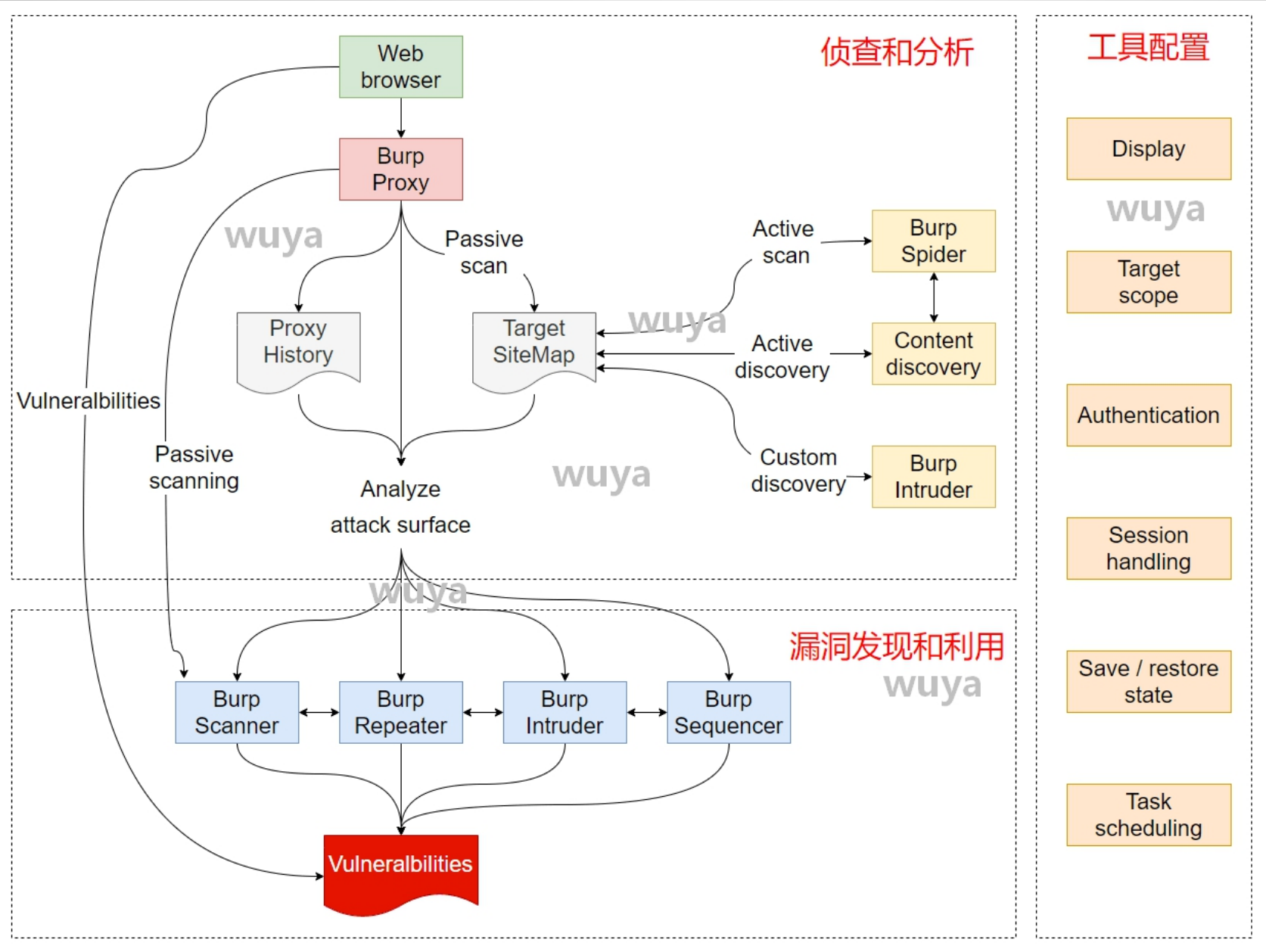


## 3.5 Burp 扫描功能

# Burp渗透测试流程



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

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

模块总体介绍:

<https://portswigger.net/burp/vulnerability-scanner>

扫描功能的使用:

<https://portswigger.net/burp/documentation/desktop/getting-started/running-your-first-scan>

收录的漏洞

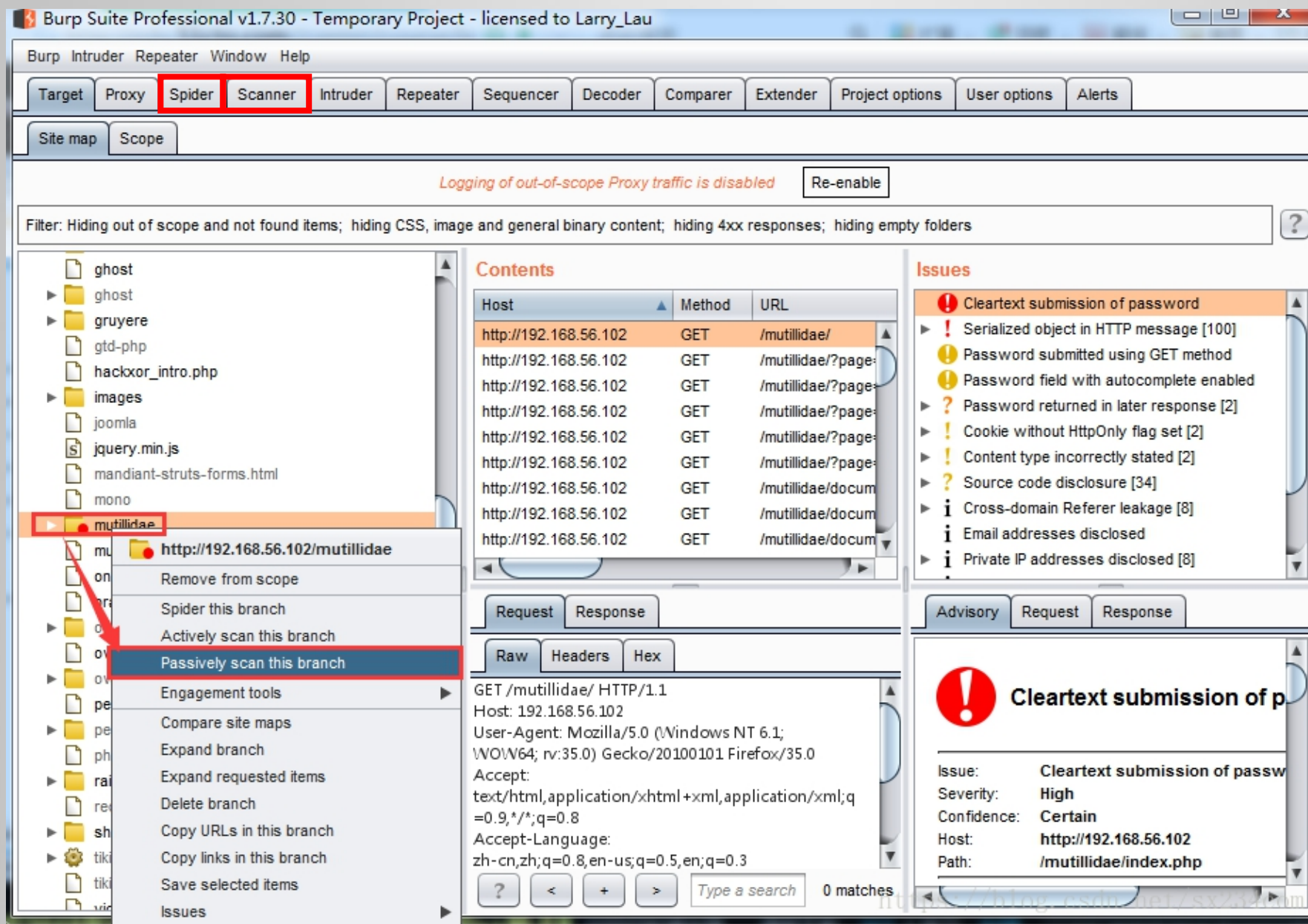
<https://portswigger.net/kb/issues>

- 1、漏洞扫描整体介绍
- 2、使用BP漏扫功能
- 3、生成扫描报告

# 01

## 漏洞扫描整体介绍

AWVS、Appscan、Nessus、Openvas、Goby、  
Xray、ZAP.....



爬行 Crwal  
审计 Audit

Tasks

New scan

New live task

Running

Paused

Finished

Live task

Search...

1. Live passive crawl from Proxy (all traffic)

Add links. Add item, itself, same ...

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 requests (0 errors)

Capturing:

View details >>

Event log

Filter

Critical

Error

Info

Debug

Search...

Time	Type	Source	
19:35:33 14 4月 2022	Info	Suite	This version of B
19:35:32 14 4月 2022	Info	Proxy	Proxy service sta



# 核心内容

内容	描述
Scan (主动扫描)	给定地址，爬取内容，检测漏洞
Live task (被动扫描)	对经过Proxy、Repeater、Intruder的请求进行漏洞检测
live passive crawl from proxy(all traffic)	来自Proxy的被动流量抓取
live audit from proxy(all traffic)	流量的实时审计

Actively Scan: 主动扫描 = Crawl and audit

Passively Scan: 被动扫描 = Live audit

方式：爬取所有链接，检测漏洞

特点：发送大量请求

使用场合：开发、测试环境

针对漏洞：

客户端的漏洞，如XSS、HTTP头注入、操作重定向。

服务端的漏洞，如SQL注入、命令行注入、文件遍历。

# 被动扫描

方式：只检测经过BP代理服务器的地址，不爬取

特点：发送有限请求

使用场合：生产环境

针对漏洞：

提交的密码为未加密的明文。

不安全的cookie的属性，例如缺少HttpOnly和安全标志。

cookie的范围缺失。

跨域脚本包含和站点引用泄露。

表单值自动填充，尤其是密码。

SSL保护的内容缓存。

目录列表。

提交密码后应答延迟。

session令牌的不安全传输。

敏感信息泄露，例如内部IP地址、电子邮件地址、堆栈跟踪等信息泄露。

不安全的ViewState 的配置。

错误或不规范的Content-Type指令。

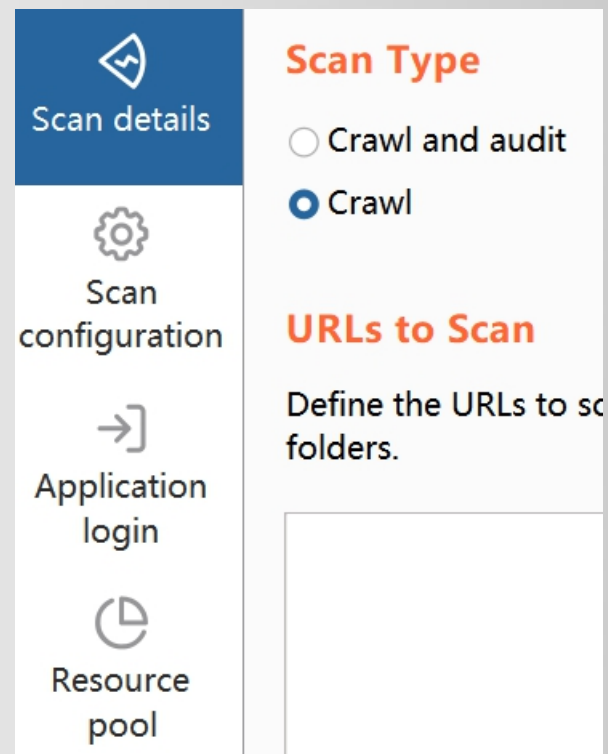
# 02

## 使用BP漏扫功能

# 主动扫描的类型

Crawl 爬行（建立站点地图）  
Audit 审计（扫描漏洞）

Scan Configuration: 爬行和审计的设置  
Application login: 账号密码  
Resource pool: 线程池设置



The screenshot shows a web interface for configuring a scan. On the left is a sidebar with four items: 'Scan details' (selected, with a magnifying glass icon), 'Scan configuration' (with a gear icon), 'Application login' (with a right arrow icon), and 'Resource pool' (with a circular arrow icon). The main content area is titled 'Scan details' and contains two sections. The first section, 'Scan Type', has two radio buttons: 'Crawl and audit' (unselected) and 'Crawl' (selected). The second section, 'URLs to Scan', has the text 'Define the URLs to scan folders.' followed by a large, empty text input box.

内容	翻译	作用
Crwal Optimization	爬行的优化	最大链接深度 更快还是更完整
Crwal Limits	爬行最大限制	最大时间 最多链接 最大请求数
Login Functions	登录注册	登录操作：自动注册 用无效的用户名主动触发登录失败
Handling Application	错误处理	爬行过程中的错误处理，比如超时
Miscellaneous [,misə'leiniəs]	杂项	杂项

内容	翻译	作用
Audit Optimization	审计优化	扫描的速度和精确度
Issues Reported	问题报告	报告哪些漏洞：根据扫描类型或者漏洞类型来过滤，默认全选
Handling Application Errors During Audit	审计过程出错的 处理	比如连接失败和传输超时默认：如果一个插入点连续失败两次，就跳过，不再发送请求（接口挂了） 如果连续两个插入点失败，跳过其他的插入点（网站挂了）
Insertion Point Types	插入点的类型	URL参数值、Body里面的参数值、Cookie值、参数名字、HTTP请求头、Body完整内容、URL文件名、URL目录
Modifying Parameter Locations	插入点位置	替换，交叉检测



内容	翻译	作用
Ignored insertion Point	忽略的插入点	
Frequently Occurring Insertion Points	插入点相同时	当大量的插入点结果没有区别的时候，更加高效地扫描。
Misc Insertion Point Options	杂项	一个插入点的最大请求数量
JavaScript Analysis	JavaScript审计	

# 主动扫描的类型

Scan: 输入URL或者URL右键

Live Task: 从其他模块获取到流量

Live Task:

Audit 不会爬行

passive crawl 会爬行

# 03

## 生成扫描报告

# 扫描报告



## 右键导出

<https://portswigger.net/burp/samplereport/burpscannersamplereport>

### Issue activity

Filter High Medium Low Irrelevant

#	Task	Time
100	5	10:00 10:00 07/07/2018
99	5	
98	5	
97	5	
96	5	
95	5	
94	5	

**i** **User agent-dep**

Add comment

Highlight

Set severity

Set confidence

Report issue

Thank you for watching

无涯老师