

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: "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 compressed archive, with a yellow text overlay "Click for download" pointing to it.

| 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 v8.2.2. The page has a dark header with the GitHub logo and navigation links. Below the header, there's a section titled "v8.2.2" with a "Latest" badge. The release description includes "New functionality" (Docker image now supports nginx) and "Bug fixes" (three issues). A yellow box highlights the "Assets" section, with a yellow text overlay "Click for download" pointing to it. The assets list includes "webgoat-server-8.2.2.jar" (91.9 MB) and "webwoit-8.2.2.jar" (51.3 MB).

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

| Asset | Size |
|--|---------|
| 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

```
Microsoft Windows [版本 10.0.19044.186]
(c) Microsoft Corporation。著作權所有，並保留一切權利。

C:\Users\aaaron\Downloads> java -jar webgoat-server-8.2.2.jar
17:45:40.993 [main] INFO org.owasp.webgoat.StartWebGoat - Starting WebGoat with args:


/\ \ / _ \ | | |   O      /\ \ \ \ 
( W )_/_ \|_|_|_|_|_\|_|_|_|_) ) ) ) )
=====||=====|__|=//_/ // // 

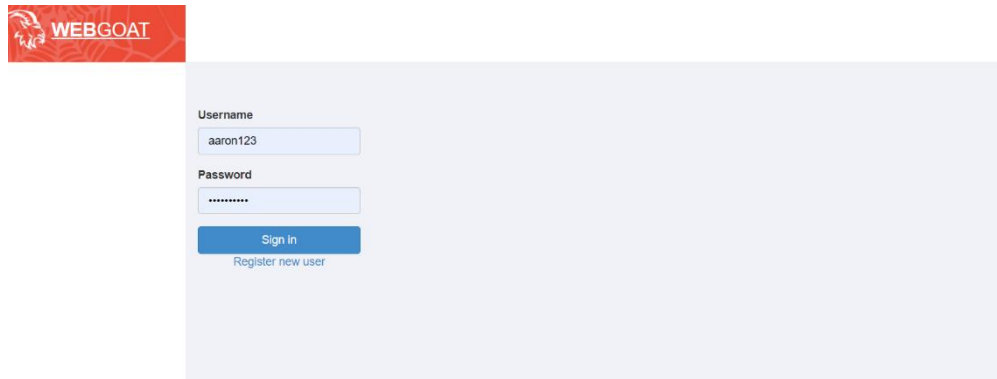
:: Spring Boot ::                (v2.4.3)

2022-05-11 17:45:43.896 INFO 68116 --- [           main] org.owasp.webgoat.StartWebGoat : Starting StartWebGo
 at v8.2.2 using Java 18.0.1.1 on LAPTOP-8E50FUG6 with PID 68116 (C:\Users\aaaron\Downloads\webgoat-server-8.2.2.jar start
 ed by aaaron in C:\Users\aaaron\Downloads)
2022-05-11 17:45:43.898 DEBUG 68116 --- [           main] org.owasp.webgoat.StartWebGoat : Running with Spring
Boot v2.4.3, Spring v5.3.4
2022-05-11 17:45:43.899 INFO 68116 --- [           main] org.owasp.webgoat.StartWebGoat : No active profile s
et, falling back to default profiles: default
2022-05-11 17:45:47.603 INFO 68116 --- [           main] .s.d.r.c.RepositoryConfigurationDelegate : Bootstrapping Sprin
g Data JPA repositories in DEFAULT mode.
2022-05-11 17:45:47.844 INFO 68116 --- [           main] .s.d.r.c.RepositoryConfigurationDelegate : Finished Spring Dat
a repository scanning in 227 ms. Found 2 JPA repository interfaces.
2022-05-11 17:45:48.991 WARN 68116 --- [           main] io Undertow websockets.jsr : UT026010: Buffer po
ol was not set on WebSocketDeploymentInfo, the default pool will be used
```

>>顯示出成功畫面

WebGoat-HTTP Basic

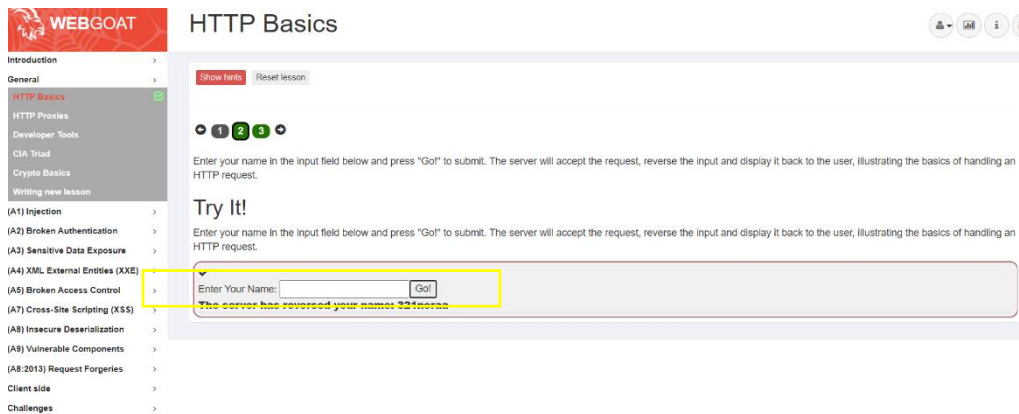
登入 WebGoat



The image shows the WebGoat login interface. On the left is a red sidebar with the 'WEBGOAT' logo. The main area is light gray and contains a login form with the following elements:

- Username:** A text input field containing 'aaron123'.
- Password:** A password input field with masked characters '*****'.
- Sign in:** A blue button.
- Register new user:** A smaller, lighter blue link below the sign in button.

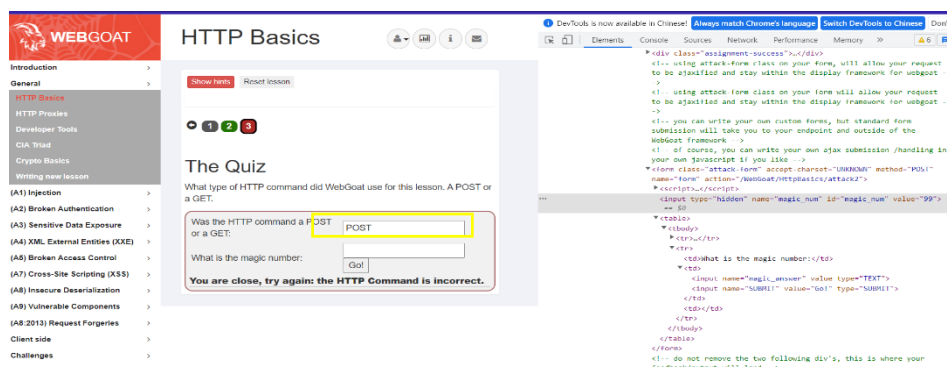
輸入名稱並提交



The image shows the 'HTTP Basics' lesson page in WebGoat. It features a sidebar on the left 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', and 'Writing new lesson'. The main content area is titled 'HTTP Basics' and includes a 'Show hints' button and a 'Reset lesson' button. Below these are three numbered steps (1, 2, 3) with step 2 being the active one. The instructions state: '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.' A 'Try It!' section follows, with the same instructions. At the bottom, there is a form with an 'Enter Your Name:' label, a text input field, and a 'Go!' button. A yellow box highlights this input area. Below the input field, the text 'The server has reversed your name: 324notas' is displayed.

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。

學習心得

在查詢資料時了解到 WebGoat 是用於進行 web 漏洞實驗的應用平台，用來說明 web 應用中存在的安全漏洞。WebGoat 運行在帶有 java 虛擬機的平台之上，在學習間覺得 WebGoat 不但要對網站架構熟悉，通訊協議，測試流程與測試工具使用，漏洞利用腳本編寫，還要有豐富的經驗積累等，每一項能力中都需要精進研究，深度研究，才能進階到更高的程度，這個過程中少不了網路同儕的引導、個人的努力和堅持。對於網路安全學習需要付出的絕非一朝一夕，這期間除了知識的積累，更重要的是實踐，只有在實踐中學會發現問題，解決問題，才能讓我們所學的知識真正做到學以致用！也感謝老師的教導。