

WebGoat 學習筆記

前言

Webgoat是專門用來練習漏洞的Web應用程式，所以裡面的網頁都是漏洞百出，因此官方建議使用WebGoat練習時，最好要把網路中斷。此外WebGoat只供教育使用，在裡面學到的任何技術都不能拿去測試外面的網頁，以免觸法。

WebGoat怎麼安裝

Github上可以看到，安裝WebGoat有四種方法：

1. *Standalone*
2. *Run using Docker*
3. *Run from the sources*
4. *Run with custom*

這邊我使用的是第一種

一、首先要先確定電腦裡有裝JRE

[Java SE Downloads][<https://www.oracle.com/java/technologies/downloads/>]

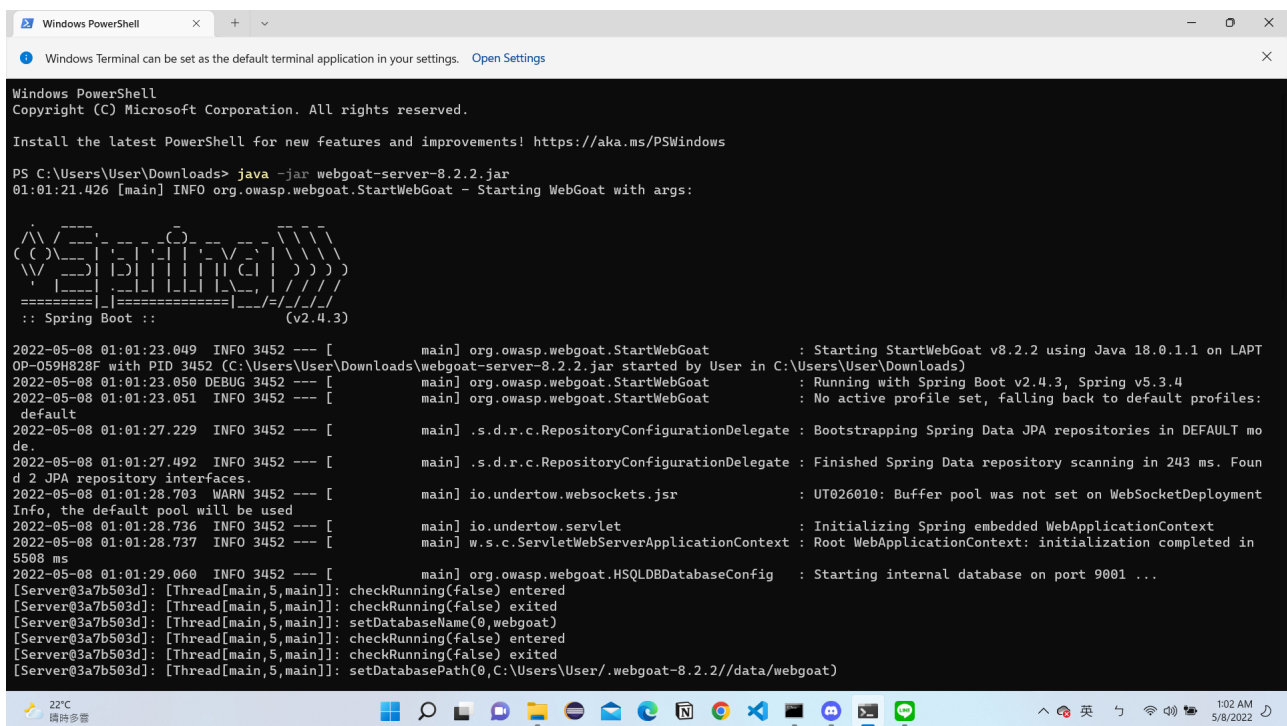
二、到Github上下載最新的WebGoat

[WebGoat Downloads][<https://github.com/WebGoat/WebGoat/releases>]

三、執行下載的檔案

```
java -jar webgoat-server-8.1.0.jar [ - server.port=8080] [ -  
server.address=localhost]
```

出現這個頁面就是成功喔！到這裡的朋友已經成功一半了：)



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\User\Downloads> java -jar webgoat-server-8.2.2.jar
01:01:21.426 [main] INFO org.owasp.webgoat.StartWebGoat - Starting WebGoat with args:

:: Spring Boot :: (v2.4.3)

2022-05-08 01:01:23.049 INFO 3452 --- [main] org.owasp.webgoat.StartWebGoat : Starting StartWebGoat v8.2.2 using Java 18.0.1.1 on LAPTOP-059H828F with PID 3452 (C:\Users\User\Downloads\webgoat-server-8.2.2.jar started by User in C:\Users\User\Downloads)
2022-05-08 01:01:23.050 DEBUG 3452 --- [main] org.owasp.webgoat.StartWebGoat : Running with Spring Boot v2.4.3, Spring v5.3.4
2022-05-08 01:01:23.051 INFO 3452 --- [main] org.owasp.webgoat.StartWebGoat : No active profile set, falling back to default profiles: default
2022-05-08 01:01:27.229 INFO 3452 --- [main] .s.d.r.c.RepositoryConfigurationDelegate : Bootstrapping Spring Data JPA repositories in DEFAULT mode.
2022-05-08 01:01:27.492 INFO 3452 --- [main] .s.d.r.c.RepositoryConfigurationDelegate : Finished Spring Data repository scanning in 243 ms. Found 2 JPA repository interfaces.
2022-05-08 01:01:28.703 WARN 3452 --- [main] io.undertow.websockets.jsr : UT0026010: Buffer pool was not set on WebSocketDeploymentInfo, the default pool will be used
2022-05-08 01:01:28.736 INFO 3452 --- [main] io.undertow.servlet : Initializing Spring embedded WebApplicationContext
2022-05-08 01:01:28.737 INFO 3452 --- [main] w.s.c.ServletWebServerApplicationContext : Root WebApplicationContext: initialization completed in 5508 ms
2022-05-08 01:01:29.060 INFO 3452 --- [main] org.owasp.webgoat.HSQLDBDatabaseConfig : Starting internal database on port 9001 ...
[Server@3a7b503d]: [Thread[main,5,main]]: checkRunning(false) entered
[Server@3a7b503d]: [Thread[main,5,main]]: checkRunning(false) exited
[Server@3a7b503d]: [Thread[main,5,main]]: setDatabaseName(0,webgoat)
[Server@3a7b503d]: [Thread[main,5,main]]: checkRunning(false) entered
[Server@3a7b503d]: [Thread[main,5,main]]: checkRunning(false) exited
[Server@3a7b503d]: [Thread[main,5,main]]: setDatabasePath(0,C:\Users\User\.webgoat-8.2.2\data/webgoat)
```

四、輸入上述所設定的Port及Server網址

[WebGoat][http://localhost:8080/WebGoat]

五、心得

其實我在做這個練習的過程中花最多時間的就是安裝WebGoat，來來回回應該就花了兩天的時間，雖然是斷斷續續的但其實不知不覺就花了好幾個小時，原因大致分為：

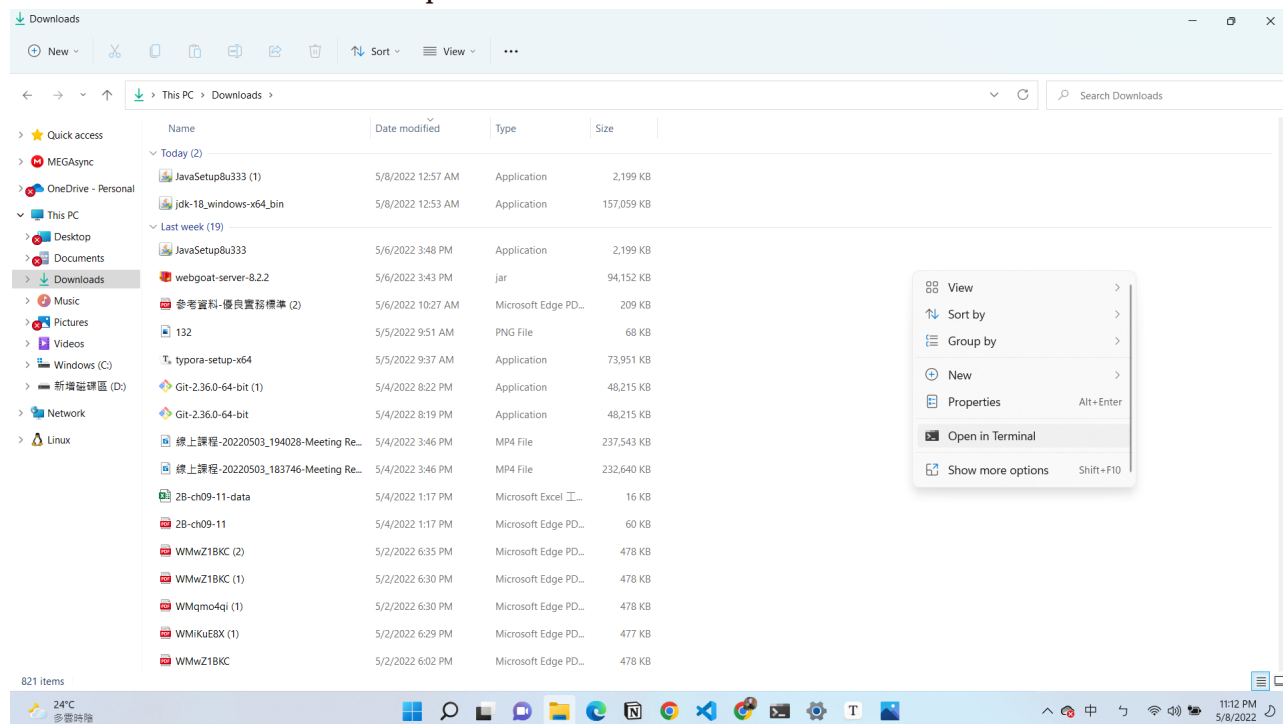
1. 第一次自己使用這種 *Command Prompt* 的介面安裝程式
2. 找錯方向

1. 沒有自己使用 **Command Prompt** 安裝程式的經驗

雖然看似很蠢，但我覺得沒有相關使用經驗，同時又沒有人教的時候，真的會犯一些看似很低級的錯誤，因此這邊提供一些淺見給一些毫無經驗的人

要開 **Windows Powershell** 去做安裝

找到你下載的路徑右鍵點選 **Open in Terminal** ，一般來說會在**Downloads**



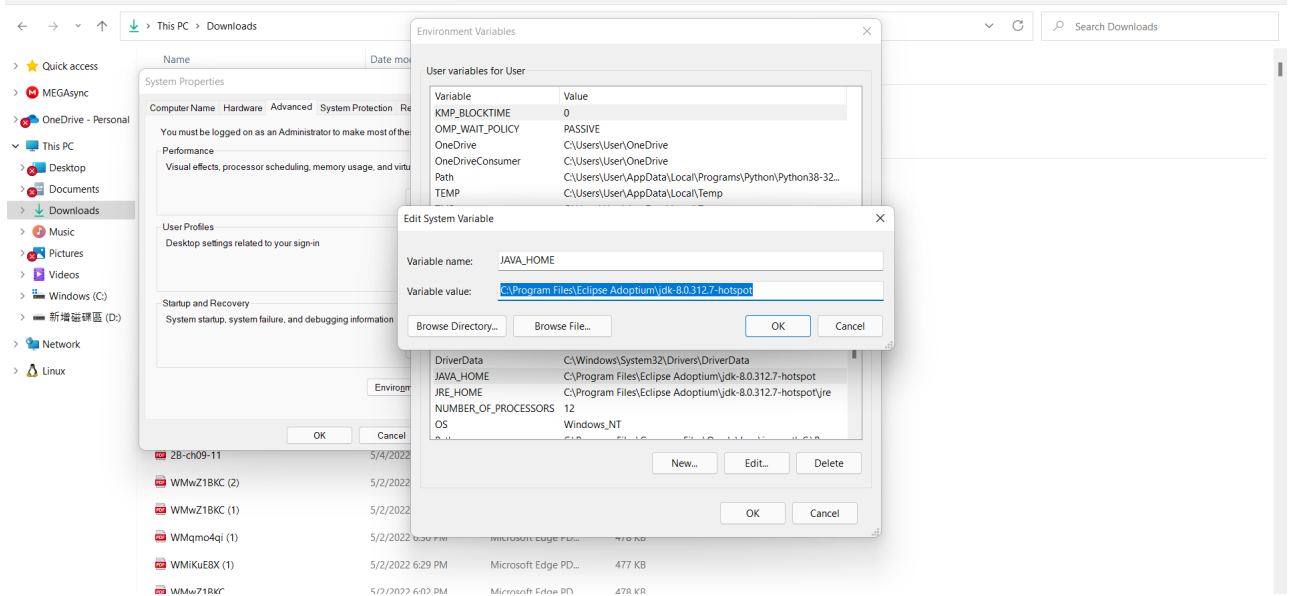
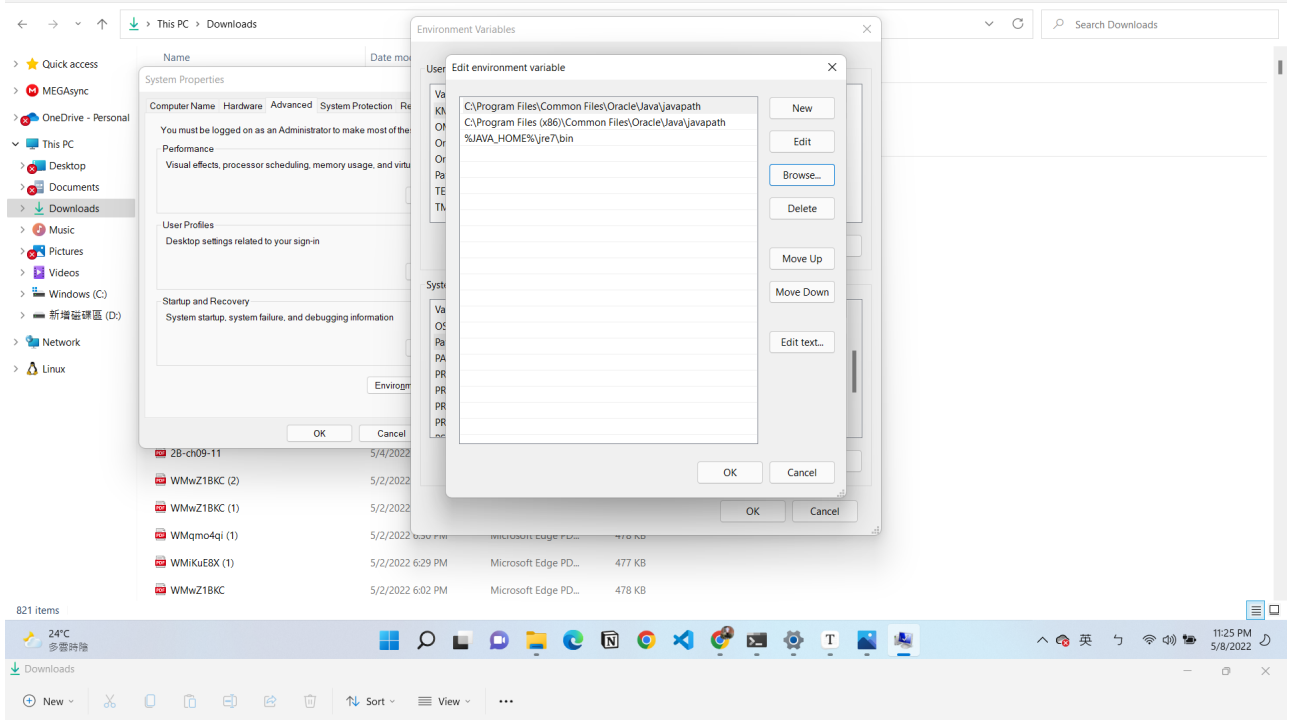
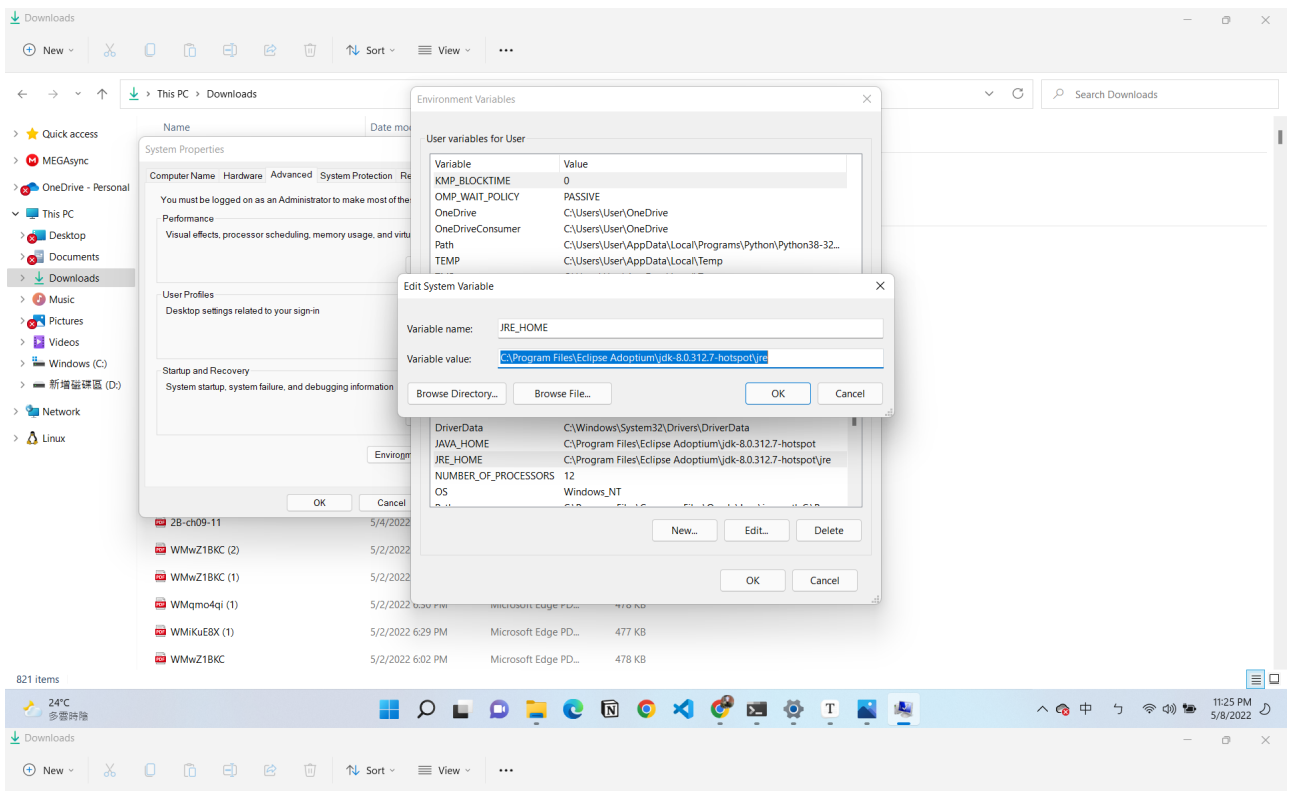
廣泛閱讀找資料很重要

盡最大的努力從GitHub、Medium等等網站去找學習資源，問人是很好的方法，從小到大我們都被鼓勵有問題就應該去問，然而並不是隨時都有人可以問，因此在現在這個網路資源豐富的時代，我們其實應該盡可能去找資料，訓練自己獨立解決問題，從中可以提升你兩個能力：

1. 下關鍵字字的準確度
2. 閱讀能力
3. 讀懂電腦回傳給你哪些錯誤

2. 找錯方向

在找錯誤的過程中，曾經有一度以為是環境變數的問題，隨然現在還不確定是不是因為環境變數，但從錯誤中也學到另一個看問題的角度，可能未來有相關問題的時候就會把環境變數列為其中一個需要注意的要素。



821 Items

24°C
多雲時晴

