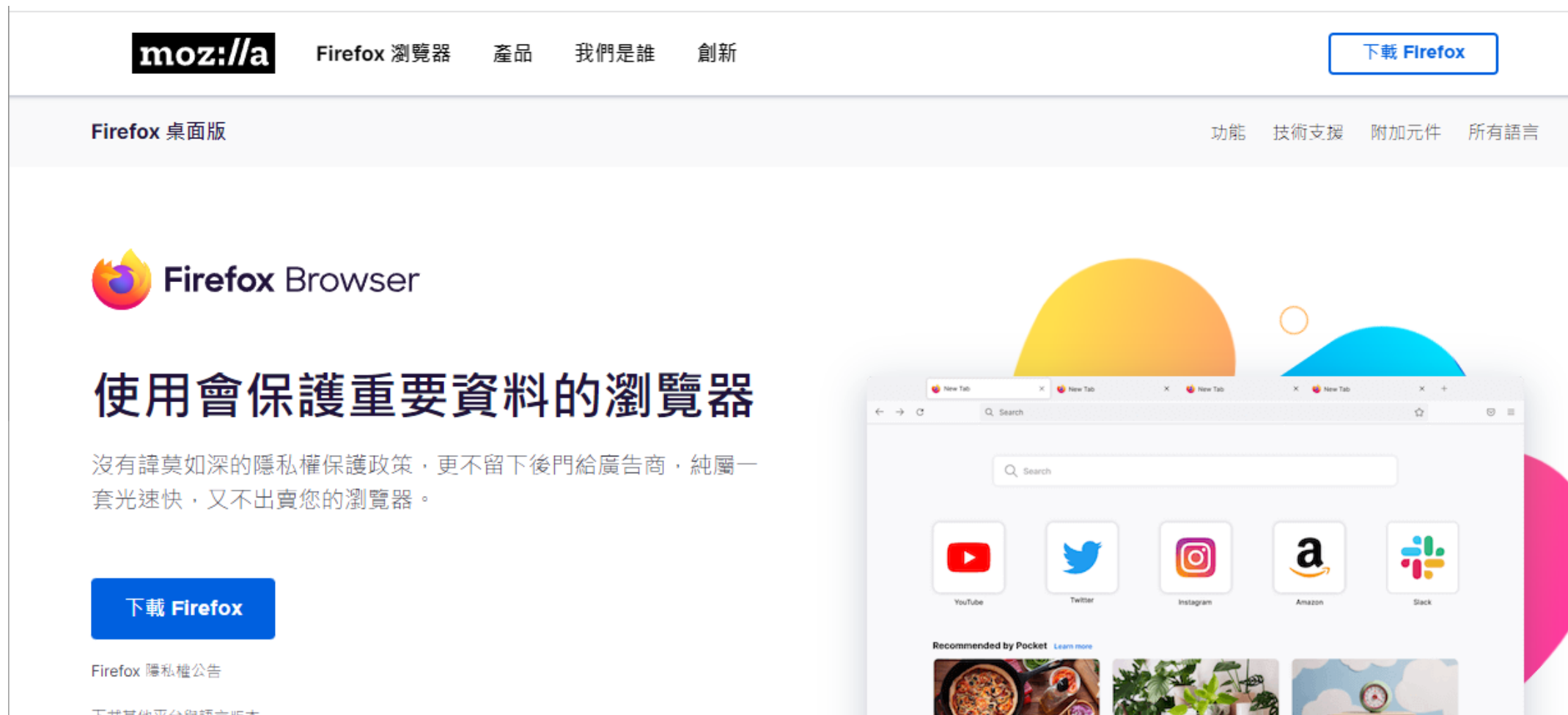


弱點掃描與滲透測試

2022/10/31

下載Firefox瀏覽器

- <https://www.mozilla.org/zh-TW/firefox/new/>



下載- Java

- <https://www.oracle.com/tw/java/technologies/downloads/#java8>

Java 19

Java 17

Java SE Development Kit 19.0.1 downloads

Thank you for downloading this release of the Java™ Platform, Standard Edition Development Kit (JDK™). The JDK is a development environment for building applications and components using the Java programming language.

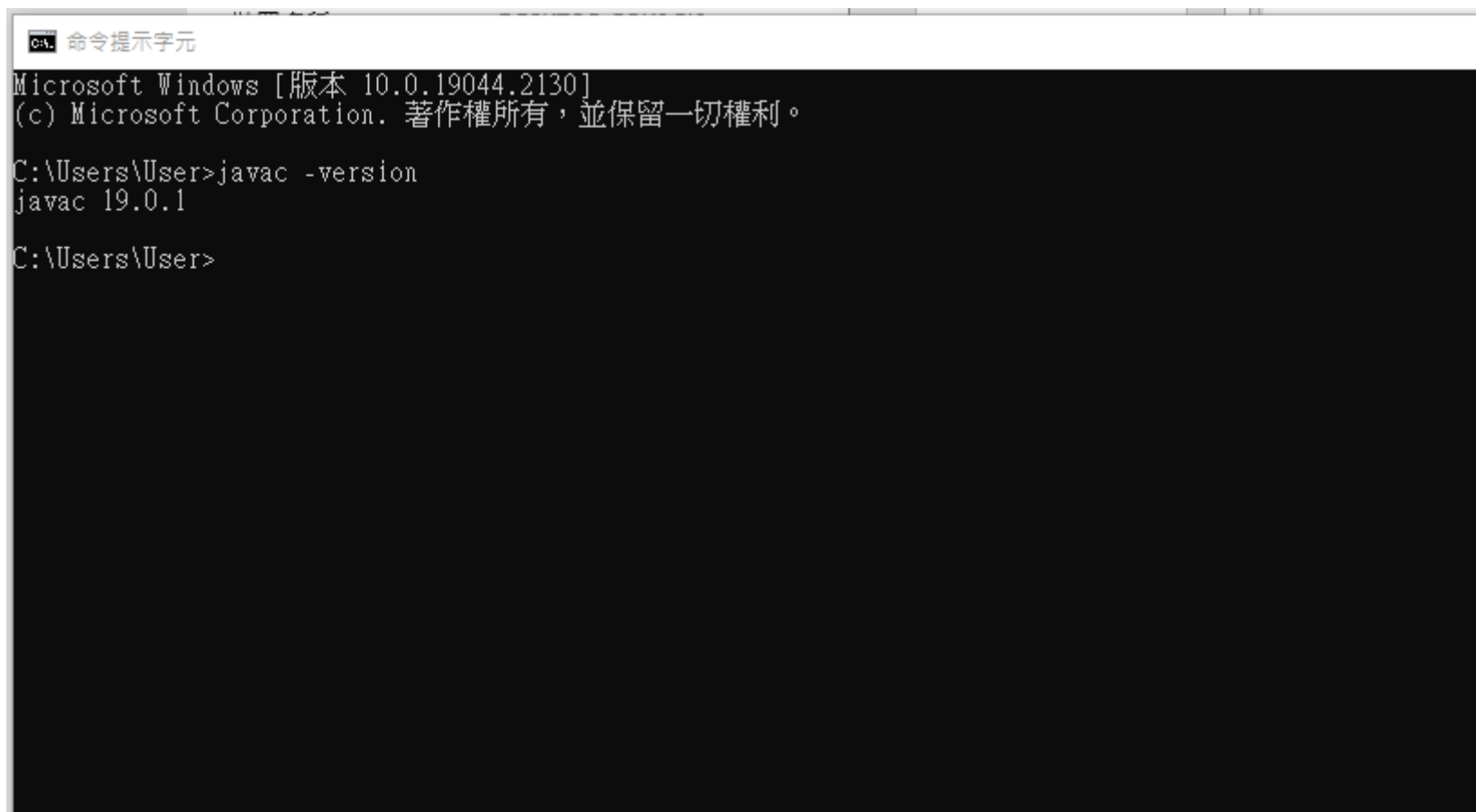
The JDK includes tools for developing and testing programs written in the Java programming language and running on the Java platform.

Linux macOS **Windows**

Product/file description	File size	Download
x64 Compressed Archive	179.13 MB	https://download.oracle.com/java/19/latest/jdk-19_windows-x64_bin.zip (sha256)
x64 Installer	158.91 MB	https://download.oracle.com/java/19/latest/jdk-19_windows-x64_bin.exe (sha256)
x64 MSI Installer	157.76 MB	https://download.oracle.com/java/19/latest/jdk-19_windows-x64_bin.msi (sha256)

檢查java版本

`javac -version`

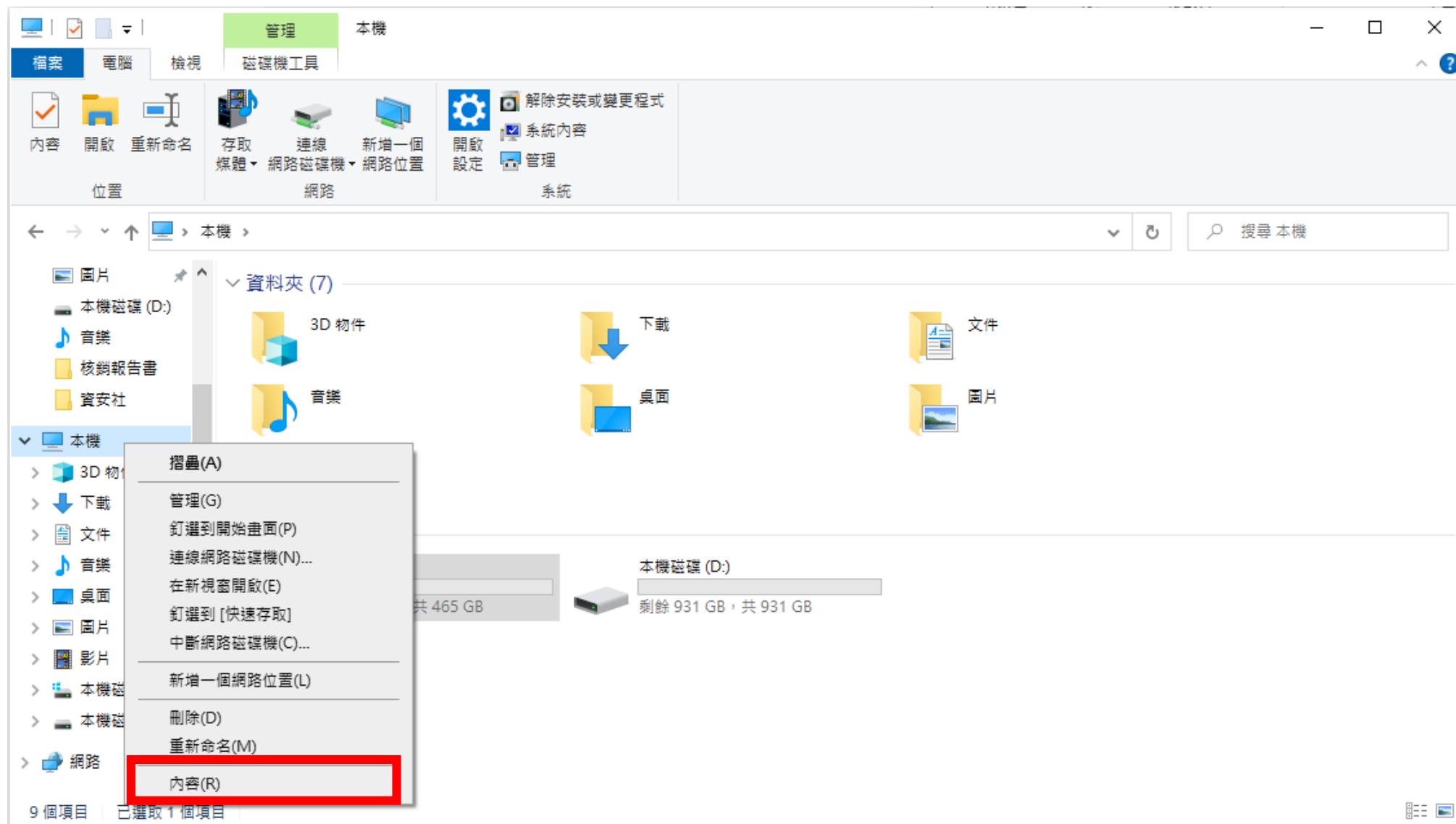


```
命令提示字元
Microsoft Windows [版本 10.0.19044.2130]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。

C:\Users\User>javac -version
javac 19.0.1

C:\Users\User>
```

設定環境變數



設定環境變數-選取進階系統設定

The screenshot shows the Windows Settings application. On the left is a navigation pane with categories like 'System', 'Display', 'Sound', etc. The main area is titled '關於' (About) and contains system information. A red rectangle highlights the '進階系統設定' (Advanced system settings) link in the right-hand '相關設定' (Related settings) section.

設定

首頁

尋找設定

系統

顯示器

音效

通知與動作

專注輔助

電源與睡眠

儲存體

平板

多工

投影到此電腦

關於

系統正在監控並保護您的電腦。

[參閱 Windows 安全性中的詳細資訊](#)

裝置規格

裝置名稱	DESKTOP-RBK9GI9
處理器	12th Gen Intel(R) Core(TM) i5-12400F 2.50 GHz
已安裝記憶體(RAM)	16.0 GB (15.9 GB 可用)
裝置識別碼	0FE24F14-4E6E-40E9-86D4-93F06091C8D2
產品識別碼	00326-00895-54571-AAOEM
系統類型	64 位元作業系統, x64 型處理器
手寫筆與觸控	此顯示器不提供手寫筆或觸控式輸入功能

複製

重新命名此電腦

Windows 規格

版本	Windows 10 家用版
版本	21H2

相關設定

- [BitLocker 設定](#)
- [裝置管理員](#)
- [遠端桌面](#)
- [系統保護](#)
- [進階系統設定](#)**
- [重新命名此電腦 \(進階\)](#)

取得協助

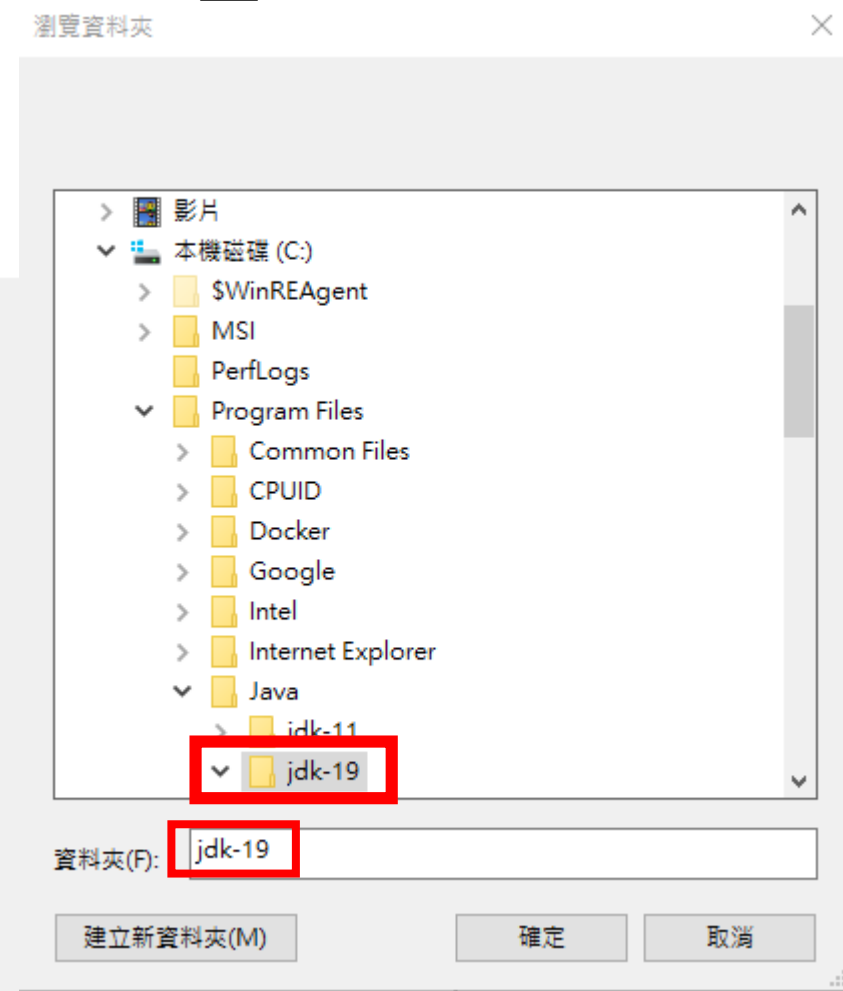
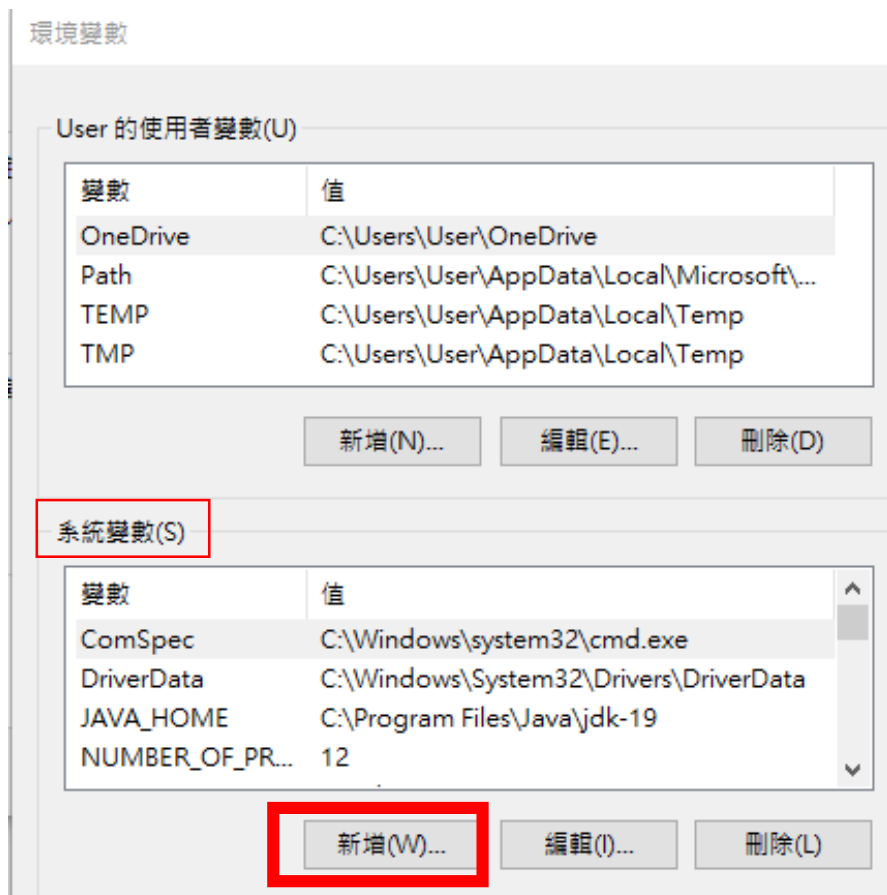
提供意見反應

設定環境變數-找到環境變數

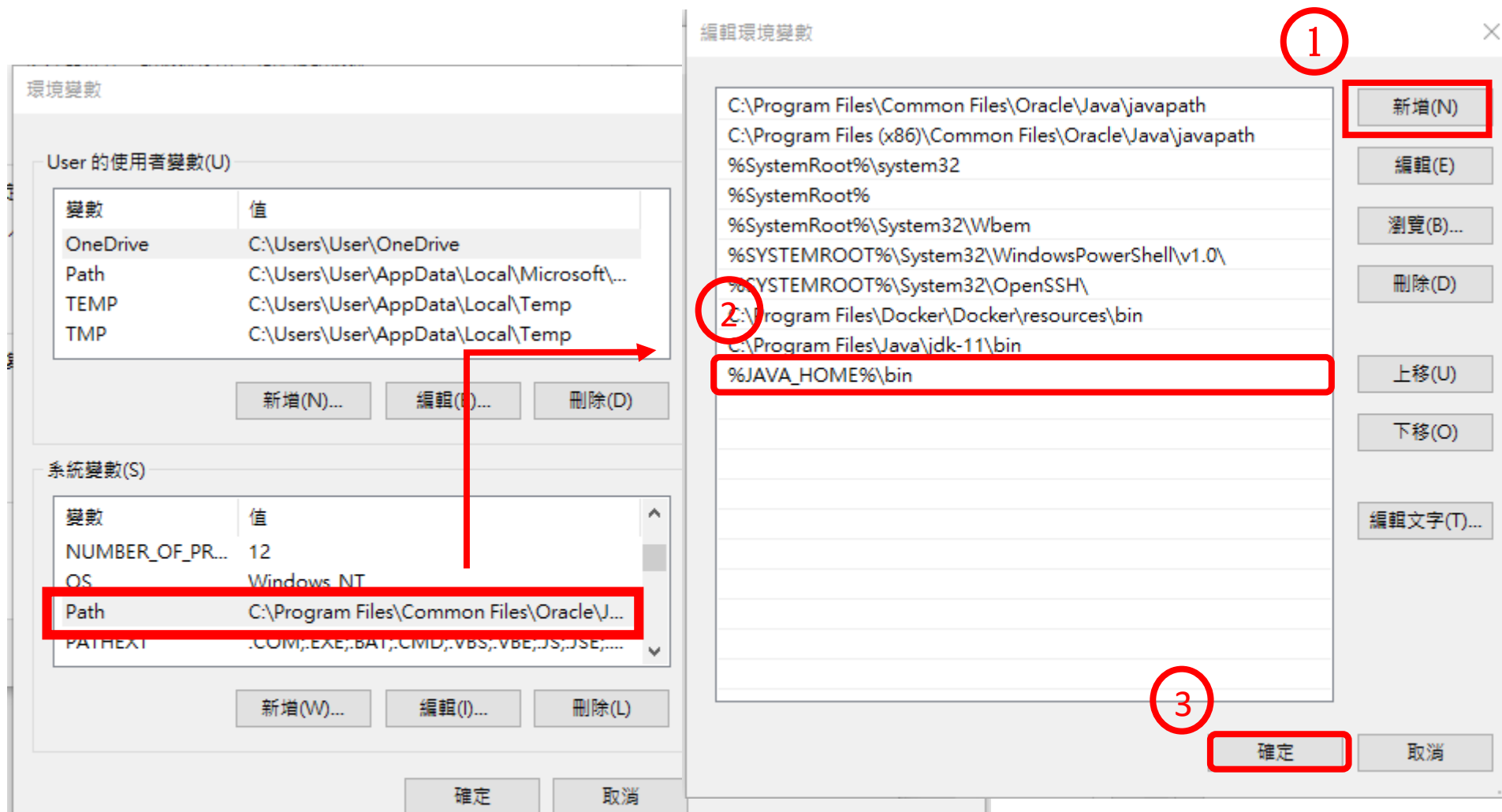


設定環境變數-系統變數增加JAVA_HOME

添加：JAVA_HOME

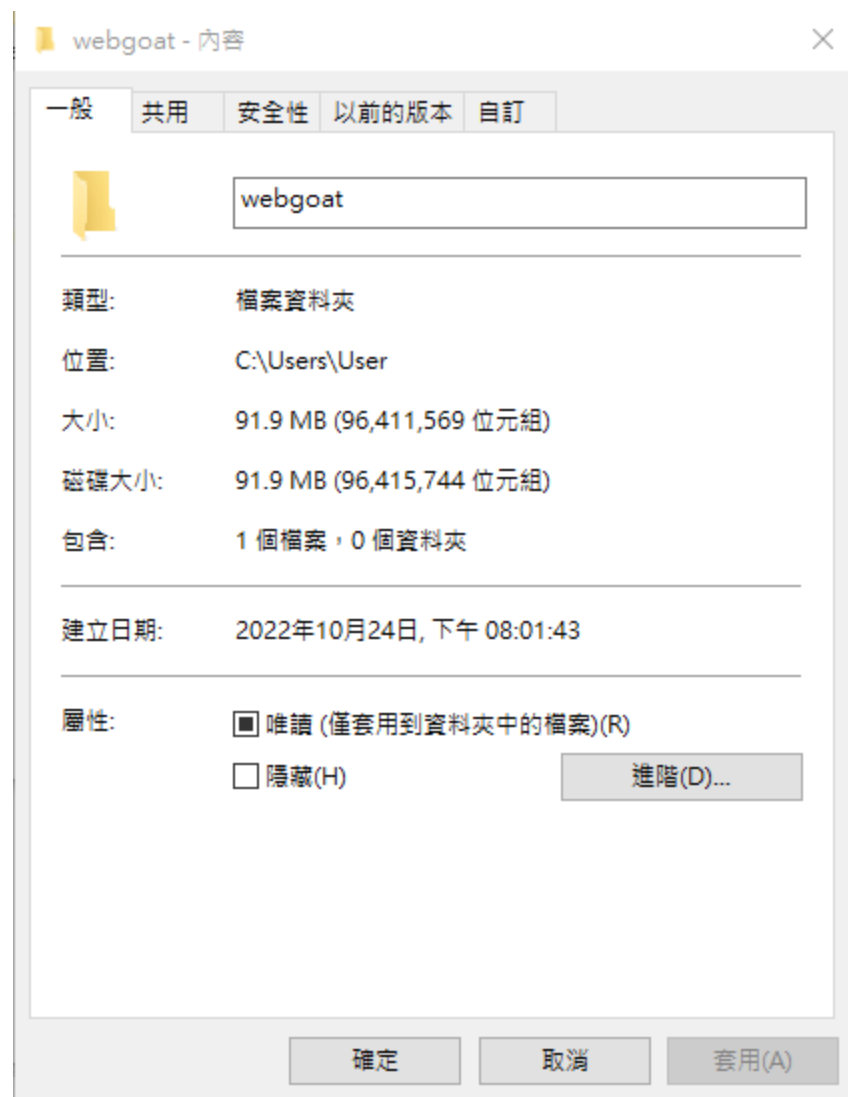


設定環境變數-系統變數Path增加bin



太好了，終於處理完java了
再來處理webgoat

在User/User底下創一個資料夾-webgoat



下載-WebGoat

- <https://github.com/WebGoat/WebGoat/releases>

v8.2.2

Latest

Version 8.2.2





New functionality

- Docker image now supports nginx when browsing to <http://localhost> a landing page is shown.

Bug fixes

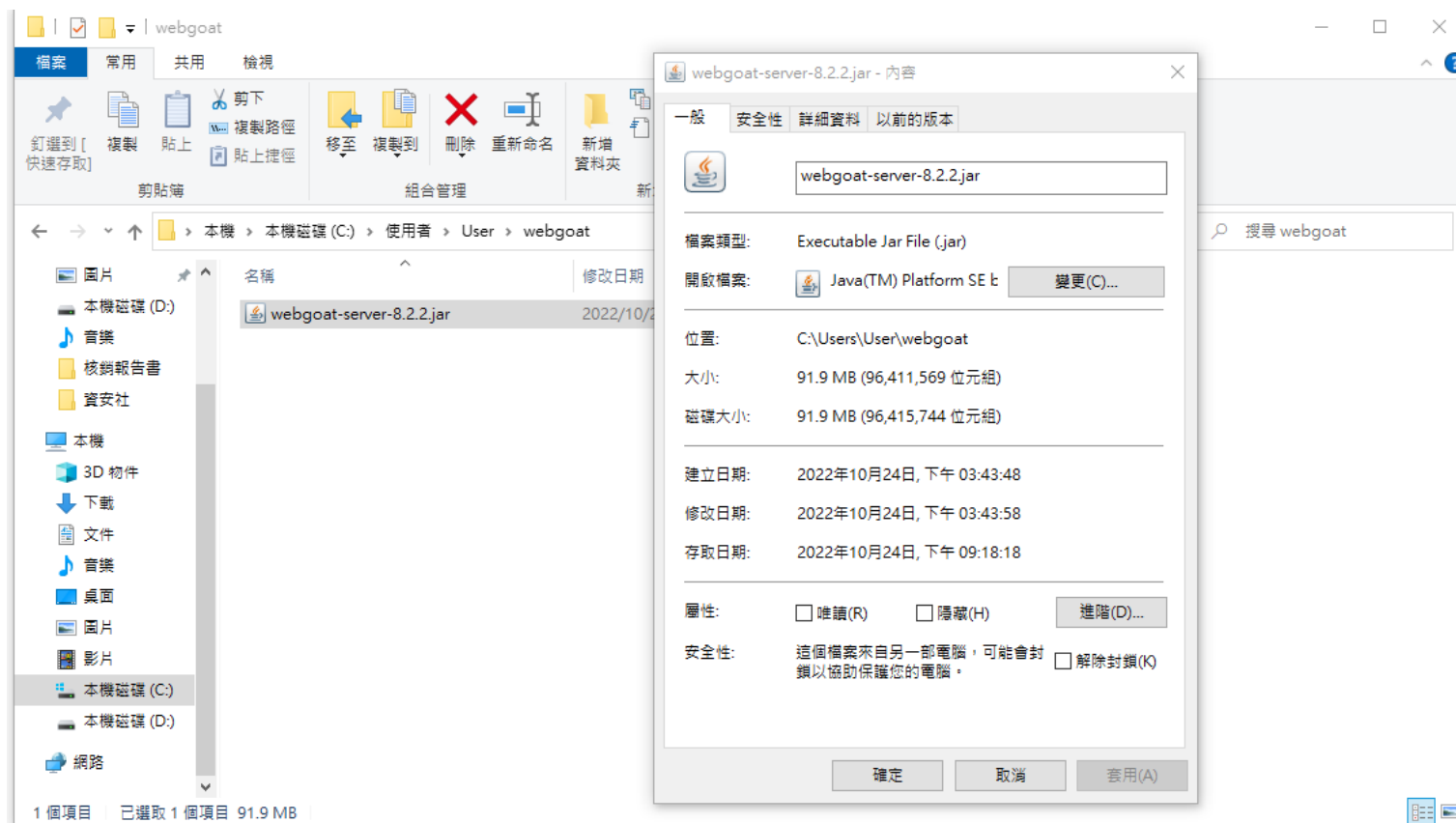
- [#1039 jwt-7-Code review](#)
- [#1031 SQL Injection \(intro\) 5: Data Control Language \(DCL\) the wiki's solution is not correct](#)
- [#1027 Webgoat 8.2.1 Vulnerable_Components_12 Shows internal server error](#)

▼ Assets 4

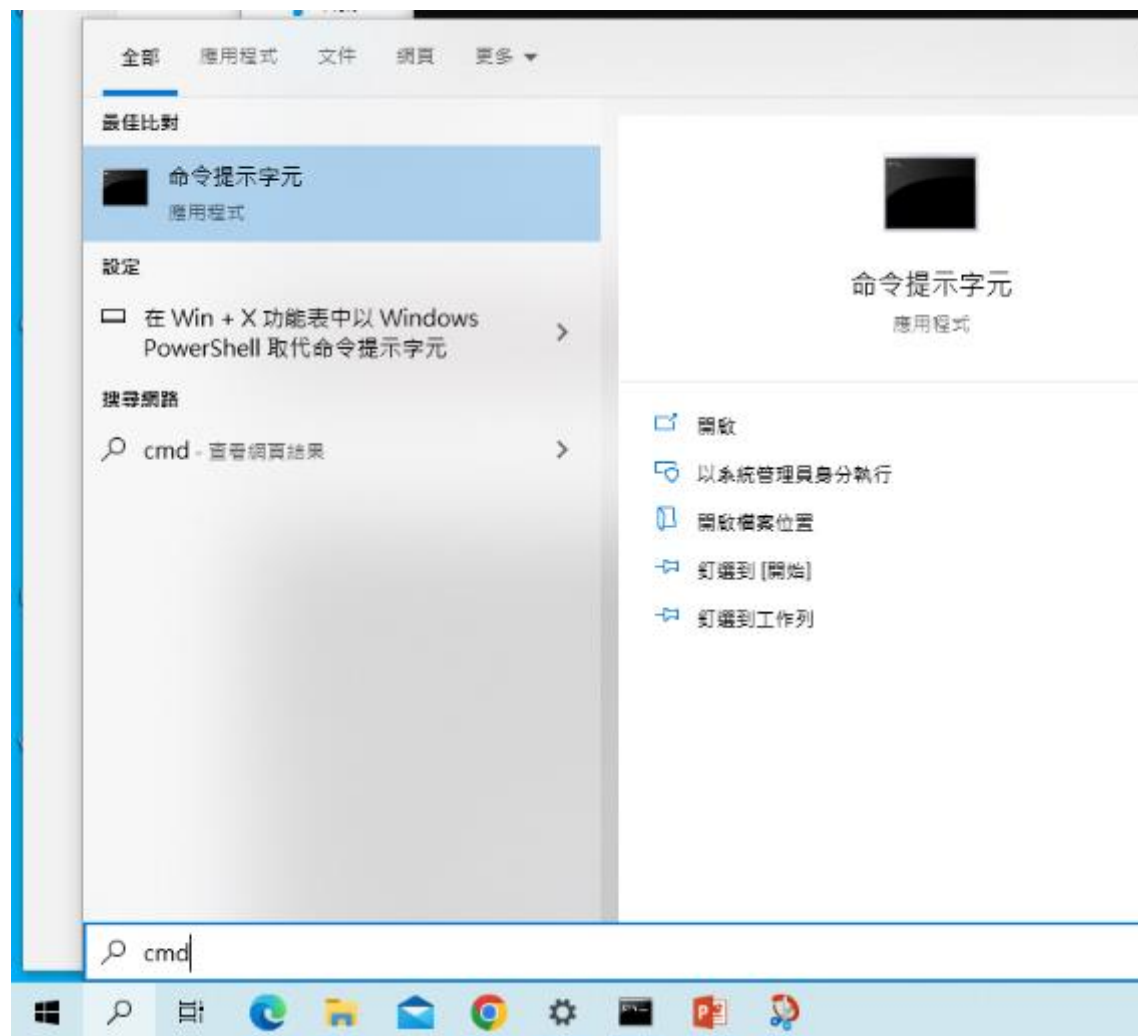
 webgoat-server-8.2.2.jar	91.9 MB	05 Sep 2021
 webwolf-8.2.2.jar	51.3 MB	05 Sep 2021
 Source code (zip)		05 Sep 2021
 Source code (tar.gz)		05 Sep 2021

 27  4  9  6 39 people reacted

找到檔案的位置，C:\Users\User\webgoat



開以終端機，搜尋欄輸入cmd



進入存放webgoat-server-8.2.2的資料夾

```
cd webgoat
```

命令提示字元

```
Microsoft Windows [版本 10.0.19044.2130]  
(c) Microsoft Corporation. 著作權所有，並保留一切權利
```

```
C:\Users\User>cd webgoat 你的資料夾位置
```

```
C:\Users\User\webgoat>
```



把網路關掉，避免被攻擊

開以webgoat伺服器

```
java -jar webgoat-server-8.2.2.jar
```

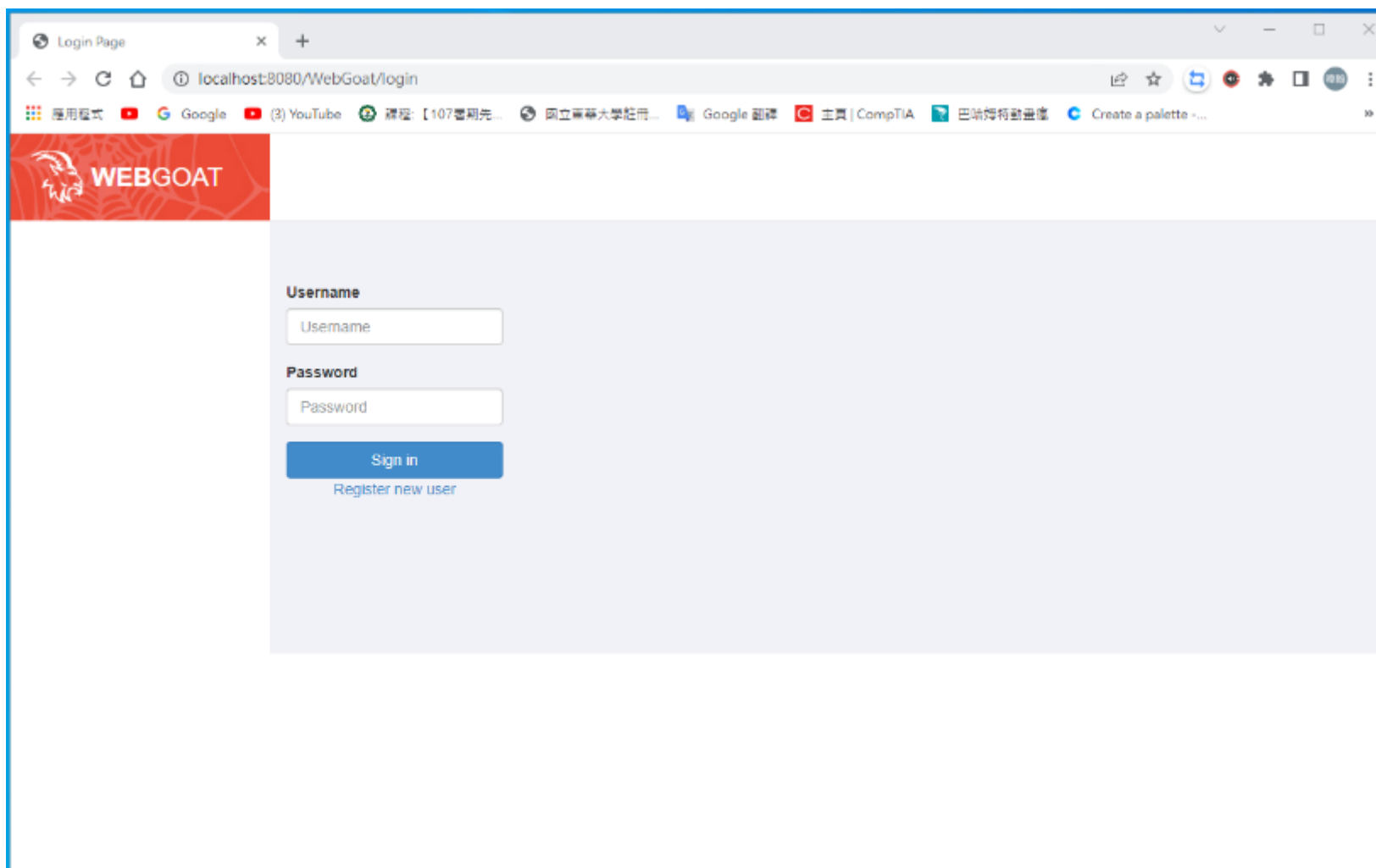
```
C:\Users\User>cd webgoat
C:\Users\User\webgoat>java -jar webgoat-server-8.2.2.jar
21:46:25.557 [main] INFO org.owasp.webgoat.StartWebGoat - Starting WebGoat with args:

:: Spring Boot ::
(v2.4.3)

2022-10-24 21:46:26.355 INFO 996 --- [main] org.owasp.webgoat.StartWebGoat : Starting StartWebGoat v8.2.2 using Java 19.0.1 on DESKTOP-RBK9GI9 with PID 996 (C:\Users\User\webgoat\webgoat-server-8.2.2.jar started by User in C:\Users\User\webgoat)
2022-10-24 21:46:26.356 DEBUG 996 --- [main] org.owasp.webgoat.StartWebGoat : Running with Spring Boot v2.4.3, Spring v5.3.4
2022-10-24 21:46:26.356 INFO 996 --- [main] org.owasp.webgoat.StartWebGoat : No active profile set, falling back to default profiles: default
2022-10-24 21:46:27.969 INFO 996 --- [main] .s.d.r.c.RepositoryConfigurationDelegate : Bootstrapping Spring Data JPA repositories in DEFAULT mode.
2022-10-24 21:46:28.069 INFO 996 --- [main] .s.d.r.c.RepositoryConfigurationDelegate : Finished Spring Data repository scanning in 92 ms. Found 2 JPA repository interfaces.
2022-10-24 21:46:28.608 WARN 996 --- [main] io.undertow.websockets.jsr : UT026010: Buffer pool was not set on WebSocketDeploymentInfo, the default pool will be used
2022-10-24 21:46:28.622 INFO 996 --- [main] io.undertow.servlet : Initializing Spring e
```

開啟本地端網頁


<http://localhost:8080/WebGoat/login>



很重要！Webgoat作為教育目的，請不要拿
這個去打外面的網站

認識POST與GET





1

**WEBGOAT**

- Introduction >
- General >
- HTTP Basics** ✓
- HTTP Proxies
- Developer Tools
- CIA Triad
- Crypto Basics
- Writing new lesson

- (A1) Injection >
- (A2) Broken Authentication >
- (A3) Sensitive Data Exposure >
- (A4) XML External Entities (XXE) >
- (A5) Broken Access Control >
- (A7) Cross-Site Scripting (XSS) >
- (A8) Insecure Deserialization >
- (A9) Vulnerable Components >
- (A8:2013) Request Forgeries >
- Client side >
- Challenges >

HTTP Basics



Reset lesson

1 2 3 +

Concept

This lesson presents the basics for understanding the transfer of data between the browser and the web application and how to trap a request/response with a HTTP proxy.

Goals

The user should become familiar with the features of WebGoat by manipulating the above buttons to view hints, show the HTTP request parameters, the HTTP request cookies, and the Java source code. You may also try using [OWASP Zed Attack Proxy](#) for the first time.

How HTTP works:

All HTTP transactions follow the same general format. Each client request and server response has three parts: the request or response line, a header section and the entity body.

The client initiates a transaction as follows:

- The client contacts the server and sends a document request. A GET request can have url parameters and those parameters will be available in the web access logs.
 - GET /index.html?param=value HTTP/1.0
- Next, the client sends optional header information to inform the server of its configuration and the document formats it will accept.
 - User-Agent: Mozilla/4.06 Accept: image/gif,image/jpeg, /
- In a POST request, the user supplied data will follow the optional headers and is not part of the contained within the POST URL.

尋找傳遞資料的方式

WEBGOAT

Introduction >
General >
HTTP Basics ✓
HTTP Proxies
Developer Tools
CIA Triad
Crypto Basics
Writing new lesson

(A1) Injection >
(A2) Broken Authentication >
(A3) Sensitive Data Exposure >
(A4) XML External Entities (XXE) >
(A5) Broken Access Control >
(A7) Cross-Site Scripting (XSS) >
(A8) Insecure Deserialization >

HTTP Basics

Show hints Reset lesson

1

2

Enter your name in the input field below and press "Go!" to submit. The server will accept the request, reverse the input and display it back to the user, illustrating the basics of handling an HTTP request.

Try It!

Enter your name in the input field below and press "Go!" to submit. The server will accept the request, reverse the input and display it back to the user, illustrating the basics of handling an HTTP request.

Enter Your Name: Go!

2 輸入姓名，查看傳輸位置

HTTP Basics



Show hints

Reset lesson



Enter your name in the input field below and press "Go!" to submit. The server will accept the request, reverse the input and display it back to the user, illustrating the basics of handling an HTTP request.

Try It!

Enter your name in the input field below and press "Go!" to submit. The server will accept the request, reverse the input and display it back to the user, illustrating the basics of handling an HTTP request.

Enter Your Name:

Enter your name in the input field below and press "Go!" to submit. The server will accept the request, reverse the input and display it back to the user, illustrating the basics of handling an HTTP request.

Try It!

Enter your name in the input field below and press "Go!" to submit. The server will accept the request, reverse the input and display it back to the user, illustrating the basics of handling an HTTP request.



Enter Your Name:

The server has reversed your name: 987654321

按下F12，點選Element，找找看是用甚麼方式傳輸







提示:查看CSS頁面區塊

有找到POST嗎

```
<!-- if including attack, reuse this section, leave classes in place -->  
▼<div class="attack-container">  
  ▶<div class="assignment-success">...</div>  
  <!-- using attack-form class on your form will allow your request to be  
    ajaxified and stay within the display framework for webgoat -->  
  <!-- you can write your own custom forms, but standard form submission  
    will take you to your endpoint and outside of the WebGoat framework -->  
  <!-- of course, you can write your own ajax submission /handling in your  
    own javascript if you like -->  
  ▼<form class="attack-form" accept-charset="UNKNOWN" method="POST" name="for  
    m" action="/WebGoat/HttpBasics/attack1">  
    ▶<div id="lessonContent">...</div>  
  </form>  
  <!-- do not remove the two following div's, this is where your  
    feedback/output will land -->  
  <div class="attack-feedback" style>The server has reversed your name:  
    987654321</div>  
  <div class="attack-output" style></div>  
  <!-- ... of course, you can move them if you want to, but that will not  
    look consistent to other lessons -->  
</div>  
</div>
```


第三題，同樣方法找到是POST還是GET

HTTP Basics



Show hints

Reset lesson

← 1 2 3

The Quiz

What type of HTTP command did WebGoat use for this lesson. A POST or a GET.

✓

Was the HTTP command a POST or a GET:

What is the magic number:

Go!

Congratulations. You have successfully completed the assignment.

提示:查看F12的Network

先隨便輸入，查看傳輸值

HTTP Basics

Reset lesson

← 1 2 3 →

The Quiz

What type of HTTP command did WebGoat use for this lesson. A POST or a GET.

Was the HTTP command a POST or a GET:

What is the magic number:

Go!

DevTools is now available in Chinese! Always match Chrome's language Switch DevTools to Chinese Don't show again

Elements

Console

Sources

Network

Performance

Memory

Application

Security

Lighthouse

>>

2

2

1

Preserve log

Disable cache

No throttling

att

Invert

Hide data URLs

All

Fetch/XHR

JS

CSS

Img

Media

Font

Doc

WS

Wasm

Manifest

Other

Has blocked cookies

Blocked Requests

3rd-party requests

10000 ms

20000 ms

30000 ms

40000 ms

50000 ms

60000 ms

70000 ms

80000 ms

90000 ms

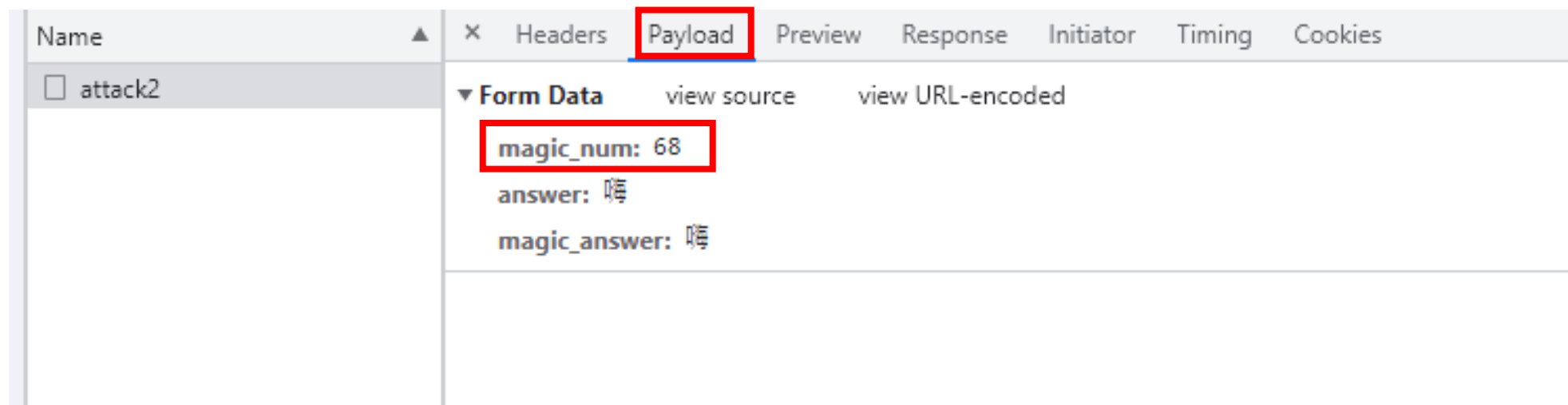
Name	Status	Type	Initiator	Size	Time	Waterfall
<div><div></div> attack2</div>	200	xhr	VM115427:jquery.min.js:2	433 B	132 ms	

找到傳輸方式

The screenshot displays the 'Headers' tab in a web browser's developer tools. The left sidebar shows a list of requests, with 'attack2' selected. The main panel shows the details of the selected request. The 'Request Method' is highlighted as 'POST'. The 'Status Code' is '200 OK'. The 'Remote Address' is '127.0.0.1:8080'. The 'Referrer Policy' is 'strict-origin-when-cross-origin'. The 'Response Headers' section shows various headers including 'Connection: keep-alive', 'Content-Type: application/json', 'Date: Tue, 25 Oct 2022 03:57:27 GMT', 'Transfer-Encoding: chunked', 'X-Content-Type-Options: nosniff', 'X-Frame-Options: DENY', and 'X-XSS-Protection: 1; mode=block'. The 'Request Headers' section shows various headers including 'Accept: */*', 'Accept-Encoding: gzip, deflate, br', 'Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7', 'Connection: keep-alive', 'Content-Length: 52', and 'Content-Type: application/x-www-form-urlencoded; charset=UTF-8'.

Name	Headers	Payload	Preview	Response	Initiator	Timing	Cookies
attack2	<p>General</p> <p>Request URL: <code>http://localhost:8080/WebGoat/HttpBasics/attack2</code></p> <p>Request Method: POST</p> <p>Status Code: 🟢 200 OK</p> <p>Remote Address: 127.0.0.1:8080</p> <p>Referrer Policy: strict-origin-when-cross-origin</p> <p>Response Headers View source</p> <p>Connection: keep-alive</p> <p>Content-Type: application/json</p> <p>Date: Tue, 25 Oct 2022 03:57:27 GMT</p> <p>Transfer-Encoding: chunked</p> <p>X-Content-Type-Options: nosniff</p> <p>X-Frame-Options: DENY</p> <p>X-XSS-Protection: 1; mode=block</p> <p>Request Headers View source</p> <p>Accept: */*</p> <p>Accept-Encoding: gzip, deflate, br</p> <p>Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7</p> <p>Connection: keep-alive</p> <p>Content-Length: 52</p> <p>Content-Type: application/x-www-form-urlencoded; charset=UTF-8</p>						

在Payload找到剛剛傳輸的資料



Good! 完成第一題了

Reset lesson



The Quiz

What type of HTTP command did WebGoat use for this lesson. A POST or a GET.




Was the HTTP command a POST or a GET:


What is the magic number:

Go!

Congratulations. You have successfully completed the assignment.

認識Proxy


 **WEBGOAT**

- Introduction >
- General >
- HTTP Basics 
- HTTP Proxies**
- Developer Tools
- CIA Triad
- Crypto Basics
- Writing new lesson

- (A1) Injection >
- (A2) Broken Authentication >
- (A3) Sensitive Data Exposure >
- (A4) XML External Entities (XXE) >
- (A5) Broken Access Control >
- (A7) Cross-Site Scripting (XSS) >
- (A8) Insecure Deserialization >
- (A9) Vulnerable Components >
- (A8:2013) Request Forgeries >
- Client side >
- Challenges >

HTTP Proxies

Reset lesson

1 2 3 4 5 6 7 8 9 10 

What's a HTTP Proxy

A proxy is some forwarder application that connects your http client to backend resources. HTTP clients can be browsers, or applications like curl, SOAP UI, Postman, etc. Usually these proxies are used for routing and getting access to internet when there is no direct connection to internet from the client itself. HTTP proxies are therefore also ideal when you are testing your application. You can always use the proxy log records to see what was actually sent from client to server. So you can check the request and response headers and the XML, JSON or other payload.

HTTP Proxies receive requests from a client and relay them. They also typically record them. They act as a man-in-the-middle. It even works fine with or without HTTPS as long as your client or browser trusts the certificate of the HTTP Proxy.

ZAP Proxy Capabilities

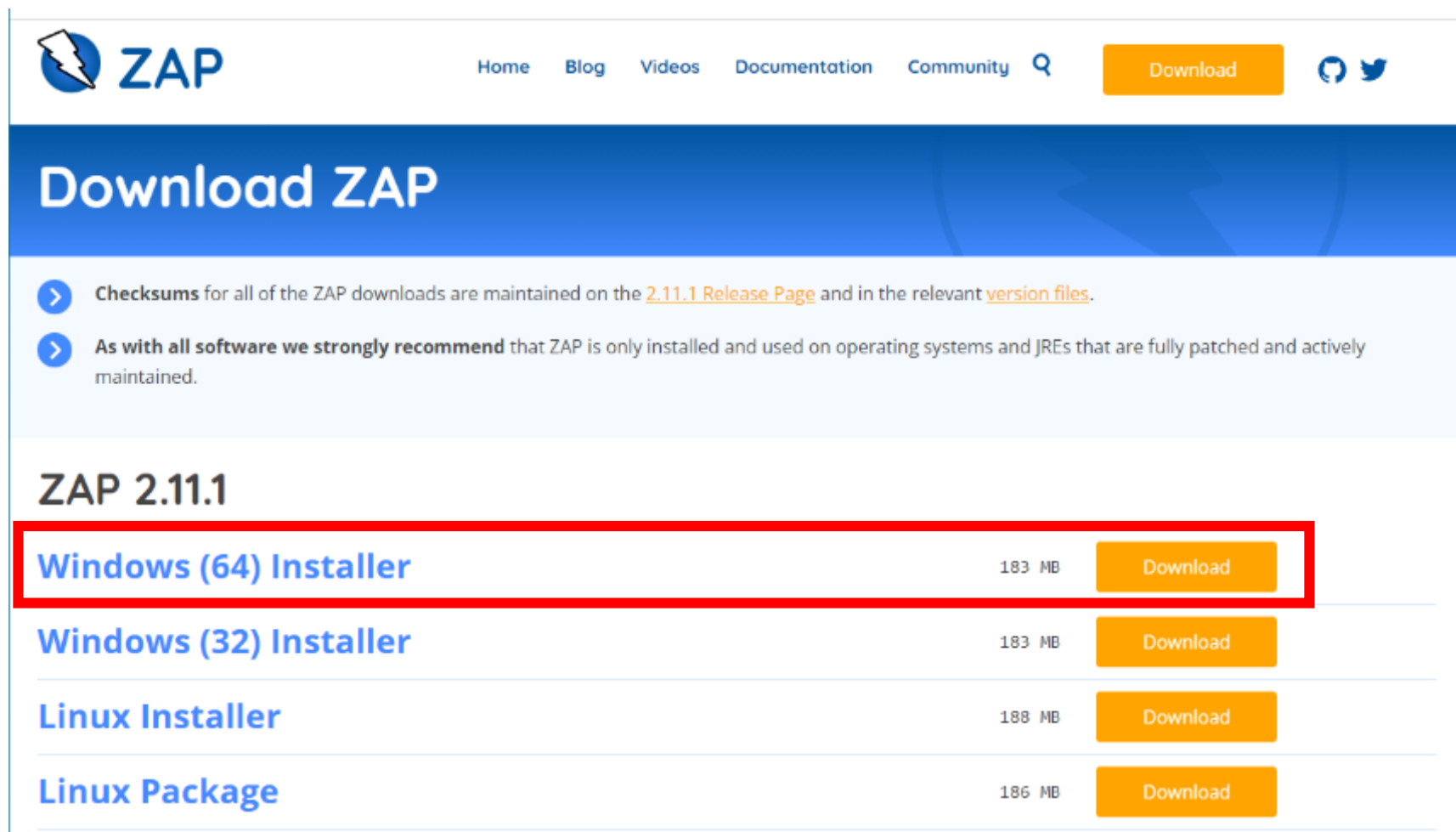
With ZAP you can record traffic, inspect traffic, modify requests and response from and to your browser, and get reports on a range of known vulnerabilities that are detected by ZAP through the inspection of the traffic. The passive and active reporting on security issues is usually used in Continuous Delivery pipelines that use a GUI-less ZAP. Here we will use ZAP interactively and mainly to see and modify requests in order to find vulnerabilities and solve assignments. ZAP has a graphical user interface, but now also has a HUD Heads-On-Display which uses a websocket connection between the browser and the ZAP proxy.

Proxy傳輸方式



下載ZAP

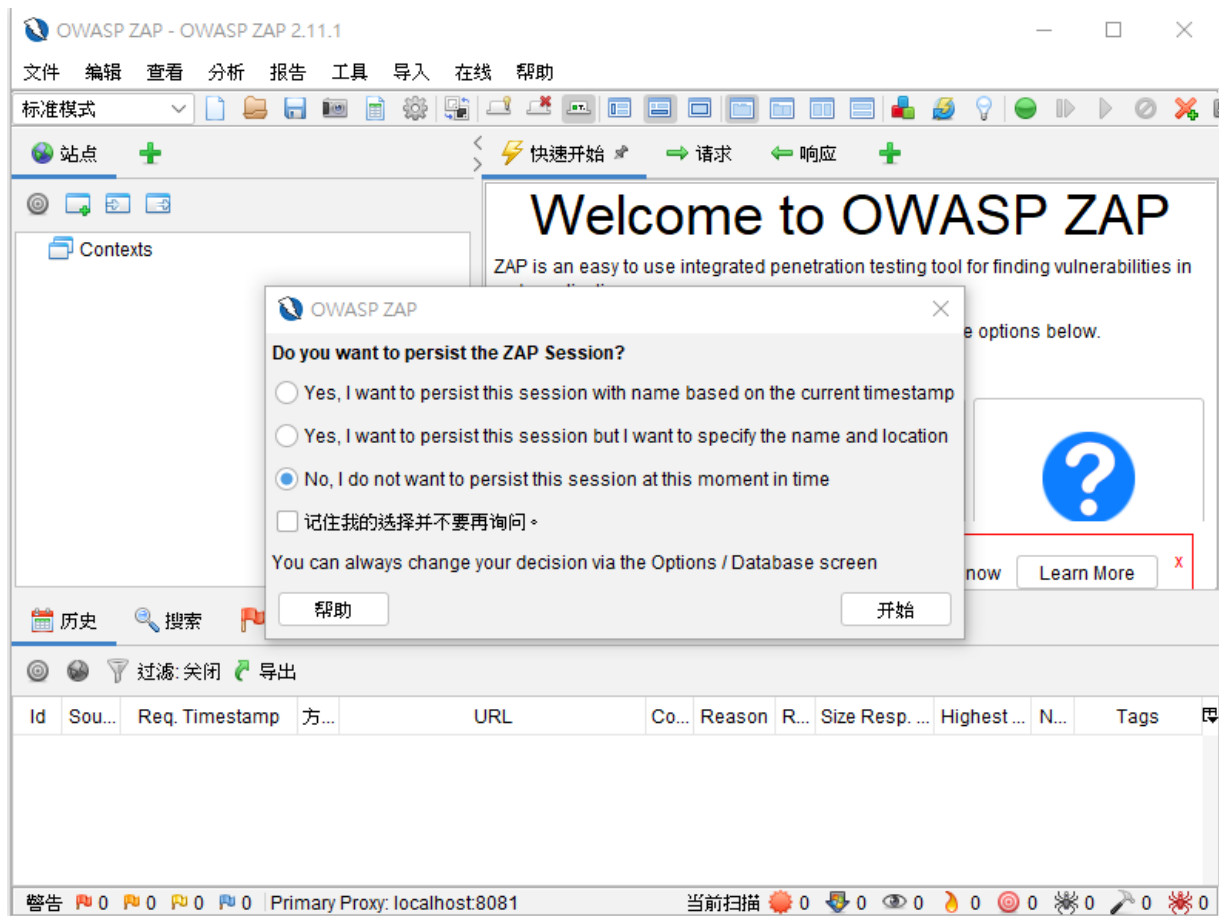
- <https://www.zaproxy.org/download/>



The screenshot shows the ZAP website's download page. At the top is the ZAP logo and a navigation bar with links for Home, Blog, Videos, Documentation, and Community, along with a search icon and a 'Download' button. Below the navigation bar is a large blue banner with the text 'Download ZAP'. Underneath the banner, there are two informational points: one about checksums and another recommending that ZAP be installed on fully patched operating systems and JREs. The main section is titled 'ZAP 2.11.1' and contains a table of download links for different operating systems. The first row, 'Windows (64) Installer', is highlighted with a red border. The table lists the file size for each installer and provides a 'Download' button for each.

Operating System	File Size	Download Button
Windows (64) Installer	183 MB	Download
Windows (32) Installer	183 MB	Download
Linux Installer	188 MB	Download
Linux Package	186 MB	Download

打開ZAP



設定代理端口

OWASP ZAP - OWASP ZAP 2.11.1

File Edit View Analyse Report Tools Im

Standard Mode

Sites

Contexts

- Default Context
- Sites

History Search Alerts Outp

Filter: OFF Export

Id Sou... Req. Timestamp Met...

Options

- Display
- Dynamic SSL Certificates
- Encode/Decode
- Extensions
- Forced Browse
- Form Handler
- Fuzzer
- Global Alert Filters
- Global Exclude URL
- GraphQL
- HTTP Sessions
- HUD
- JVM
- Keyboard
- Language
- Local Proxies**
- OAST
- Passive Scan Rules
- Passive Scan Tags
- Passive Scanner
- Quick Start Launch
- Replacer
- Rule Configuration
- Scripts
- Search
- Selenium
- Spider

Local Proxies

Local Proxy

Address: 127.0.0.1

Port (e.g. 8080): 8081

Set your browser proxy setting using the above. The HTTP port and HTTPS port must be the same port as above.

☐ Behind NAT

☒ Remove Unsupported Encodings

☒ Always unzip gzipped content

Security Protocols

☐ SSLv2Hello ☒ SSL 3 ☒ TLS 1 ☒ TLS 1.1 ☒ TLS 1.2 ☐ TLS 1.3

Additional Proxies

Enabled	Address ^	Port
---------	-----------	------

☐ Remove Without Confirmation

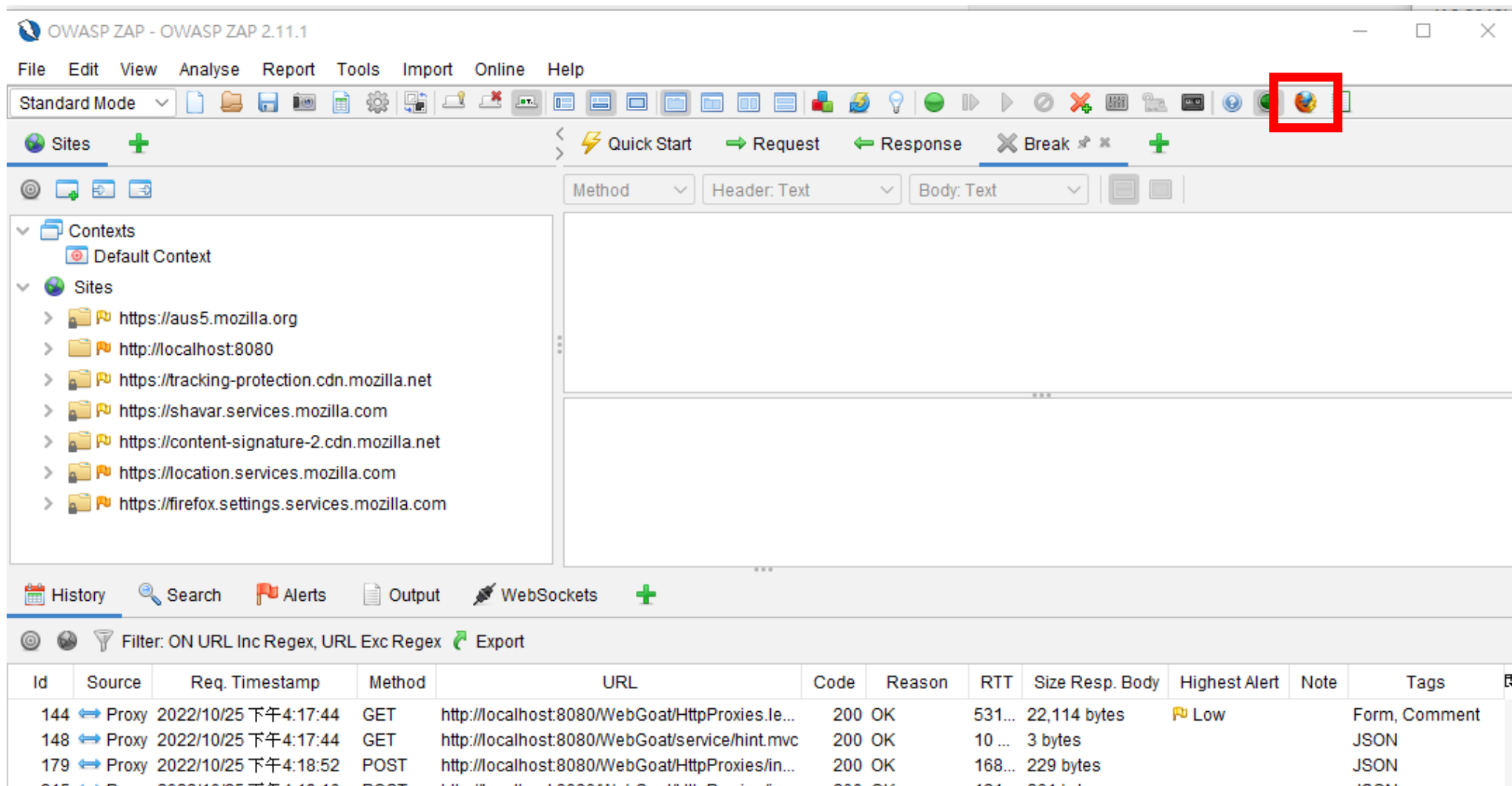
Reset to Factory Defaults

Cancel OK

Alerts 0 0 0 0 0 Primary Proxy: localhost:8081 Current Scans 0 0 0 0 0 0 0 0 0 0

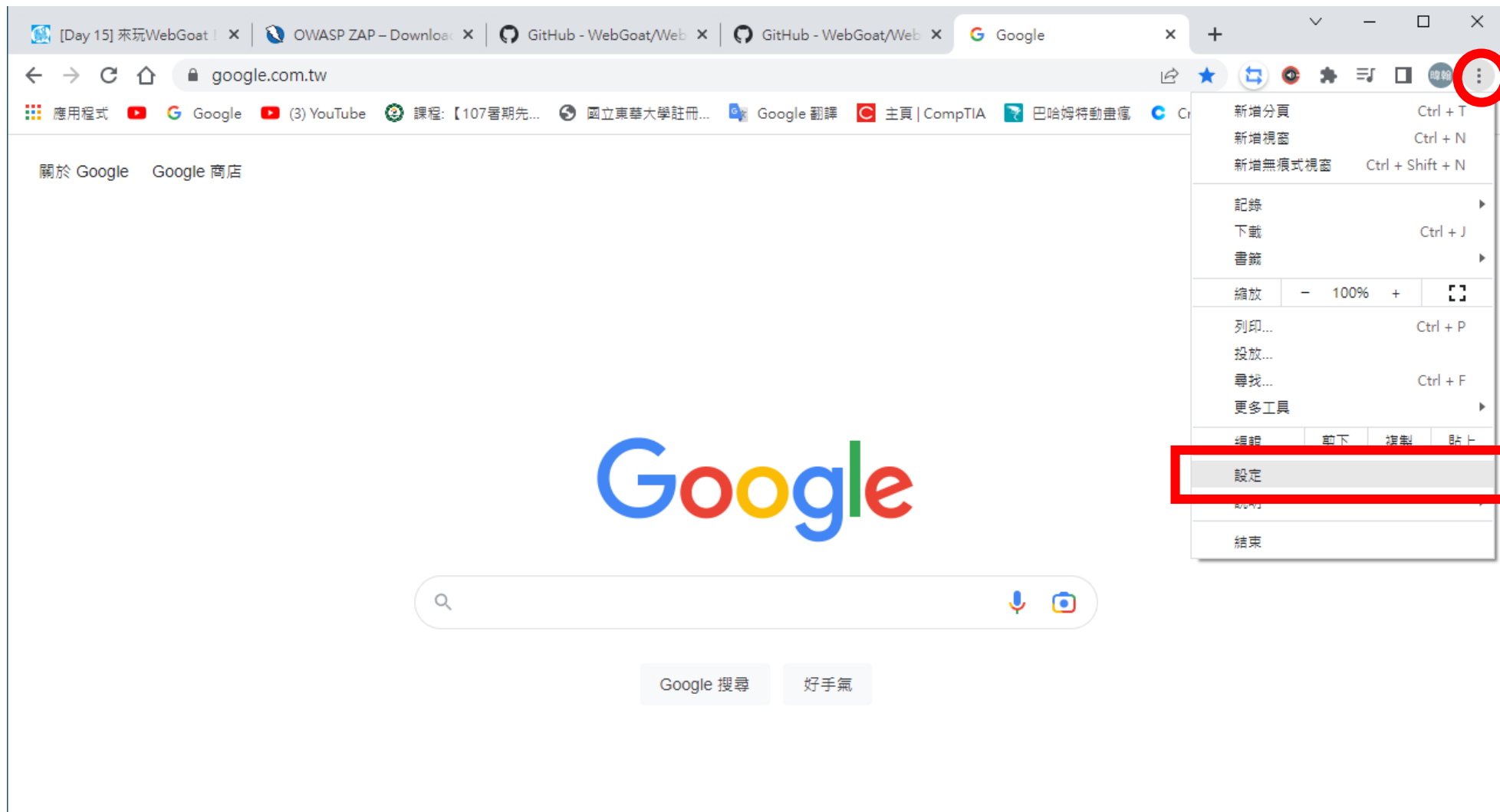
Port記著等等可能會用到

開啟瀏覽器

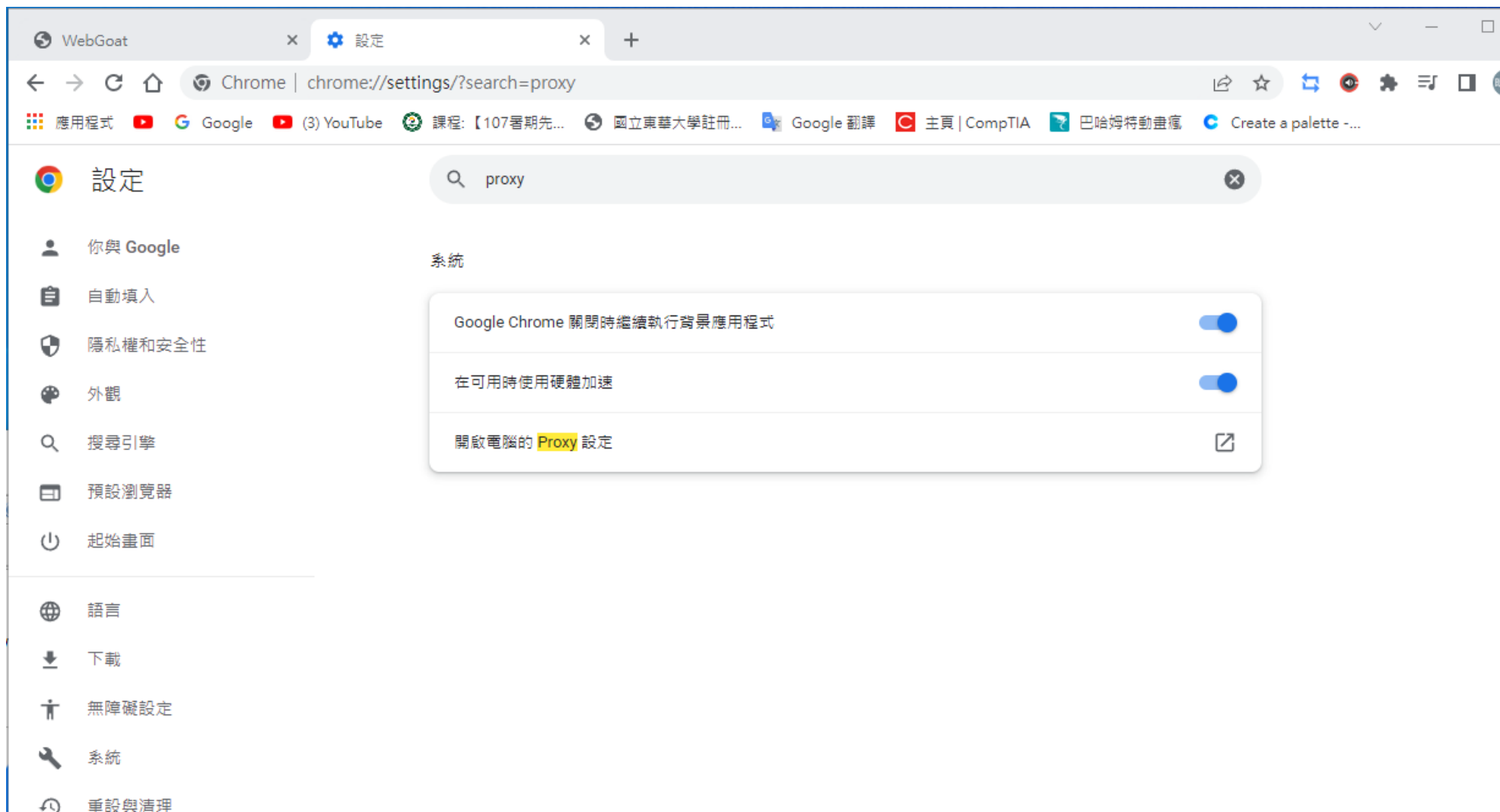


用Firefox瀏覽器
正常來說ZAP應該在掃了
想學學Chrome怎麼掃嗎

瀏覽器設定proxy



尋找proxy設定頁面



填上IP跟Port

← 設定

首頁

尋找設定

網路和網路網路

狀態

乙太網路

Wi-Fi

VPN

飛機模式

行動熱點

Proxy

Proxy

VPN 連線 *

自動偵測設定

☒ 開啟

使用設定指令碼

☐ 關閉

指令碼位址

儲存

手動 Proxy 設定

針對乙太網路或 Wi-Fi 連線使用 Proxy 伺服器。這些設定不會應用到 VPN 連線。

使用 Proxy 伺服器

☒ 開啟

位址

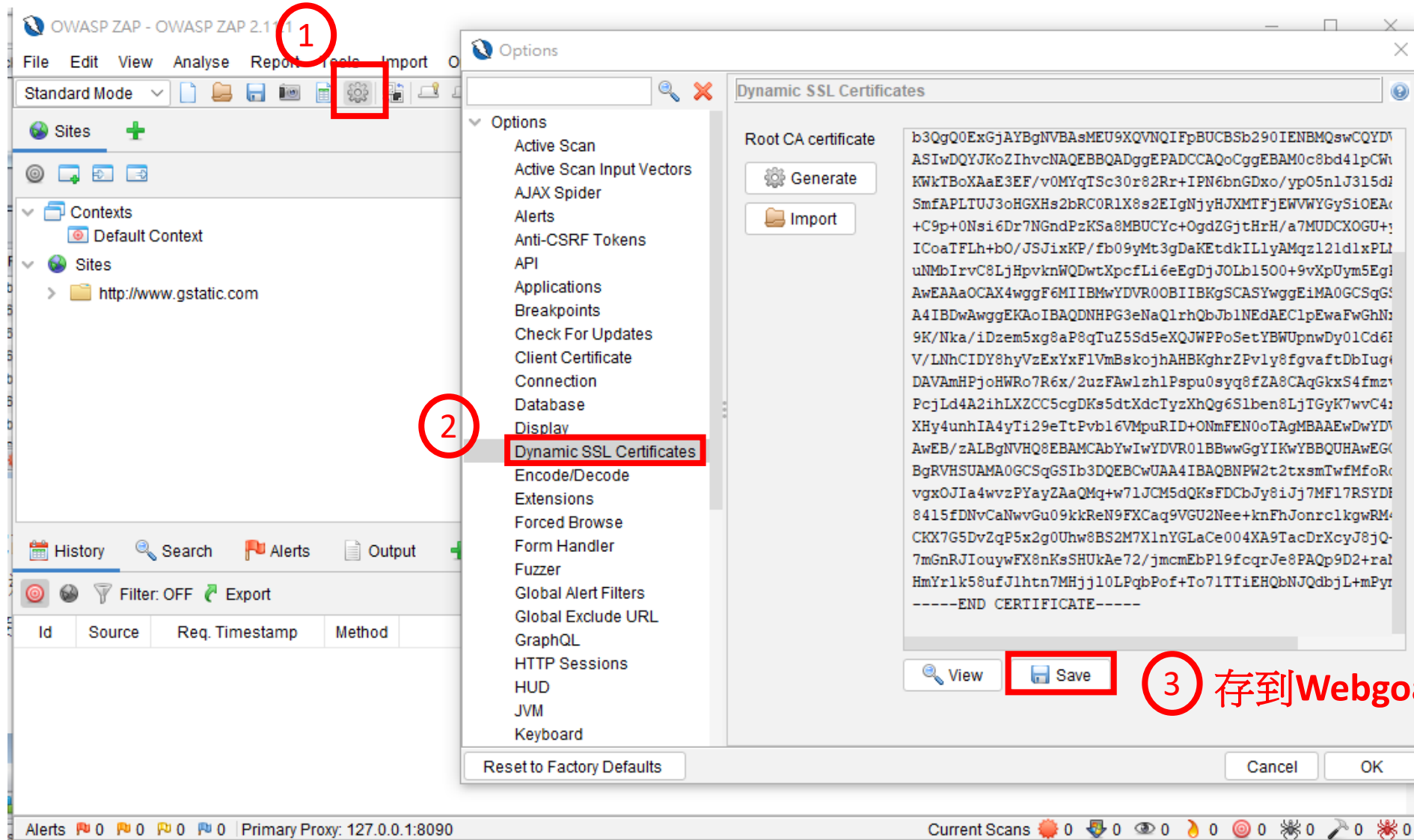
連接埠

不要為下列項目的位址使用 Proxy 伺服器，請使用分號 (;) 來分隔每個項目。

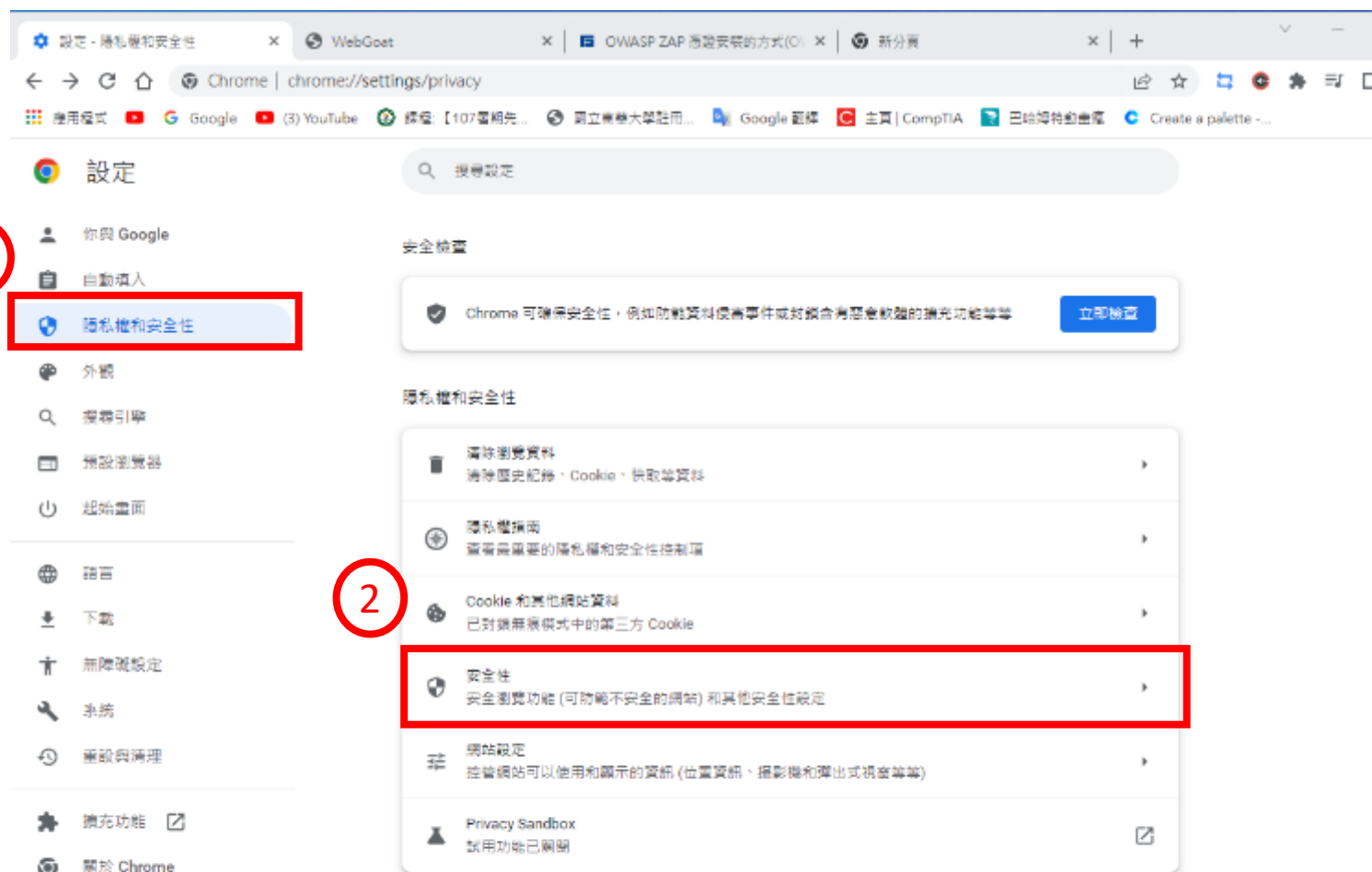
☐ 不要為近端 (內部網路) 位址使用 Proxy 伺服器

儲存

Chrome如果沒有..... 應該是少了憑證



匯入憑證



稱會經過加密，任何人 (包括 Google) 都無法讀取。

無防護 (不建議)

- ☐ 無法封鎖不安全的網站、下載內容和擴充功能。在 Gmail 和 Google 搜尋等其他 Google 服務中，安全瀏覽功能的防護機制仍然會發揮作用 (在適用情況下)。

進階

一律使用安全連線

將瀏覽路徑升級至 HTTPS，並在載入不支援該協定的網站前發出警告



使用安全 DNS

判斷如何透過安全連線連上網站



- ☒ 使用目前的服務供應商
可能無法隨時使用安全 DNS

☐ 包含 自訂

管理手機

控管要使用哪些手機做為安全金鑰



管理憑證

管理 HTTPS/SSL 憑證和設定



Google 進階保護計畫

保護任何容易成為攻擊目標的使用者，確保他們的帳戶安全無虞





憑證存放區

憑證存放區是用來存放憑證的系統區域。

Windows 可自動選取憑

☐ 自動根據憑證類型

☒ 將所有憑證放入以

憑證存放區:

個人

選取憑證存放區

選取您要使用的憑證存放區(C)

- 個人
- 受信任的根憑證授權單位
- 企業信任
- 中繼憑證授權單位
- 受信任的發行者**
- 沒有信任的憑證
- 第三方根憑證授權單位
- 受信任的...

☐ 顯示實體存放區(S)

確定

取消

OWASP ZAP - OWASP ZAP 2.11.1

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites +

Quick Start Request Response Break +

Contexts

- Default Context
- Sites
 - https://firefox-settings-attachments.cdn.mozilla.net
 - https://tracking-protection.cdn.mozilla.net
 - https://shavar.services.mozilla.com
 - https://content-signature-2.cdn.mozilla.net
 - https://firefox.settings.services.mozilla.com
 - http://localhost:8080

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack:

Use traditional spider: ☒

Use ajax spider: ☒ with

Progress: manually stopped

History Search Alerts Output Spider AJAX Spider Active Scan WebSockets +

Filter: ON URL Inc Regex Export

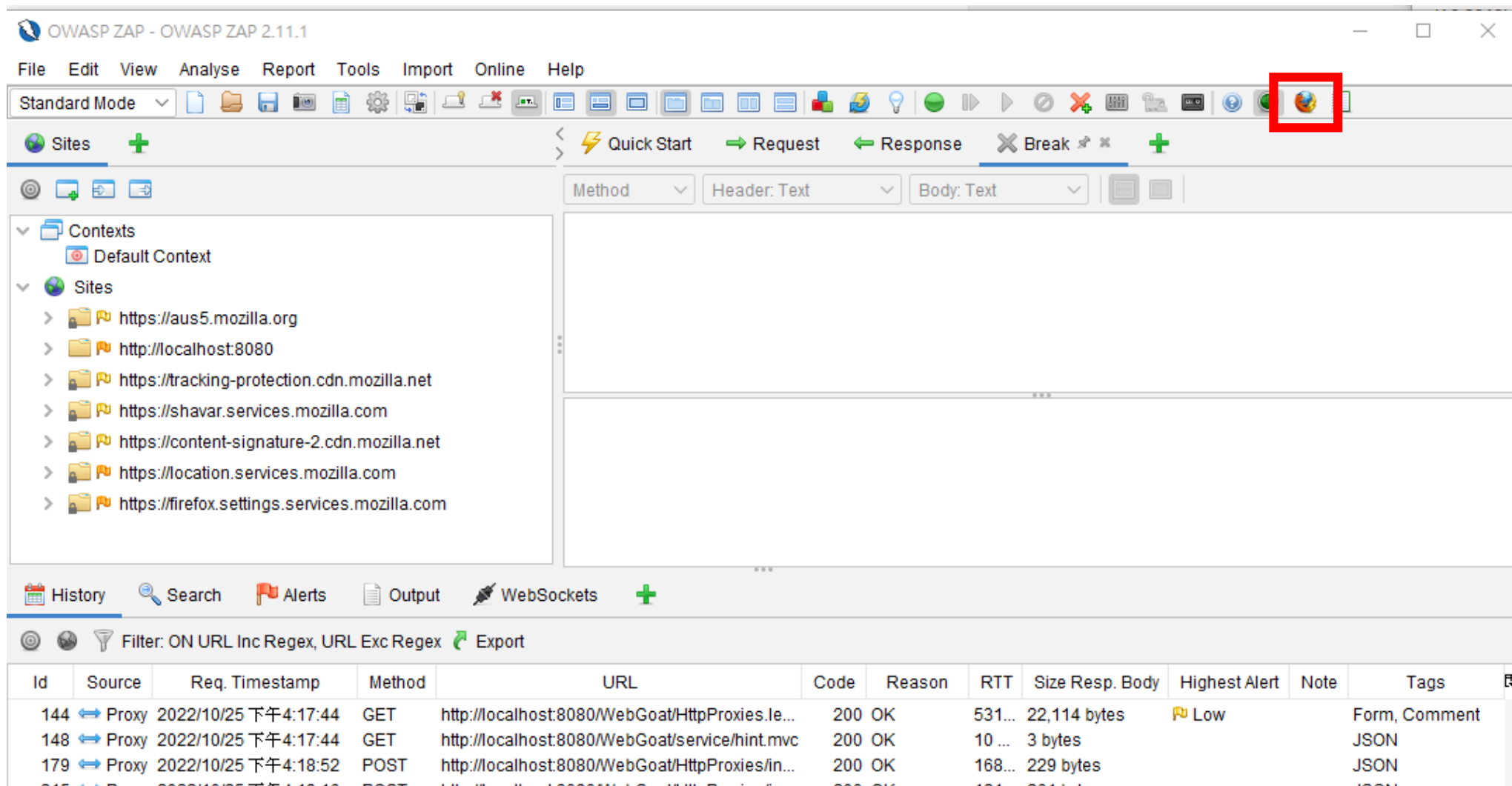
Id	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1,032	Proxy	2022/10/25 下午3:34:05	GET	http://localhost:8080/WebGoat/service/lesso...	200	OK	116...	183 bytes			JSON
1,033	Proxy	2022/10/25 下午3:34:08	GET	http://localhost:8080/WebGoat/service/lesso...	200	OK	118...	7,676 bytes			JSON
1,034	Proxy	2022/10/25 下午3:34:10	GET	http://localhost:8080/WebGoat/service/lesso...	200	OK	113...	183 bytes			JSON
1,035	Proxy	2022/10/25 下午3:34:13	GET	http://localhost:8080/WebGoat/service/lesso...	200	OK	117...	7,676 bytes			JSON
1,036	Proxy	2022/10/25 下午3:34:15	GET	http://localhost:8080/WebGoat/service/lesso...	200	OK	122...	183 bytes			JSON
1,037	Proxy	2022/10/25 下午3:34:18	GET	http://localhost:8080/WebGoat/service/lesso...	200	OK	106...	7,676 bytes			JSON
1,038	Proxy	2022/10/25 下午3:34:20	GET	http://localhost:8080/WebGoat/service/lesso...	200	OK	113...	183 bytes			JSON

Alerts 0 2 6 3 Primary Proxy: 127.0.0.1:8082 Current Scans 0 0 0 0 0 0 0 0 0 0

Chrome應該有再掃了吧

接下來以Firebox來做竄改內容

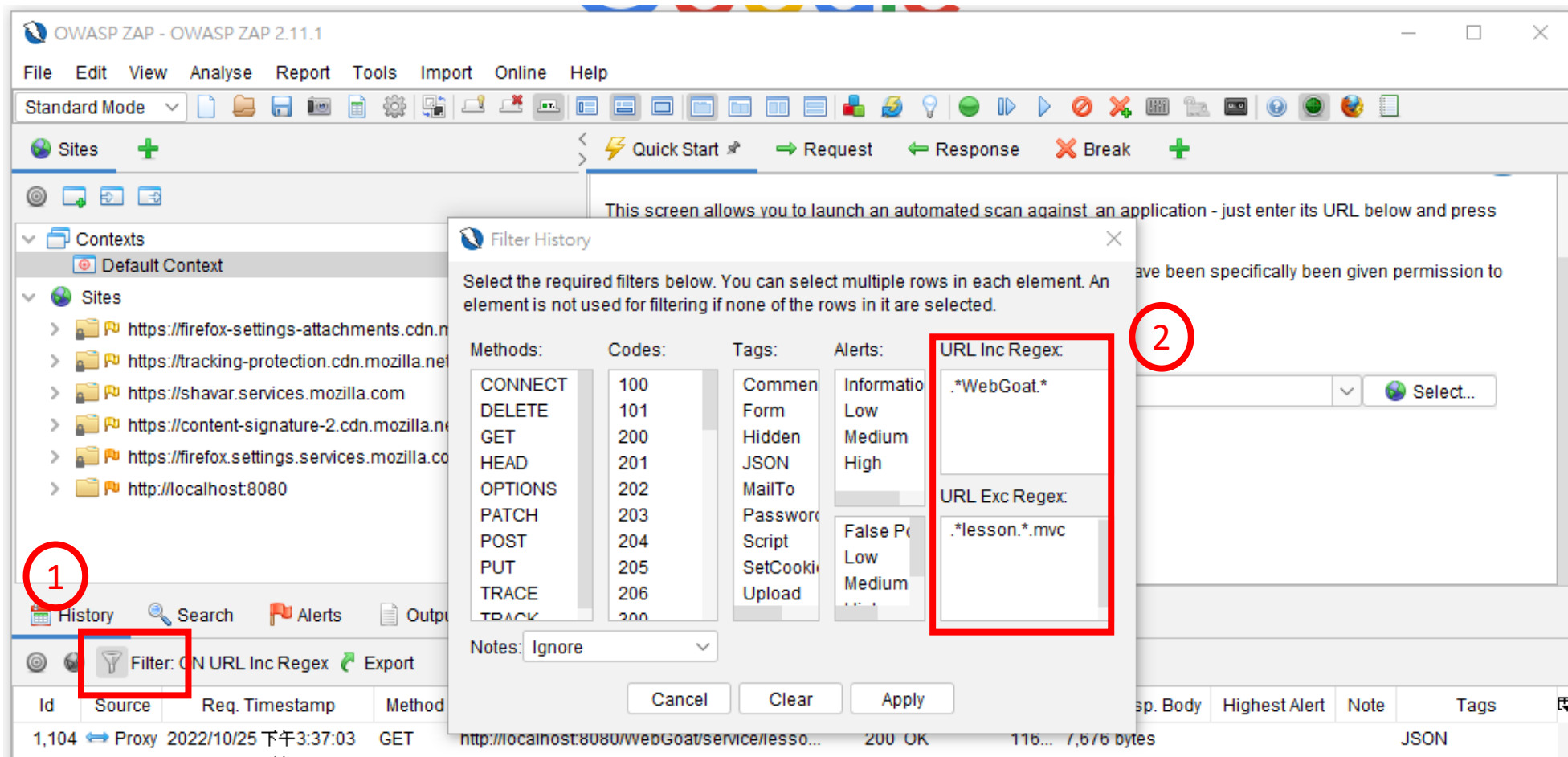
開啟瀏覽器



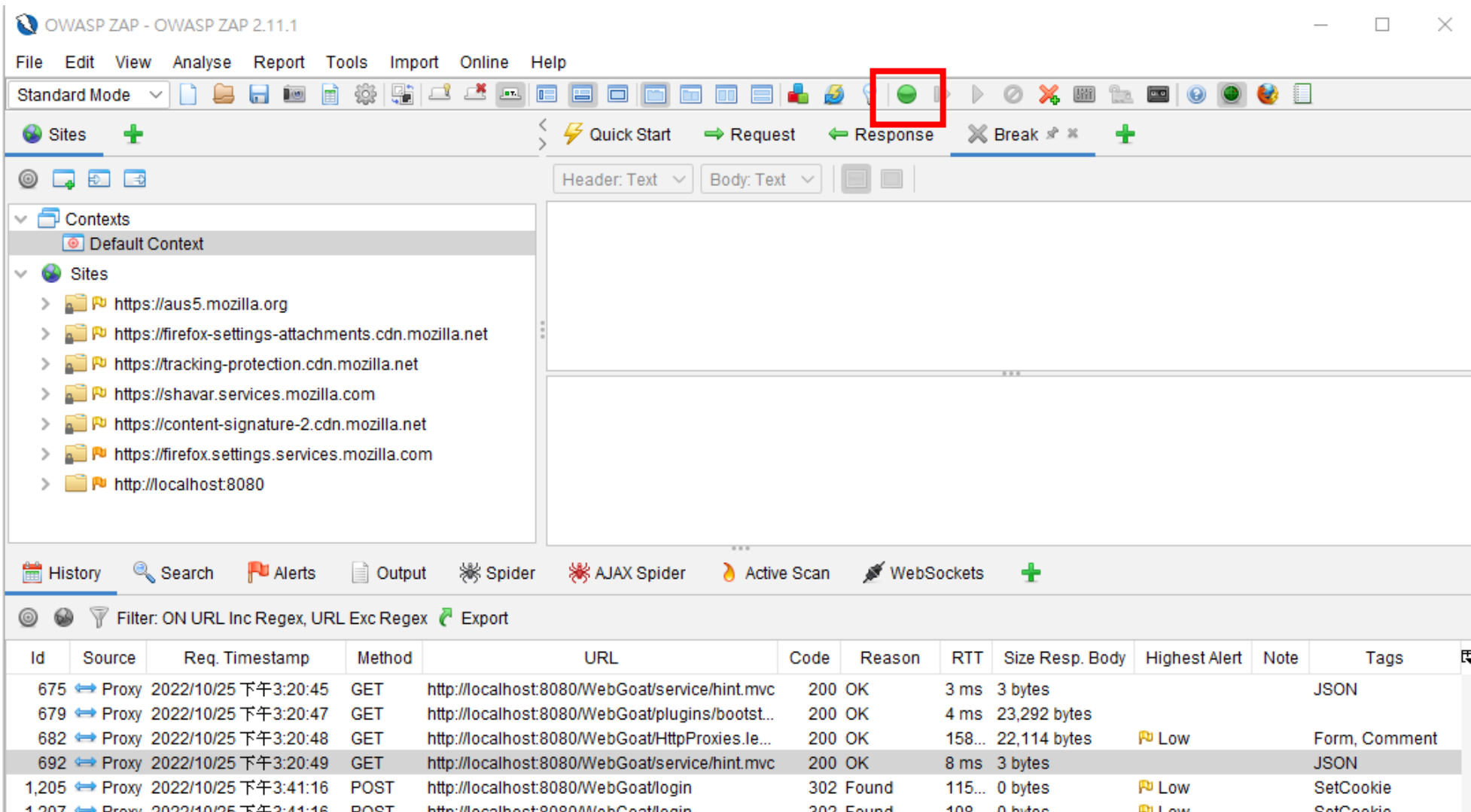
試試過濾器

.*WebGoat.*

.*lesson.*.mvc



如果要竄改內容，點選綠色按鈕



The screenshot shows the OWASP ZAP 2.11.1 application window. The title bar reads "OWASP ZAP - OWASP ZAP 2.11.1". The menu bar includes File, Edit, View, Analyse, Report, Tools, Import, Online, and Help. The toolbar contains various icons for file operations, analysis, and testing. A red rectangle highlights a green circular button with a white 'X' inside, which is the 'Edit Response' button. Below the toolbar, the 'Standard Mode' dropdown is visible. The main interface is divided into several panes. On the left, the 'Sites' pane shows a tree view with 'Contexts' and 'Default Context' expanded, listing several URLs including mozilla.org and localhost:8080. The central pane shows the 'Response' tab selected, with 'Header: Text' and 'Body: Text' dropdowns. The bottom pane shows a list of HTTP history entries. The status bar at the bottom indicates the filter is 'ON URL Inc Regex, URL Exc Regex' and provides an 'Export' button.

Id	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
675	Proxy	2022/10/25 下午3:20:45	GET	http://localhost:8080/WebGoat/service/hint.mvc	200	OK	3 ms	3 bytes			JSON
679	Proxy	2022/10/25 下午3:20:47	GET	http://localhost:8080/WebGoat/plugins/bootst...	200	OK	4 ms	23,292 bytes			
682	Proxy	2022/10/25 下午3:20:48	GET	http://localhost:8080/WebGoat/HttpProxies.le...	200	OK	158...	22,114 bytes	Low		Form, Comment
692	Proxy	2022/10/25 下午3:20:49	GET	http://localhost:8080/WebGoat/service/hint.mvc	200	OK	8 ms	3 bytes			JSON
1,205	Proxy	2022/10/25 下午3:41:16	POST	http://localhost:8080/WebGoat/login	302	Found	115...	0 bytes	Low		SetCookie
1,207	Proxy	2022/10/25 下午3:41:16	POST	http://localhost:8080/WebGoat/login	202	Found	108...	0 bytes	Low		SetCookie


點完綠綠按鈕後，點第六個分頁

Intercept and modify a request

Set up the intercept as noted above and then submit the form/request below by clicking the submit button. When your request is intercepted (hits the breakpoint), modify it as follows.

- Change the Method to GET
- Add a header 'x-request-intercepted:true'
- Remove the request body and instead send 'changeMe' as query string parameter and set the value to 'Requests are tampered easily' (without the single quotes)

Then let the request continue through (by hitting the play button).

 The two play buttons behave a little differently, but we'll let you tinker and figure that out for yourself.

doesn't matter really

Submit

Please try again. Make sure to make all the changes. And case sensitivity may matter ... or not, you never know!

再來我們要依他給的題目竄改傳遞的內容



HTTP Message



Request

Response

```
GET http://localhost:8080/WebGoat/HttpProxies/intercept-request HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0)
Gecko/20100101 Firefox/106.0
Accept: */*
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.5,en;q=0.3
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
x-request-intercepted:true
Content-Length: 30
Origin: https://localhost:8080
```

```
changeMe=Requests+are+tampered+easily
```

完成後按continue

完成應該長這樣






The two play buttons behave a little differently, but we'll let you tinker and figure that out for yourself.



Well done, you tampered the request as expected

買台電視八

 **WEBGOAT**

- Introduction >
- General >
- (A1) Injection >
- (A2) Broken Authentication >
- (A3) Sensitive Data Exposure >
- (A4) XML External Entities (XXE) >
- (A5) Broken Access Control >
- (A7) Cross-Site Scripting (XSS) >
- (A8) Insecure Deserialization >
- (A9) Vulnerable Components >
- (A8-2013) Request Forgeries >
- Client side >**
 - Bypass front-end restrictions 
 - Client side filtering
 - XXE: Introduction 
- Challenges >

HTML tampering


Show hints Reset lesson

◀ 1 2 3 ▶

Try it yourself

In an online store you ordered a new TV, try to buy one or more TVs for a lower price.

✓

Product	Quantity	Price	Total	
 55" M5510 White Full HD Smart TV by Samsung Status: In Stock	1	2999.99	\$2999.99	✕ Remove
Subtotal			\$2999.99	
Shipping costs			\$0.00	
Total			\$2999.99	

[Continue Shopping](#) [Checkout ▶](#)

Well done, you just bought a TV at a discount

打開ZAP，改一下數字

HTTP Message

RequestResponse

```
POST http://localhost:8080/WebGoat/HtmlTampering/task HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0)
Gecko/20100101 Firefox/106.0
Accept: */*
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.5,en;q=0.3
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 19
Origin: https://localhost:8080
Connection: keep-alive
```


QTY=1000&Total=0

StepContinueDrop

Try it yourself

In an online store you ordered a new TV, try to buy one or more TVs for a lower price.

✓

Product	Quantity	Price	Total	
<div></div> <div><div>55" M5510 White Full HD Smart TV</div><div>by Samsung</div><div>Status: In Stock</div></div>	<input type="text" value="1"/>	2999.99	\$2999.99	<div>✕ Remove</div>
			Subtotal	\$2999.99
			Shipping costs	\$0.00
			Total	\$2999.99
<div><div><div>🛒 Continue Shopping</div><div>Checkout ▶</div></div></div>				

Well done, you just bought a TV at a discount