

# Web 系统测试

## 4.8 渗透测试—Intruder

# 目 录

---

➤ 什么是Intruder

➤ Intruder怎样使用

## ➤ Intruder: 入侵

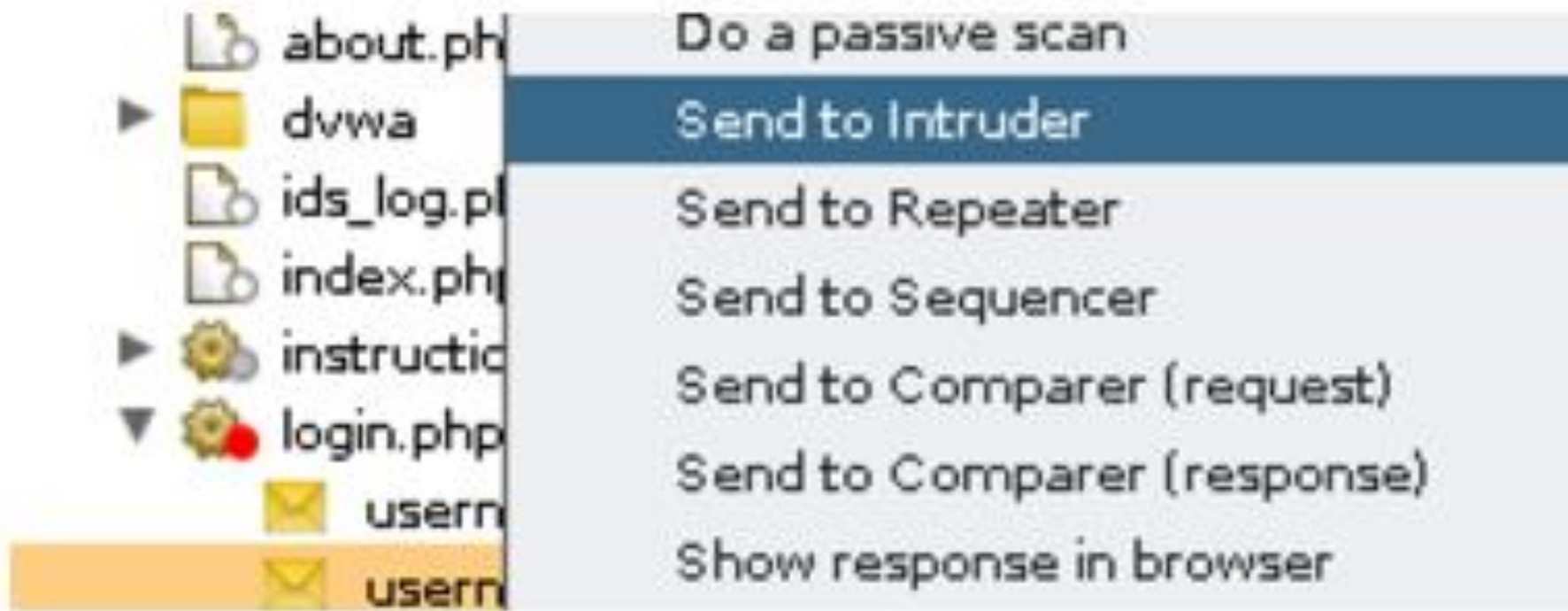
## ➤ 工作原理:

- 在原始请求数据的基础上，通过修改各种原始请求数据的基础上，通过修改各种请求参数，以获取不同的请求应答。每一次请求中，Intruder通常会携带一个或多个有效载荷（Payload），在不同位置进行攻击重放，通过应答数据的比对分析来获得需要的特征数据

- 标识符枚举Web应用程序经常使用标识符来引用用户、账户、资产等数据信息
- 在特定场景提取有用的数据
- 模糊测试输入型漏洞
  - SQL注入
  - 跨站点脚本
  - 文件路径遍历

1. 正常启动，完成代理设置
2. 进入历史日志（History）子选项卡,查找可能存在问题的请求日志，并通过右击菜单，发送到Intruder

- 在使用爆破的时候会用到Intruder，在Target页面对目标右键发送到Intruder

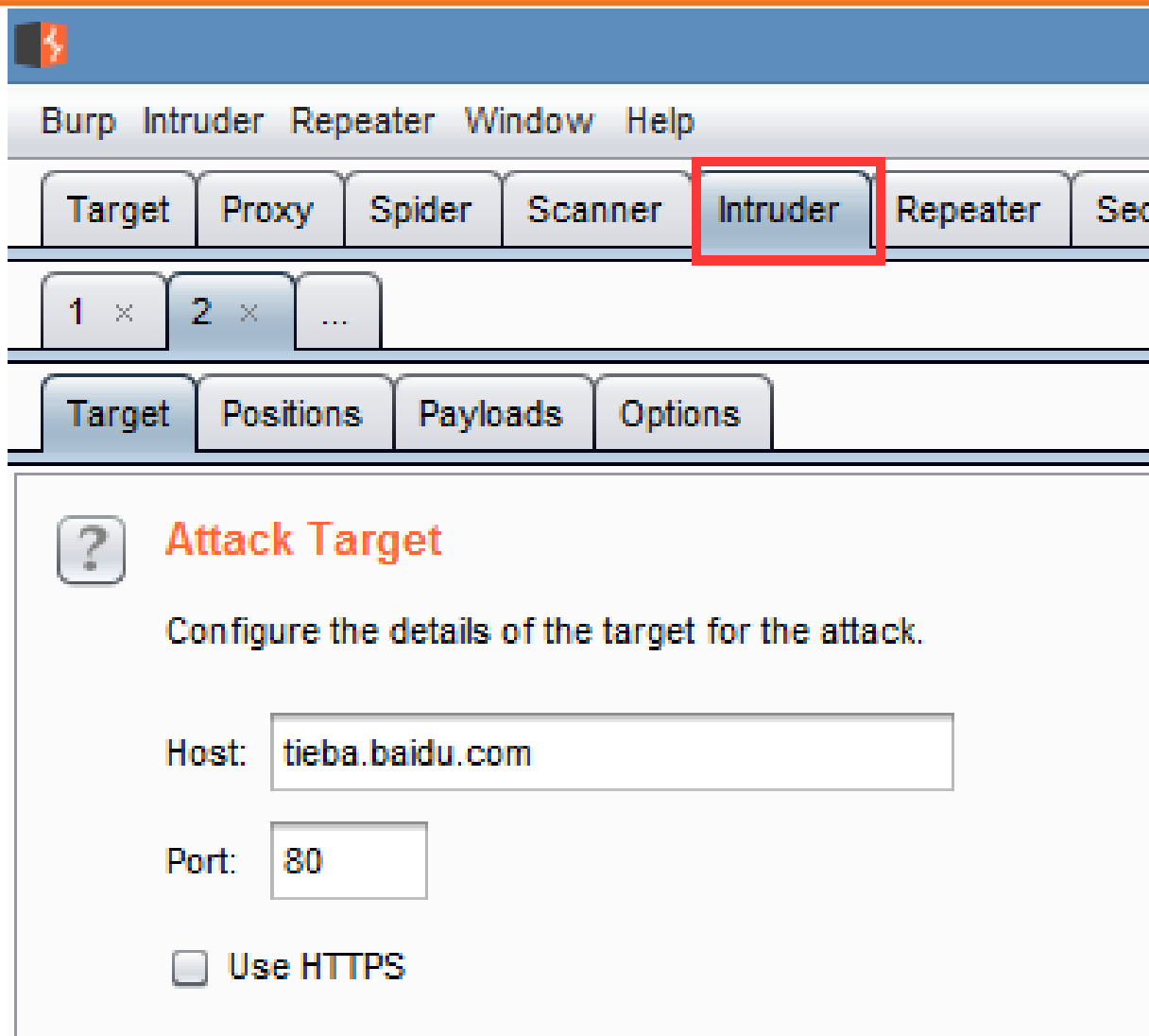


# Intruder使用

➤在Intruder模块中查看： 第一步：首先要选择使用Intruder的位置以及攻击类型（Attack type）



## ➤ 攻击目标设置



The screenshot shows the Burp Suite Intruder window. The 'Intruder' tab is selected and highlighted with a red box. Below the tabs, there are two tabs: 'Target' and 'Positions'. The 'Target' tab is active, showing the 'Attack Target' section. The 'Host' field is set to 'tieba.baidu.com' and the 'Port' field is set to '80'. The 'Use HTTPS' checkbox is unchecked.

1 x 2 x ...

Target Positions Payloads Options

? **Attack Target**

Configure the details of the target for the attack.

Host: tieba.baidu.com

Port: 80

☐ Use HTTPS



## ➤Payload类型与处理

### ●Simple list

### 简单列表

- 通过配置一个字符串列表作为payload，也可以手工添加字符串列表或从文件加载字符串列表。可以是XSS脚本，CGI脚本，SQL注入脚本，数字，大、小写字母，用户名、密码、表单域的字段名、IIS文件名和目录名等

## ➤Payload类型与处理

### ●Runtimefile

指定文件

- 选择一个文件
- 运行时，Burp Intruder将读取文件的每一行作为一个Payload

## ➤Payload类型与处理

### ●Custom iterator

### 自定义迭代器

- 共有8个占位，每个占位可以指定简单列表的payload类型，然后根据占位的多少，与每一个简单列表的Payload进行笛卡尔积，生成最终的Payload列表

# Question