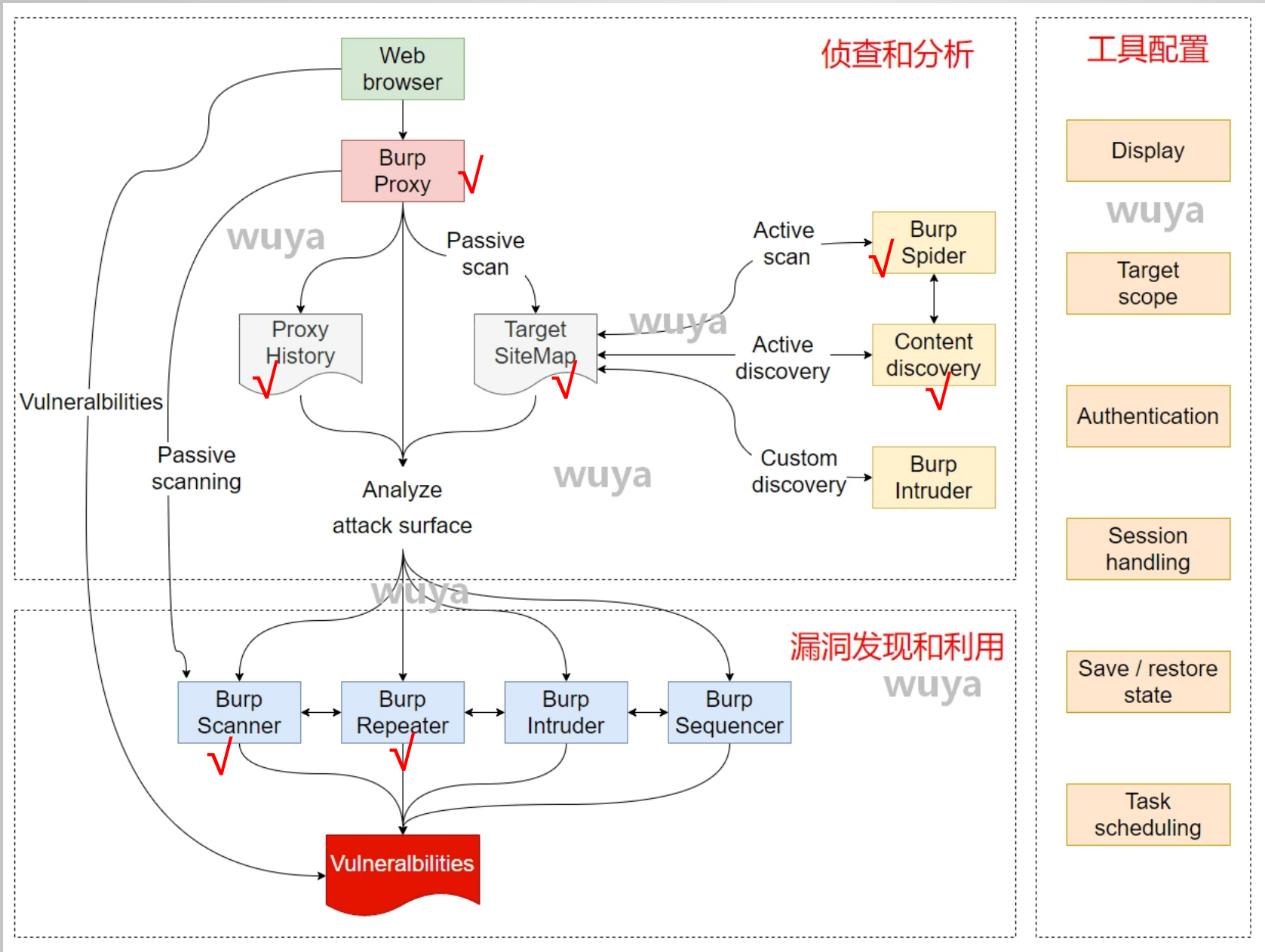
3.7 Burp Intruder

Burp渗透测试流程



参考资料

https://portswigger.net/burp/documentation/desktop/tools/intruder

课程大纲

八方网域
bafangwy.com

1、Intruder模块作用与原理
2、Intruder实现密码暴力破解
3、Intruder其他攻击模式
4、Intruder标记结果
5、Intruder获得CSRF Token

01 Intruder模块作用与原理

原理

http://xxx.wuya.com/bbs/index.php?name=wuyanzu&motto=go

对请求参数进行修改，分析响应内容，获得特征数据

本质：
1、自动化发起HTTP请求
2、基于现成字典或者生成字典

用途

1、猜测用户名、密码等
2、寻找参数、目录等
3、枚举商品ID、验证码等
4、模糊测试（FUZZ）
……

可替代工具：
wfuzz（全部功能）、dirb（目录扫描）、hydra（暴破）……

02 Intruder实现暴力破解

靶场环境

八方网域
bafangwy.com

dvwa
参考“教程合集”——
27-PHP、Apache环境中部署DVWA.pdf

流程

1、从其他模块发送或者手动填写
2、选择攻击模式 Attack type
3、选择攻击字段 Positions
4、设置payload
5、其他设置（线程池等）
6、发起攻击
7、查看结果

攻击模式

Sniper	狙击手
Battering ram	攻城锤
Pitchfork	草叉
Cluster bomb	榴霰[xiàn]弹

payload type-1

类别	名称	描述
Simple list	简单字典	添加、粘贴或者从文件读取字典，或者使用预定义的字典
Runtime file	运行时文件	运行时，Burp Intruder将读取文件的每一行作为一个Payload
Custom iterator	自定义迭代器	这个是占位填充的一种方式，最多8位
Character substitution	字符替换	把字典里面相应的字符进行替换
Case modification	大小写修改	要不要保持原样的，要不要全部大写的，要不要全小写的，要不要驼峰命名的
Recrusvive grep	递归查找	用来提取相应数据的比如拿到PHPSESSIONID，拿到TOKEN等等，可以通过格式匹配抓取到对应的字段值。

https://portswigger.net/burp/documentation/desktop/tools/intruder/payloads/types

payload type-2

类别	名称	描述
Illegal unicode	非法Unicode编码	用于绕过正则表达式的过滤验证
Character blocks	字符块	比如生成100A，200个+号，300个数字1等等
numbers	数字组合	
dates	日期组合	
Brute forcer	暴力破解	暴力枚举，最后一位先固定，然后一个个改
Null payloads	空payload	不需要设置payload

payload type-3

类别	名称	描述
Character frobber	字符frobber	依次修改指定字符串在每个字符位置的值，每次都是在原字符上递增一个该字符的ASCII码。
Bit flipper	Bit翻转	对预设的Payload原始值，按照比特位，依次进行修改
Username generator	用户名生成器	主要用于用户名和email帐号的自动生成
ECB block shuffler	ECB加密块洗牌	基于ECB加密模式的Payload生成器
Extension-generated	Burp Payload生成插件	基于Burp插件来生成Payload值，需要安装插件
Copy other payload	Payload复制	是将其他位置的参数复制到Payload位置上（比如密码要输入两遍）

2234
1334
1244
1235

03 Intruder其他攻击模式

Battering ram 攻城锤

所有字段的值相同，来自同一个字典

Pitchfork 草叉

从多个字典提取值，赋给多个字段，按顺序一一对应

例如：
100个用户名
50个密码
最终请求次数：50次

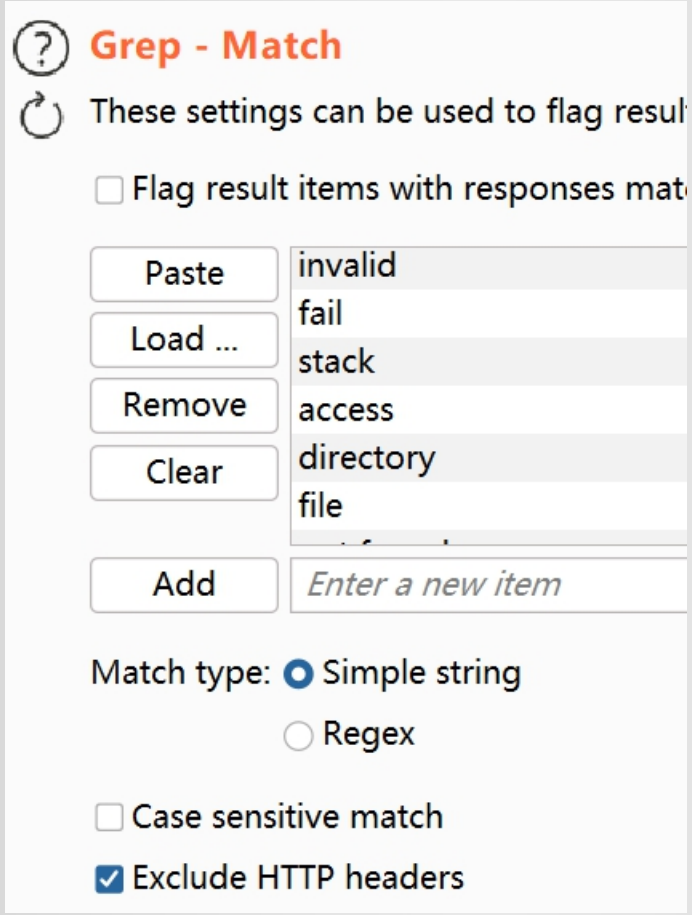
Cluster bomb 榴霰弹

所有字典全部交叉验证

例如：
100个用户名
50个密码
最终请求次数：5000次

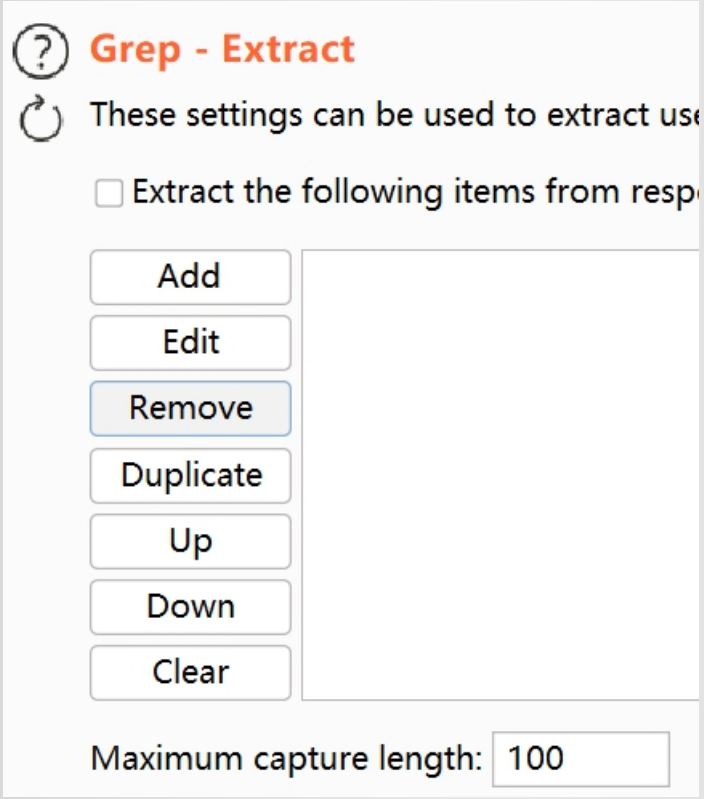
04 Intruder标记结果

Grep Match



05 Intruder获得CSRF Token

Grep Extract



06 Intruder暴破验证码

Thank you for watching