**資安學習筆記**

1. **WebGoat**

WebGoat是一個OWASP用來演示web漏洞實驗的應用程序，用來說明web應用中存在的安全漏洞。

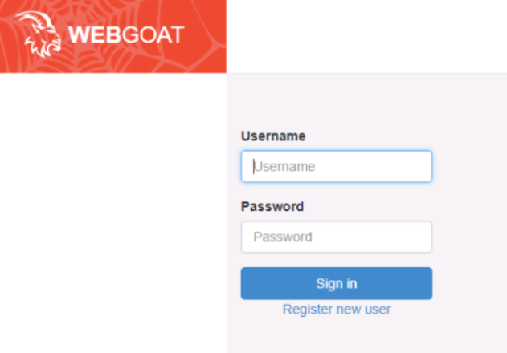
WebGoat運行在帶有java虛擬機的平台之上，當前提供的訓練課程有30多個。其中包括：跨站點腳本攻擊、訪問控制、線程安全、操作隱藏字段、操縱參數、字符串型SQL注入、web服務、危險的HTML註釋等等，還有其他很多我不知道的東西(冏)。

**安裝與啟動**

(reference : https://pjchender.dev/internet/is-note-webgoat/)

(reference : https://www.kjnotes.com/devtools/35)

1. 安裝Java JDK
2. 下載webgoat-server ( webwolf也可在此下載)
3. 透過終端機安裝 webgoat
4. 啟動 webgoat server
5. 啟動 webwolf server

 正常來說照著做最後成功的畫面



失敗.jpg

**心得：**

老師上課時講得滿有趣的，可惜當時無法跟著一起操作(搭車中，只記得操作時需要記得段開網路，不然很危險)，回到家後不知為何一直卡在安裝步驟(很懊惱)，只好自己上網查資料@@

Windows Powershell的操作似乎也不行，問同學對方很好心的提供我很多網站(但還是不大OK)，範例演練也不太懂，只能跟一步算一步，老師講得很好但自己上課能聽懂的似乎真的滿有限的，只希望未來課程能更好的理解上課內容。謝謝~

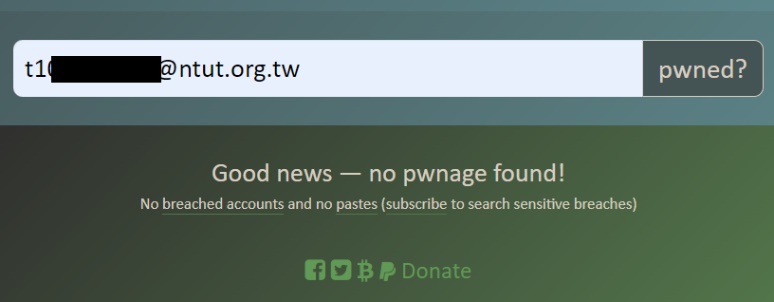
1. **Account Auditing**

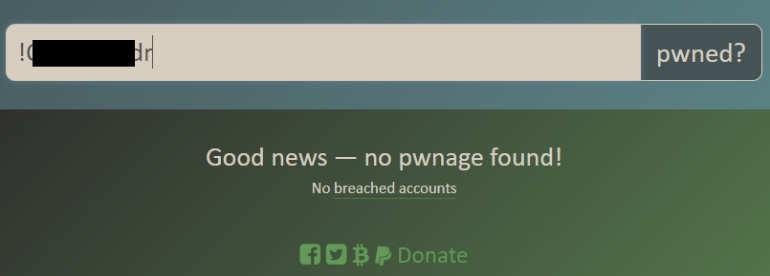
(reference : https://www.businesstoday.com.tw/article/category/80392/post/201808070017/)

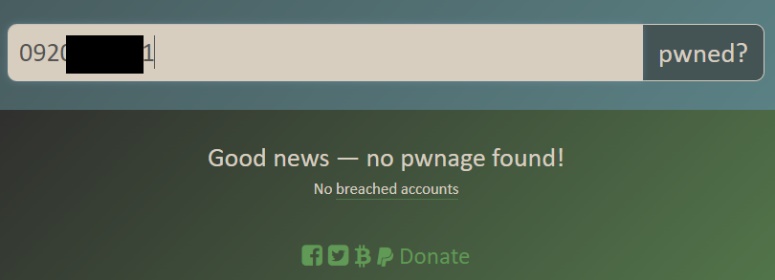
用這個網站可以查詢電子郵件地址或密碼是否已成為已知的洩露數據。感覺很實用的網站(或者該說是目前上課到現在我最懂在幹嘛的東西，汗)

網址：https://haveibeenpwned.com/

**實測：**

 學校的gmail信箱

 常用密碼

 手機號碼

**心得：**

目前是看起來都滿安全的，其實滿意外的，畢竟現在個資洩漏新聞這麼多，還以為早就曝露光光了@@。

1. **temp**