替黑箱分析工具加入 X 光技術

原文網址：

http://blog.fortify.com/blog/2011/06/27/Adding-X-Ray-technology-to-black-box-analysis-tools-Part-1

http://blog.fortify.com/blog/2011/08/04/Adding-X-Ray-technology-to-black-box-analysis-tools-Part-2

黑箱分析工具（例如 HP 的 WebInspect，以下簡稱 WI）會根據 Web 伺服器回傳的回應進行分析，以便評估 Web 應用程式遭受攻擊行為的影響。然而，在缺乏對 Web 應用程式服務器端狀態充分了解的狀況下，WI 只能在應用程式回應的內容與傳送給它的攻擊之間的差異，推測出關連性。事實上，具備正確錯誤處理的 Web 伺服器或 Web 應用程式，簡直是不可能讓黑箱分析工具找出絲毫的弱點。那我們要如何克服此一限制呢？

Fortify SecurityScope（簡稱 SS）可以安裝在 Web 應用程式伺服器上，觀察部署在其上 Web 應用程式的執行，比方說，每個呼叫資料庫查詢的 API 都可以被檢查到。這讓 SS 深入洞察 Web 應用程式的行為，這正是 WI 所欠缺的部分，從而使 SS 更精確且成功地報告出 WI 所無法報出的弱點。此外，WI 可以善用 SS 來瞭解特定攻擊的意圖。SS 可使用此資訊，來確認 WI 打算藉由這種攻擊行動的成功執行與否。這會隱藏在 WI 與 SS 之間的溝通管道，將使得檢測結果更加準確！

讓我們來看看，WI 與 SS 之間的互動流程。首先，WI 會送出 http://web/index?name=a' or '1'='1 的攻擊請求給 Web 伺服器。此外，WI 會通知 SS 它試圖利用 ' or '1'='1 進行 SQL 隱碼攻擊。

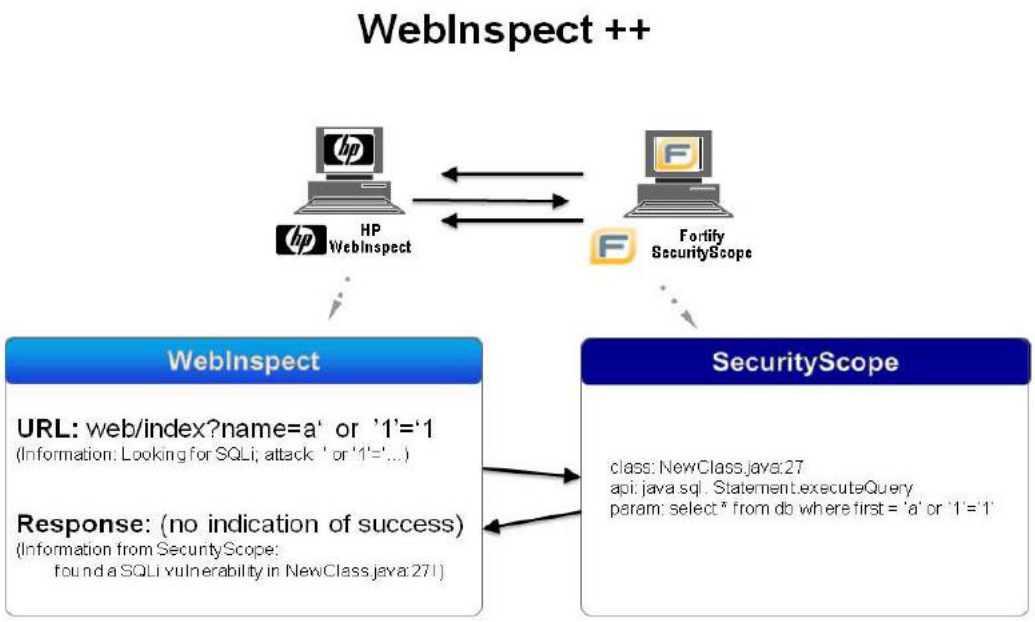
接著，SecurityScope 檢查執行的 java.sql. Statement.executeQuery() 程式碼，它所傳入的參數如下：

select * from db where first = 'a' or '1'='1' (NewClass.java:27)

不論所傳回的回應串流是什麼，透過 WI 與 SS 之間的溝通管道，WI 都會知道這個漏洞。

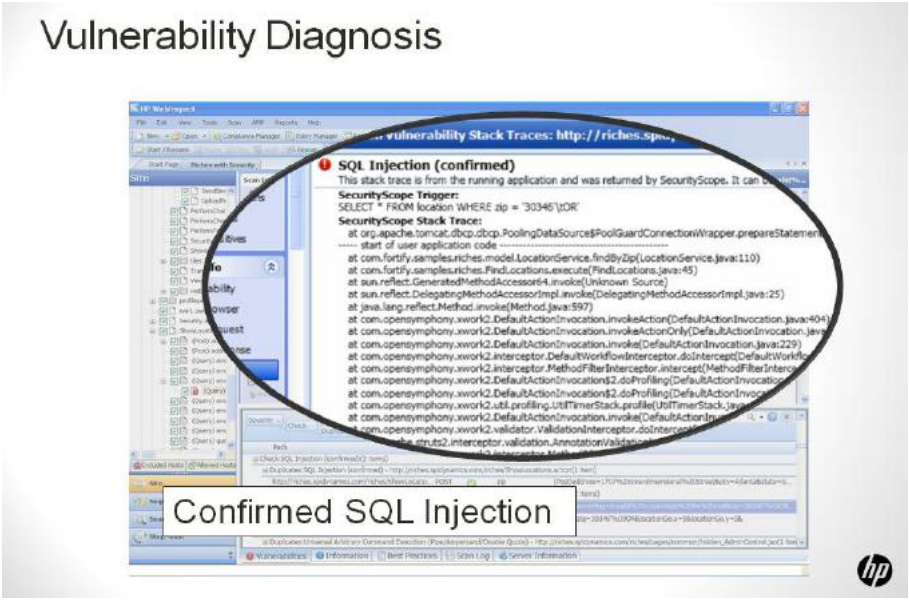
GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

WebInspect 與 SecurrityScope 合作無間



WebInspect 確認弱點

此種技術大大地改善隱碼錯誤的結果，這些隱碼錯誤包含：SQL 隱碼、跨網站指令碼（Cross-site scripting，簡稱為 XSS）、命令隱碼（Command Injection）、本機檔案加入（Local File Inclusion，簡稱 LFI）、遠端檔案加入（Remote File Inclusion，縮寫成 RFI）、以及檔案上傳。

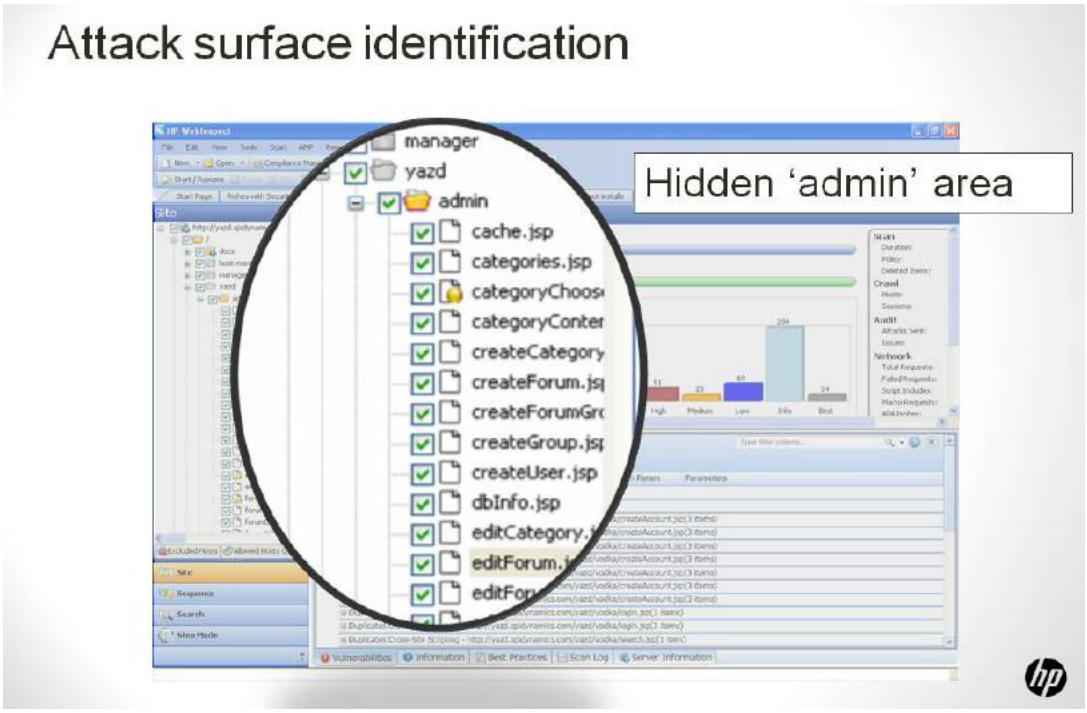


GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

藉由導入隱藏於 HP WebInspect 與 Fortify SecurityScope 之間的溝通管道，可以找出更精確的結果。等一下，別急，還有其他的呢。當此種溝通管道存在時，改善找到「隱藏」網頁中的問題涵蓋度，是微不足道的。SS 可以引領 WI，來找出那些高階網頁爬蟲（Web Crawler）難以或不可能找到的每個項目。以前不能被滲透的網頁，現在可以被滲透。以前被造訪過的網頁，現在可以更深入地滲透，透過 WI 與 SS 的溝通管道，讓黑箱分析隱藏或難以找到的參數。在足夠的時間內，蓄意的攻擊者可以找出這些難以找到的連結與參數。現在，他們被簡化成黑箱分析與安全測試工具。舉例來說，以前沒被發現到管理者網頁，現在將被進行攻擊：

攻擊表面確認

藉由 WI 與 SS 的溝通管道可以更快速獲得穩固的程式碼，這是另外一個好處。身為資安人員，與開發團隊討論黑箱分析的結果，是相當令人沮喪的。所有開發人員想聽到的是，如何修復他們的軟體；而所有的資安人員可以提供的卻是如何攻破軟體。由於 SS 可以觀察執行在伺服器上的程式碼，它可以將詳盡的入侵點（Point-of-exploit）傳回給黑箱分析工具。詳細的原始層級資料可以被彙整成固定的報告，此舉得以讓開發人員據以提出因應之道。



原始層級資料

事實上，在這個應用本身，多個結果擁有單一入侵點並非罕見。因此，由觀察員所提供的資訊可以被用來分組並複製結果，將使得結果更加可行。

GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

Actionable Details