公告本

發明專利說明書

（本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※申請案號：95146762

※申請日期：95.12.13　　※IPC分類：G06F 21/00 (2006.01)

一、發明名稱：（中文/英文）

分析網頁元素以偵測網頁弱點之系統、方法及其記錄媒體

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

財團法人資訊工業策進會

INSTITUTE FOR INFORMATION INDUSTRY

代表人：（中文/英文）

高成炎　/ KAO, CHENG YAN

住居所或營業所地址：（中文/英文）

臺北市大安區和平東路2段106號11樓

11F., No.106, Sec. 2, Heping E. Rd., Da-an District, Taipei City , Taiwan R.O.C.

國籍：（中文/英文）

中華民國　/ Taiwan, R.O.C.

三、發明人（共 2 人）

姓　名：（中文/英文）

高新傑　/KAO, HSIN CHIEH

林志鴻　/LIN, CHIH HUNG

國　籍：（中文/英文）

中華民國　/ Taiwan, R.O.C.

中華民國　/ Taiwan, R.O.C.

四、聲明事項：

□ 主張專利法第二十二條第二項□第一款或□第二款規定之事實，其事實發生日期為：　年　月　日。

□ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

□有主張專利法第二十七條第一項國際優先權：

□無主張專利法第二十七條第一項國際優先權：

□ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

□ 主張專利法第三十條生物材料：

□須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

□不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

一種偵測網頁弱點之系統及其方法，特別是指一種分析網頁元素以偵測網頁弱點之系統及其方法。

【先前技術】

超文字標記語言（HyperText Markup Language; HTML）是一種標記語言，由許多的元素（element）組成，如「第 1 圖」所示，元素 100a 至少包含一個由「<」與「>」所形成的標籤（tag）110，在標籤 110 中至少要記錄元素 100a 的元素名稱 111，並視情況選擇是否需要記錄元素屬性（attribute），如標籤 110 中便記錄了「name=""」及「value=""」兩個元素屬性 112，而元素 100d 便沒有記錄元素屬性。另一種元素的型態如元素 100b，主要係由一個起始標籤 110a 與一個結束標籤 110b 組成，則起始標籤 110a 與結束標籤 110b 間所包含的資料「測試連結」為元素 100b 的元素內容 103。還有一種元素的型態，如元素 100c，除了具有起始標籤 110a 與結束標籤 110b 之外，還包含了其他元素，例如元素 100c 包含元素 100a 與元素 100b，則稱元素 100c 為「複合元素」，複合元素中被包含的元素稱為複合元素的「子元素」，意即元素 100a 與元素 100b 為元素 100c 的子元素。

網頁瀏覽器（browser）可以在讀入包含各個元素的網頁後，以各元素所對應的呈現方式將網頁中所記錄的資訊呈現在使用者的眼前。網頁中之各元素在網頁伺服器中產生的方式基本上可以被分為兩大類：當網頁伺服器由被請求的目標網頁所對應的檔案

中讀出各元素之後，就立刻傳送至網頁瀏覽器，這樣的網頁通常被稱為靜態網頁；相對於此，當網頁中除了元素之外，還包含有程式碼，則網頁伺服器會先執行程式碼，才會依據被執行的程式產生各個元素並傳送給網頁瀏覽器，此種網頁的呈現方式往往會依據被請求時所附帶的請求參數不同而有不同的結果，這樣的網頁稱為動態網頁。

隨著網際網路的興起，越來越多的服務透過超文字標記語言在使用者的網頁瀏覽器上呈現，為了滿足服務提供者的各種需求，動態網頁開始被廣泛的使用，甚至大部分的使用動態網頁的服務都已經與資料庫結合，在使用者提供使用者資料之後，可以讓服務越來越個人化。

然而，個人化的服務必須將使用者的部分個人資料存放在網頁伺服器上，因此容易造成有心人士的覬覦，而希望能夠從網頁伺服器竊取儲存在網頁伺服器上的使用者資料，於是有心人士便會對網頁伺服器展開攻擊以期能夠取得儲存在網頁伺服器上的資料，通常是利用網頁伺服器上所執行的程式有安全性上的漏洞，或是動態網頁所包含的程式碼有撰寫上的缺陷來攻擊網頁伺服器，一旦被成功的攻擊，造成的損失往往相當巨大。

鑒於以上的問題，開始有偵測網頁弱點的軟體或服務，但是，目前所提供的軟體或服務大多只是單純的掃描網頁中的其他鏈結(link)，因此往往容易重複的偵測相同的網頁，造成偵測效率的低落，另外，目前提供的軟體沒有掃瞄間接的網頁，如「第 2 圖」所示，當掃描網頁伺服器 200 上的網頁 index.php 時，僅會由未

登入前的網頁的原始碼中掃描出可鏈結至 cart.php 與 login.php，並無法掃描出會員登入後的 index.php 會出現 member.php 的鏈結（link），造成測試覆蓋率不足，而為了增加測試覆蓋率，美國專利6996845號專利案以使用帳號密碼登入網站後取得登入才可以得到的網頁或以關鍵字進行搜尋來取得更多的網頁，而後掃描出新取得的網頁中的鏈結，這樣的偵測弱點的方式雖然可以取得較多的網頁，但若登入後還會依據不同的權限產生不同的網頁，則仍無法取得足夠數量的網頁來防範目前種類繁多的攻擊，所以，如何盡可能的偵測間接的網頁以提昇測試覆蓋率同時提升偵測速度，則成為偵測網頁弱點的軟體或服務待解決的問題。

【發明內容】

鑒於以上的問題，本發明的目的在於提供一種偵測網頁弱點之系統、方法及其記錄媒體，係分析目標網頁中的元素並轉換可提供攻擊的元素為可攻擊元件，而後依據可攻擊元件進行滲透測試來獲得更多的目標網頁，透過將元素轉換可攻擊元件的方式可以過濾不需要測試的元素以及重複的元素，如此可以提升測試涵蓋率並加快偵測的速度，藉以解決先前技術所提到之問題。

為達上述目的，本發明所揭露之系統，包括有：資料傳輸模組、網頁分析模組、轉換模組、測試模組。

本發明所揭露之方法，包括有下列步驟：發送請求至網頁伺服器以下載第一目標網頁；分析第一目標網頁以提取第一目標網頁中可提供攻擊之至少一第一元素；轉換第一元素為第一可攻擊元件；以第一可攻擊元件發送請求至網頁伺服器以進行滲透測

試；當滲透測試成功時，下載至少一第二目標網頁，並由第二目標網頁中提取可提供攻擊之至少一第二元素，及轉換第二元素為第二可攻擊元件，並以第二可攻擊元件再次發出請求進行滲透測試。

本發明所揭露之方法則可以透過記錄媒體形式將對應的電腦可執行程式碼記錄在記錄媒體中，經由電腦執行後達到相同目的。

有關本發明之詳細特徵與實作，茲配合圖示在實施方式中詳細說明如下，其內容足以使任何熟習相關技藝者了解本發明之技術內容並據以實施，且根據本說明書所揭露之內容及圖式，任何熟習相關技藝者可輕易地理解本發明相關之目的及優點。

【實施方式】

網頁弱點偵測分為滲透測試與非滲透測試兩種，滲透測試是指可以取得其他權限或隱藏資料的攻擊，例如資料隱碼（SQL Injection）、緩衝區溢位（Buffer Overflow）、提升存取權限（Privilege Escalation）、目錄穿越（Directory Traversal）等；非滲透測試是指造成服務癱瘓或使服務需求者產生損失的攻擊，例如阻斷服務（Denial of Service; DoS）、跨站程式（Cross Site Scripting; XSS）等。

以下先以「第 3 圖」本發明所提之分析網頁元素以偵測網頁弱點之系統架構圖來說明本發明的系統運作。如圖所示，本發明之系統含有資料傳輸模組 310、網頁分析模組 320、轉換模組 330、測試模組 350。其中資料傳輸模組 310 負責發送請求至網頁伺服器 200，並接收網頁伺服器 200 回應先前發送之請求所傳

回之第一目標網頁；網頁分析模組 320 負責由資料傳輸模組 310 下載之第一目標網頁中分析出可提供攻擊之第一元素；轉換模組 330 負責將網頁分析模組 320 所分析出的第一元素轉換為第一可攻擊元件；測試模組 350 負責以轉換模組 330 轉換產生之第一可攻擊元件對網頁伺服器 200 進行滲透測試。

以下將以一個實施例來解說本發明的運作系統與方法，並請參照「第 4A 圖」及「第 4B 圖」，為本發明所提之分析網頁元素以偵測網頁弱點之方法流程圖。

當執行有本發明的電子裝置 300 在進行網頁弱點偵測時，首先會由資料傳輸模組 310 透過網路對要進行網頁弱點偵測的網頁伺服器 200 發出下載一個目標網頁的請求，一般而言，在未指定目標網頁的情況之下，目標網頁通常會是網頁伺服器的首頁，在本實施例中目標網頁即以首頁 index.php 為例，其中，index.php 的網頁原始碼中記錄了 login.php 以及 cart.php 兩個鏈結，如「第 5A 圖」所示。網頁伺服器在接收到下載 index.php 的請求後會使用網路將 index.php 傳回給本發明的資料傳輸模組 310（步驟 410），隨後，本發明的網頁分析模組 320 會分析 index.php 的網頁原始碼，並由轉換模組 330 將網頁分析模組 320 分析所得的可提供攻擊的元素轉換為提供測試模組 350 進行測試的可攻擊元件（步驟 430）。

在網頁分析模組 320 分析 index.php 的網頁原始碼之後，可以提取出 index.php 中的各個元素，如「第 5A 圖」所示，index.php 中可以提取的元素包含有 HTML、BODY、FORM、INPUT、A

等。接著網頁分析模組 320 會由提取出的各元素中選出可提供網頁攻擊的元素，在本實施例中，網頁分析模組 320 會將各元素與「第 6 圖」所示之可攻擊元素表 600 比較，當元素名稱以及元素屬性與可攻擊元素表 600 中的元素名稱欄 610 及元素屬性欄 620 中所記錄的資料相同時，該元素即為可提供攻擊的元素。

一般來說，可攻擊元素表 600 中所記錄的元素包含有三種，第一種是元素屬性與鏈結有關的元素，例如具有「href」元素屬性的元素「A」、具有「src」元素屬性的元素「IMG」；第二種是元素屬性與變數有關的元素，例如具有「name」及「value」元素屬性的元素「INPUT」及以子元素為元素屬性的複合元素「FORM」；第三種是元素屬性與程式碼相關的元素，例如具有「onclick」、「ondblclick」等元素屬性的元素「DIV」。

而在本發明中，選出可提供攻擊的元素之方法並不以上述之方式為限，其他可判斷出可提供攻擊之元素之方法本發明均可使用。

接著，本發明的轉換模組 330 將轉換可提供網頁攻擊的元素為可攻擊元件，藉以提供測試模組 350 進行滲透測試以得到新的目標網頁，例如轉換模組 330 可以將元素名稱為「FORM」的第一元素 510 的元素屬性「action=login.php」轉換為新的目標網頁「login.php」，並將元素屬性「method」及第一元素 510 的 INPUT 子元素的 name 與 value 等元素屬性轉換為對應目標網頁 login.php 的請求參數。而後轉換模組 330 會繼續提取目標網頁 index.php 中其他可提供攻擊的元素，例如還可由第二元素 520

的元素屬性「href=cart.php?do=display」得知新的目標網頁為cart.php?do=display，且沒有額外的請求參數。

以下進一步說明提取並轉換元素為可攻擊元件的方法（步驟430），如「第4B圖」所示，首先會將第一元素510由目標網頁index.php提取出來（步驟431），並判斷被提取出來的第一元素510是否可提供攻擊（步驟432），在本實施例中的判斷方法是將第一元素510與可攻擊元素表600中的資料比較，由「第6圖」可以得知第一元素510的元素名稱「FORM」與其具有的屬性名稱「action」存在於可攻擊元素表600中，因此判斷第一元素510為可提供攻擊的元素，若被提取出來的元素不為可提供攻擊的元素（不存在於可攻擊元素表600中），則結束這一次的轉換，並重新提取下一個元素進行轉換（步驟431）。

在判斷出第一元素510為可提供攻擊的元素（步驟432）後，則會進一步判斷第一元素510是否為「複合元素」（步驟433），非「複合元素」即為「單一元素」，其中，單一元素為一個具有可提供網頁攻擊的屬性的元素，例如元素「IMG」包含的屬性「src」可提供攻擊；複合元素由一個主元素及一組子元素所組成，各元素分開時無法提供攻擊，例如元素「FORM」，必須要與「INPUT」、「SELECT」、「TEXTAREA」等子元素組合後，使用子元素的屬性（例如「name=...」等元素屬性）才可提供網頁攻擊。在本實施例中，若可攻擊元素表600中的子元素欄630記錄有子元素的元素即為複合元素。由於第一元素510的元素名稱為「FORM」，在子元素欄630中所記錄其子元素包含有BUTTON、INPUT、

SELECT、TEXTAREA 等元素，因此，可以判斷出第一元素 510 為複合元素（步驟 433）。當元素為「複合元素」時，其隨後的元素均為其之子元素，直到被提取的元素為該元素的結束標籤為止。如「第 5A 圖」所示，由於第一元素 510 包含的第一個標籤（第一標籤 511）為「起始標籤」（步驟 435），於是可以建立第一可攻擊元件（步驟 436），其攻擊目標可依據第一標籤 511 中記錄的元素屬性 action 設定為「login.php」，並以元素屬性 method 設定請求參數為「method=post」，而後提取到的元素為第一元素 510 的第一子元素，第一子元素剛好由一個第二標籤 512 所組成，由於第一子元素的元素名稱被記錄在可攻擊元素表 600 的子元素欄 630 中，因此可以判斷出第一子元素 512 並非「起始標籤」與「結束標籤」（步驟 437），因此轉換模組 330 會由第一子元素的元素屬性設定第一可攻擊元件的請求參數為「account=」（步驟 438），第二子元素 513 同樣由一個第三標籤 513 所組成，也同樣不是「起始標籤」與「結束標籤」（步驟 437），所以轉換模組 330 會設定請求參數為「password=」（步驟 438），第一元素 510 的最後一個標籤，也就是第四標籤 514 為「結束標籤」，因此轉換模組 330 會結束第一可攻擊元件的設定（步驟 439），完成建立第一可攻擊元件，若本實施例以鏈結串列（Linked List）來實做可攻擊元件，則第一可攻擊元件 710 會如「第 7 圖」所示。

接著提取目標網頁 index.php 中的下一個元素，也就是元素名稱為 A 的第二元素 520（步驟 431），判斷第二元素 520 為可提供攻擊的元素後（步驟 432），會進一步判斷出第二元素為「單一

元素」(步驟 433),於是轉換模組 330 會由第二元素 520 的屬性「 href=cart.php?do=display 」中得到攻擊目標為「cart.php?do=display」(步驟 434)。

在目標網頁 index.php 中所有可提供攻擊的元素都被提取出來並轉換為可攻擊元件(步驟 420)後,本發明的測試模組 350 會開始進行滲透測試(步驟 442),本實施例在此以使用資料隱碼的方法進行滲透測試。首先,測試模組 350 會由記憶體中讀出第一第一可攻擊元件(例如攻擊目標為 login.php,請求參數為 method=post、account=、password=),接著設定 account 的值為攻擊網頁伺服器的攻擊語法,並透過資料傳輸模組 310 以 POST 的方式傳送請求參數給網頁伺服器,藉以向網頁伺服器發出下載目標網頁 login.php 的請求,網頁伺服器在接收到請求後會先執行 login.php 中的程式碼來產生要回傳的網頁的各元素(或稱作原始碼),若 login.php 具有資料隱碼的弱點,則設定在 account 中的攻擊語法將會被執行,因而使得原先在 login.php 中的程式碼無法正確的被執行,所以網頁伺服器 200 誤認本發明已成功的登入,因此會回傳登入成功的網頁,若 login.php 中的程式碼在網頁伺服器 200 執行後,會使得網頁伺服器 200 傳回 index.php,則網頁伺服器 200 會傳送登入成功後的 index.php 給資料傳輸模組 310(步驟 410)。

接著網頁分析模組 320 會對新接收的 index.php 進行與原始的 index.php 相同的分析,並由轉換模組 330 轉換出可攻擊元件(步驟 420),如「第 5B 圖」所示,新的 index.php 可提取出三

個可提供網頁攻擊的元素，分別為第三元素 530、第四元素 540 及第五元素 550，在轉換模組 330 轉換第三元素 530、第四元素 540 為可攻擊元件之後，可以得到新的目標網頁為 login.php?do=logou、cart.php?do=display，而在轉換模組 330 轉換第五元素 550 為可攻擊元件後，可以獲得新的目標網頁「buy.php」為一個間接的網頁，由此可以得知本發明可以有效的取得間接的網頁，藉以提高本發明的測試覆蓋率。

另外，網頁分析模組 320 提取出的元素中鏈結時，網頁分析模組 320 會進一步的過濾鏈結中的部份字串，使得鏈結中的變數的值被去除，例如在新的 index.php 中的元素經過分析並轉換完成（步驟 420）後，測試模組 350 會再次由記憶體中判斷並讀出未以資料隱碼進行過滲透測試的可攻擊元件（步驟 441），當讀出的第二可攻擊元件的攻擊目標為 cart.php?do=display 時，若網頁分析模組在提取元素時，便已經將鏈結中的變數的值去除，則讀出的第二可攻擊元件的攻擊目標會變為 cart.php?do=，如此測試模組 350 便可以資料隱碼的方式設定 do 的值為攻擊網頁伺服器的語法，進行滲透測試，若可成功的進行滲透測試（步驟 443），則再次分析並轉換網頁伺服器傳送過來的新的網頁中的各元素，若失敗則再次判斷是否有其他不是第一或第二可攻擊元件的可攻擊元件可以讀取（步驟 441），以繼續以資料隱碼進行滲透測試，如此不斷重複上述的過程，直到所有可攻擊元件都以資料隱碼的方式進行過滲透測試為止。當所有的可攻擊元件都以資料隱碼的方式測試完成後，測試模組會再使用其他的攻擊方式再次以所有

可攻擊元件進行滲透測試。如此反覆進行，即可進可能的偵測出所有間接的網頁，成功解決先前技術所提之測試覆蓋率低下的問題。

在上述的測試過程中，網頁分析模組 320 往往會分析出相同的元素以致於轉換模組 330 會轉換出相同的可攻擊元件，如此將使得測試模組 350 進行測試時以相同的可攻擊元件重複測試，為了避免重複測試的問題，在上述的轉換模組 330 將可提供攻擊的元素轉換為可攻擊元件時（步驟 430），可以進一步判斷當前轉換產生的可攻擊元件與已被儲存的可攻擊元件是否相同（步驟 434），若相同則不再儲存，以免測試模組 350 以相同的可攻擊元件進行滲透測試。如「第 7 圖」所示，在轉換第四元素 540 為第四可攻擊元件後，會與第一至第三可攻擊元件（710、720、730）進行比較，首先會比對元件名稱，也就是比對第四可攻擊元件的名稱「A」與第一可攻擊元件 710 的第一元件名稱 711 是否相同，由於第一可元件名稱 711 為 FORM，所以不相同，於是會開始比對第二可攻擊元件 720，由於第二可攻擊元件 720 的第二元件名稱 721 為 A 與第四可攻擊元件的元件名稱相同，所以會進一步比對請求參數，所以接著會讀取第四可攻擊元件的第一個請求參數的參數名稱 href 與參數值 cart.php?do=display 及第二可攻擊元件的第一個請求參數的第一參數名稱 7221 與第一參數值 7222 進行比較，由於第一參數名稱也為 href，且第一參數值 7222 也為 cart.php?do=display，因此第二可攻擊元件 720 的第一個請求參數與第四可攻擊元件的第一個請求參數相同，由於第四可攻擊元

件與第二可攻擊元件均沒有其他請求參數，所以可以判定第四可攻擊元件與第二可攻擊元件完全相同，所以不將第四可攻擊元件加入可攻擊元件列表中。

若上述之第四或第二可攻擊元件其中之一額外包含有其他請求參數，則會判斷第四與第二可攻擊元件不相同；另外，因為請求參數的排列順序並不影響請求目標網頁的結果，因此在比對時要若第一參數不同，則還需要比對其他的所有參數。

當網頁分析模組 320 有過濾鏈結中的變數的值時，本發明可以避免重複測試相同的可攻擊元件，例如，上述之第二可攻擊元件的攻擊目標被網頁分析模組 320 過濾掉鏈結中的變數的值後攻擊目標將變為 cart.php?do=，如此一來，若網頁分析模組 320 分析出的元素中具有 cart.php?do=add 的鏈結，經過網頁分析模組 320 過濾變數的值後，經由轉換模組 330 所轉換出來的第六可攻擊元件中的目標網頁將為 cart.php?do=，與第二可攻擊元件的攻擊目標相同，則第六可攻擊元件將不會被加入可攻擊列表中，因此本發明可以避免不斷的測試加入 Session Key 或是加入時間等變數的值的相同鏈結，明顯的優於習知的測試方式。

而在測試模組 350 以可供及元件進行滲透測試並判斷滲透測試成功之後，可以記錄可攻擊元件可以成功的進行滲透測試，以回報給使用者查閱，例如在上述的實施例中，測試模組 350 使用第一可攻擊元件進行滲透測試（步驟 442）後，可以判斷接收的頁面 index.php 是否包含有已登入的資訊，例如尋找「登出」的字詞，接收到的頁面包含有已登入的資訊，則可以判斷滲透攻擊

成功完成（步驟443），因此可以記錄第一可攻擊元件可進行滲透測試（步驟444）。

另外，由於目前攻擊方式除了可以使用滲透測試來測試之外，還可以再以非滲透測試的方式進行測試，因此當測試模組350完成滲透測試後，更可以對網頁伺服器200進行非滲透測試，在本實施例中將以跨站程式的方式為例，測試模組350首先會讀出一個可攻擊元件，例如為第三可攻擊元件（buy.php?msg=），於是本發明會設定 msg 的值為特定程式碼，並以「buy.php?msg=特定程式碼」向網頁伺服器發出請求，若網頁 buy.php 具有跨站程式的弱點，則網頁伺服器200在執行 buy.php 中的程式碼時，會將測試模組350輸入的特定程式碼存入資料庫中，使得之後下載 buy.php 時，先前所輸入的特定程式碼便會包含在其中，如此一來，網頁瀏覽器在將呈現 buy.php 中的各元素時，將會執行先前所輸入的特定程式碼。跟著本發明會判斷是否還有未進行非滲透測試的可攻擊元件，若有的話，則會以之繼續進行非滲透測試。直到所有的測試完成為止。

此外，本發明所提之分析網頁元素以偵測網頁弱點之記錄媒體係在由電腦執行記錄媒體中所儲存之程式後，可以進行如上實施例所述之步驟。

再者，本發明之分析網頁元素以偵測網頁弱點之方法，可實現於硬體、軟體或硬體與軟體之組合中，亦可在電腦系統中以集中方式實現或以不同元件散佈於若干互連之電腦系統的分散方式實現。

雖然本發明以前述之較佳實施例揭露如上，然其並非用以限定本發明，任何熟習相像技藝者，在不脫離本發明之精神和範圍內，所為之更動與潤飾，均屬本發明之專利保護範圍，因此本發明之專利保護範圍須視本說明書所附之申請專利範圍所界定者為準。

【圖式簡單說明】

第 1 圖係習知之元素組成圖。

第 2 圖係本發明實施例所提之網頁伺服器中具有之網頁示意圖。

第 3 圖係本發明所提之分析網頁元素以偵測網頁弱點之系統架構圖。

第 4A 圖係本發明所提之分析網頁元素以偵測網頁弱點之方法流程圖。

第 4B 圖係本發明所提之分析網頁元素以偵測網頁弱點之提取及轉換元素之方法流程圖。

第 5A 圖係本發明實施例所提之登入前之 index.php 之網頁原始碼。

第 5B 圖係本發明實施例所提之登入後之 index.php 之網頁原始碼。

第 6 圖係本發明實施例所提之可攻擊元素表。

第 7 圖係本發明實施例所提之可攻擊元件示意圖。

【主要元件符號說明】

100a	元素
100b	元素
100c	元素
100d	元素
103	元素內容
110	標籤
110a	起始標籤
110b	結束標籤
111	元素名稱
112	元素屬性
200	網頁伺服器
300	電子裝置
310	資料傳輸模組
320	網頁分析模組
330	轉換模組
350	測試模組
390	儲存模組
510	第一元素
511	第一標籤
512	第二標籤
513	第三標籤
514	第四標籤
520	第二元素

530 第三元素

540 第四元素

550 第五元素

600 可攻擊元素表

610 元素名稱欄

620 元素屬性欄

630 子元素欄

710 第一可攻擊元件

711 第一元件名稱

720 第二可攻擊元件

721 第二元件名稱

7221 第一參數名稱

7222 第一參數值

730 第三可攻擊元件

步驟 410 下載目標網頁

步驟 430 由目標網頁提取元素並轉換為可攻擊元件

步驟 441 是否有未經過滲透測試之元件

步驟 442 進行滲透測試

步驟 443 滲透測試是否成功

步驟 449 記錄元件可進行攻擊

步驟 451 是否有未經過非滲透測試之元件

步驟 452 進行非滲透測試

步驟 453 非滲透測試是否成功

步驟 459　記錄元件可被攻擊

步驟 431　提取元素

步驟 432　元素是否可提供攻擊

步驟 433　元素是否為複合元素

步驟 434　元素是否與其它元件不同

步驟 435　元素是否為起始標籤

步驟 436　建立元件

步驟 437　元素是否為結束標籤

步驟 438　設定請求參數

步驟 439　結束設定元件

五、中文發明摘要：

一種分析網頁元素以偵測網頁弱點之系統、方法及其記錄媒體，係向網頁伺服器請求目標網頁後，分析（parse）目標網頁中的元素，由分析所得各元素中提取（fetch）出可提供攻擊的元素並將之轉換為可攻擊元件，而後使用所有的可攻擊元件對網頁伺服器進行滲透攻擊（Penetrable Test）以下載更多間接的網頁，藉以提升測試覆蓋率。另外，透過將可提供攻擊的元素轉換為可攻擊元件的方式，可以過濾重複或不需測試的元素，進而加快偵測的速度。

六、英文發明摘要：

十、申請專利範圍：

1. 一種分析網頁元素以偵測網頁弱點之方法，係應用於一電子裝置上，該方法包含下列步驟：

發送請求至一網頁伺服器以下載一第一目標網頁；

分析該第一目標網頁以提取該第一目標網頁中可提供攻擊之至少一第一元素；

轉換該第一元素為一第一可攻擊元件；

以該第一可攻擊元件發送請求至該網頁伺服器以進行一滲透測試；及

當該滲透測試成功時，下載至少一第二目標網頁，並由該第二目標網頁中提取可提供攻擊之至少一第二元素，及轉換該第二元素為第二可攻擊元件，並以該第二可攻擊元件再次發出請求進行該滲透測試。

2. 如申請專利範圍第 1 項所述之分析網頁元素以偵測網頁弱點之方法，其中該方法更包含以該分析該第一目標網頁以提取該第一目標網頁中可提供攻擊之至少一第一元素之步驟更包含過濾該第一元素中之一鏈結之一變數之值，使具有相同之該變數之名稱之各鏈結轉換為相同之該第一可攻擊元件。

3. 如申請專利範圍第 1 項所述之分析網頁元素以偵測網頁弱點之方法，其中該轉換該第一元素為該第一可攻擊元件之步驟更包含下列步驟：

判斷該第一元素為單一元素或複合元素；

當該第一元素為單一元素時，設定對應該第一元素之該第

一可攻擊元件為該第一元素之元素屬性值；

當該第一元素為複合元素時，判斷該第一元素中之各標籤之種類；

當該標籤之種類為一起始標籤時，設定對應該第一元素之該第一可攻擊元件中之一目標網頁為該第一元素之元素屬性值；

當該標籤之種類不為該起始標籤與一終止標籤時，設定對應該第一元素之該第一可攻擊元件中之各下載參數為該標籤所對應之各子元素之各屬性；及

當該標籤之種類為該終止標籤時，結束該第一可攻擊元件之設定。

4. 如申請專利範圍第 1 項所述之分析網頁元素以偵測網頁弱點之方法，其中該方法更包含判斷該第一可攻擊元件與一可攻擊元件列表中之所有可攻擊元件均不同時，儲存該第一可攻擊元件至該可攻擊元件列表中之步驟。

5. 如申請專利範圍第 1 項所述之分析網頁元素以偵測網頁弱點之方法，其中該進行該滲透測試之步驟更包含於該滲透測試成功時，記錄該第一可攻擊元件可成功進行該滲透測試之步驟。

6. 如申請專利範圍第 1 項所述之分析網頁元素以偵測網頁弱點之方法，其中該方法更包含以該第一可攻擊元件發送請求至該網頁伺服器，以進行一非滲透測試之步驟。

7. 如申請專利範圍第 6 項所述之分析網頁元素以偵測網頁弱點之方法，其中該進行該非滲透測試之步驟更包含於該非滲透測

試成功時，記錄該第一可攻擊元件可成功進行該非滲透測試之步驟。

8. 一種分析網頁元素以偵測網頁弱點之系統，係應用於一電子裝置上，該系統包含：

一資料傳輸模組，用以發送請求至一網頁伺服器以下載一第一目標網頁；

一網頁分析模組，用以分析該第一目標網頁以提取該第一目標網頁中可提供攻擊之至少一第一元素；

一轉換模組，用以將該至少一第一元素轉換為相對應之至少一第一可攻擊元件；及

一測試模組，用以透過該資料傳輸模組向該網頁伺服器發出對應該第一可攻擊元件之請求以進行一滲透測試，當該滲透測試成功時，透過該資料傳輸模組接收至少一第二目標網頁；

其中，該網頁分析模組於該測試模組接收到該第二目標網頁後，分析該第二目標網頁以提取至少一第二元素，並由該轉換模組將該第二元素轉換為第二可攻擊元件後，以第二可攻擊元件進行該滲透測試。

9. 如申請專利範圍第 8 項所述之分析網頁元素以偵測網頁弱點之系統，其中該網頁分析模組更用以過濾該第一元素中之一鏈結之一變數之值。

10. 如申請專利範圍第 8 項所述之分析網頁元素以偵測網頁弱點之系統，其中該測試模組更用以透過該資料傳輸模組向該網頁伺服器發出對應該第一可攻擊元件之請求以進行一非滲透性

測試。

11. 如申請專利範圍第 8 項所述之分析網頁元素以偵測網頁弱點之系統，其中該測試模組更用以記錄該第一可攻擊元件可對該網頁伺服器進行該滲透測試。

12. 如申請專利範圍第 8 項所述之分析網頁元素以偵測網頁弱點之系統，其中該系統更包含一儲存模組，用以於該網頁分析模組判斷該第一可攻擊元件與該儲存模組中儲存之所有可攻擊元件均不同時，儲存該第一可攻擊元件至該儲存模組中。

13. 一種分析網頁元素以偵測網頁弱點之記錄媒體，記錄有電腦可執行之電腦程式碼，用以於電腦中執行下列步驟：

發送請求至一網頁伺服器以下載一第一目標網頁；

分析該第一目標網頁以提取該第一目標網頁中可提供攻擊之至少一第一元素；

轉換該第一元素為一第一可攻擊元件；

以該第一可攻擊元件發送請求至該網頁伺服器以進行一滲透測試；及

當該滲透測試成功時，下載至少一第二目標網頁，並由該第二目標網頁中提取可提供攻擊之至少一第二元素，及轉換該第二元素為第二可攻擊元件，並以該第二可攻擊元件再次發出請求進行該滲透測試。

14. 如申請專利範圍第 13 項所述之分析網頁元素以偵測網頁弱點之記錄媒體，其中該記錄媒體更包含使電腦在執行轉換該第一元素為該第一可攻擊元件之步驟時，更包含執行以該分析該第

一目標網頁以提取該第一目標網頁中可提供攻擊之至少一第一元素之步驟更包含過濾該第一元素中之一鏈結之一變數之值，使具有相同之該變數之名稱之各鏈結轉換為相同之該第一可攻擊元件。

15. 如申請專利範圍第 13 項所述之分析網頁元素以偵測網頁弱點之記錄媒體，其中該記錄媒體更包含使電腦在執行轉換該第一元素為該第一可攻擊元件之步驟時，更包含執行下列步驟：

判斷該第一元素為單一元素或複合元素；

當該第一元素為單一元素時，設定對應該第一元素之該第一可攻擊元件為該第一元素之元素屬性值；

當該第一元素為複合元素時，判斷該第一元素中之各標籤之種類；

當該標籤之種類為一起始標籤時，設定對應該第一元素之該第一可攻擊元件中之一目標網頁為該第一元素之元素屬性值；

當該標籤之種類不為該起始標籤與一終止標籤時，設定對應該第一元素之該第一可攻擊元件中之各下載參數為該標籤所對應之各子元素之各屬性；及

當該標籤之種類為該終止標籤時，結束該第一可攻擊元件之設定。

16. 如申請專利範圍第 13 項所述之分析網頁元素以偵測網頁弱點之記錄媒體，其中該記錄媒體更包含使電腦判斷該第一可攻擊元件與一可攻擊元件列表中之所有可攻擊元件均不同時，儲存

該第一可攻擊元件至該可攻擊元件列表中之步驟。

17. 如申請專利範圍第 13 項所述之分析網頁元素以偵測網頁弱點之記錄媒體，其中該記錄媒體更包含使電腦進行該滲透測試成功時，記錄該第一可攻擊元件可成功進行該滲透測試之步驟。

18. 如申請專利範圍第 13 項所述之分析網頁元素以偵測網頁弱點之記錄媒體，其中該記錄媒體更包含使電腦以該第一可攻擊元件發送請求至該網頁伺服器，以進行一非滲透測試之步驟。

19. 如申請專利範圍第 18 項所述之分析網頁元素以偵測網頁弱點之記錄媒體，其中該記錄媒體更包含使電腦於該非滲透測試成功時，記錄該第一可攻擊元件可成功進行該非滲透測試之步驟。

七、指定代表圖：

(一)本案指定代表圖為：第（ 4A ）圖。

(二)本代表圖之元件符號簡單說明：

步驟 410　下載目標網頁

步驟 430　由目標網頁提取元素並轉換為可攻擊元件

步驟 441　是否有未經過滲透測試之元件

步驟 442　進行滲透測試

步驟 443　滲透測試是否成功

步驟 449　記錄元件可進行攻擊

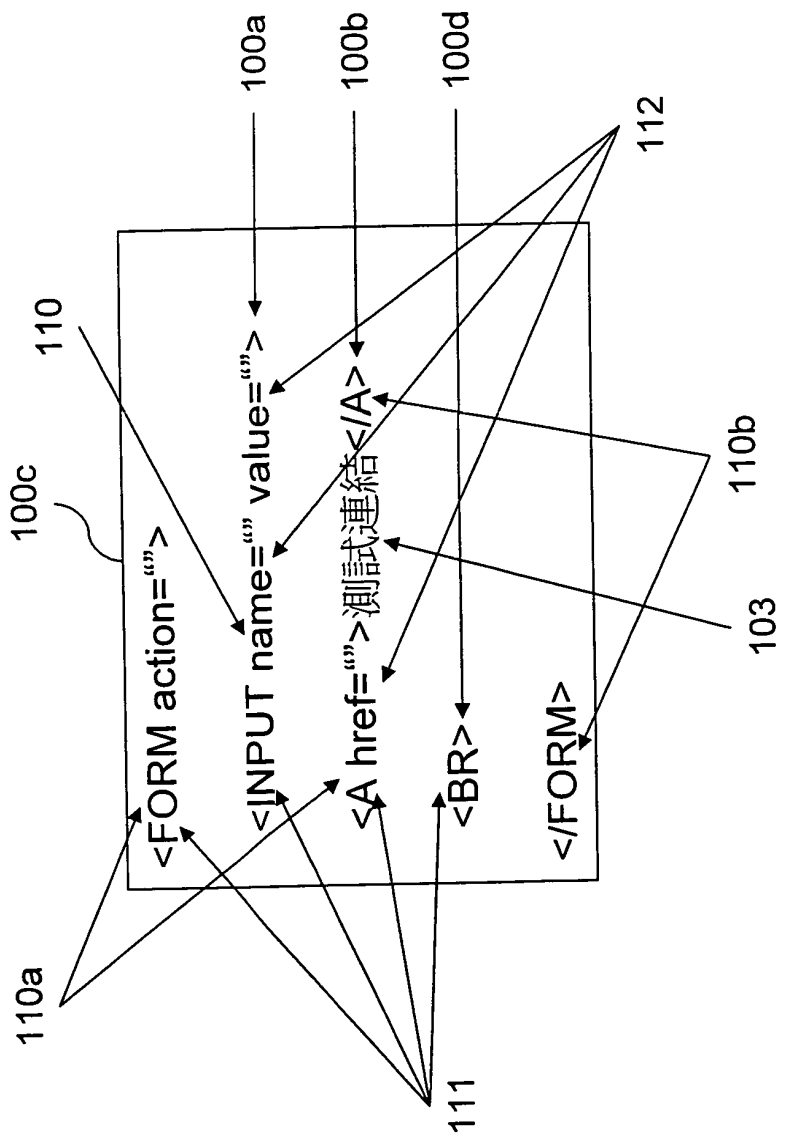
步驟 451　是否有未經過非滲透測試之元件

步驟 452　進行非滲透測試

步驟 453　非滲透測試是否成功

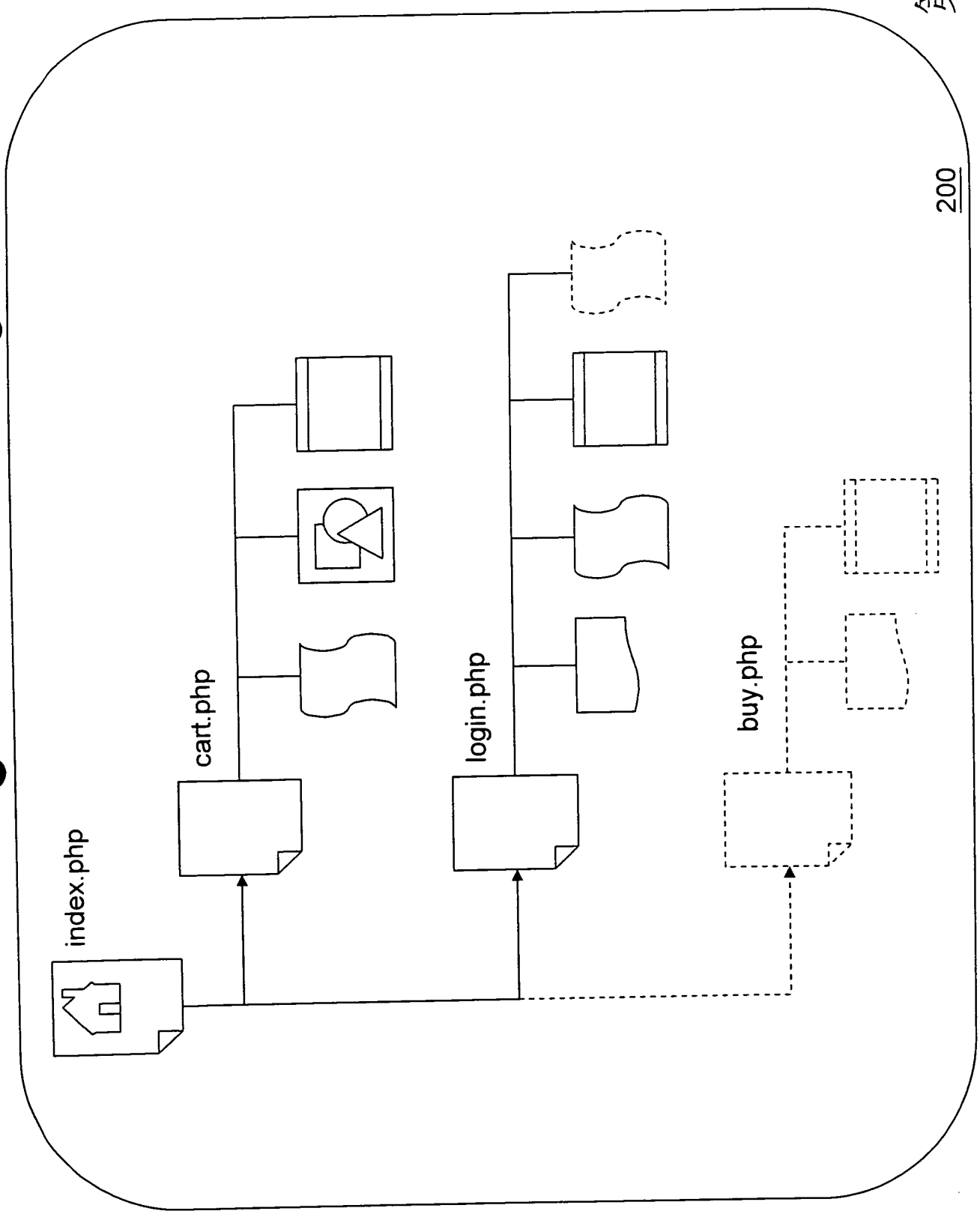
步驟 459　記錄元件可被攻擊

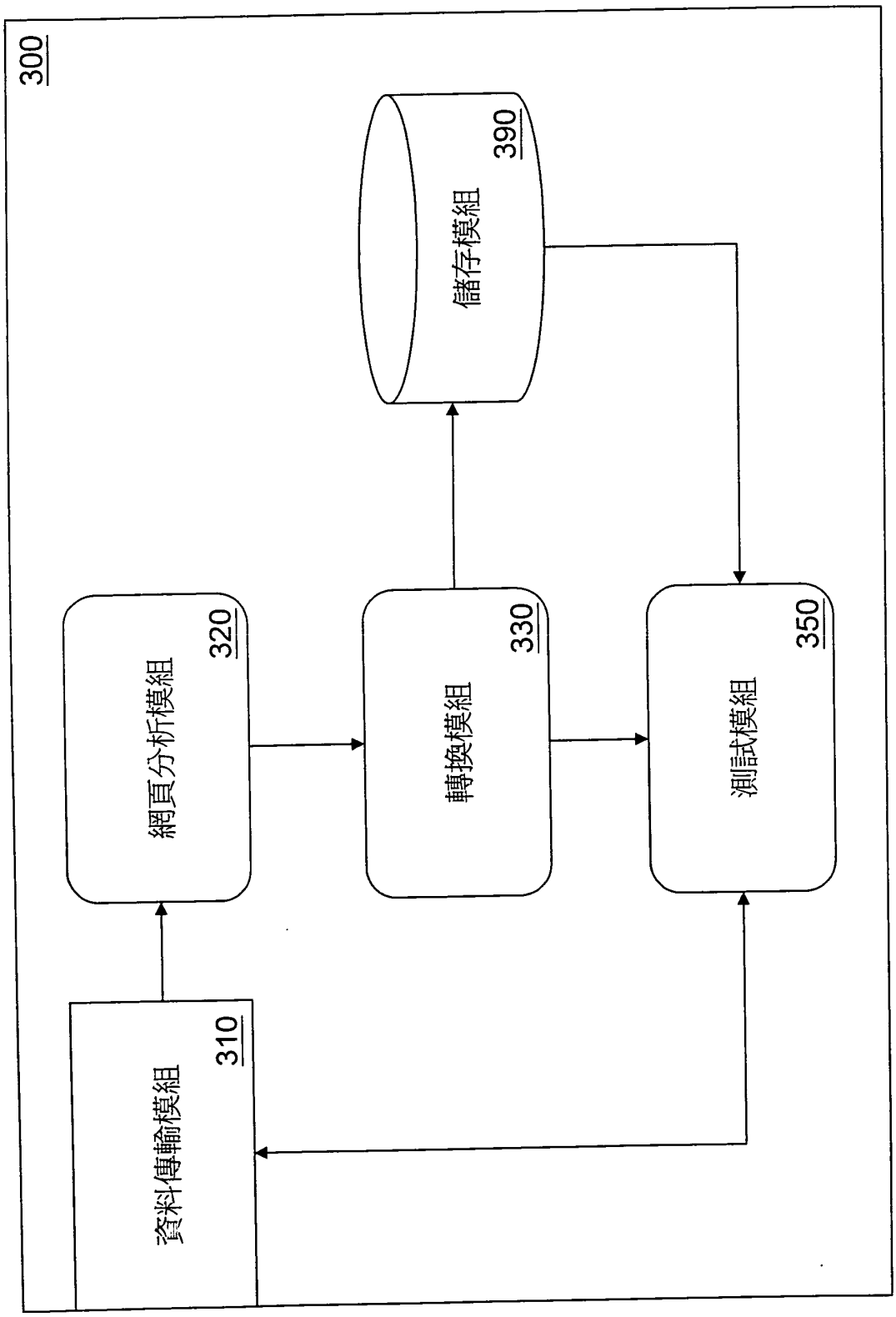
八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：



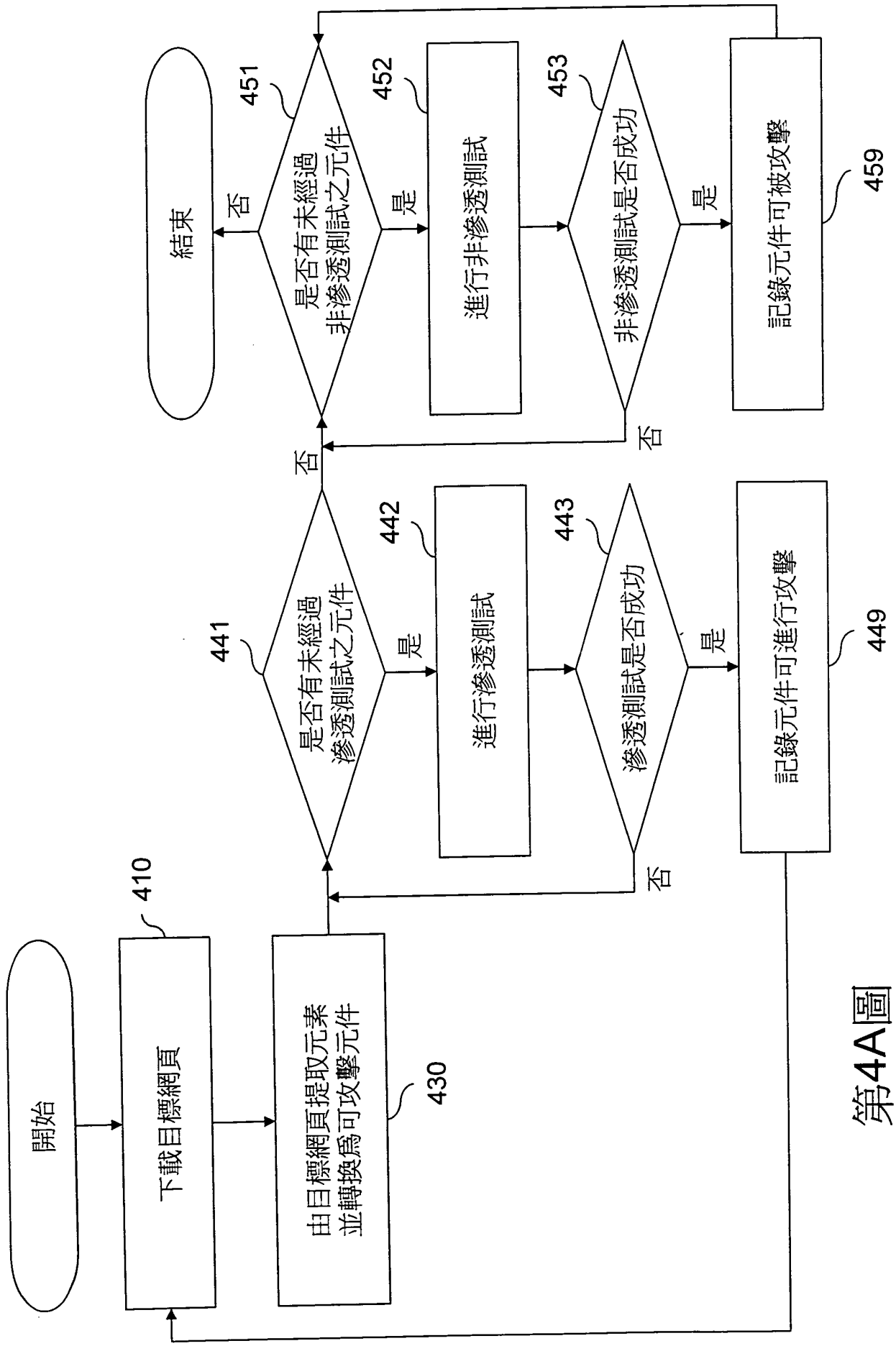
第1圖 (習知技術)

第2圖

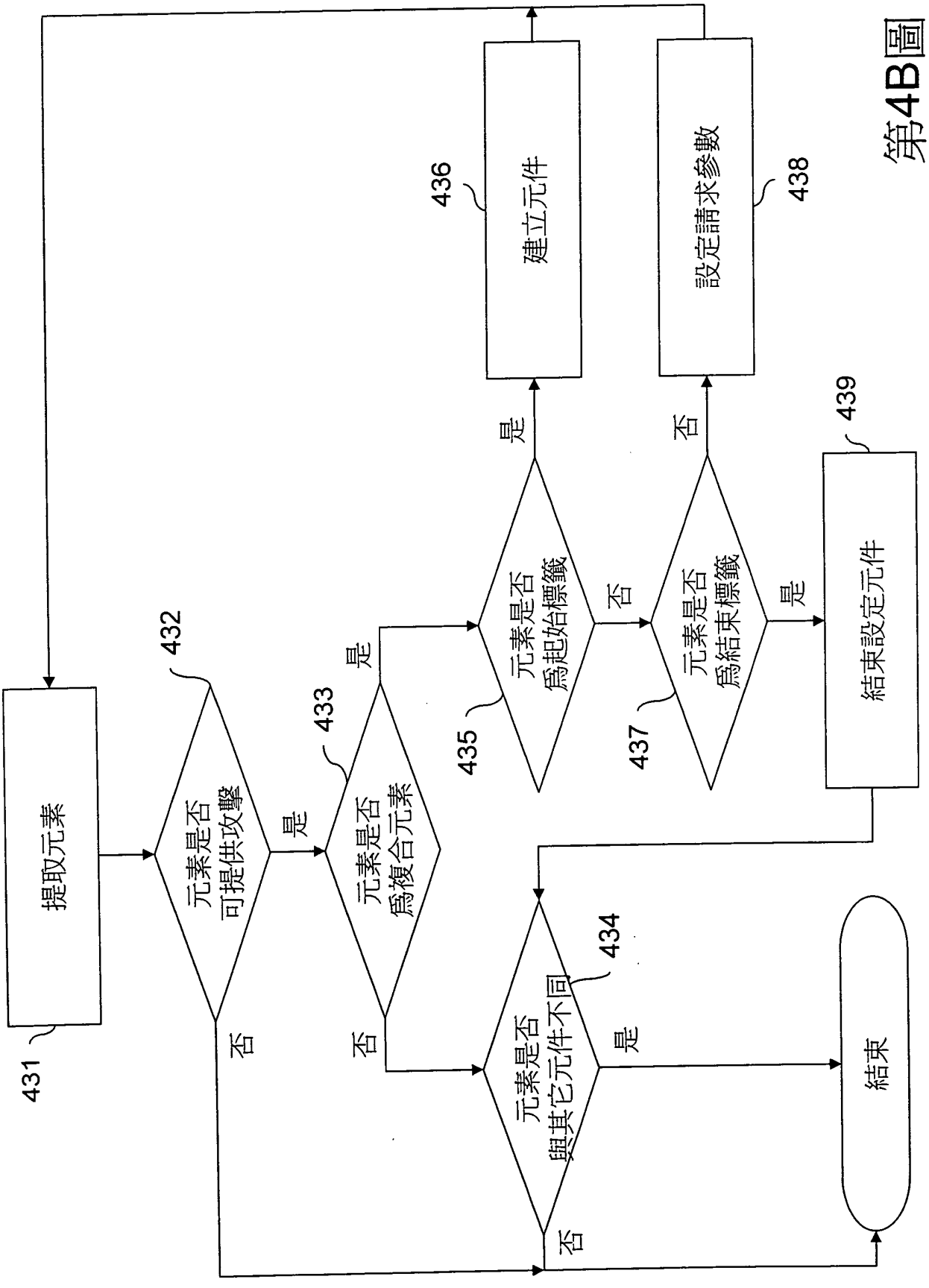




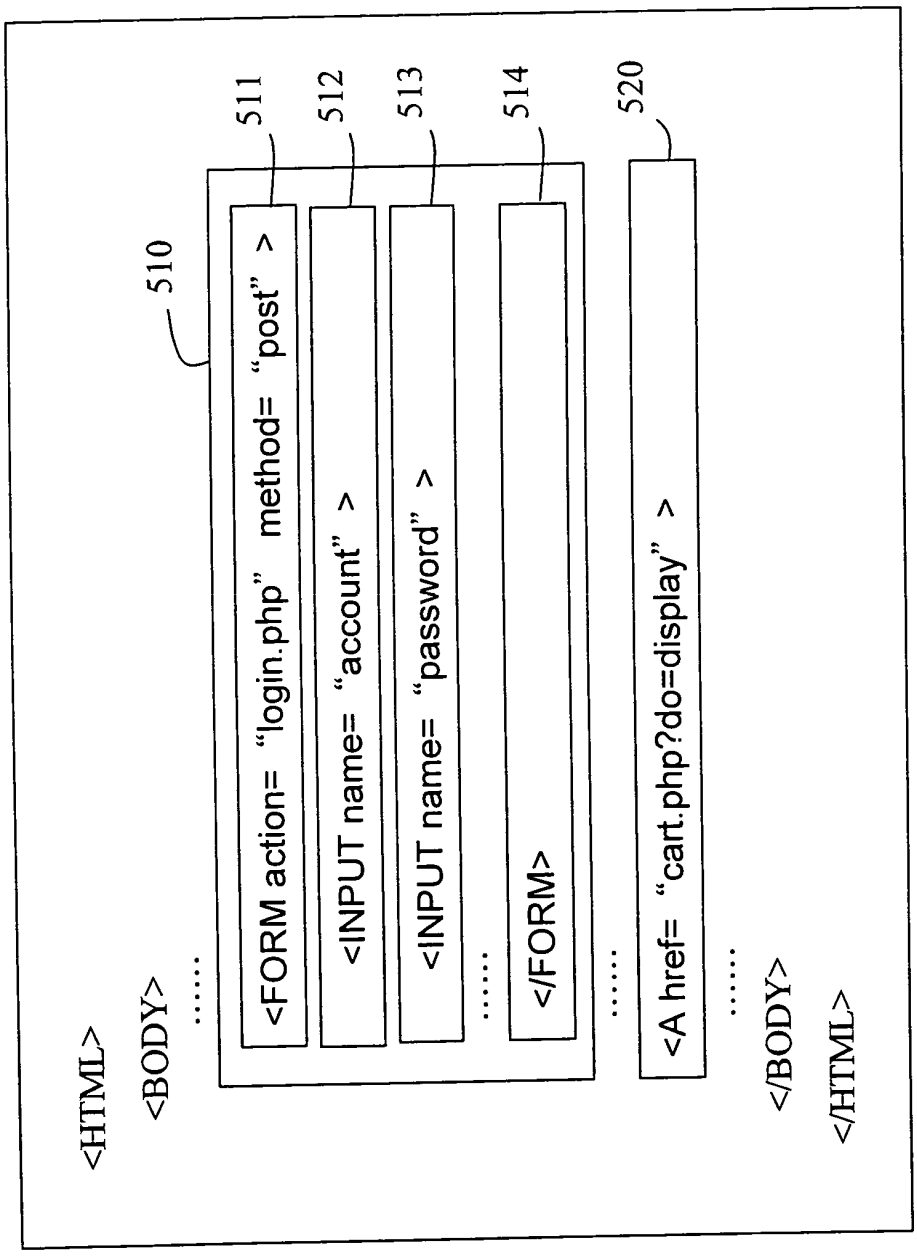
第3圖


開始
下載目標網頁
410
由目標網頁提取元素
並轉換爲可攻擊元件
430
是否有未經過
滲透測試之元件
441
是
進行滲透測試
442
滲透測試是否成功
443
是
記錄元件可進行攻擊
449
否
否
是否有未經過
非滲透測試之元件
451
是
進行非滲透測試
452
非滲透測試是否成功
453
是
記錄元件可被攻擊
459
否
結束

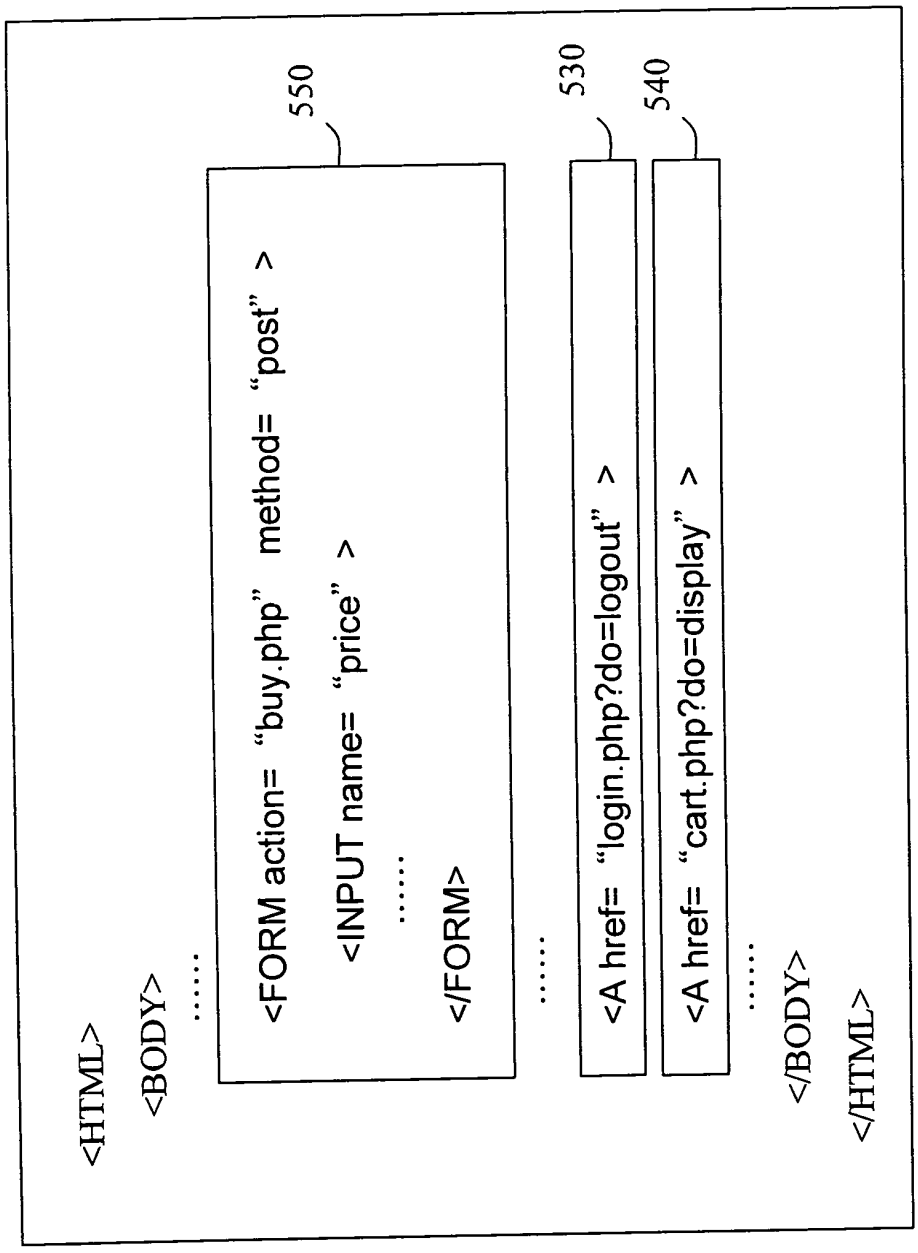
第4A圖


提取元素
431
元素是否
可提供攻擊
432
是
否
元素是否
爲複合元素
433
是
否
元素是否
爲起始標籤
435
是
否
建立元件
436
元素是否
爲結束標籤
437
是
否
設定請求參數
438
結束設定元件
439
元素是否
與其它元件不同
434
是
否
結束

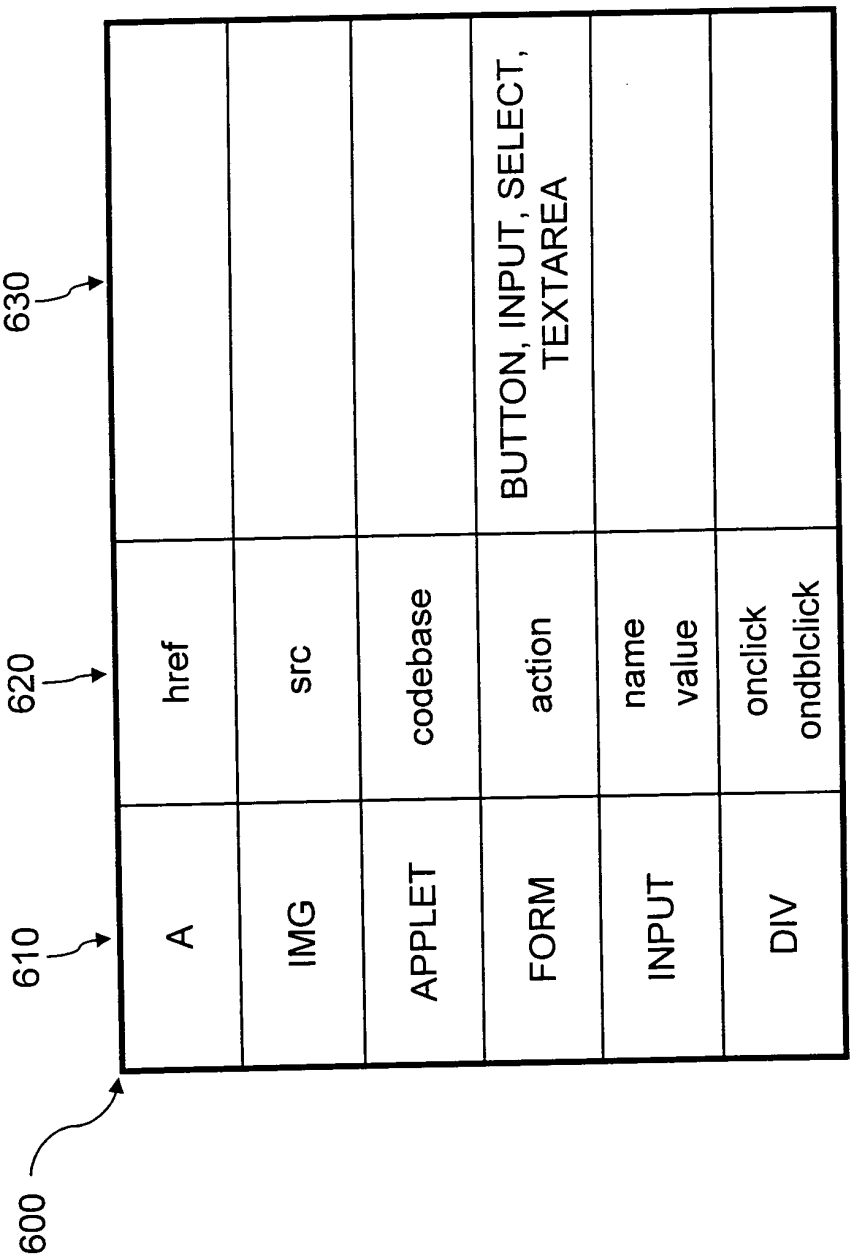
第4B圖


<HTML>
<BODY>
.....
510
<FORM action= "login.php" method= "post" >
<INPUT name= "account" >
<INPUT name= "password" >
.....
</FORM>
.....
<A href= "cart.php?do=display" >
.....
</BODY>
</HTML>
511
512
513
514
520

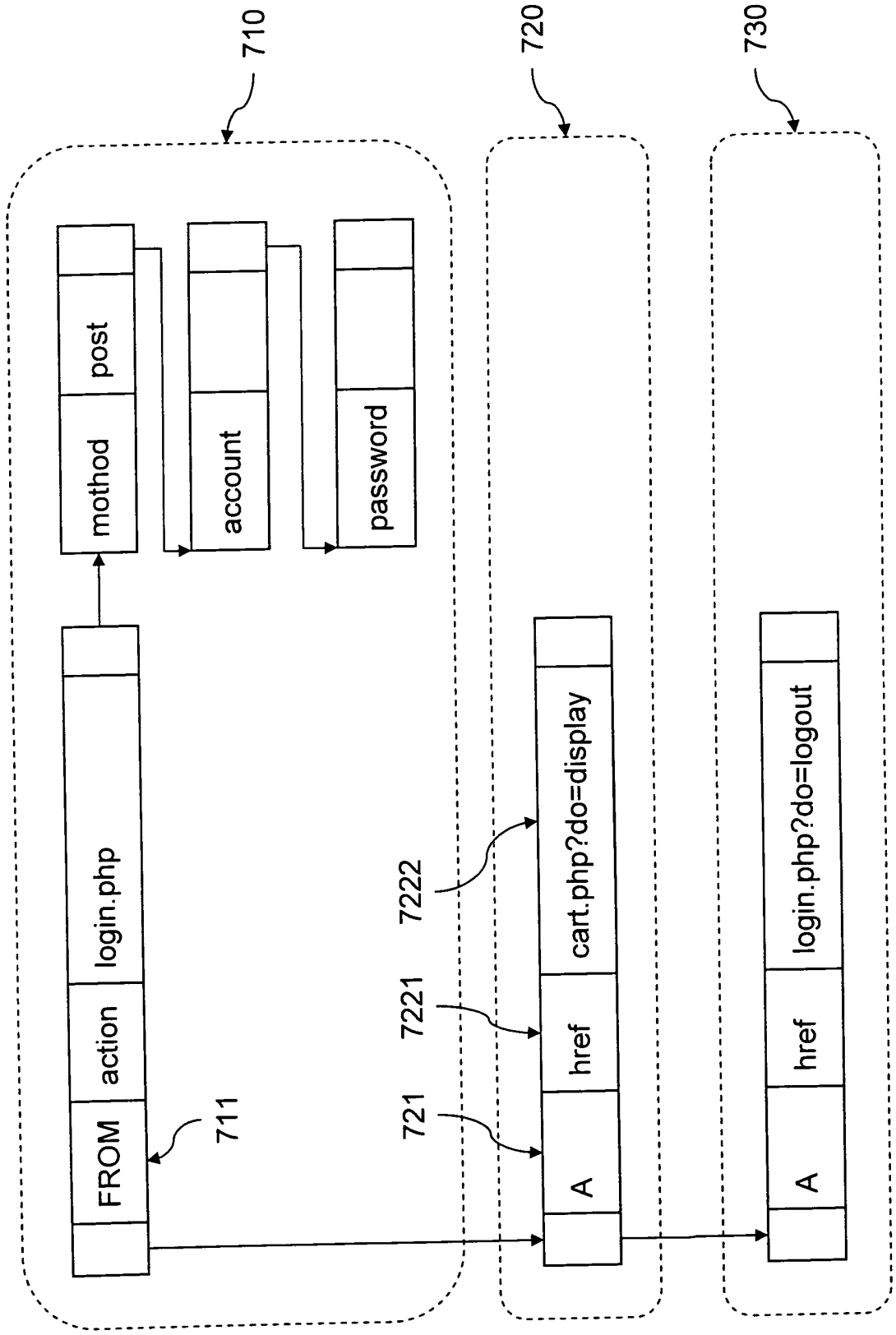
第5A圖


<HTML>
<BODY>
.....
<FORM action= "buy.php" method= "post" >
<INPUT name= "price" >
.....
</FORM>
.....
<A href= "login.php?do=logout" >
<A href= "cart.php?do=display" >
.....
</BODY>
</HTML>
550
530
540

第5B圖


600
610
620
630
A
href
IMG
src
APPLET
codebase
FORM
action
BUTTON, INPUT, SELECT, TEXTAREA
INPUT
name
value
DIV
onclick
ondblclick

第6圖


710
720
730
mothod
post
account
password
FROM
action
login.php
711
721
7221
7222
A
href
cart.php?do=display
A
href
login.php?do=logout

第7圖