建立國軍網頁資安攻擊事件分類模式之研究

作者簡介

廖秀華上尉，指職軍官班92年班、國防大學理工學院98年班資訊科學所；曾任排長、教官、隊長，現任職於通信電子資訊學校學員生總隊部學生大隊一中隊。

提要

一、網頁攻擊方式隨資訊技術之進步而不斷變化，攻擊者可從任何一個地方針對國軍網頁漏洞進行攻擊，使管理者無法即時管控。

二、針對跨站腳本或資料隱碼等類似攻擊並無一套完整的防制方法，目前僅能針對每個攻擊進行分析及分類。

三、提出分類法的目的除使國軍官兵更瞭解攻擊事件發生的原因外，亦可針對相關軟體弱點進行修補或風險移轉，更利於發現新的攻擊手法時，快速尋找類似攻擊的前案，並參考其解決方案，以期縮短事件處置時間及減低其損失及風險。

關鍵詞：電腦攻擊、網路攻擊、網頁攻擊、分類法

前　言

鑑於國防部電腦緊急應變處理中心（CERT）的事件回報數逐年增加且攻擊技術也日趨複雜，以致不同的攻擊者使用不同的攻擊方式或工具，造成了不同的影響或損害；也可能進一步針對不同的目標做不同類型的攻擊。為能使國軍官兵更瞭解攻擊行為所使用的技術，本文將綜整早期較具重要性的分類法，並參酌新科技方法，整理並歸納出符於現況的分類法。接著則針對開放網頁軟體安全計畫組織（OWASP）[1]於2009年針對目前網路應用攻擊型態最常見的兩大網頁安全性問題（即跨站腳本攻擊和資料隱碼攻擊）進行探討，並套用新的分類標準，以驗證此分類法的可行性；驗證的結果將有助於國軍網路攻擊事件之防範。

背景知識

分類法是知識和部分相關定義分開的一種分類組合。而分類是區分和排序的一種程序，為使分類法能夠更完整、合理和有用，將以先前的理論為基礎來發展一個明確且有效的分類法。

Howard於1998年認為良好的分類法應符合下列六項必要條件[2]：

一、互斥：每個攻擊只能分在一個類別裡，不可重疊。

二、詳盡：可包含所有的可能性。

三、清楚：須清楚且明確的，以便不管是誰分類還是能清楚瞭解。

四、可重複使用：此分類法可重複的使用。

五、接受：須符合邏輯且憑直覺就可以得知的分類法，才能獲得大家的認可。

六、有用：在探索的領域裡能藉由使用此分類，而獲得更深刻的理解。

Lough於2001年則是認為好的分類法須符合的條件如下[3]：

一、接受：分類法要讓大家可以認可。

二、可理解：分類法要讓資訊安全領域的專業人員與非專業人員都很容易瞭解。

三、完整／耗盡（包含全部）：要包含所有可能的攻擊，每個攻擊都能分到相對應的類別中。

四、決定論：清楚定義分類所需的步驟。

五、互斥：每一個攻擊只能分到一個類別中。

六、可重複使用：分類法可以被重複的使用。

七、使用相同的專業術語：使用一些已經存在於其他分類法中的術語，才能讓人很容易上手，並且不會混淆。

八、定義術語的意義：不要讓術語的意義混淆。

九、清楚（不會含糊不清）：每一個

1　http://owasp.org.tw/blog/2007/05/owasp2007webowasp.html

2　Ivan Krsul,"A Common Language for Computer Security Incidents, " Purdue University, West Lafayette,U.S.A, 1997, pp. 1～23.

3　Simon Hansman, Ray Hunt, "A taxonomy of network and computer attacks," Computer Security,No.24, Elsevier,June 2004 ,pp.1～13.

分類的類別都要有清楚定義。

十、有幫助：一個有幫助的分類法能被資訊安全產業所使用。

現有分類法

藉由分類法來分析攻擊者所使用的工具、執行過程及影響得知可能遭受的攻擊方式和目的，不僅可供使用者或管理者在最短的時效做最快速的事件處置，也可將分析事件的來源和過程做成資料庫，以便管理者日後可對類似的攻擊做相同快速的反應處置，而在縮短處理時效之際，便可減少金錢上的重大損失。以下將分別介紹幾種早期較具重要性的分類法：

一、霍華（Howard）分類法

霍華於1997年針對電腦和網路攻擊所提出的分類法以攻擊過程為主，主要是考慮到攻擊者的行動方式與目的（如圖一）。

其分類法將攻擊分成五個階段：

㈠攻擊者：意指發起攻擊的攻擊者類型，例如駭客。

㈡工具：意指攻擊者獲得存取所使用的工具，例如駭客（攻擊者）是藉由語法或程式錯誤進行攻擊。

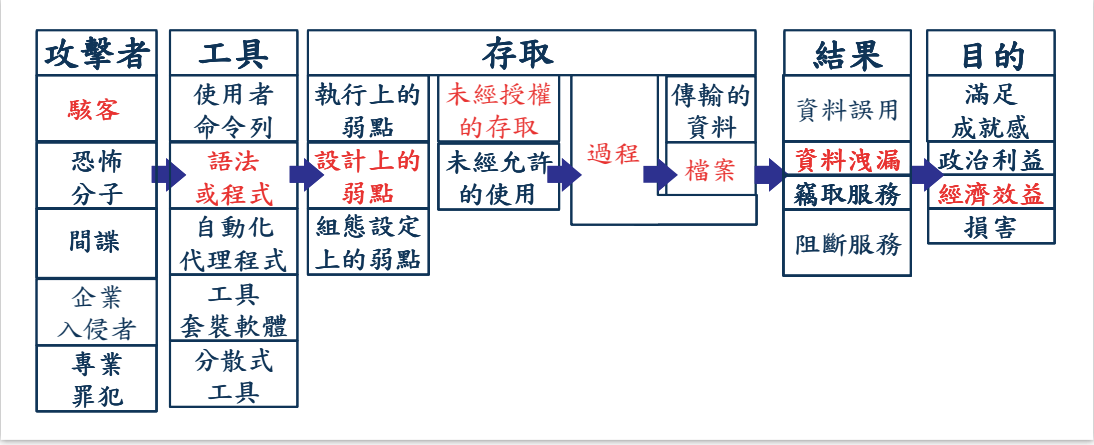
㈢存取：意指透過執行上、設計上或結構上的弱點獲得存取，例如駭客藉由程式設計上的弱點針對檔案進行未經授權的存取動作。

㈣結果：意指一旦獲得存取就可達到毀損或洩露資訊的目的，例如駭客針對特定檔案進行不當存取而造成資料洩漏。

㈤目的：意指攻擊者的目的可能具有金錢上的利益，例如駭客攻擊的目的可能是為了存取銀行裡的個人帳號資料。

二、古納羅（Gonzalo Alvarez）和索博丹（Slobodan Petrovic）分類法

古納羅和索博丹於2003年針對網頁攻擊提出另一種分類法。根據他們多年來的分析觀察，發現超文件傳輸協定（HTTP）及超文件傳輸安全協定（HTTPS）目前已變成攻擊者做為網頁攻擊或瀏覽器攻擊的主要威脅，甚至也注意到大部分的網頁攻擊其實都是針對網頁伺服器。所以他們將網頁攻擊分類法分成攻擊點、利用的弱點、針對的服務、執行



圖一　霍華以攻擊過程為主的分類法

資料來源：Howard, J. D., and Longstaff, T. A.,"A Common Language for Computer Security Incidents, " Sandia National Laboratories, New Mexico, California, 1997, pp.1～25.

動作、輸入長度、超文件傳輸協定標頭、超文件傳輸協定的請求動作、針對的目標、影響範圍、獲得權限等十個階段（如圖二）[4]，紅色字體的部分則是利用此分類法將跨站腳本攻擊方式分類後的結果。

其分類法將攻擊分成十個階段：

㈠攻擊點：攻擊的起始端。

㈡利用的弱點：此攻擊所運用的弱點。

㈢受到的威脅：影響資料機密性、完整性或系統可用性的攻擊。

㈣執行動作：藉由網頁伺服器產生的弱點，以致攻擊時所執行的動作造成了威脅或損害。

㈤輸入長度：用戶端向伺服器端提出超文件傳輸協定請求時，所傳送的參數長度。

㈥超文件傳輸協定標頭：為用戶端提出請求後伺服器端所回應的訊息內容。

㈦超文件傳輸協定的請求動作：為用戶端向伺服器端提出請求所執行的動作。

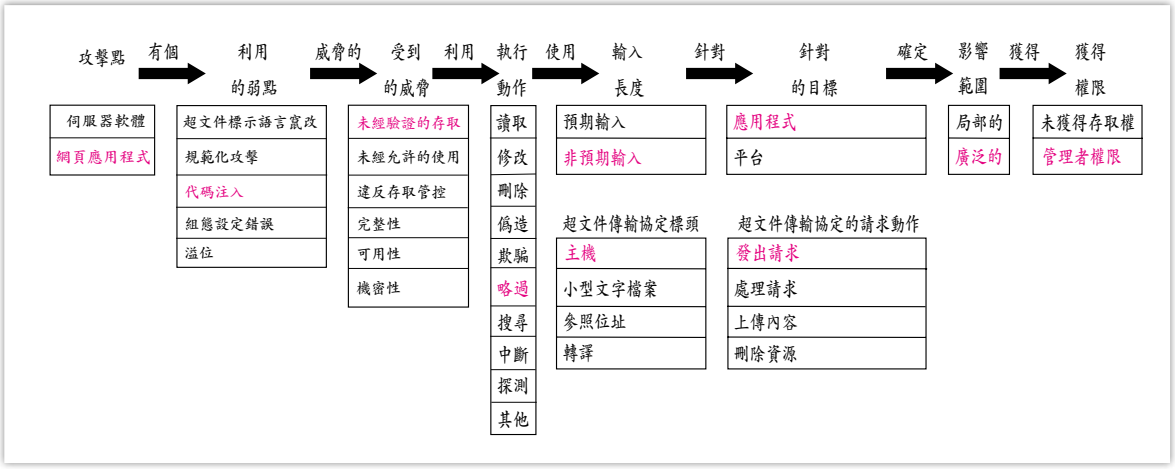
㈧針對的目標：意指攻擊目標為何。

㈨影響範圍：攻擊網頁伺服器後所造成的影響是局部的（例如個人使用者）或是廣泛的（例如所有瀏覽此網頁的使用者）。

㈩獲得權限：攻擊成功後所獲得的使用權限為何。

三、賽門（Simon Hansman）和雷（Ray Hunt）分類法

賽門和雷是認為分類的詳細描述對攻擊分類是有幫助的，而霍華的分類法，就是針對攻擊過程提供了一個好的概要敘述，但是為了避免每天檢視電腦及網路所面臨的攻擊類型，而且紅色警戒蠕蟲很難使用霍華的分類法去分類，於是賽門和雷



圖二　古納羅和索博丹以網頁攻擊過程為主的分類法

資料來源：Alvarez, G., and Petrovic, S.,"A new taxonomy of Web attacks suitable for efficient encoding," Computer & Security, volume 22, Issue 5, July 2003, pp.435～449.

4　Alvarez, G., and Petrovic, S.,"A new taxonomy of Web attacks suitable for efficient encoding," Computer & Security,volume 22, Issue 5, July, 2003, pp.435～449.

於2005年提出可明確將蠕蟲、病毒和緩衝區溢位等攻擊方式分類的分類法。主要目的是對固定的攻擊方式提供有用且實際的分類。不但容易將攻擊方式歸到各個類別中，也有助於瞭解攻擊相關資訊（如表一）。

其分類法是從四個方向來看，所提出的分類法主要如下：

㈠攻擊：意指攻擊方式名稱，例如以紅色代碼病毒為攻擊方式。

㈡攻擊方式：意指以何種攻擊方式，例如以文件感染病毒為攻擊方式。

㈢攻擊目標：意指被攻擊的目標，例如紅色代碼病毒可藉由作業系統未修補的漏洞進行攻擊。

㈣利用的弱點：意指此攻擊所運用的弱點，例如紅色代碼病毒藉由作業系統未修補的漏洞執行攻擊者所下達的任何指令。

㈤影響：意指攻擊成功後所造成的影響為何，例如以紅色代碼病毒為攻擊方式，將可能造成文件損壞。

㈥其他：意指遭受攻擊後所造成的其他影響，例如損害、花費、繁殖、防禦。其中損害意指攻擊後造成的所有損害，花費意指回復遭受攻擊前的狀態所要花費的金錢，繁殖意指攻擊所散布的速度，防禦則是指對這個攻擊所做的防禦。

四、瑪麗亞（Maria Kjaerland）分類法

瑪麗亞於2006年提出的分類法是依據電腦緊急應變處理協調中心（CERT/CC）的回報事件做分析，並將攻擊事件的來源、攻擊時所使用的方法、攻擊後所受的影響，以及事件的受害者四個方面和霍華依據攻擊者、工具、存取、結果和目的等五個階段相比較（如表二），可使管

表一　賽門和雷提出的攻擊數量分類結果

攻擊	攻擊方式	攻擊目標	利用的弱點	影響
Blaster病毒	網路蠕蟲	Windows NT 4.0, 2000 XP, Server 2003等作業系統	允許遠端攻擊者執行任意字串	拒絕服務攻擊
紅色代碼病毒	文件感染病毒	Windows 95.98作業系統及IIS 4,5,6.0測試版等網際網路資訊服務	允許遠端攻擊者執行任意指令	訊息文件損壞
使用John the Ripper密碼破解工具	猜測密碼攻擊	Unix作業系統及Windows NT, 2000, XP	系統配置錯誤	緩衝區溢位及拒絕服務攻擊
妳坦蠕蟲	郵件蠕蟲	網頁瀏覽器5.5 SP1及早期的5.01 SP2	允許遠端攻擊者執行任意指令的編碼	訊息文件損壞
Sobig.F蠕蟲	郵件蠕蟲	資料庫管理系統(SQL Server 2000)	允許遠端攻擊者執行拒絕服務攻擊或執行任意代碼	緩衝區溢位及拒絕服務攻擊

資料來源：Hansman, S., and Hunt, R.,"A taxonomy of network and computer attacks," Computer & Security, volume 24, Issue 1, February 2005, pp.31～43.

理者可以更瞭解攻擊者類型、各種攻擊方式，以及不同的來源攻擊所造成的各種影響。

其分類法主要從四個方向來看：

㈠事件的來源。

㈡攻擊者執行攻擊所使用的方法。

㈢攻擊後所受的影響。

㈣事件的受害者。

綜整上述的分類法，可藉由表三看出各個分類法的優缺點。

新分類法建立之流程

參考前述四種分類法及分類原則，並檢驗上述四種分類法是否符合分類法原

表二　瑪麗亞提出的分類過程

事件的來源	攻擊者執行攻擊所使用的方法	攻擊後所受的影響	事件的受害者
商業網域 政府網域 教育網域 使用者 未知	濫用資源 使用者洩漏 社交工程 病毒 網頁漏洞 木馬 蠕蟲 偵察 拒絕服務攻擊	破壞 扭曲 毀壞 洩漏 未知	商業網域 政府網域

資料來源：Kjaerland, M.,"A taxonomy and comparison of computer security incidents from the commercial and government sectors," Computer & Security, volume 25, Issue 7, October 2006, pp.522～538.

表三　分類法比較結果

	霍華分類法	賽門和雷分類法	瑪麗亞分類法	古納羅和索博丹分類法
分類方式	將攻擊分成五個階段： 1.攻擊者 2.工具 3.存取 4.結果 5.目的	主要分成四個方向： 1.攻擊方式 2.攻擊目標 3.利用的弱點 4.影響 5.其他	主要分成四個方面： 1.攻擊事件的來源 2.攻擊者執行攻擊所使用的方法 3.攻擊後所受的影響 4.事件的受害者	主要分成十個階段： 1.攻擊點 2.利用的弱點 3.受到的威脅 4.執行動作 5.輸入長度 6.超文件傳輸協定標頭 7.超文件傳輸協定的請求動作 8.針對的目標 9.影響範圍 10.獲得權限
優點	著重在攻擊的動機與目的	容易將攻擊歸到各個類別中	可瞭解攻擊者類型、各種攻擊方式，以及不一樣的攻擊來源所造成的影響	可幫助開發人員或程式設計師更瞭解攻擊事件並建立更安全的網頁應用程式

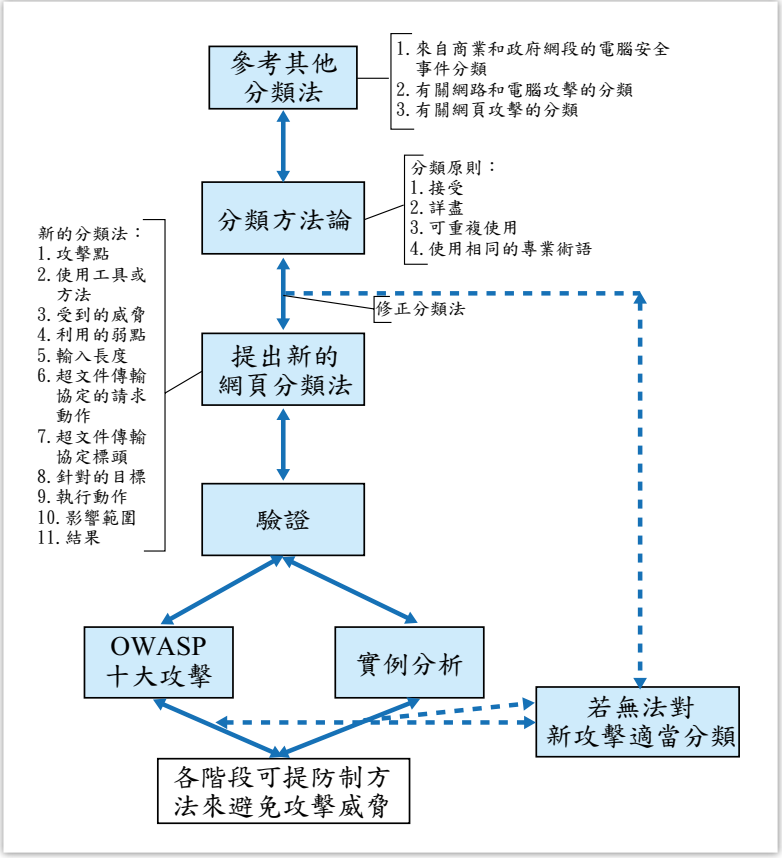
缺點	1.無法預測下一步執行動作 2.結果分類較不完整	1.無法分析和描述混合式攻擊 2.無法推斷出可能的攻擊情境	1.依據電腦緊急應變處理小組分類事件做分析，如無回報事件，準確性將降低 2.無法預測下一步執行動作	1.無法得知攻擊時所使用的方式 2.受攻擊的目標和結果分類較不完整
實務上的貢獻	可以清楚的顯示不同的目標如何遭受不同的來源攻擊及影響	1.清楚瞭解分類及攻擊相關資訊 2.清楚描述被攻擊的目標	透過多維排列和最小空間分析技術去比較商業網域和政府網域網路事件報告中的差異	以防火牆及入侵偵測系統為例，可藉由此分類法減少記錄檔多餘的種類敘述，增加儲存空間的容量

資料來源：作者整理

則，再依分類原則對分類方法做修訂，以建立新分類法（如圖三）。提出分類法後，會再以OWASP十大攻擊（包含注入攻擊、跨站腳本攻擊、遭破壞的鑑別和連線管理、不安全的物件參考、跨網站冒名請求、網站安全組態不當設定、未適當限制的URL存取、未驗證的網頁重新導向、不安全的加密儲存、不安全的傳輸防護）中的前兩大攻擊和實際案例來驗證此分類法的可行性，為的就是能夠針對各階段分別提出防制方法，以避免系統遭受攻擊的威脅。若有新的攻擊事件無法分類時，將持續修正此分類法。

一、新的分類標準

綜整霍華於1997年及洛克於2001年所提出的經驗，在此作者認為針對資訊網頁攻擊的分類應不具互斥性，如此才能顯現特徵的重要性。有部分的單一事件在描述時可能會被判讀成兩種分類。例如關聯式資料庫管理系統（MySQL）命令列模式存在「超文件標示語言（HTML）語法注射」弱點的事件裡，因為關聯式資料庫管理系統命令列模式無法適當處理超文件標示語言語法所使用的特殊字元，而導致攻擊者可任意注入超文件標示語言語法或是爪哇腳本語言



圖三　新分類法建立的流程

資料來源：作者繪製

（JavaScript），使得個人資料遭竊取。此案例則可能被分類到「輸入驗證攻擊類別」或是「資料隱碼（SQL Injection）攻擊類別」裡，此時如果分類法具有互斥性，則無法驗證往後分類系統的容錯性，並使得攻擊過程或攻擊後的結果等特徵必須被更改。所以本研究提出適用於網頁攻擊的分類法至少應具備以下原則：

㈠接受：須符合邏輯且憑直覺就可以得知的分類法才能獲得大家的認可。

㈡詳盡：可包含所有攻擊的可能性。

㈢可重複使用：無論是由誰分類，分類法都可以被重複使用。

㈣使用相同的專業術語：使用已經存在於其他分類法中的術語，並清楚明確的表示；一方面可使初學者或管理者容易分類，一方面也能清楚瞭解，較不易混淆。

二、新的分類法

以霍華的分類過程為基礎，將上述分類法整合成圖四，紅字部分為額外新增的項目，以符合上述的分類必要條件。

針對此分類表裡的圈圈部分乃為額外增加的類別項目，而各個主要類別項目的定義則是參考自古納羅和索博丹以及霍華所針對的固定攻擊方式和網頁攻擊。其類別項目定義如下：

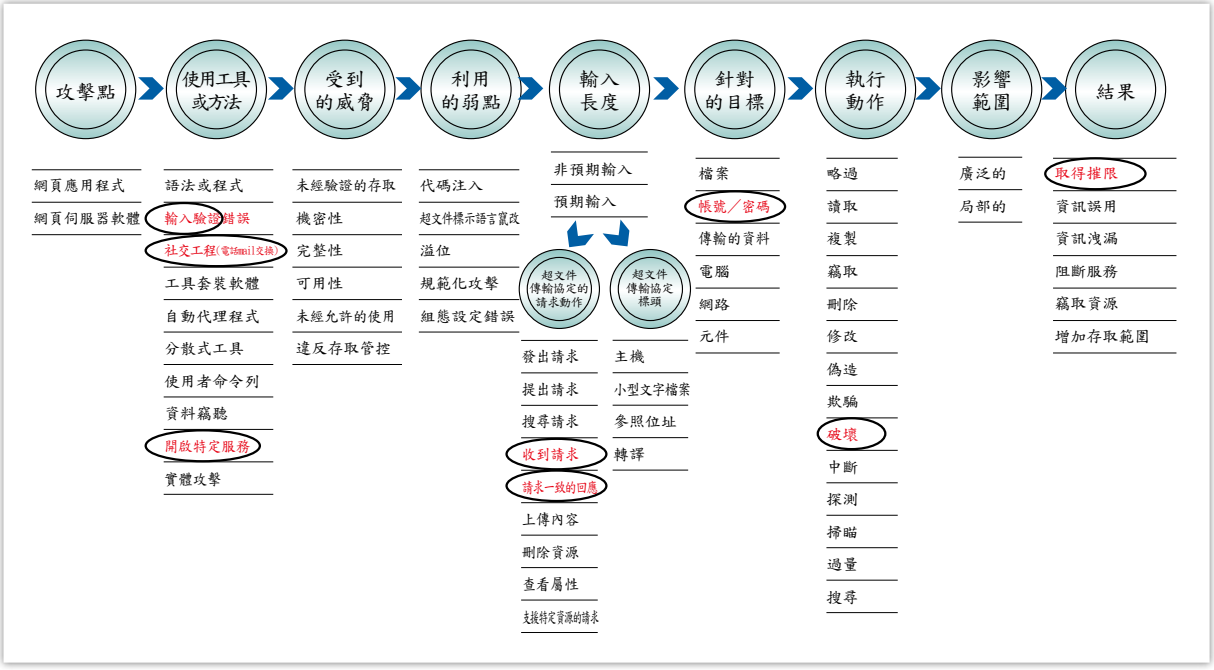
㈠攻擊點：攻擊的起始端。

㈡使用工具或方法：藉由電腦或網路產生的弱點，進而利用一些工具或方法進行存取。

㈢受到的威脅：影響資料機密性、完整性或系統可用性的攻擊。

㈣利用的弱點：此攻擊所運用的弱點為何。

㈤輸入長度：用戶端向伺服器端提出超文件傳輸協定請求時，所傳送的參數長度。



圖四　分類法整合表

資料來源：作者整理

㈥超文件傳輸協定的請求動作：為用戶端向伺服器端提出請求所執行的動作。

㈦超文件傳輸協定標頭：為用戶端提出請求後伺服器端所回應的訊息內容。

㈧針對的目標：意指攻擊目標為何。

㈨執行動作：藉由網頁伺服器產生的弱點，使攻擊時所執行的動作造成了威脅或損害。

㈩影響範圍：攻擊網頁伺服器後所造成的影響是局部的（例如伺服主機）或是廣泛的（例如所有瀏覽此網頁的使用者）。

㈠㈠結果：攻擊成功後所造成的損失為何。

三、驗證實驗

本研究驗證方式是藉由國軍網路上的網站來實施驗證，該網站上的系統組合如表四。此類組合共有715個漏洞，而漏洞掃瞄則是以Acunetix v6.5為工具。此工具可掃瞄下列5大類的漏洞：

㈠可自動偵測跨網站程式碼。

㈡注入結構化查詢語言（SQL）程式碼。

㈢檔案引入（File Inclusion）。

㈣目錄遊走（Directory Traversal）。

㈤搜尋弱點權限目錄。

利用此掃瞄工具對網站掃瞄可能潛藏的「跨站腳本攻擊」和「資料隱碼攻擊」漏洞，再從超文件傳輸協定請求和回應訊息中藉由關鍵字來分類，以驗證是否有攻擊漏洞。

㈠將跨站腳本攻擊漏洞訊息套用新的分類標準

所謂跨站腳本攻擊是藉由動態網頁的特性，利用開發者沒有嚴格限制回傳參數及過濾輸入之特殊字元，將具攻擊性的JavaScript、VB Script、ActiveX，或flash程式碼植入所進行的攻擊。表五是針對跨站腳本攻擊語法所做的分類結果，此處只擷取該實際運作網站上5個案例的分類結果。第1個案例即說明著被掃瞄的網站可能遭受攻擊的網頁為.../mis/c_timetable/query/query_by_tunit_rep.asp，只要在超文件傳輸協定請求動作（POST）的某個參數（teachunit），加上某段程式碼（1>"><ScRiPt%20%0d%0a>alert（472977287221）%3B</ScRiPt>）後，便有可能造成跨站腳本攻擊。針對此案例分類後的結果為：

1.因遭受攻擊的是.../mis/c_timetable/query/query_by_tunit_rep.asp網頁，所以判斷「攻擊點」為「網頁應用程式」。

2.此漏洞只要植入某段程式碼，便有可能造成跨站腳本攻擊（XSS）。所以判斷「使用工具或方法」為「語法或程式」。但也有可能是因為程式開發者沒有嚴格限制回傳參數及過濾輸入之特殊字元，所以也可以判斷為「輸入驗證錯誤」的方式。另外也可藉由「社交工程」的方式間接造成跨站腳本攻擊，或是利用「工具套裝軟體」等方式植入惡意程式碼。

表四　案例網站基本資料列表

Target:http://www.xxx.mil.tw/
Server:Microsoft-IIS/6.0
Operating system:Windows
Web Server:Microsoft-IIS/6.0
Technologies:ASP, ASP. NET, PHP, Perl, mod_ssl, mod_perl,
Mod_python, OpenSSL, FrontPage, JRun, Ruby
Open ports:21/ftp, 80/http

資料來源：作者整理

表五　跨站腳本攻擊語法分類表

主要被影響的網頁：This vulnerability affects /**mis/c_timetable/query/query_by_tunit_rep.asp**
1.攻擊語法： The POST variable *teachunit* has been set to *1>″ ><ScRiPt%20%0d%0a>alert(472977287221)%3B</ScRiPt>*
攻擊事件分類： 語法或程式　機密性　Trnaslate 電腦　竊取　阻斷服務 社交工程　可用性　溢位　Referer 傳輸的資料 複製　資訊洩漏 輸入驗證錯誤　完整性　HTML竄改　Hosst 帳號　讀取　資訊誤用 網頁應用程式→工具套裝軟體→未經授權的存取→代碼注入→　非預期輸入　→GET→ Cookie→檔案→　略過→ 廣泛的→ 取得權限
2.攻擊語法： The POST variable *teachunit* has been set to *1<ltextarea><ScRiPt%20%0d%0a>alert(472977287221)%3B</ScRiPt>*
攻擊事件分類： 語法或程式　機密性　Trnaslate 電腦　竊取　阻斷服務 社交工程　可用性　溢位　Referer 傳輸的資料 複製　資訊洩漏 輸入驗證錯誤　完整性　HTML竄改　Hosst 帳號　讀取　資訊誤用 網頁應用程式→工具套裝軟體→未經授權的存取→代碼注入→　非預期輸入　→GET→ Cookie→檔案→　略過→ 廣泛的→ 取得權限
3.攻擊語法： The POST variable *teachunit* has been set to *1<DIV+STYLE=″ width:expression(alert(474067287645)%3B″ >*
攻擊事件分類： 語法或程式　機密性　Trnaslate 電腦　竊取　阻斷服務 社交工程　可用性　溢位　Referer 傳輸的資料 複製　資訊洩漏 輸入驗證錯誤　完整性　HTML竄改　Hosst 帳號　讀取　資訊誤用 網頁應用程式→工具套裝軟體→未經授權的存取→代碼注入→　非預期輸入　→GET→ Cookie→檔案→　略過→ 廣泛的→ 取得權限
4.攻擊語法： The POST variable *teachunit* has been set to *1<ltitle><ScRiPt%20%0d%0a>alert(473897287576)%3B</ScRiPt>*
攻擊事件分類： 語法或程式　機密性　Trnaslate 電腦　竊取　阻斷服務 社交工程　可用性　溢位　Referer 傳輸的資料 複製　資訊洩漏 輸入驗證錯誤　完整性　HTML竄改　Hosst 帳號　讀取　資訊誤用 網頁應用程式→工具套裝軟體→未經授權的存取→代碼注入→　非預期輸入　→GET→ Cookie→檔案→　略過→ 廣泛的→ 取得權限
5.攻擊語法： The POST variable *teachunit* has been set to *email@some<ScRiPt%20%0d%0a>alert(473017287221)%3B</ScRiPt>Domain.com*
攻擊事件分類： 語法或程式　機密性　Trnaslate 電腦　竊取　阻斷服務 社交工程　可用性　溢位　Referer 傳輸的資料 複製　資訊洩漏 輸入驗證錯誤　完整性　HTML竄改　Hosst 帳號　讀取　資訊誤用 網頁應用程式→工具套裝軟體→未經授權的存取→代碼注入→　非預期輸入　→GET→ Cookie→檔案→　略過→ 廣泛的→ 取得權限

資料來源：作者整理

3.經過「使用工具或方法」的分類後，可判定系統潛藏著「未經授權存取」的威脅，也間接影響到資料的「機密性」、「完整性」及系統的「可用性」。

4.此漏洞所「利用的弱點」可以是「代碼注入」，但也有可能是藉由「超文件標示語言竄改」或「溢位」所造成的。

5.「輸入長度」則是以輸入的參數是否導致網頁被修改或使程式碼自動執行的部分來判斷，在此判斷為「非預期輸入」。

6.從超文件傳輸協定請求和回應訊息中可看出，用戶端向伺服器端所提出的「超文件傳輸協定的請求動作」為「請求

動作」。

7.由超文件傳輸協定請求和回應訊息中也可看出「超文件傳輸協定標頭」包含「主機」（Host）、「小型文字檔案」（Cookie）、「參照位址」（Referer）、「轉譯」（Translate）。

8.當攻擊者利用此漏洞登入系統後，「針對的目標」便有可能是重要的「檔案」、「帳號」或正在「傳輸的資料」，進而取得「電腦」的控制權限。

9.在此攻擊過程中，「執行的動作」可能是先「略過」驗證機制，然後「讀取」、「複製」或「竊取」重要檔案或帳號。

10.「影響的範圍」不單只限於此網頁而已，只要其他合法使用者在瀏覽此網頁時，不經意的執行了部分的惡意程式碼，也會跟著被植入惡意程式碼，甚至被間接的導向到惡意網站，屬於「廣泛的」影響範圍。

11.最後在「結果」的部分，攻擊者可能在「取得權限」後，便在未經允許的情況下使用了重要資訊或資源，此為「資訊誤用」及「竊取資源」，進而造成「資訊洩漏」。

㈡將資料隱碼攻擊漏洞訊息套用新的分類標準

所謂資料隱碼攻擊則是在輸入的字串之中夾帶SQL指令，在設計不良的程式當中忽略了檢查，因此這些被夾帶進去的指令就會被資料庫伺服器誤認為是正常的SQL指令而執行，這就是資料隱碼攻擊。在此針對資料隱碼攻擊語法所做的分類結果，列舉5個案例的分類結果於表六。第1個案例即說明著被掃瞄的網站可能遭受攻擊的網頁為.../mis/c_timetable/query/query_by_tunit_rep.asp，只要在超文件傳輸協定請求動作（POST）的某個參數（oneseven），加上某個特殊符號（'）後，便有可能造成資料隱碼攻擊，其餘的攻擊語法，以此類推。針對以上敘述，我們不但可以看出此分類法的優點就是能將所有的實際案例以分類的方式將攻擊過程描述出來，用於後續的防範，但缺點就在於人為判斷時的差異性。

四、防護措施

會產生跨站腳本攻擊和資料隱碼攻擊的主要原因，無非就是因為程式開發人員缺乏網頁安全性相關知識，所以在網頁程式撰寫時，無設計過濾檢測所要傳遞的參數或特殊字元的機制。如果開發人員能夠在使用者輸入欄位，針對特殊符號或字串加入過濾檢核的功能，便能夠阻擋此類的網站攻擊手法了。例如以本研究案例總數715個案例來看，有95%是利用語法程式上的弱點進行攻擊，有5%則是利用輸入驗證錯誤的弱點[5]。所以如果開發人員能夠在使用者輸入欄位確實針對「<」、「>」、「%」、「/」、「（）」、「&」、「'」、「;」、「--」、「=」、「"」、「or」等符號進行過濾且不予輸出至網頁，或是限定欄位長度的輸入，限制用戶端和伺服器端相互傳遞的參數格式，便能夠阻擋95%的網站攻擊了[6]。在此即針對上述分析訊息中，篩選

5 http://zh.wikipedia.org/wiki/HTTP .

6 http://msdn.microsoft.com/zh-tw/library/system.net.httprequestheader（VS.95）.aspx .

表六　資料隱碼攻擊語法分類表

主要被影響的網頁：This vulnerability affects /**mis/c_timetable/query/query_by_tunit_rep.asp**
1.攻擊語法： The POST variable *oneseven* has been set to _′
攻擊事件分類： 語法或程式　機密性　Trnaslate 電腦　竊取　阻斷服務 社交工程　可用性　溢位　Referer 傳輸的資料 複製　資訊洩漏 輸入驗證錯誤　完整性　HTML竄改　Hosst 帳號　讀取　資訊誤用 網頁應用程式→工具套裝軟體→未經授權的存取→代碼注入→ 非預期輸入 →GET→ Cookie→檔案→ 略過→ 廣泛的→ 取得權限
2.攻擊語法： The POST variable *oneseven* has been set to *%00′*
攻擊事件分類： 語法或程式　機密性　Trnaslate 電腦　竊取　阻斷服務 社交工程　可用性　溢位　Referer 傳輸的資料 複製　資訊洩漏 輸入驗證錯誤　完整性　HTML竄改　Hosst 帳號　讀取　資訊誤用 網頁應用程式→工具套裝軟體→未經授權的存取→代碼注入→ 非預期輸入 →GET→ Cookie→檔案→ 略過→ 廣泛的→ 取得權限
3.攻擊語法： The POST variable *oneseven* has been set to \′
攻擊事件分類： 語法或程式　機密性　Trnaslate 電腦　竊取　阻斷服務 社交工程　可用性　溢位　Referer 傳輸的資料 複製　資訊洩漏 輸入驗證錯誤　完整性　HTML竄改　Hosst 帳號　讀取　資訊誤用 網頁應用程式→工具套裝軟體→未經授權的存取→代碼注入→ 非預期輸入 →GET→ Cookie→檔案→ 略過→ 廣泛的→ 取得權限
4.攻擊語法： The POST variable *oneseven* has been set to *%F0%27%27%F0%22%22*
攻擊事件分類： 語法或程式　機密性　Trnaslate 電腦　竊取　阻斷服務 社交工程　可用性　溢位　Referer 傳輸的資料 複製　資訊洩漏 輸入驗證錯誤　完整性　HTML竄改　Hosst 帳號　讀取　資訊誤用 網頁應用程式→工具套裝軟體→未經授權的存取→代碼注入→ 非預期輸入 →GET→ Cookie→檔案→ 略過→ 廣泛的→ 取得權限
5.攻擊語法： The POST variable *oneseven* has been set to \′
攻擊事件分類： 語法或程式　機密性　Trnaslate 電腦　竊取　阻斷服務 社交工程　可用性　溢位　Referer 傳輸的資料 複製　資訊洩漏 輸入驗證錯誤　完整性　HTML竄改　Hosst 帳號　讀取　資訊誤用 網頁應用程式→工具套裝軟體→未經授權的存取→代碼注入→ 非預期輸入 →GET→ Cookie→檔案→ 略過→ 廣泛的→ 取得權限

資料來源：作者整理

出下列符號及字串。網管人員或使用者可利用下列特殊符號或字串自行檢測網站是否具有此類潛藏性的漏洞，並加以防範，表七和表八即是將特殊的符號及字串做統一資源定位位址（URL）編碼。至於為什麼要做統一資源定位位址的解碼和編碼，其轉換的原理是當共用閘道介面（CGI）程式在讀資料時，都會先進行解碼的工作，而共用閘道介面程式與參數直接寫成統一資源定位位址時，為了能清楚辨識字元，在傳送前瀏覽器會將統一資源定位位址做編碼的工作，例如：

表七　可能造成資料隱碼攻擊的符號字串表

特殊符號和字串	URL編碼
'	%27
"	%22
%	%25
<script>alert(number)</script>	%3Cscript%3Ealert%28number%29%3C%2Fscript%3E
<ScRiPt%20%0a%0d>alert(number)%3B</ScRiPt>	%3CScRiPt%2520%250a%250d%3Ealert%28number%29%253B%3C%2FScRiPt%3E
>'><ScRiPt%20%0a%0d>alert(number)%3B</ScRiPt>	%3E%27%3E%3CScRiPt%2520%250a%250d%3Ealert%28number%29%253B%3C%2FScRiPt%3E
>"><ScRiPt%20%0a%0d>alert(number)%3B</ScRiPt>	%3E%22%3E%3CScRiPt%2520%250a%250d%3Ealert%28number%29%253B%3C%2FScRiPt%3E
--><ScRiPt%20%0a%0d>alert(number)%3B</ScRiPt>	--%3E%3CScRiPt%2520%250a%250d%3Ealert%28number%29%253B%3C%2FScRiPt%3E
<ScRiPt+src=http://testphp.acunetix.com/xss.js?number></ScRiPt>	%3CScRiPt%2Bsrc%3Dhttp%3A%2F%2Ftestphp.acunetix.com%2Fxss.js%3Fnumber%3E%3C%2FScRiPt%3E
<script/xss+src=http://testphp.acunetix.com/xss.js?number></script>	%3Cscript%2Fxss%2Bsrc%3Dhttp%3A%2F%2Ftestphp.acunetix.com%2Fxss.js%3Fnumber%3E%3C%2Fscript%3E
</textarea><ScRiPt%20%0a%0d>alert(number)%3B</ScRiPt>	%3C%2Ftextarea%3E%3CScRiPt%2520%250a%250d%3Ealert%28number%29%253B%3C%2FScRiPt%3E
</title><ScRiPt%20%0a%0d>alert(number)%3B</ScRiPt>	%3C%2Ftitle%3E%3CScRiPt%2520%250a%250d%3Ealert%28number%29%253B%3C%2FScRiPt%3E
<body+onload=alert(number)>	%3Cbody%2Bonload%3Dalert%28number%29%3E
<img+src=http://testphp.acunetix.com/dot.gif+onload=alert(number)>	%3Cimg%2Bsrc%3Dhttp%3A%2F%2Ftestphp.acunetix.com%2Fdot.gif%2Bonload%3Dalert%28number%29%3E
<ScRiPt%20%0a%0d>alert(number)%3B</ScRiPt>	%3C%2Fdiv%3E%3CScRiPt%2520%250a%250d%3Ealert%28number%29%253B%3C%2FScRiPt%3E
<iframe/+/onload=alert(number)></iframe>	%3Ciframe%2F%2B%2Fonload%3Dalert%28number%29%3E%3C%2Fiframe%3E
email@some<ScRiPt%20%0a%0d>alert(number)%3B</ScRiPt>domain.com	email%40some%3CScRiPt%2520%250a%250d%3Ealert%28number%29%253B%3C%2FScRiPt%3Edomain.com

資料來源：作者整理

http://www.xxx.mil.tw/mis/ c_timetable/query/query_xxx_xxx.asp?qym=99%2F07&una = una%3D%B3q%B8%EA%A8t%B2%CE%B2%D5'這一行統一資源定位位址實際上會被編碼成：http://www.xxx.mil.tw/mis/c_timetable/query/query_xxx_xxx.asp?qym%3D99%252F07%26+una+%3D+una=%25B3q%25B8%25EA%25A8t%25B2%25CE%25B2%25D5%27，其中空格的地方會用"+"（加號）取代，特殊字元也會被轉換成對應的美國資訊互換標準代碼（ASCII）16進位碼，例如"="、"%"、"&"、" ' "可分別被編碼成%3D、%25、%26和%27[7]。

五、結果分析

經由本研究實際掃瞄715個案例來看，不管是針對資料隱碼攻擊、跨站腳本攻擊漏洞或是目前最常見的網頁十大攻擊，我們都可以藉由上述的分類結果得知跨站腳本攻擊和資料隱碼攻擊發生時可能使用的攻擊方式、系統受到的威脅、執行的動作、針對的目標及攻擊後可能造成的損害（如表五、表六）。也分別利用這些分類結果提出相對的防護措施，如攻擊方式為植入某段程式碼或符號，網站設計者便可在伺服器端針對這些字串或符號的輸入加以過濾及驗證，或是限定輸入欄位的長度（如表

7　http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=1288 .

表八　可能造成跨站腳本攻擊的符號字串表

特殊符號和字串	URL編碼
'	%27
'"	%27%22
\'	%5C%27
\"	%5C%22
%00'	%2500%27
%2527	%252527
JyI%3D	JyI%253D
1+and+31337-31337=0	1%2Band%2B31337-31337%3D0
2+and+31337-31337=0	2%2Band%2B31337-31337%3D0
33+and+31337-31337=0	33%2Band%2B31337-31337%3D0
38+and+31337-31337=0	38%2Band%2B31337-31337%3D0
56+and+31337-31337=0	56%2Band%2B31337-31337%3D0
73+and+31337-31337=0	73%2Band%2B31337-31337%3D0
789+and+31337-31337=0	789%2Band%2B31337-31337%3D0
33+and+31337-31337=0+--+	33%2Band%2B31337-31337%3D0%2B--%2B
38+and+31337-31337=0+--+	38%2Band%2B31337-31337%3D0%2B--%2B
56+and+31337-31337=0+--+	56%2Band%2B31337-31337%3D0%2B--%2B
73+and+31337-31337=0+--+	73%2Band%2B31337-31337%3D0%2B--%2B
789+and+31337-31337=0+--+	789%2Band%2B31337-31337%3D0%2B--%2B
1236841219+and+31337-31337=0&partid=33	1236841219%2Band%2B31337-31337%3D0%26partid%3D33
1236151439+and+31337-31337=0&partid=73	1236151439%2Band%2B31337-31337%3D0%26partid%3D73
1236841219+and+31337-31337=0+--+&partid=33	1236841219%2Band%2B31337-31337%3D0%2B--%2B%26partid%3D33
1236151439+and+31337-31337=0+--+&partid=73	1236151439%2Band%2B31337-31337%3D0%2B--%2B%26partid%3D73
1+and+31337-31337=0&pageNum_RecBull=1	1%2Band%2B31337-31337%3D0%26pageNum_RecBull%3D1
38+and+31337-31337=0&pageNum_RecBull=1	38%2Band%2B31337-31337%3D0%26pageNum_RecBull%3D1
38+and+31337-31337=0+--+&pageNum_RecBull=1	38%2Band%2B31337-31337%3D0%2B--%2B%26pageNum_RecBull%3D1

資料來源：作者整理

七、表八）。但如果是以社交工程的攻擊方式，那就要檢討內部的資安教育及宣導，同時也可針對受攻擊的目標做防範，例如帳號/密碼或檔案部分，則可加強資料庫帳號及權限管理，以減少損害範圍。這也再次證明本研究所歸納的分類法不但可將攻擊事件過程詳細分類，也符合本研究所提出的「接受」、「詳盡」、「可重複使用」、「使用相同的專業術語」四項分類標準的原則。

結　論

本文所歸納出的分類法乃是彙整霍華於1997年及洛克於2001年針對電腦和網路攻擊分類法，賽門和雷於2005年針對蠕蟲、病毒和緩衝區溢位等攻擊分類法，瑪麗亞於2006年針對電腦緊急應變處理中心的回報事件，利用多維排列和最小空間分析技術分類法，以及古納羅和索博丹於2003年針對網頁攻擊分類法做一個綜合性的整理，並提出另一個新的分類標準，最後再以開放網頁軟體安全計畫組織於2009年所公布的十大網頁攻擊來驗證此分類法的可用性。

從實際驗證分析來看，此分類法目前已包含所有攻擊的可能性，可將此分類法實際運用在國軍資安攻擊事件的分類，並藉由可能造成國軍網頁攻擊的漏洞，提出適當的預防措施或建議，以縮短事件處置時間及減低其損失及風險。

收件：100年4月16日
修正：100年4月18日
接受：100年4月19日