Web 系统测试

4.4 Web安全测试—漏洞扫描

河北师范大学软件学院
Software College of Hebei Normal University

内容回顾

- 安全测试基础知识
  - 什么是安全测试
  - 什么是Web安全测试
  - 什么是渗透测试
  - Web安全可能存在的漏洞
- HTTP协议
  - 协议内容

内容回顾

- HTTP请求流程
- 请求头、响应头
- Cookie 和Session

➢信息收集

- 搜集子域名（搜索语法）
- 收集服务器操作系统信息
- 收集服务器开放端口信息

目 录

- 什么是漏洞扫描
- 为什么进行漏洞扫描
- 怎样进行漏洞扫描

什么是漏洞扫描

- 通过扫描等手段对指定的远程或者本地计算机系统的安全性进行检测，发现可利用漏洞的一种安全检测（渗透攻击）行为

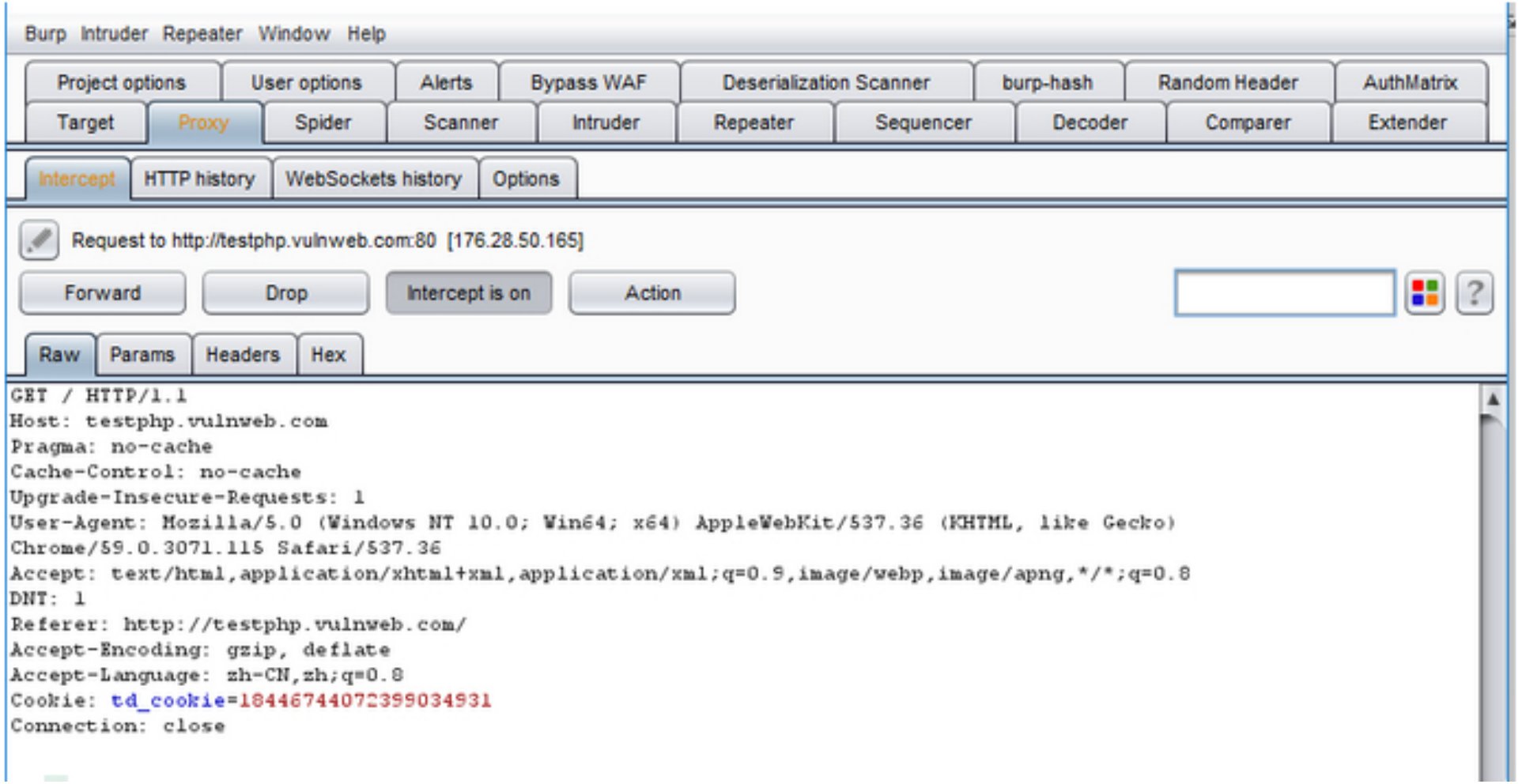
为什么进行漏洞扫描

- 了解网络的安全设置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级
- 网络管理员能根据扫描的结果更正网络安全漏洞和系统中的错误设置，在黑客攻击前进行防范

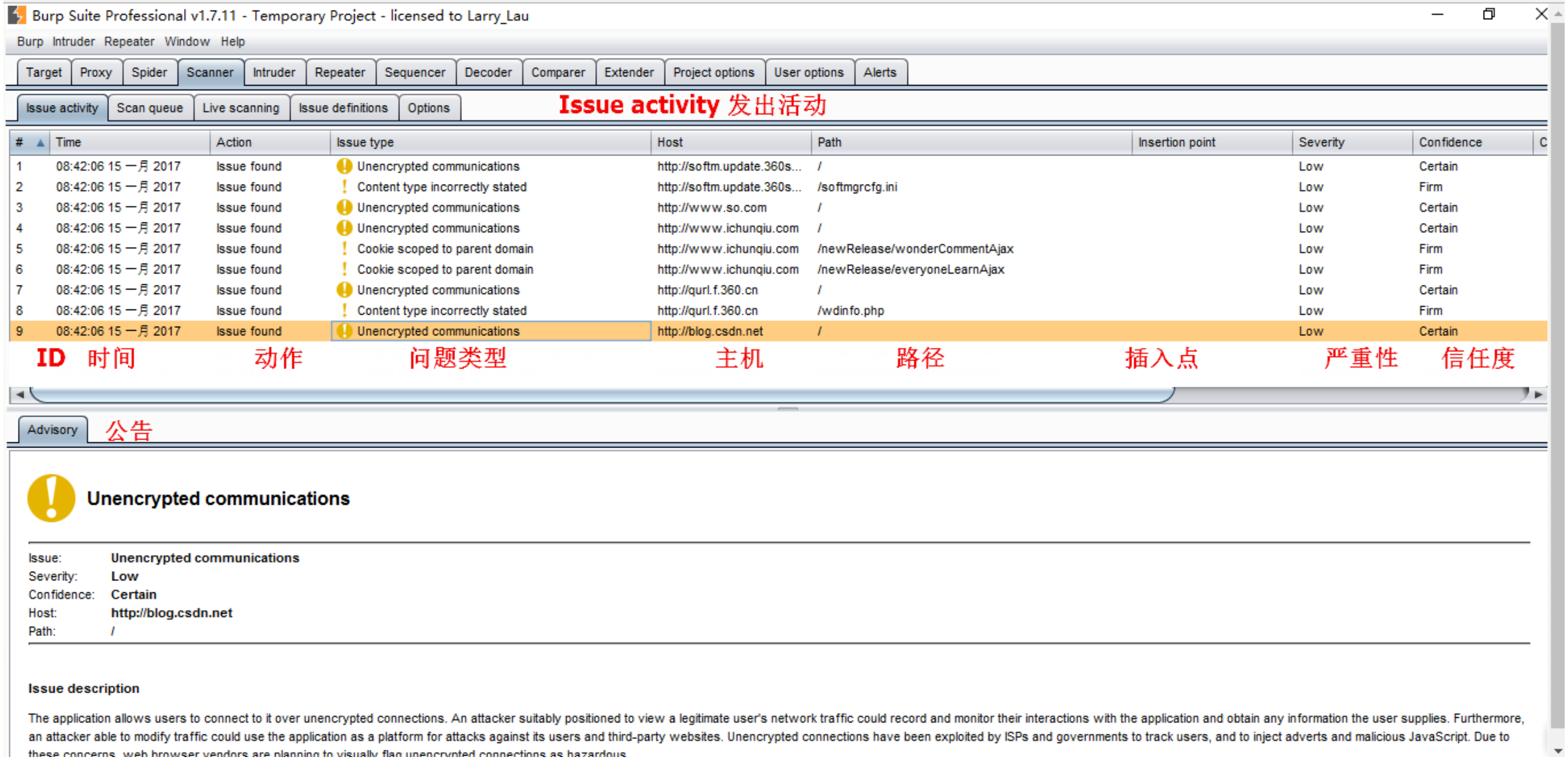
怎样进行漏洞扫描

- 漏洞扫描可以使用的工具
  - Burp Suit　WVS　AppScan
- 漏洞扫描步骤
  - 抓包功能开启
  - 单击数据包区域，右键，选择“Do an active scan（激活主动扫描）”
  - 点击按钮之后，burp Suite会提示是否激活扫描，选择“是”
  - 这时“Scanner（扫描）”按钮会亮起，开始进行扫描

抓包功能

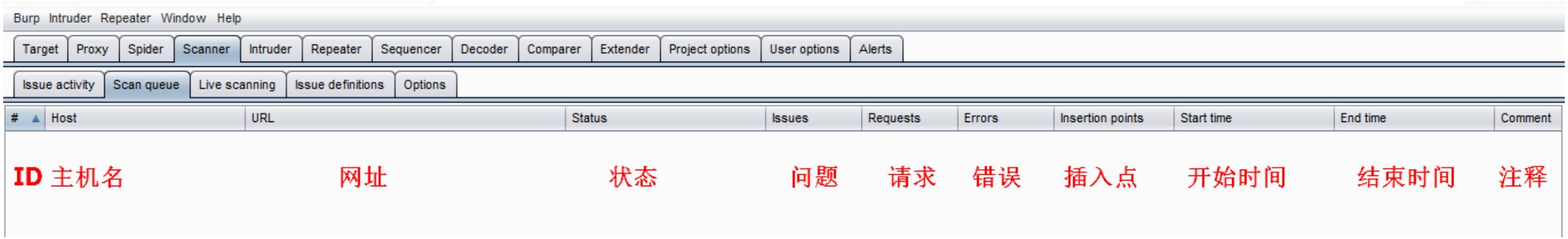

Burp Intruder Repeater Window Help
Project options
User options
Alerts
Bypass WAF
Deserialization Scanner
burp-hash
Random Header
AuthMatrix
Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Intercept
HTTP history
WebSockets history
Options
Request to http://testphp.vulnweb.com:80 [176.28.50.165]
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
GET / HTTP/1.1
Host: testphp.vulnweb.com
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/59.0.3071.115 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
DNT: 1
Referer: http://testphp.vulnweb.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: td_cookie=18446744072399034931
Connection: close

扫描


Burp Suite Professional v1.7.11 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Issue activity Scan queue Live scanning Issue definitions Options
Issue activity 发出活动
Time Action Issue type Host Path Insertion point Severity Confidence
1 08:42:06 15 一月 2017 Issue found Unencrypted communications http://softm.update.360s... / Low Certain
2 08:42:06 15 一月 2017 Issue found Content type incorrectly stated http://softm.update.360s... /softmgrcfg.ini Low Firm
3 08:42:06 15 一月 2017 Issue found Unencrypted communications http://www.so.com / Low Certain
4 08:42:06 15 一月 2017 Issue found Unencrypted communications http://www.ichunqiu.com / Low Certain
5 08:42:06 15 一月 2017 Issue found Cookie scoped to parent domain http://www.ichunqiu.com /newRelease/wonderCommentAjax Low Firm
6 08:42:06 15 一月 2017 Issue found Cookie scoped to parent domain http://www.ichunqiu.com /newRelease/everyoneLearnAjax Low Firm
7 08:42:06 15 一月 2017 Issue found Unencrypted communications http://qurl.f.360.cn / Low Certain
8 08:42:06 15 一月 2017 Issue found Content type incorrectly stated http://qurl.f.360.cn /wdinfo.php Low Firm
9 08:42:06 15 一月 2017 Issue found Unencrypted communications http://blog.csdn.net / Low Certain
ID 时间 动作 问题类型 主机 路径 插入点 严重性 信任度
Advisory 公告
Unencrypted communications
Issue: Unencrypted communications
Severity: Low
Confidence: Certain
Host: http://blog.csdn.net
Path: /
Issue description
The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites. Unencrypted connections have been exploited by ISPs and governments to track users, and to inject adverts and malicious JavaScript. Due to these concerns, web browser vendors are planning to visually flag unencrypted connections as hazardous

扫描队列

➢**Scan queue 扫描队列，这里将显示扫描队列的状态 进度 结果等**

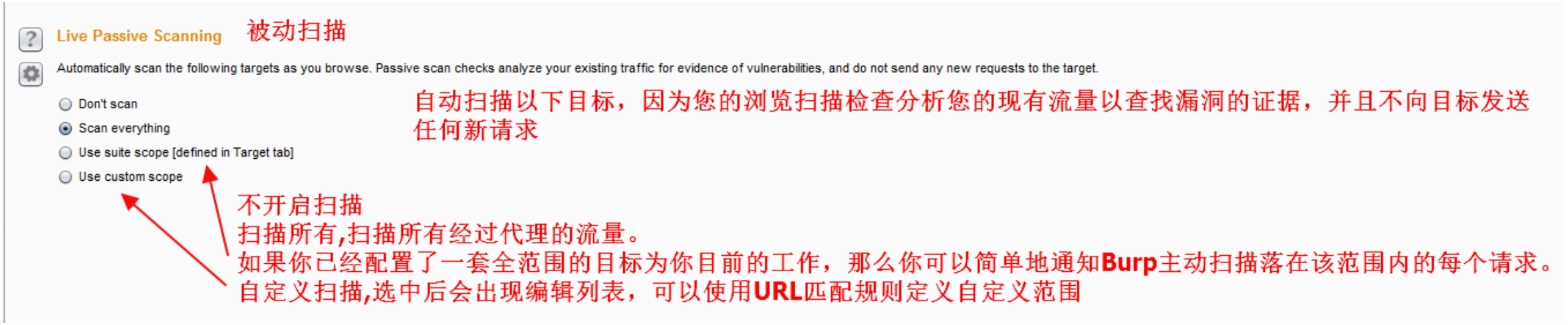


Live Active Scanning

➢Live Active Scanning：积极扫描

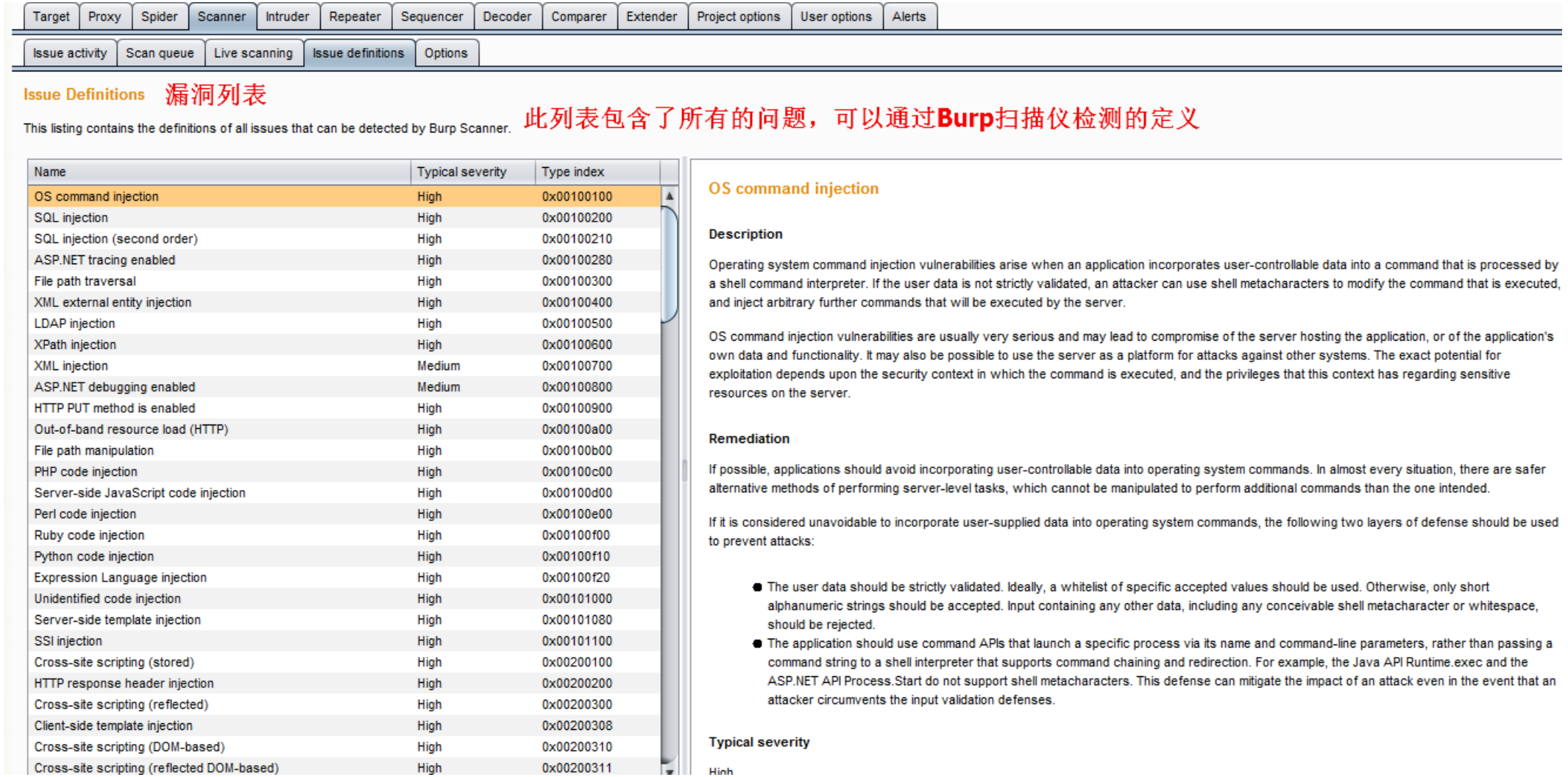
Live Passive Scanning

➢**Live Passive Scanning：被动扫描。只分析流量不发送任何请求**



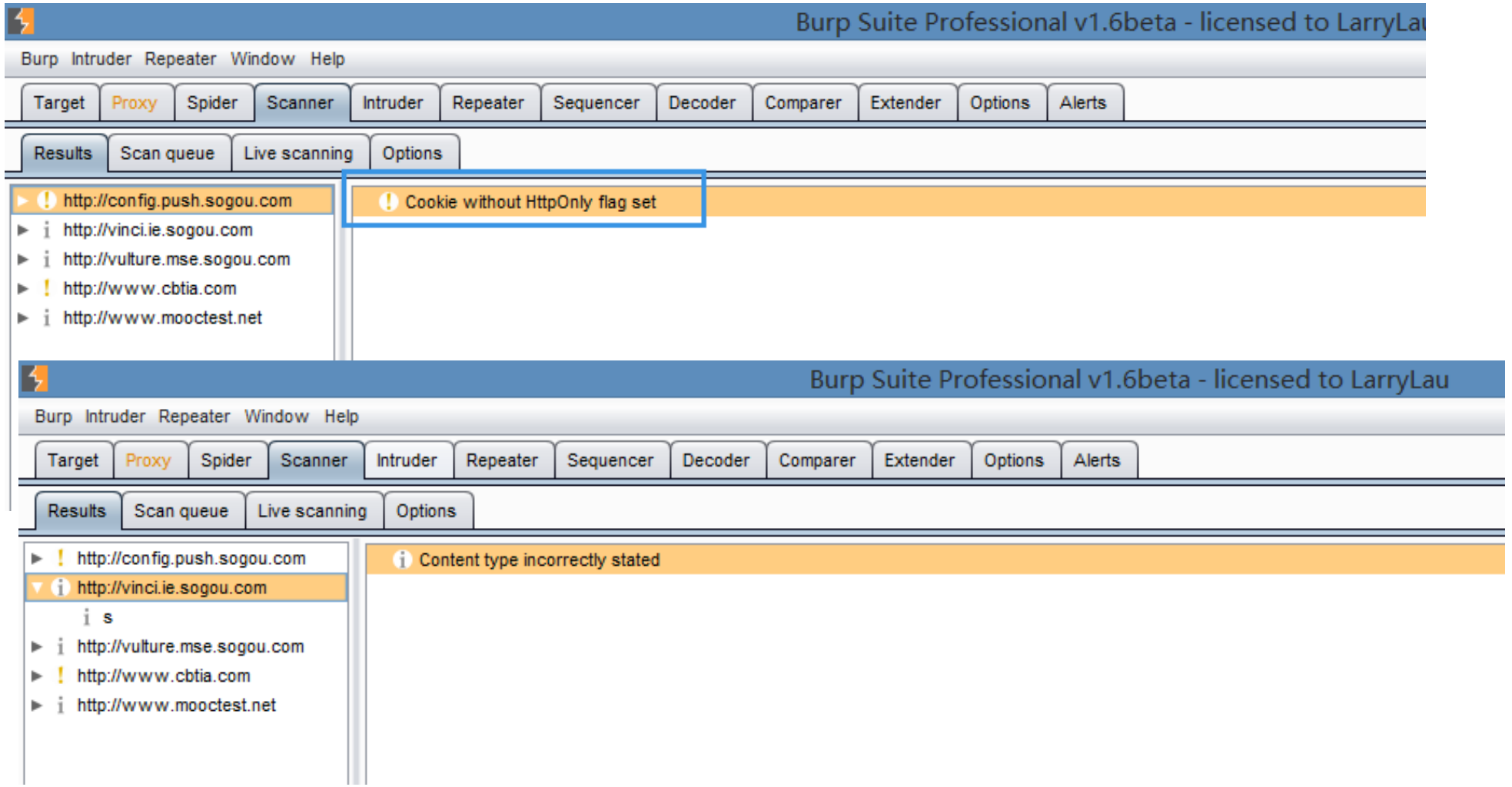
Issue Definitions

➢漏洞列表，列出了burp可以扫描到的漏洞详情

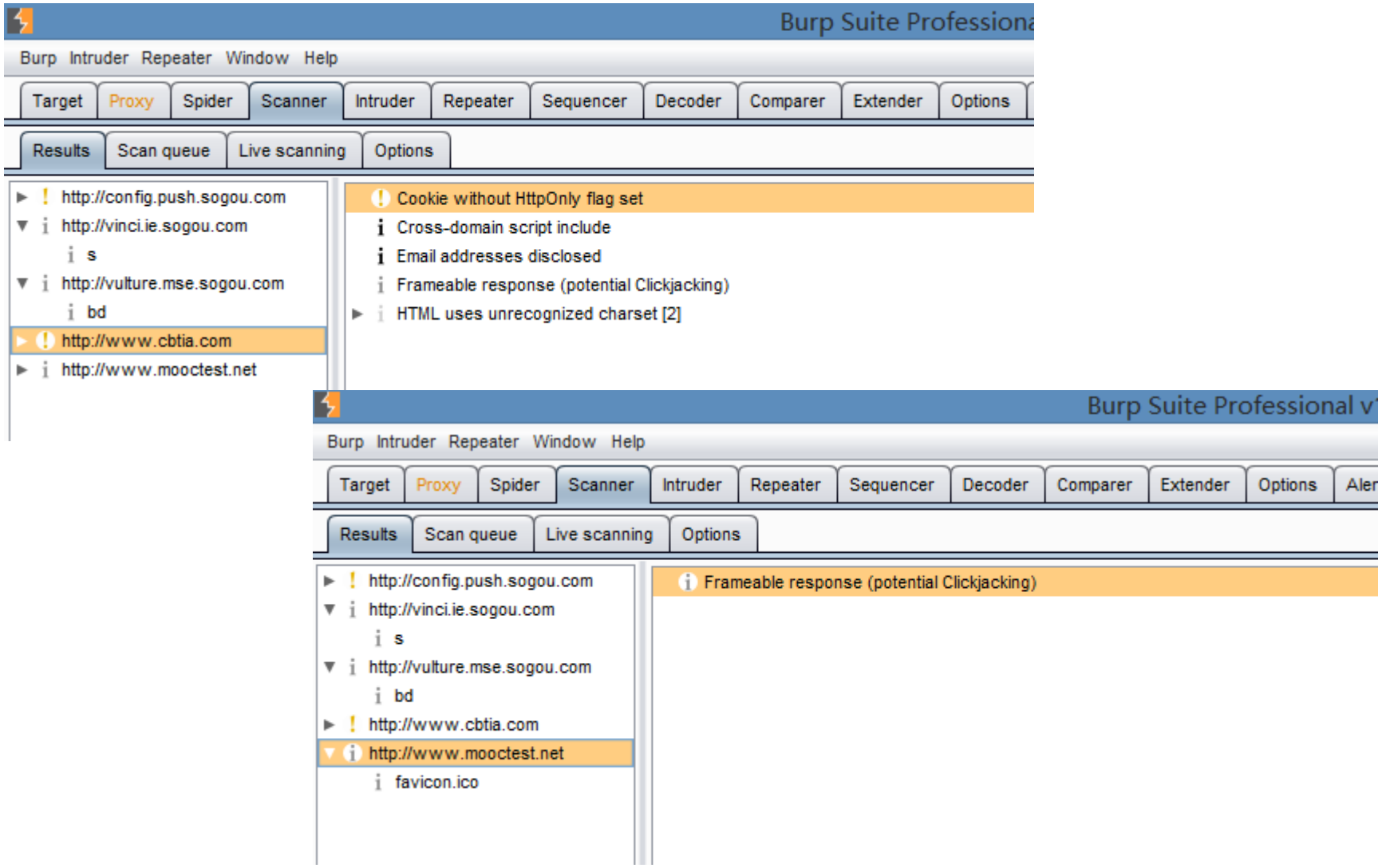


扫描后结果

➢**www.cbtia.com**



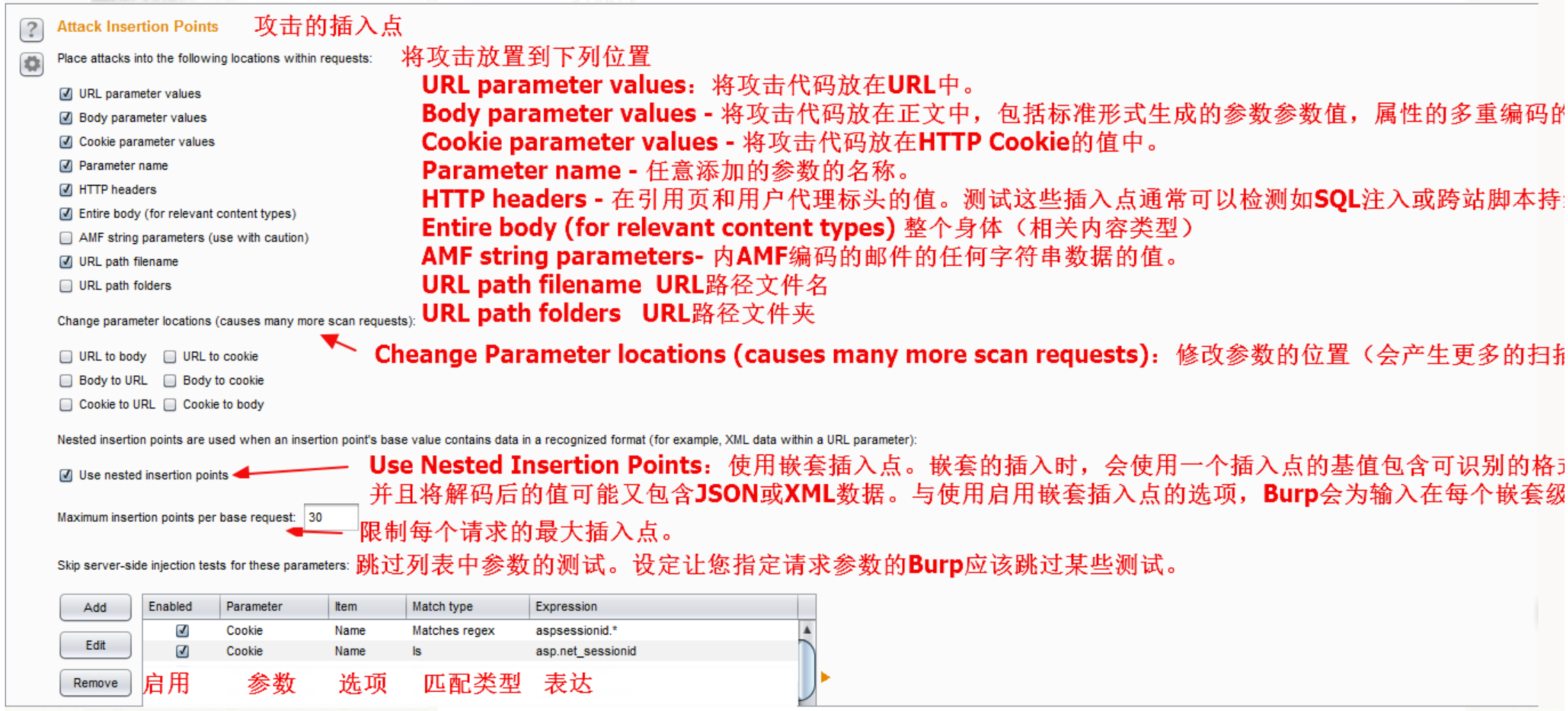
扫描后结果


Burp Suite Professiona
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options
Results Scan queue Live scanning Options
http://config.push.sogou.com
http://vinci.ie.sogou.com
s
http://vulture.mse.sogou.com
bd
http://www.cbtia.com
http://www.mooctest.net
Cookie without HttpOnly flag set
Cross-domain script include
Email addresses disclosed
Frameable response (potential Clickjacking)
HTML uses unrecognized charset [2]
Burp Suite Professional v
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options
Results Scan queue Live scanning Options
http://config.push.sogou.com
http://vinci.ie.sogou.com
s
http://vulture.mse.sogou.com
bd
http://www.cbtia.com
http://www.mooctest.net
favicon.ico
Frameable response (potential Clickjacking)

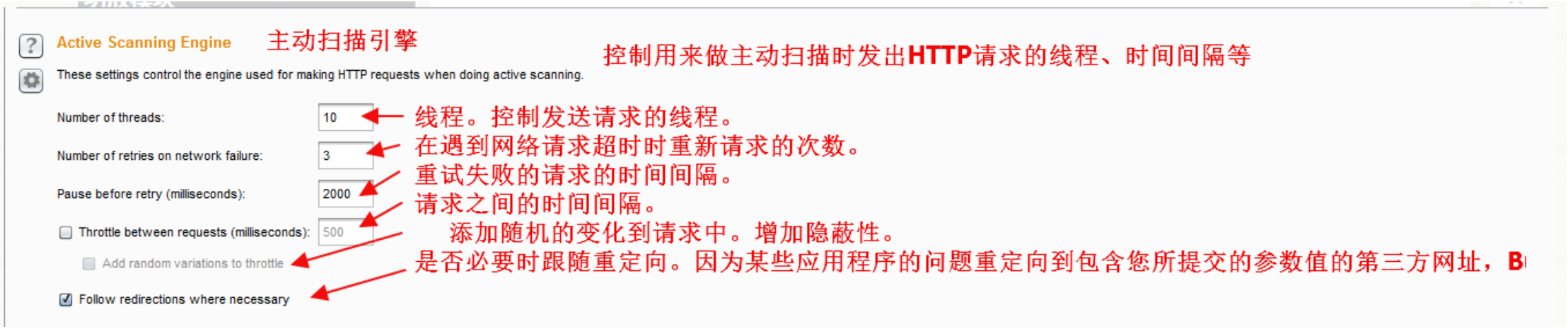
Options

- 包含Burp扫描选项进行攻击的插入点，主动扫描引擎，主动扫描优化，主动扫描区和被动扫描区域

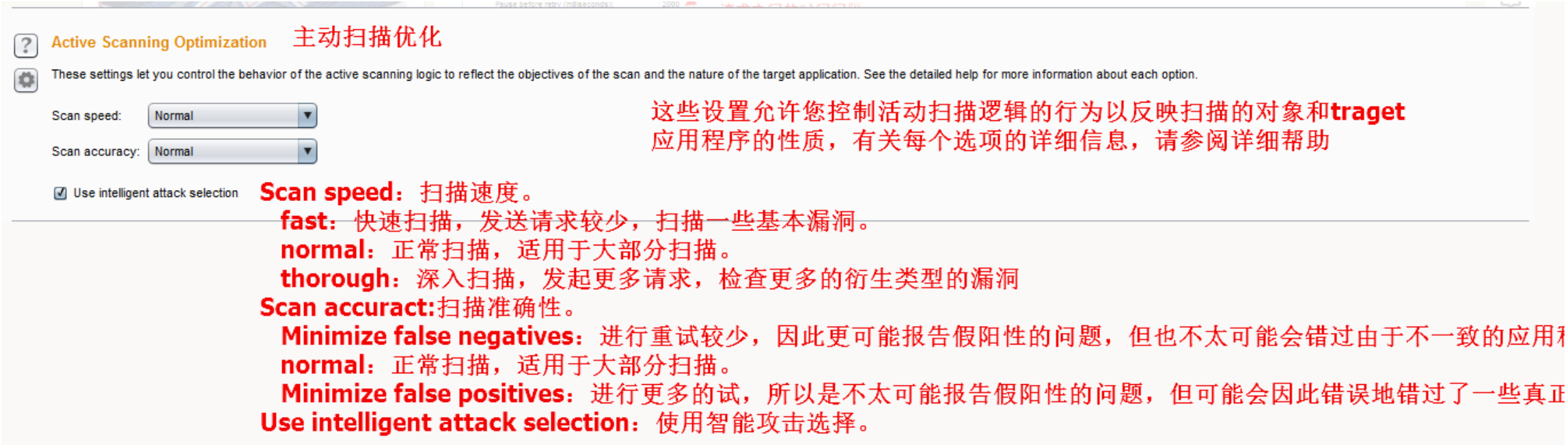
Option---Attack Insertion Points



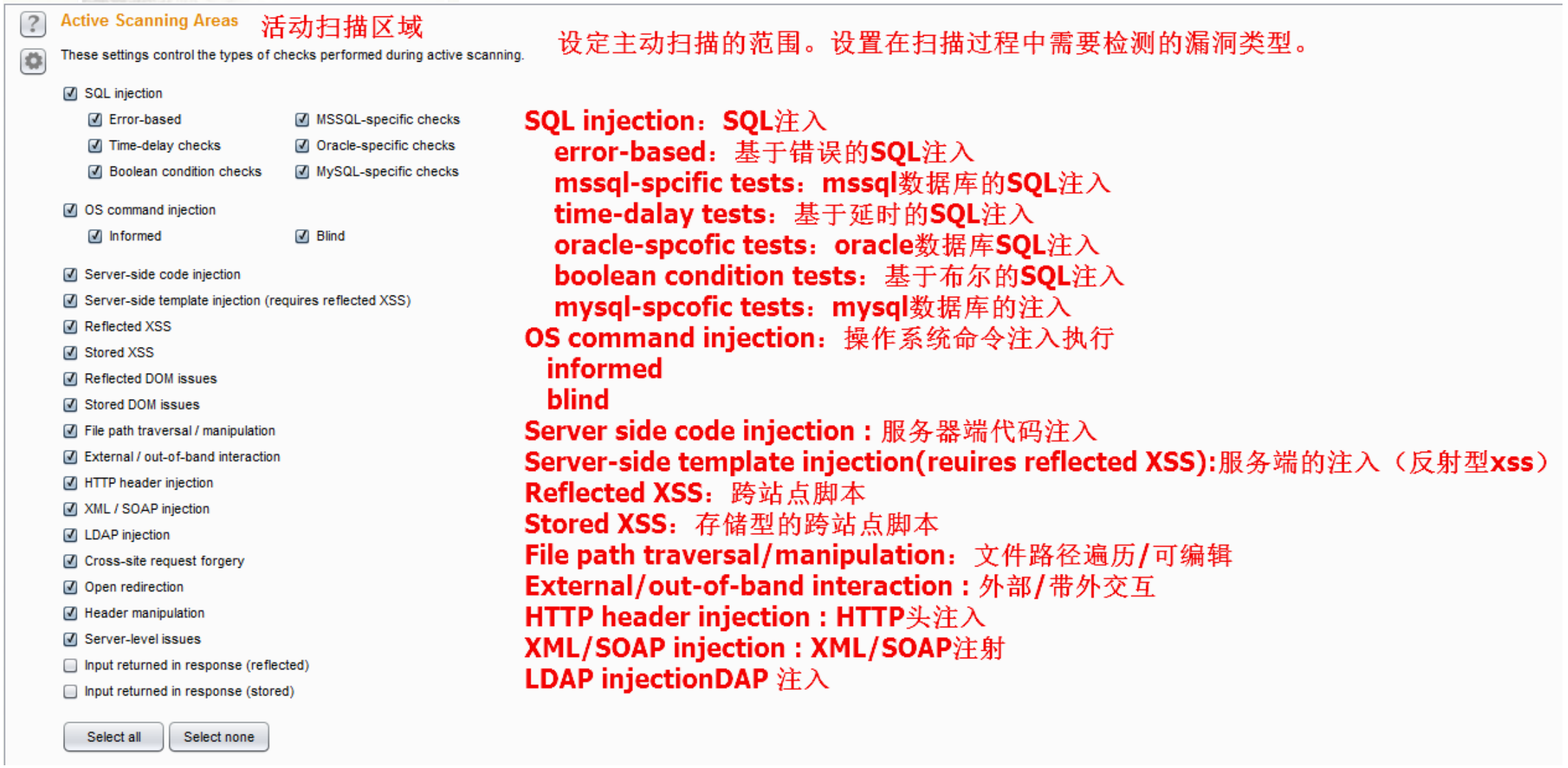
Option--- Active Scanning Engine



Option--Active Scanning Optimization



Option---Active Scanning Areas



设定主动扫描的范围。设置在扫描过程中需要检测的漏洞类型。

SQL injection：SQL注入
- **error-based：基于错误的SQL注入**
- **mssql-spcific tests：mssql数据库的SQL注入**
- **time-dalay tests：基于延时的SQL注入**
- **oracle-spcofic tests：oracle数据库SQL注入**
- **boolean condition tests：基于布尔的SQL注入**
- **mysql-spcofic tests：mysql数据库的注入**

OS command injection：操作系统命令注入执行
- **informed**
- **blind**

Server side code injection：服务器端代码注入

Server-side template injection(reuires reflected XSS):服务端的注入（反射型xss）

Reflected XSS：跨站点脚本

Stored XSS：存储型的跨站点脚本

File path traversal/manipulation：文件路径遍历/可编辑

External/out-of-band interaction：外部/带外交互

HTTP header injection：HTTP头注入

XML/SOAP injection：XML/SOAP注射

LDAP injectionDAP 注入

Option--Passive Scanning Areas

总结

- 什么是漏洞扫描
- 为什么进行漏洞扫描
- 怎样进行漏洞扫描

Question