

# Web 系统测试

## 3.4 Web安全测试——漏洞扫描

# 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

## ➤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

- HTTP请求流程
- 请求头、相应头
- 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

# 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

## ➤漏洞扫描可以使用的工具

- Burp Suit WVS AppScan

## ➤漏洞扫描步骤

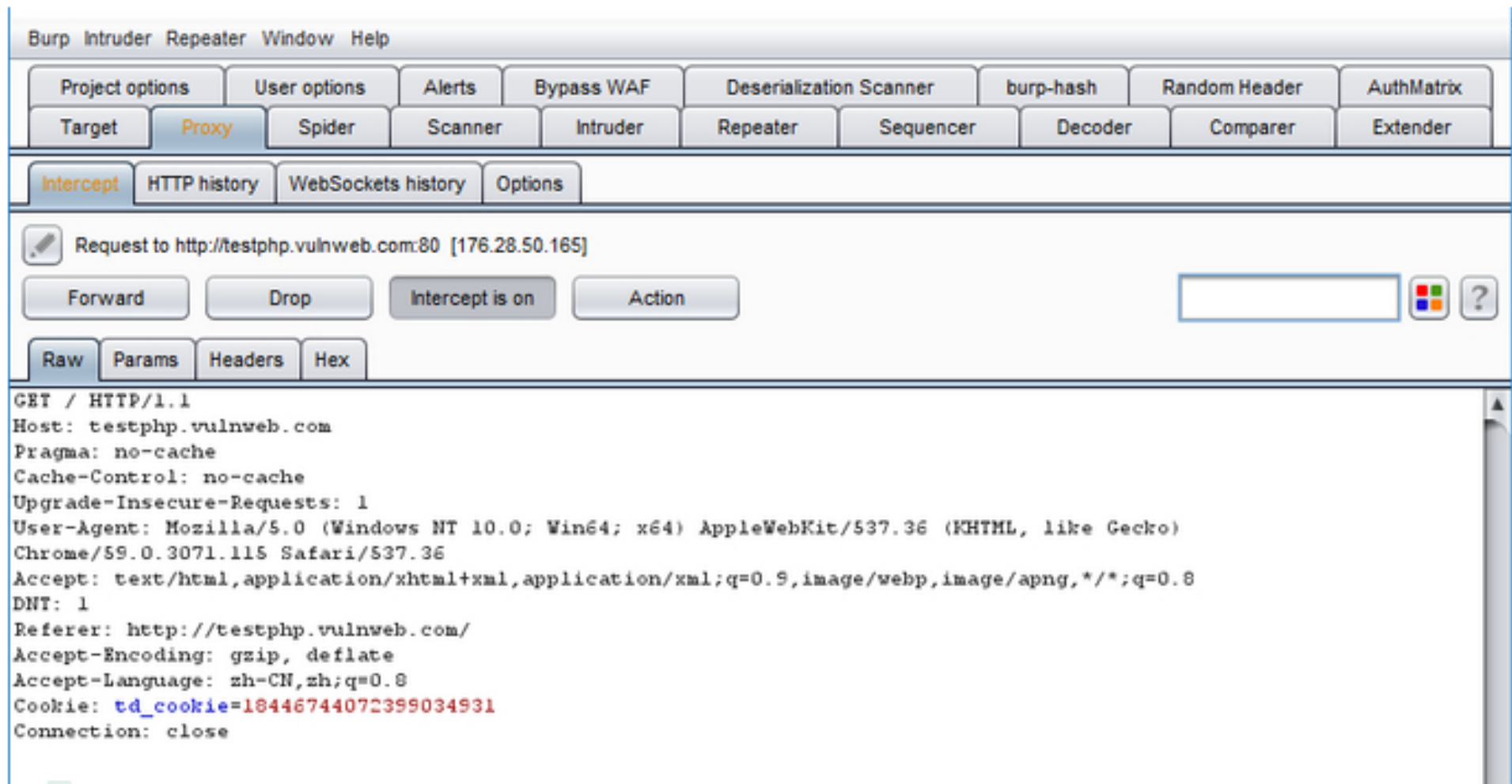
- 抓包功能开启

- 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 Suite Professional v1.7.11 - Temporary Project - licensed to Larry\_Lau

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	C
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.

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

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												
#	Host	URL	Status	Issues	Requests	Errors	Insertion points	Start time	End time	Comment		
ID	主机名	网址	状态	问题	请求	错误	插入点	开始时间	结束时间	注释		

# Live Active Scanning

## ➤Live Active Scanning: 积极扫描



The screenshot shows the 'Live scanning' tab in the Burp Suite interface. The top navigation bar includes tabs for Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, and Alerts. Below this, the 'Live scanning' tab is selected, showing options for 'Issue activity', 'Scan queue', 'Live scanning', 'Issue definitions', and 'Options'. The 'Live scanning' section is highlighted with a red arrow and the text '积极扫描' (Active Scanning). It contains a description: 'Automatically scan the following targets as you browse. Active scan checks send various malicious requests designed to identify common vulnerabilities. Use with caution.' Below the description are three radio button options: 'Don't scan' (selected), 'Use suite scope [defined in Target tab]', and 'Use custom scope'. Red annotations are present: '自动扫描以下目标，因为您的浏览活动扫描检查发送用于识别常见漏洞的各种恶意请求，谨慎使用' (Automatically scan the following targets, because your browsing activity scan checks send various malicious requests designed to identify common vulnerabilities, use with caution) next to the description; '不扫描' (Don't scan) next to the 'Don't scan' option; and '使用套件范围[在目标选项卡中定义]' (Use suite scope [defined in Target tab]) and '使用自定义范围' (Use custom scope) next to their respective options.

**Live Active Scanning** ← 积极扫描

Automatically scan the following targets as you browse. Active scan checks send various malicious requests designed to identify common vulnerabilities. Use with caution.

☒ Don't scan

☐ Use suite scope [defined in Target tab]

☐ Use custom scope

自动扫描以下目标，因为您的浏览活动扫描检查发送用于识别常见漏洞的各种恶意请求，谨慎使用

不扫描

使用套件范围[在目标选项卡中定义]

使用自定义范围

# Live Passive Scanning

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

## ? Live Passive Scanning 被动扫描

⚙ Automatically scan the following targets as you browse. Passive scan checks analyze your existing traffic for evidence of vulnerabilities, and do not send any new requests to the target.

- ☐ Don't scan
- ☒ Scan everything
- ☐ Use suite scope [defined in Target tab]
- ☐ Use custom scope

自动扫描以下目标，因为您的浏览扫描检查分析您的现有流量以查找漏洞的证据，并且不向目标发送任何新请求

不开启扫描

扫描所有,扫描所有经过代理的流量。

如果你已经配置了一套全范围的目标为你目前的工作，那么你可以简单地通知Burp主动扫描落在该范围内的每个请求。  
自定义扫描,选中后会出现编辑列表，可以使用URL匹配规则定义自定义范围

# Issue Definitions

## ➤漏洞列表，列出了burp可以扫描到的漏洞详情

TargetProxySpiderScannerIntruderRepeaterSequencerDecoderComparerExtenderProject optionsUser optionsAlerts

Issue activityScan queueLive scanningIssue definitionsOptions

Issue Definitions漏洞列表

This listing contains the definitions of all issues that can be detected by Burp Scanner. 此列表包含了所有的问题，可以通过Burp扫描仪检测的定义

Name	Typical severity	Type index
OS command injection	High	0x00100100
SQL injection	High	0x00100200
SQL injection (second order)	High	0x00100210
ASP.NET tracing enabled	High	0x00100280
File path traversal	High	0x00100300
XML external entity injection	High	0x00100400
LDAP injection	High	0x00100500
XPath injection	High	0x00100600
XML injection	Medium	0x00100700
ASP.NET debugging enabled	Medium	0x00100800
HTTP PUT method is enabled	High	0x00100900
Out-of-band resource load (HTTP)	High	0x00100a00
File path manipulation	High	0x00100b00
PHP code injection	High	0x00100c00
Server-side JavaScript code injection	High	0x00100d00
Perl code injection	High	0x00100e00
Ruby code injection	High	0x00100f00
Python code injection	High	0x00100f10
Expression Language injection	High	0x00100f20
Unidentified code injection	High	0x00101000
Server-side template injection	High	0x00101080
SSI injection	High	0x00101100
Cross-site scripting (stored)	High	0x00200100
HTTP response header injection	High	0x00200200
Cross-site scripting (reflected)	High	0x00200300
Client-side template injection	High	0x00200308
Cross-site scripting (DOM-based)	High	0x00200310
Cross-site scripting (reflected DOM-based)	High	0x00200311

OS command injection

Description

Operating system command injection vulnerabilities arise when an application incorporates user-controllable data into a command that is processed by a shell command interpreter. If the user data is not strictly validated, an attacker can use shell metacharacters to modify the command that is executed, and inject arbitrary further commands that will be executed by the server.

OS command injection vulnerabilities are usually very serious and may lead to compromise of the server hosting the application, or of the application's own data and functionality. It may also be possible to use the server as a platform for attacks against other systems. The exact potential for exploitation depends upon the security context in which the command is executed, and the privileges that this context has regarding sensitive resources on the server.

Remediation

If possible, applications should avoid incorporating user-controllable data into operating system commands. In almost every situation, there are safer alternative methods of performing server-level tasks, which cannot be manipulated to perform additional commands than the one intended.

If it is considered unavoidable to incorporate user-supplied data into operating system commands, the following two layers of defense should be used to prevent attacks:

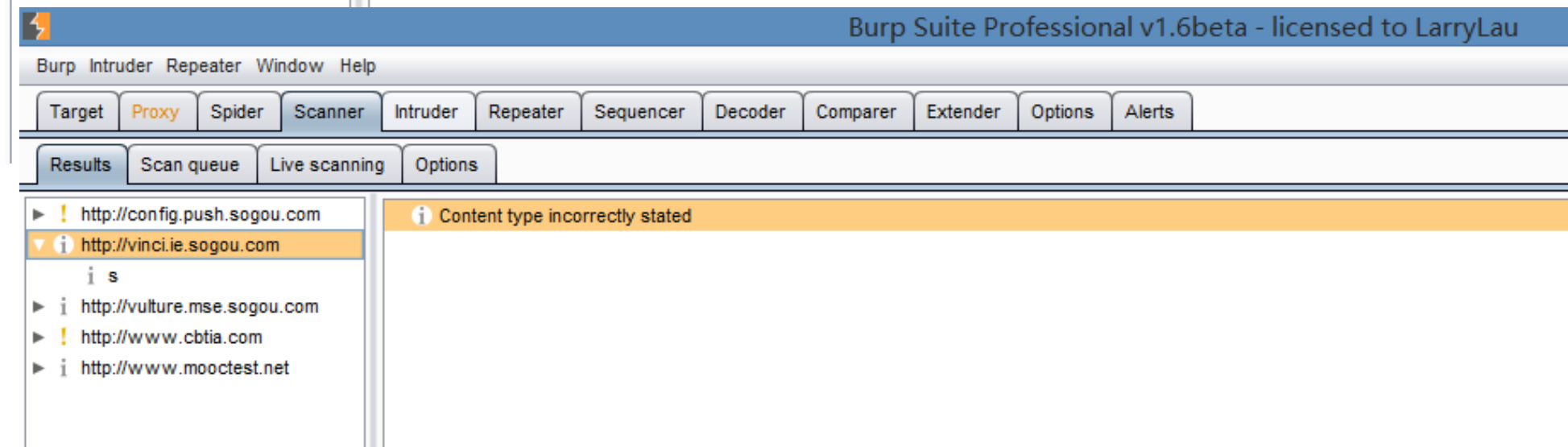
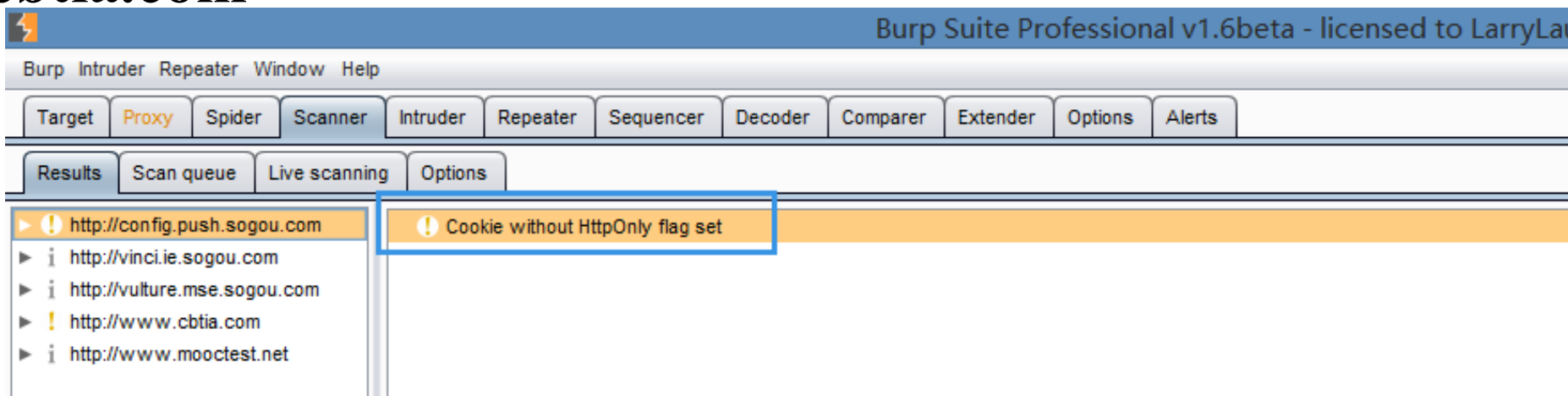
- The user data should be strictly validated. Ideally, a whitelist of specific accepted values should be used. Otherwise, only short alphanumeric strings should be accepted. Input containing any other data, including any conceivable shell metacharacter or whitespace, should be rejected.
- The application should use command APIs that launch a specific process via its name and command-line parameters, rather than passing a command string to a shell interpreter that supports command chaining and redirection. For example, the Java API Runtime.exec and the ASP.NET API Process.Start do not support shell metacharacters. This defense can mitigate the impact of an attack even in the event that an attacker circumvents the input validation defenses.

Typical severity

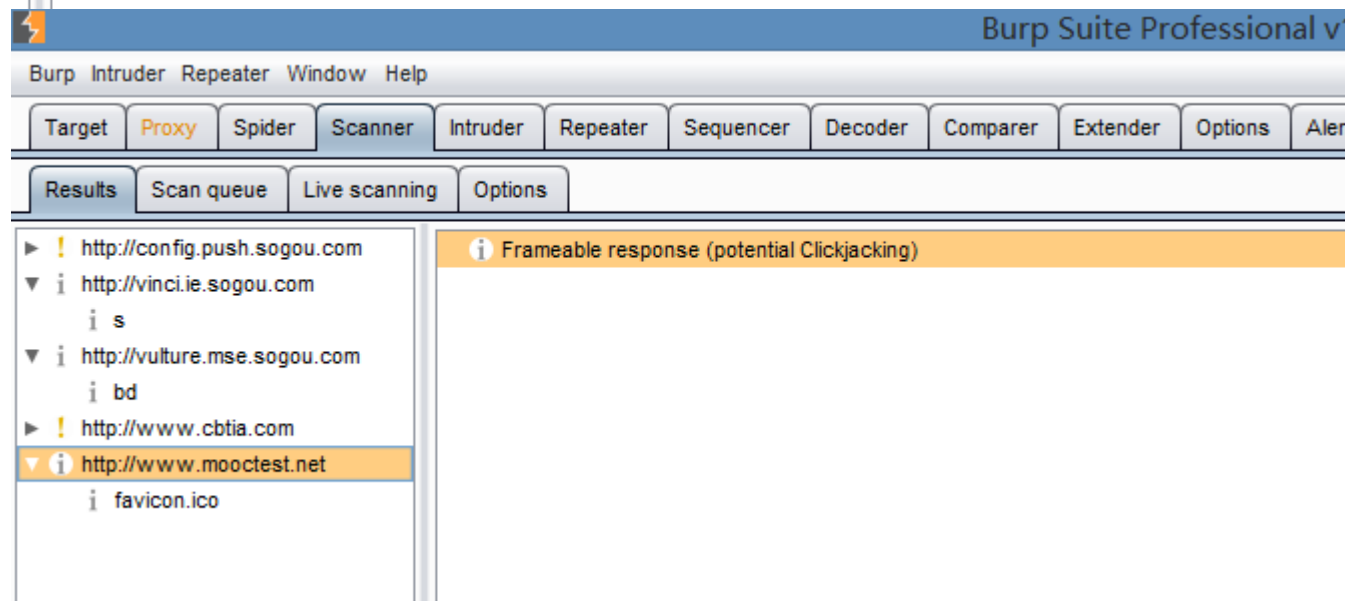
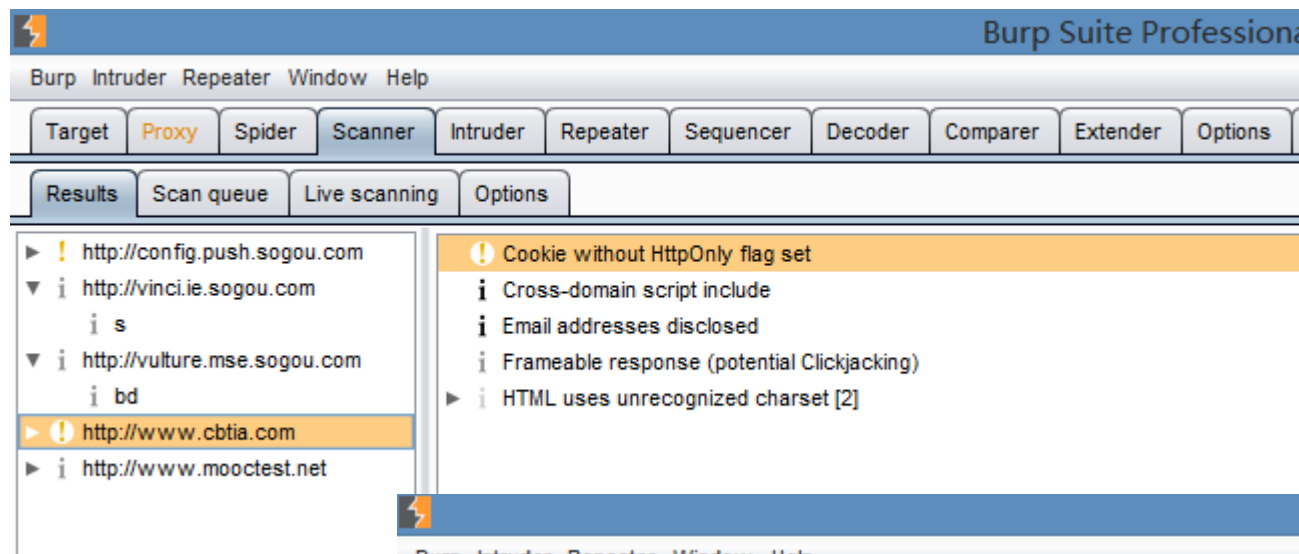
High

# 扫描后结果

➤ [www.cbtia.com](http://www.cbtia.com)



# 扫描后结果



- 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

?

Attack Insertion Points

攻击的插入点

⚙️

Place attacks into the following locations within requests:

将攻击放置到下列位置

☒ URL parameter values

☒ Body parameter values

☒ Cookie parameter values

☒ Parameter name

☒ HTTP headers

☒ Entire body (for relevant content types)

☐ AMF string parameters (use with caution)

☒ URL path filename

☐ URL path folders

URL parameter values: 将攻击代码放在URL中。

Body parameter values - 将攻击代码放在正文中，包括标准形式生成的参数参数值，属性的多重编码的

Cookie parameter values - 将攻击代码放在HTTP Cookie的值中。

Parameter name - 任意添加的参数名称。

HTTP headers - 在引用页和用户代理标头的值。测试这些插入点通常可以检测如SQL注入或跨站脚本持

Entire body (for relevant content types) 整个身体（相关内容类型）

AMF string parameters- 内AMF编码的邮件的任何字符串数据的值。

URL path filename URL路径文件名

URL path folders URL路径文件夹

Change parameter locations (causes many more scan requests):

☐ URL to body

☐ URL to cookie

☐ Body to URL

☐ Body to cookie

☐ Cookie to URL

☐ Cookie to body

Change Parameter locations (causes many more scan requests): 修改参数的位置（会产生更多的扫描请求）

Nested insertion points are used when an insertion point's base value contains data in a recognized format (for example, XML data within a URL parameter):

☒ Use nested insertion points

Use Nested Insertion Points: 使用嵌套插入点。嵌套的插入时，会使用一个插入点的基值包含可识别的格式并且将解码后的值可能又包含JSON或XML数据。与使用启用嵌套插入点的选项，Burp会为输入在每个嵌套级

Maximum insertion points per base request: 30

限制每个请求的最大插入点。

Skip server-side injection tests for these parameters:

跳过列表中参数的测试。设定让您指定请求参数的Burp应该跳过某些测试。

Add

Edit

Remove

Enabled	Parameter	Item	Match type	Expression
<input checked="" type="checkbox"/>	Cookie	Name	Matches regex	aspsessionid.*
<input checked="" type="checkbox"/>	Cookie	Name	Is	asp.net_sessionid

启用 参数 选项 匹配类型 表达

# Option--- Active Scanning Engine

**Active Scanning Engine 主动扫描引擎** 控制用来做主动扫描时发出**HTTP**请求的线程、时间间隔等

These settings control the engine used for making HTTP requests when doing active scanning.

Number of threads:  线程。控制发送请求的线程。

Number of retries on network failure:  在遇到网络请求超时时重新请求的次数。

Pause before retry (milliseconds):  重试失败的请求的时间间隔。

☐ Throttle between requests (milliseconds):  请求之间的时间间隔。

☐ Add random variations to throttle 添加随机的变化到请求中。增加隐蔽性。

☒ Follow redirections where necessary 是否必要时跟随重定向。因为某些应用程序的问题重定向到包含您所提交的参数值的第三方网址，B

# Option--Active Scanning Optimization



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

?

Active Scanning Optimization 主动扫描优化

⚙️

These settings let you control the behavior of the active scanning logic to reflect the objectives of the scan and the nature of the target application. See the detailed help for more information about each option.

Scan speed:

Normal

Scan accuracy:

Normal

☒ Use intelligent attack selection

**Scan speed:** 扫描速度。

**fast:** 快速扫描，发送请求较少，扫描一些基本漏洞。

**normal:** 正常扫描，适用于大部分扫描。

**thorough:** 深入扫描，发起更多请求，检查更多的衍生类型的漏洞

**Scan accuract:**扫描准确性。

**Minimize false negatives:** 进行重试较少，因此更可能报告假阳性的问题，但也不太可能会错过由于不一致的应用和

**normal:** 正常扫描，适用于大部分扫描。

**Minimize false positives:** 进行更多的试，所以是不太可能报告假阳性的问题，但可能会因此错误地错过了一些真正

**Use intelligent attack selection:** 使用智能攻击选择。

# Option---Active Scanning Areas



## ? Active Scanning Areas 活动扫描区域

These settings control the types of checks performed during active scanning.

- ☒ SQL injection
  - ☒ Error-based
  - ☒ Time-delay checks
  - ☒ Boolean condition checks
  - ☒ MSSQL-specific checks
  - ☒ Oracle-specific checks
  - ☒ MySQL-specific checks
- ☒ OS command injection
  - ☒ Informed
  - ☒ Blind
- ☒ Server-side code injection
- ☒ Server-side template injection (requires reflected XSS)
- ☒ Reflected XSS
- ☒ Stored XSS
- ☒ Reflected DOM issues
- ☒ Stored DOM issues
- ☒ File path traversal / manipulation
- ☒ External / out-of-band interaction
- ☒ HTTP header injection
- ☒ XML / SOAP injection
- ☒ LDAP injection
- ☒ Cross-site request forgery
- ☒ Open redirection
- ☒ Header manipulation
- ☒ Server-level issues
- ☐ Input returned in response (reflected)
- ☐ Input returned in response (stored)

Select all

Select none

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-spcofic 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



?

Passive Scanning Areas

被动扫描区

这些设置控制被动扫描期间执行的检查类型

⚙️

These settings control the types of checks performed during passive scanning.

☒ Headers

☒ Forms

☒ Links

☒ Parameters

☒ Cookies

☒ Server-level issues

☒ MIME type

☒ Caching

☒ Information disclosure

☒ Frameable responses ("Clickjacking")

☒ ASP.NET ViewState

Select all

Select none

Headers:头

Forms:表格

Links:链接

Parameters:参数

Cookies:Cookie

Server-level issues:服务端漏洞

MIME type: MIME类型（多用途互联网邮件扩展类型）

Caching:缓存

Information disclosure:信息泄漏

Frameable responses:耐燃反应（“点击劫持”）

ASP.NET ViewState:ASP.NET视图

- 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