

WebGoat 學習筆記

1. 安裝 JAVA :

https://download.oracle.com/java/18/latest/jdk-18_windows-x64_bin.zip

The screenshot shows the Oracle Java Downloads page for JDK 18. The page has a dark header with the Oracle logo and navigation links. Below the header, there's a section titled "Java Downloads" with a sub-section "Java SE Development Kit 18.0.1.1 downloads". A table lists three download options for Windows: "x64 Compressed Archive" (172.8 MB), "x64 Installer" (153.38 MB), and "x64 MSI Installer" (152.26 MB). A yellow box highlights the download link for the "x64 Compressed Archive" with the text "Click for download".

Product/file description	File size	Download
x64 Compressed Archive	172.8 MB	https://download.oracle.com/java/18/latest/jdk-18_windows-x64_bin.zip (sha256 [5])
x64 Installer	153.38 MB	https://download.oracle.com/java/18/latest/jdk-18_windows-x64_bin.exe (sha256 [5])
x64 MSI Installer	152.26 MB	https://download.oracle.com/java/18/latest/jdk-18_windows-x64_bin.msi (sha256 [5])

2. 下載 WebGoat :

[Releases · WebGoat/WebGoat · GitHub](#)

The screenshot shows the GitHub Releases page for WebGoat. The page displays the latest release, "v8.2.2", which is also labeled "Latest". Below the release title, there's a section "New functionality" and a section "Bug fixes". At the bottom, there's a section "Assets" with two files: "webgoat-server-8.2.2.jar" (91.9 MB) and "webwoit-8.2.2.jar" (51.3 MB). A yellow box highlights the "webgoat-server-8.2.2.jar" file with the text "Click for download".

05 Sep 2021
github-actions
v8.2.2
e75cfbe

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 Click for download

webgoat-server-8.2.2.jar	91.9 MB
webwoit-8.2.2.jar	51.3 MB

3.設置環境變數-JAVA_HOME：

1. 在“系統變量”下的“環境變量”窗口中選擇路徑
2. 點擊“編輯...”
3. 在“編輯環境變量”窗口中點擊“新建”
4. 輸入 %JAVA_HOME%\bin

4.執行檔案：

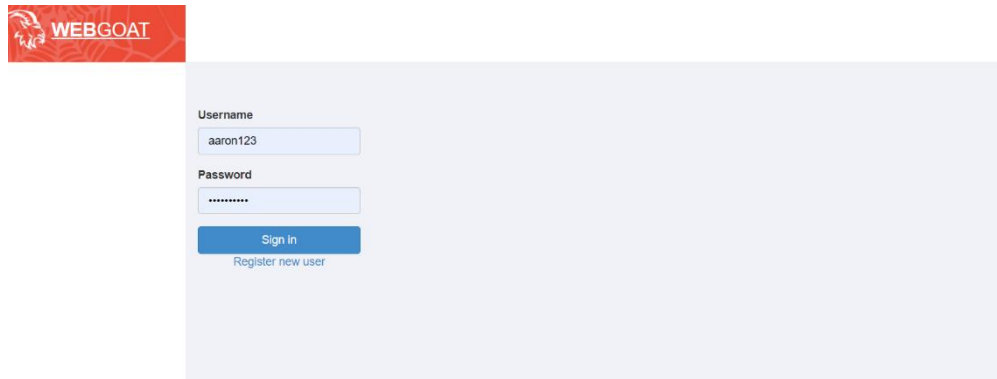
在 cmd 輸入[java -jar webgoat-server-8.2.2.jar]指令

[illegible]

>>顯示出成功畫面

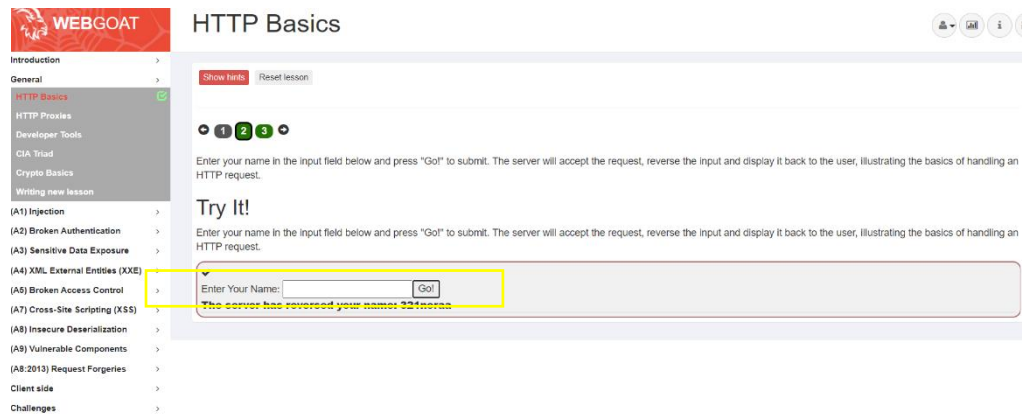
WebGoat-HTTP Basic

登入 WebGoat



The image shows the WebGoat login interface. On the left is a red header with the WebGoat logo. The main area is a light blue box containing a login form. The form has two input fields: 'Username' with the text 'aaron123' and 'Password' with masked characters '*****'. Below these fields is a blue 'Sign in' button and a smaller link 'Register new user'.

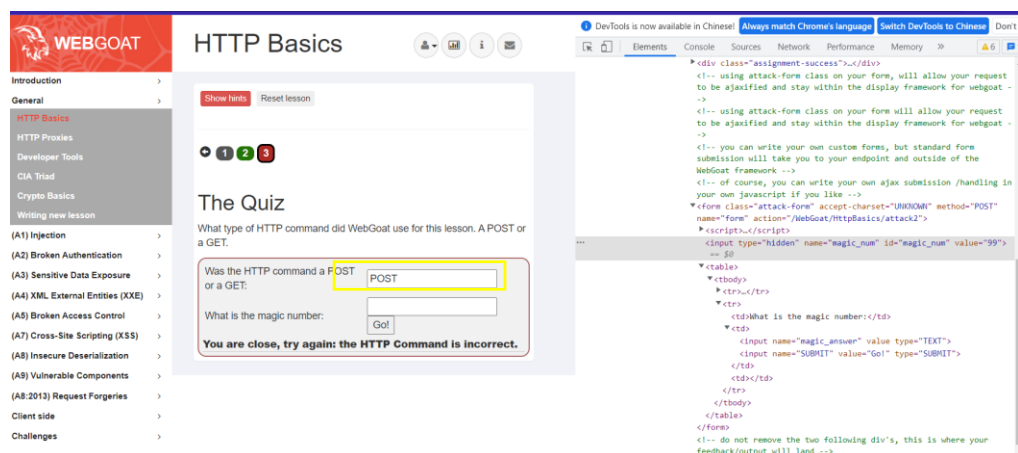
輸入名稱並提交



The image shows the WebGoat 'HTTP Basics' lesson interface. On the left is a sidebar with a list of topics, including 'Introduction', 'General', 'HTTP Basics' (which is highlighted with a green checkmark), 'HTTP Proxies', 'Developer Tools', 'CIA Triad', 'Crypto Basics', 'Writing new lesson', and a list of vulnerabilities from (A1) Injection to (A8) 2013 Request Forgeries, followed by 'Client side' and 'Challenges'. The main area is titled 'HTTP Basics' and contains a 'Show hints' button, a 'Reset lesson' button, and a progress indicator with three steps (1, 2, 3). Below this, there is a text box with instructions: '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.' This is followed by a 'Try It!' section with another instruction: '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.' At the bottom of this section is an input field labeled 'Enter Your Name:' with a 'Go!' button. A yellow box highlights this input field and button. Below the input field, the text 'The server has reversed your name: 324notas' is visible.

服務器將接受請求，反轉輸入並將其顯示給用戶，說明處理 HTTP 的請求

使用 POST(HTTP 命令)傳出



在上面練習中觀察到 HTTP 的請求是一個 POST 消息。magic number 隱藏在 web 的 JavaScript 中。查看此內容的方法之一是右鍵單擊網頁並選擇“Inspect Element”。在網頁 HTML 出現的部分中，搜索“magic”，直到確定隱藏的 magic_num 字段存儲的值。