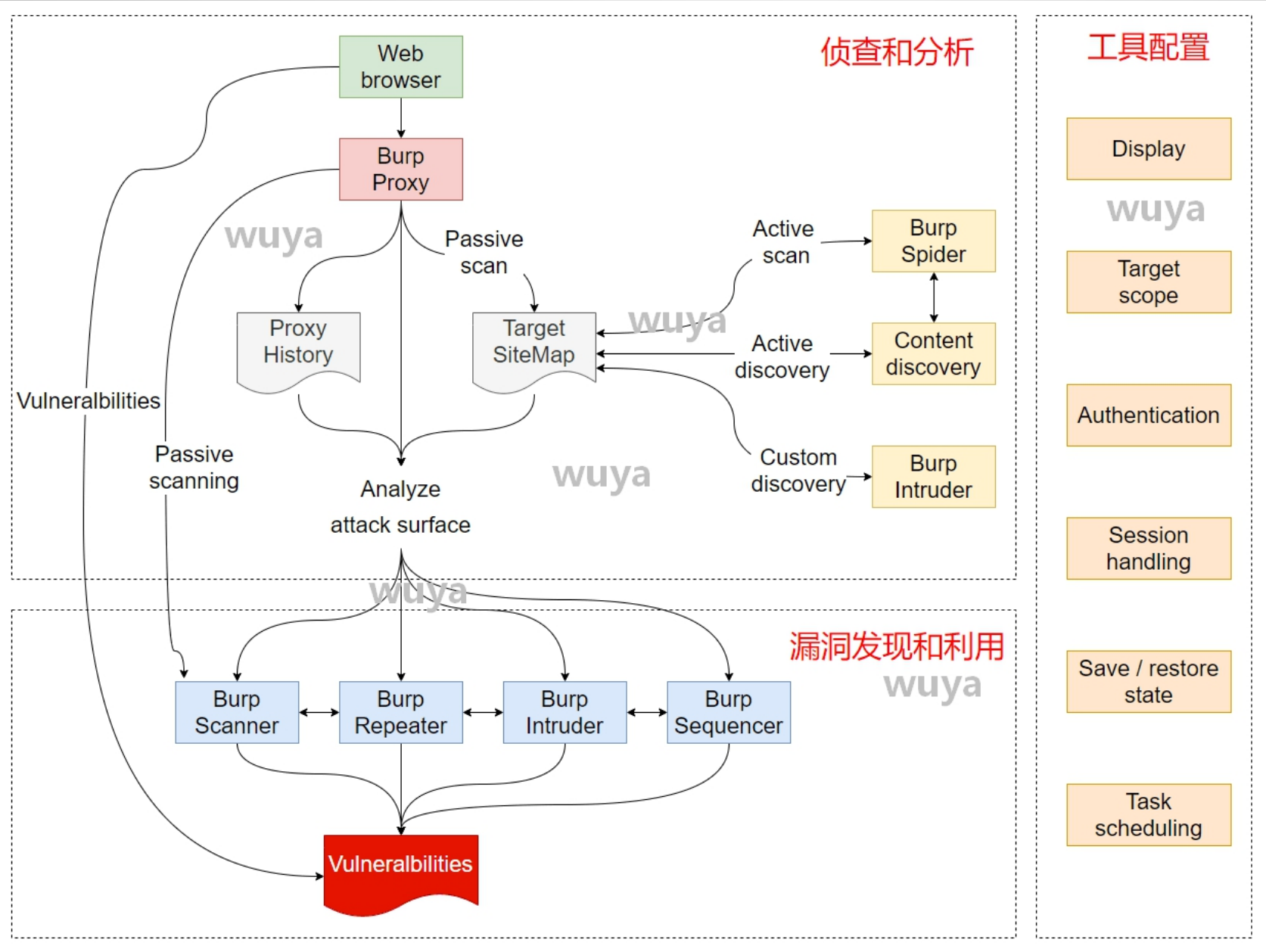


3.4 Burp Target模块

Burp渗透测试流程



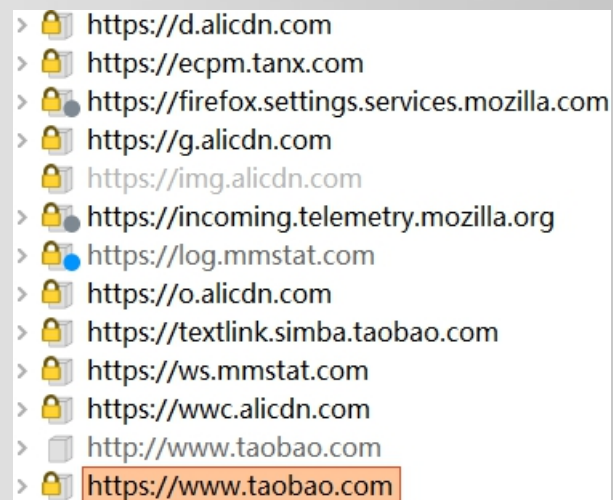
- 1、Target模块的作用
- 2、Target设置目标域
- 3、站点地图Sitemap
- 4、Target结果操作














01

Target模块的作用

与HTTP History的区别

- 1、HTTP History按时间顺序记录
- 2、Target按主机或者域名分类记录



>  <https://d.alicdn.com>
>  <https://ecpm.tanx.com>
>  <https://firefox.settings.services.mozilla.com>
>  <https://g.alicdn.com>
>  <https://img.alicdn.com>
>  <https://incoming.telemetry.mozilla.org>
>  <https://log.mmstat.com>
>  <https://o.alicdn.com>
>  <https://textlink.simba.taobao.com>
>  <https://ws.mmstat.com>
>  <https://www.alicdn.com>
>  <http://www.taobao.com>
>  <https://www.taobao.com>

Target模块的作用

- 1、把握网站的整体情况
- 2、对一次工作的域进行分析
- 3、分析网站存在的攻击面

对一个软件系统可以采取的攻击方法集合，一个软件的攻击面越大安全风险就越大。

包括：字段、协议、接口、服务、硬件的攻击点。

02

Target设置作用域

怎么算同一个域?

域1	域2	同域	原因
http://www.wuya.com/	http://www.wuya.com/index.html http://www.wuya.com/admin?a=1	YES	-
http://www.wuya.com/	https://www.wuya.com/	NO	协议
http://www.wuya.com/	http://www.wuya.cn/	NO	主域名
http://www.wuya.com/	http://blog.wuya.com/	NO	子域名
http://www.wuya.com:80/	http://www.wuya.com:7298/	NO	端口

协议、域名、端口必须相同
目录、文件、参数可以不同

如何限定域的范围？

例如：

只拦截：<https://www.wuya.com/>

不拦截：<https://www.wuya.com/blog>

- 1、限定Sitemap和HTTP history记录哪些域的内容
- 2、限定Spider抓取哪些域的内容
- 3、限定Scanner扫描哪些域的安全漏洞

03

站点地图Sitemap

站点地图记录类型

- 1、自动（爬行）
- 2、手动（浏览器访问）

04 对结果进行操作

右键菜单

Add to scope	添加作用域
Scan	
Passively scan this branch	
Actively scan this branch	
Send to Intruder	
Send to Repeater	
Send to Sequencer	
Send to Comparer	
Request in browser	
Engagement tools	交互工具
Compare site maps	站点比较
Expand branch	展开分支
Expand requested items	展开请求条目
Delete item	删除条目
Copy URLs in this branch	复制URL
Copy links in this branch	复制链接
Copy as curl command	复制为curl命令
Save selected items	保存
Issues	问题
View	
Show new site map window	
Site map documentation	

Referer字段

作用：告诉服务器当前请求是从哪个页面链接过来的

应用场景：

- 1、来源统计
- 2、防盗链

Thank you for watching

无涯老师