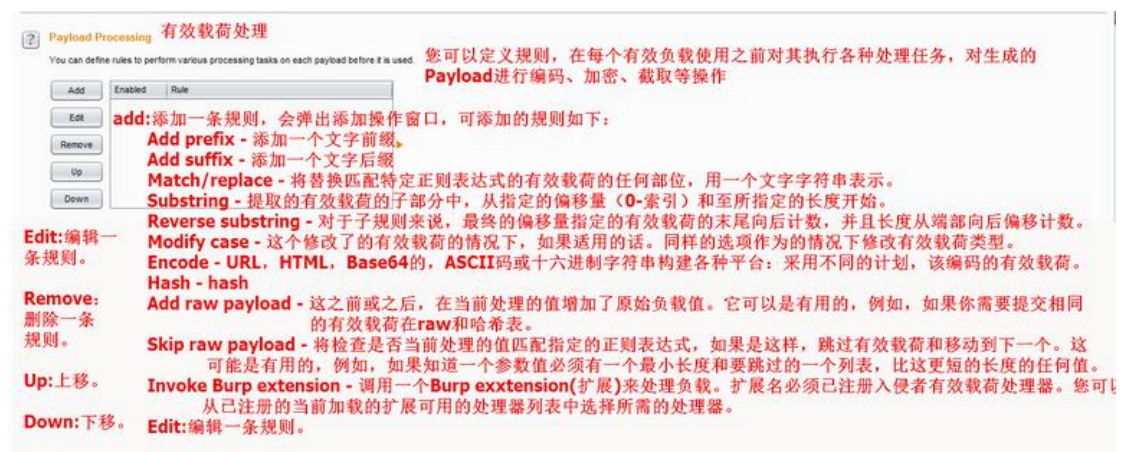
这个选项是用来配置一个或多个有效负荷的集合。如果定义了"cluster bomb"和"pitchfork"攻击类型,然后必须为每定义的有效负荷位置(最多 8 个)配置一个单独的有效负荷。使用"payload set"下拉菜单选择要配置的有效负荷。

选项 1: Payload Sets Payload 数量类型设置

选项 2: Payload Options[Simple list] 该选项会根据选项 1 中 Payload type 的设置而改变



选项 3: Payload Processing 对生成的 Payload 进行编码、加密、截取等操作



选项 4: Payload Encoding 你可以配置哪些有效载荷中的字符应该是 URL 编码的 HTTP 请求中的安全传输。任何已配置的 URL 编码最后应用，任何有效载荷处理规则执行之后。 这是推荐使用此设置进行最终 URL 编码，而不是一个有效载荷

处理规则，因为可以用来有效载荷的 grep 选项来检查响应为呼应有效载荷的最终 URL 编码应用之前。



**Options 选项卡(Options tab)** 此选项卡包含了 request headers, request engine, attack results , grep match, grep\_extrack, grep payloads 和 redirections。你可以发动攻击之前，在主要 Intruder 的 UI 上编辑这些选项，大部分设置也可以在攻击时对已在运行的窗口进行修改。

选项 1：Request Headers 这些设置控制在 Intruder 是否更新配置请求头。



如果选中 ‘update Content-Length header’ 框，Burp Intruder 会使用每个请求的 HTTP 主体长度的正确值，添加或更新这个请求里 HTTP 消息头的内容长度。这个功能对一些需要把可变长度的有效载荷插入到 HTTP 请求模板主体的攻击是很有必要的。这个 HTTP 规范和大多数 web 服务器一样，需要使用消息头内容长度来指定 HTTP 主体长度的正确值。如果没有指定正确值，目标服务器会返回一个错误，也可能返回一个未完成的请求，也可能无限期地等待接收请求里的进一步数据。

如果选中 ‘set Connection: close’ 框,则 Burp Intruder 会添加或更新 HTTP 消



息头的连接来请求在每个请求后已关闭的连接。在多数情况下，这个选项会让攻击执行得更快。

## 选项 2：Request Engine 设置发送请求的线程、超时重试等

Request Engine 请求引擎

These settings control the engine used for making HTTP requests when performing attacks.

Number of threads:

10

Number of retries on network failure:

3

Pause before retry (milliseconds):

2000

Throttle (milliseconds):

Fixed

0

Variable: start

0

step

30000

Start time:

Immediately

In 10 minutes

Paused

Fixed 固定

Variable start 变量:开始

immediately 立即

in minutes 在几分钟内

paused 已暂停

Number of threads: 线程，该选项控制攻击请求的并发数。

Number of retries on network failure: 网络故障的重试次数 - 如果出现连接错误或其他网络问题，Burp会放弃和移动之前重试的请求指定的次数。

pause before retry: 重试前等待时间，当重试失败的请求，Burp会等待指定的时间（以毫秒为单位），然后重试。

Throttle between requests: 请求之间的等待时间，Burp可以在每次请求之前等待一个指定的延迟（以毫秒为单位）。此选项很有用，以避免超载应用程序，或者是更隐蔽。

Start time: 开始时间，此选项允许您配置攻击立即启动，或在指定的延迟后，或开始处于暂停状态。

## 选项 3：Attack Results 设置攻击结果的显示。

Attack Results 攻击结果

These settings control what information is captured in attack results.

☒ Store requests

☒ Store responses

☒ Make unmodified baseline request

☐ Use denial-of-service mode (no results)

☐ Store full payloads

Store requests/responses: 存储请求/响应，这个选项确定攻击是否会保存单个请求和响应的内容

Make unmodified baseline request: 未修改的基本请求，如果选择此选项，那么除了配置的攻击请求，Burp会发出模板请求设置为基值，所有有效载荷的位置。此请求将在结果表显示为项目 # 0。使用此选项很有用，提供一个用来比较的攻击响应基地的响应。

Use denial-of-service mode: 使用拒绝服务的模式，如果选择此选项，那么攻击会发出请求，如正常，但不会等待处理从服务器收到任何答复。只要发出的每个请求，TCP连接将被关闭。这个功能可以被用来执行拒绝服务的应用层对脆弱的应用程序的攻击，通过重复发送该启动高负荷任务的服务器上，同时避免通过举办开放套接字等待服务器响应锁定了本地资源的请求。

Store full payloads: 保存完整的有效载荷。如果选择此选项，Burp将存储全部有效载荷值的结果。

## 选项 4：Grep - Match 在响应中找出存在指定的内容的一项。

Grep - Match Grep-匹配

These settings can be used to flag result items containing specified expressions.

☐ Flag result items with responses matching these expressions:

Paste

Load...

Remove

Clear

Add

error

exception

illegal

invalid

fail

stack

access

directory

Enter a new item

Match type:

Simple string

Regex

☐ Case sensitive match

☒ Exclude HTTP headers

Match type: 匹配类型，指定的表达式是否是简单的字符串或regular expressions(正则表达式)。

Case sensitive match: 区分大小写的匹配，指定检查表达式是否应区分大小写。

Exclude HTTP headers: 排除HTTP头，指定的HTTP响应头是否应被排除在检查。

选项 5: Grep - Extract 通过正则提取返回信息中的内容。



选项 6: Grep - Payloads 这些设置可以用于包含已提交的有效负载的反射的标志结果项目。如果启用了此选项，BurpSuite 会添加包含一个复选框指示当前负载的值在每个响应发现新的结果列。



选项 7: Redirections 重定向响应，控制 Burp 在进行攻击时如何处理重定向。

