

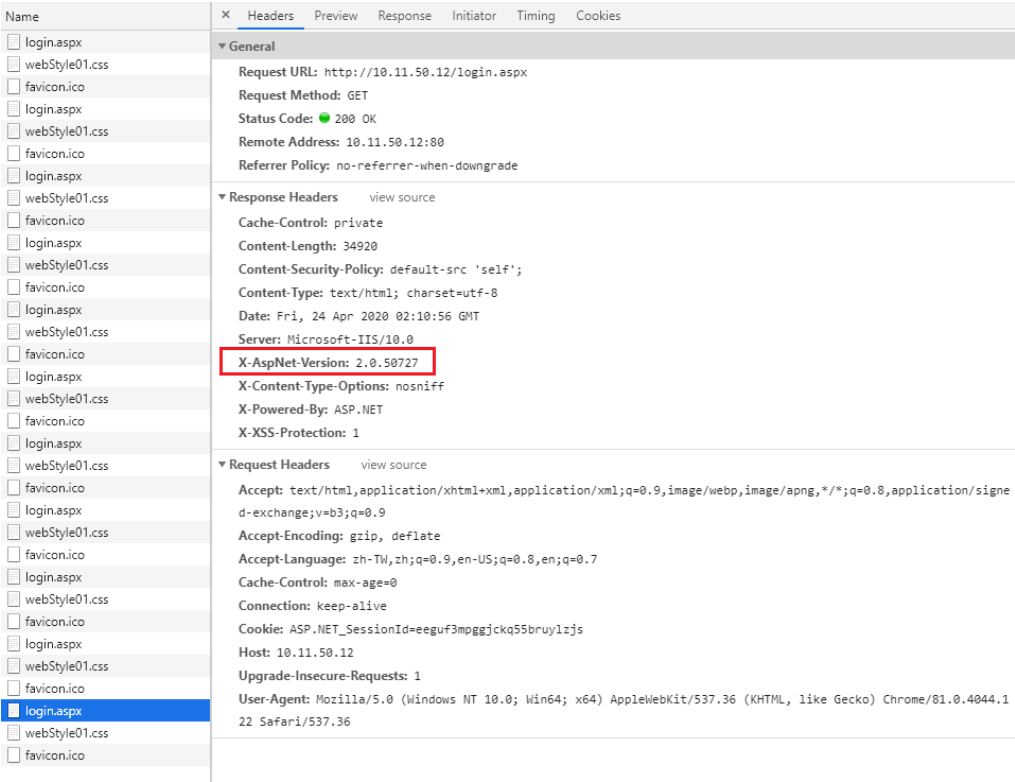
# 網站弱點-催收債協

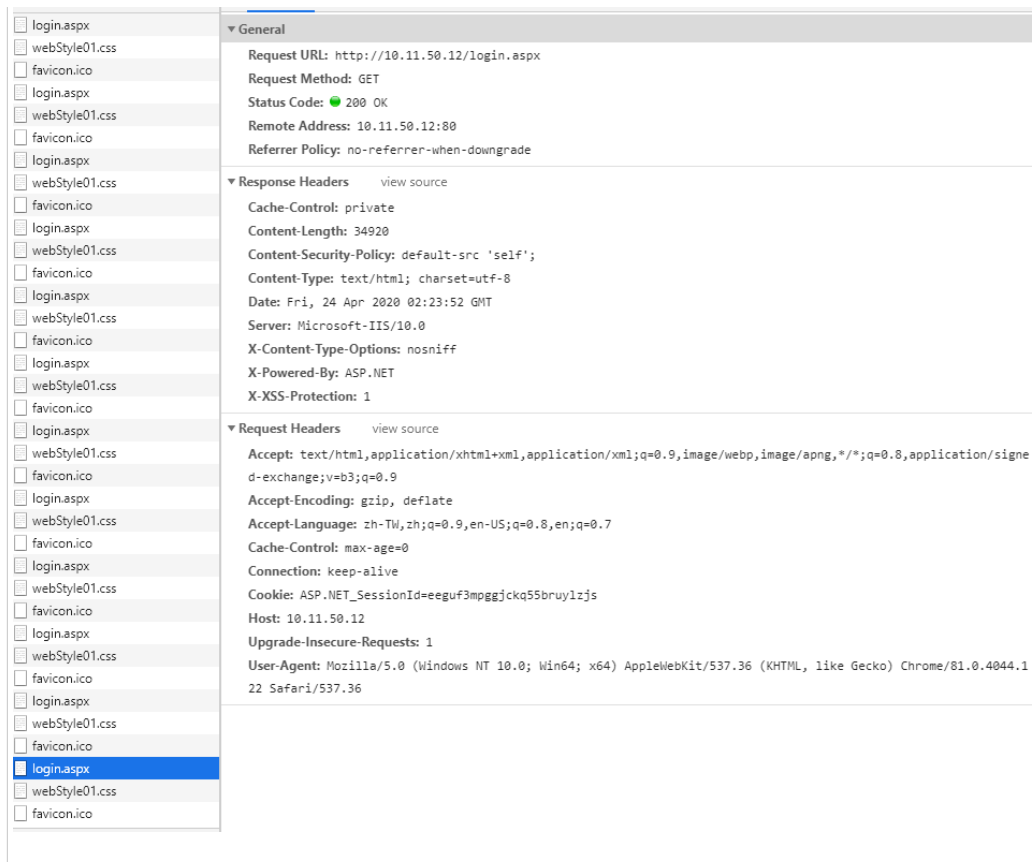
2020年4月23日 上午 10:30

## 1. Unencrypted \_\_VIEWSTATE parameter :

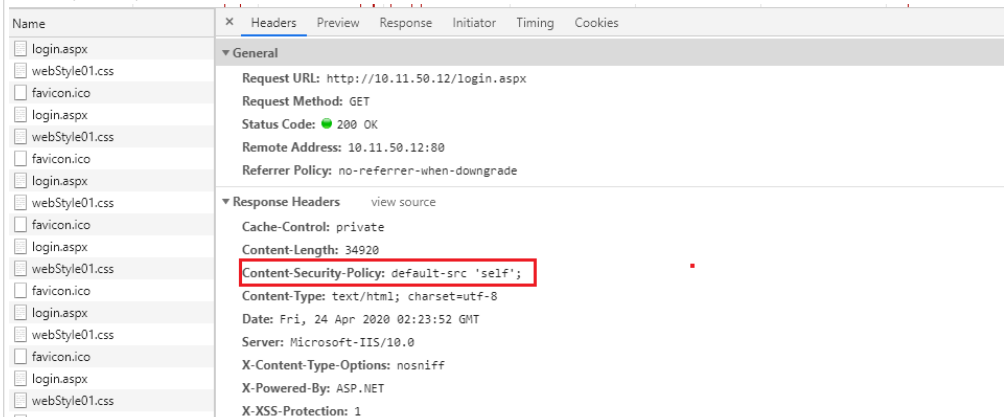
描述	The __VIEWSTATE parameter is not encrypted. To reduce the chance of someone intercepting the information stored in the ViewState, it is good design to encrypt the ViewState. To do this, set the machineKey validation type to AES. This instructs ASP.NET to encrypt the ViewState value using the Advanced Encryption Standard.
解決方式	打開 web.config 進行編輯，在 <system.web> 裡加入一行： <pre>&lt;system.web&gt;   &lt;machineKey validation="AES"/&gt; &lt;/system.web&gt;</pre>

## 2. ASP.NET version disclosure(asp.net版本被暴露) :

描述	應避免暴露 ASP.NET 的版本資訊。
解決方式	打開 web.config 進行編輯，在 <system.web> 裡加入一行： <pre>&lt;System.Web&gt;   &lt;httpRuntime enableVersionHeader="false" /&gt; &lt;/System.Web&gt;</pre>
檢測方式	<p>使用chrome進入該網站，點選F12透過 Chrome 的開發者工具，觀察 Response Headers 的資訊，可發現網站的版本資訊被曝露了。</p>  <p>修改後：.net版本號被隱藏。</p>



### 3. Clickjacking: CSP frame-ancestors missing :

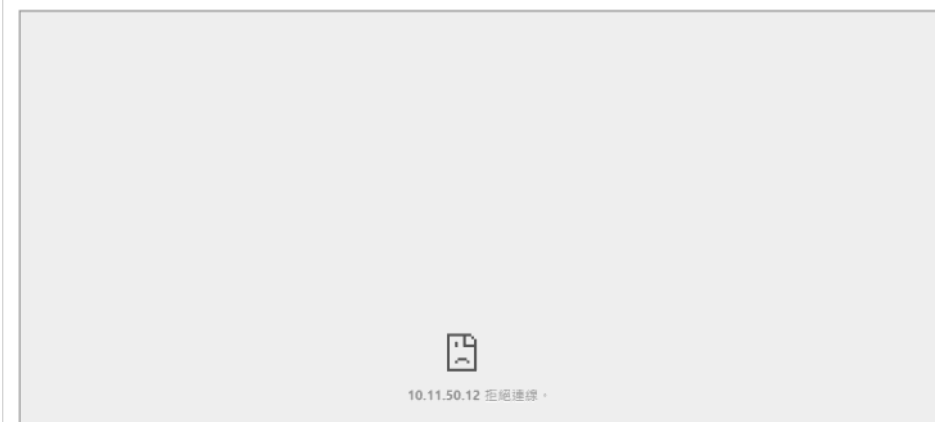
描述	可被透過iframe的html語句使用。
解決方式	<p>打開 web.config 進行編輯，在 &lt;system.web&gt; 裡加入 <b>frame-ancestors 'none'</b>:</p> <pre>&lt;system.webServer&gt; &lt;httpProtocol&gt;   &lt;customHeaders&gt;     &lt;add name="Content-Security-Policy" value="default-src 'self'; frame-ancestors 'none'" /&gt;   &lt;/customHeaders&gt; &lt;/httpProtocol&gt; &lt;/system.webServer&gt;</pre>
檢測方式	<p>使用chrome進入該網站，點選F12透過 Chrome 的開發者工具，觀察 Response Headers 的資訊，其中Content-Security-Policy表頭沒有<b>frame-ancestors</b>。</p>  <p>撰寫html呼叫使用ifrmae呼叫該網站</p> <pre>&lt;div id="page-wrapper"&gt;   &lt;iframe src="http://10.11.50.12/login.aspx" width="1024px" height="768px"&gt; &lt;/iframe&gt; &lt;/div&gt;</pre> <p>別的網站可以正常呼叫該網站</p>

催收及債權系統登入	
員工編號	<input type="text"/>
密碼	<input type="password"/>
登入	
請使用 Window 開機時登入的帳號密碼登入	

修改後Content-Security-Policy表頭有 **frame-ancestors 'none'**。

The screenshot shows the 'Response Headers' section of a web browser's developer tools. The 'Content-Security-Policy' header is highlighted with a red box, displaying the value: `default-src 'self'; frame-ancestors 'none'`. Other visible headers include 'Cache-Control: private', 'Content-Length: 34920', 'Content-Type: text/html; charset=utf-8', 'Date: Fri, 24 Apr 2020 03:16:51 GMT', 'Server: Microsoft-IIS/10.0', 'X-Content-Type-Options: nosniff', 'X-Powered-By: ASP.NET', and 'X-XSS-Protection: 1'.

其他網站無法使用iframe呼叫該網站，會被拒絕。



備註 若本身網站有使用到frame相關的tag的話可以把none改成self，frame-ancestors 'self'，允許自己的網站使用。

#### 4. Cookie(s) without Secure flag set、Cookie(s) without HttpOnly flag set：

描述 個資資料如須記錄在 Cookie，應設定httponly flag以確保只供瀏覽器存取，不能被客戶端的指令碼存取，減少 XSS 的 危害。

解決方式 打開 web.config 進行編輯，在 <system.web> 裡加入：

```
<system.web>
  <httpCookies httpOnlyCookies="true" requireSSL="true" />
</system.web>
```

若沒有使用https，則無需設定requireSSL="true"，該條弱點選接受弱點。

檢測方式 使用chrome進入該網站，點選F12透過 Chrome 的開發者工具，可看出是否修改成功。

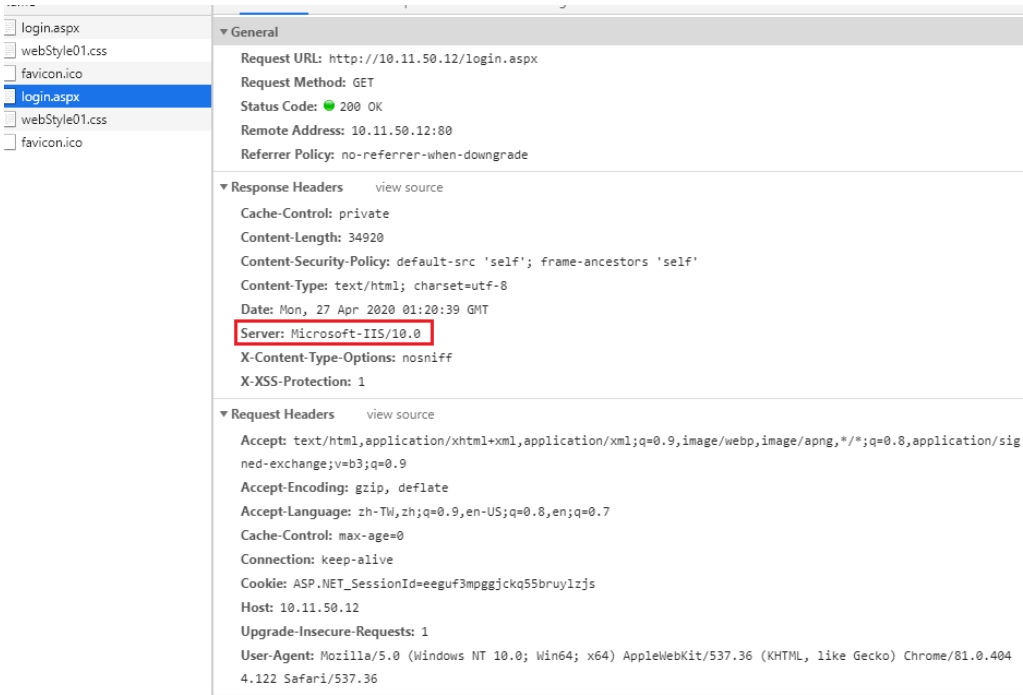
The screenshot shows the 'Application' tab of the Chrome DevTools. The 'Cookies' section is expanded, and a table of cookies is displayed. A red box highlights the 'HttpOnly' and 'Secure' columns, and another red box highlights the 'http://10.11.50.12' cookie entry.

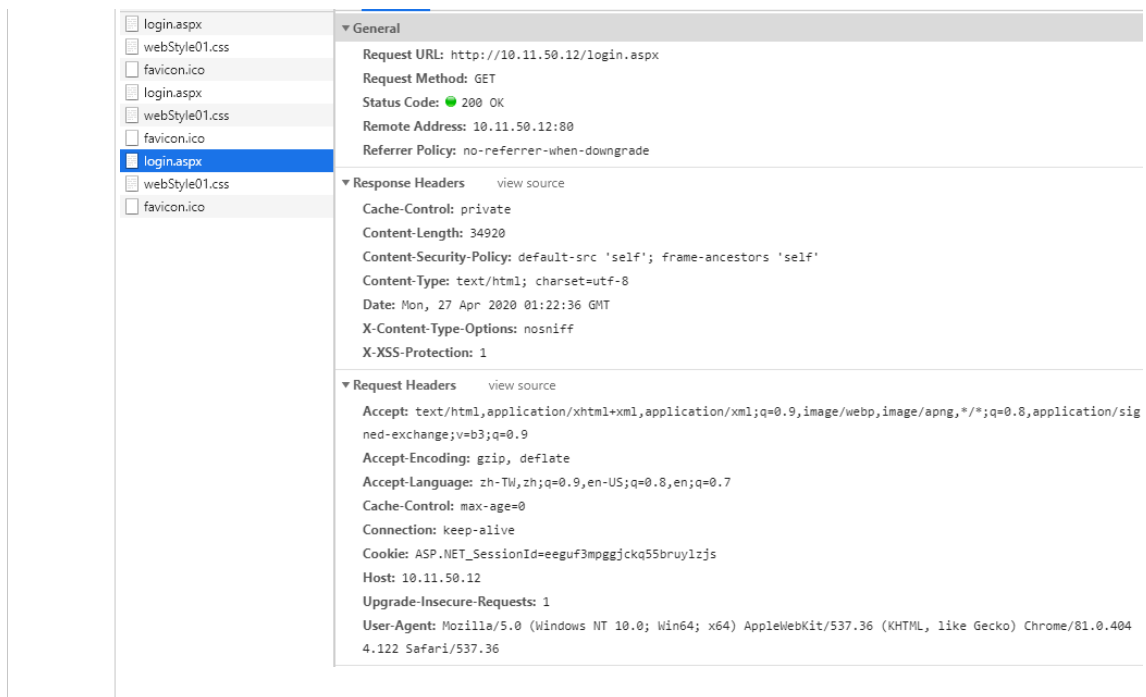
Name	Value	Dom...	Path	Expir...	Size	Http...	Secure	Sam...	Prior...
ASP.NET_SessionId	eegu3mfggjcq55bruyzjs	10.1...	/	Sessi...	41	✓			Medi...

#### 5. Login page password-guessing attack：

描述	密碼沒有限制登入次數，可能被一直登入進行密碼猜測。 PS：透過AD驗證登入超過5次就會被鎖帳號，但被鎖帳號一樣只會返回密碼錯誤，弱掃工具無法得知。
解決方式	於登入頁面加入檢核累計，使用Application物件記錄，當超過一定次數後跳頁至警示頁面。 <pre>protected void btnLogin_Click(object sender, EventArgs e) {     String userId = getLoginUserId();     if (checkLogin(userId, getLoginPassword()))     {         Response.Redirect("FrameSet.aspx");     }     else {         if (Application[userId] == null)         {             Application[userId] = 1;         }         else {             Application[userId] = Convert.ToInt32(Application[userId]) + 1;         }         if (Convert.ToInt32(Application[userId]) &gt;= 10) {             Response.Redirect("UnLock.aspx");         }     } }</pre>
檢測方式	當失敗超過10次，顯示錯誤頁面。 嘗試登入錯誤超過10次

## 6. Microsoft IIS version disclosure :

描述	IIS版本被洩漏
解決方式	IIS10以上改法(Server2016/2019):打開 web.config 進行編輯，在裡加入: <pre>&lt;security&gt;   &lt;requestFiltering removeServerHeader ="true" /&gt; &lt;/security&gt;</pre>
檢測方式	使用chrome進入該網站，點選F12透過 Chrome 的開發者工具，觀察 Response Headers 的資訊，其中Server有IIS版本號。  <p>修改號，版本號不會顯示。</p>



## 7. Password type input with auto-complete enabled :

描述	標籤Input type="password"的自動完成應該關掉。
解決方式	在登入頁面中找到，找到password標籤，加上AUTOCOMPLETE="off"。 <INPUT TYPE="password" AUTOCOMPLETE="off">

## 8. 遺漏或不安全的標頭：

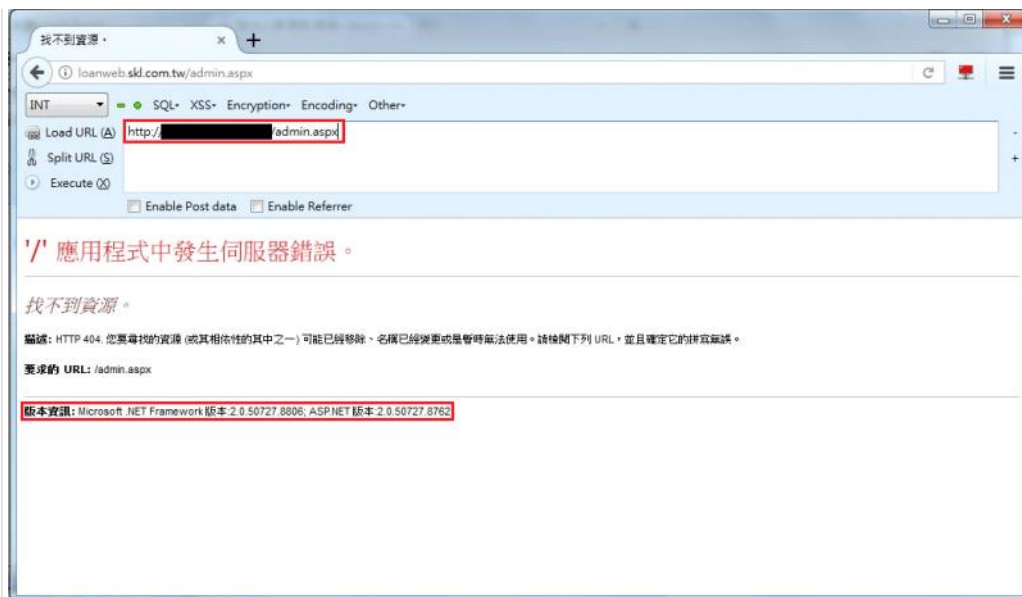
描述	<div>遺漏或不安全的"X-Frame-Options"標頭</div> <div>遺漏或不安全的"X-Content-Type-Options"標頭</div> <div>遺漏或不安全的"X-XSS-Protection"標頭</div>
解決方式	於web.config中增加以下程式。 <pre>&lt;system.webServer&gt;   &lt;httpProtocol&gt;     &lt;customHeaders&gt;       &lt;add name="X-Frame-Options" value="SAMEORIGIN" /&gt;       &lt;add name="X-Content-Type-Options" value="nosniff" /&gt;       &lt;add name="X-XSS-Protection" value="1; mode=block" /&gt;     &lt;/customHeaders&gt;   &lt;/httpProtocol&gt; &lt;/system.webServer&gt;</pre>

## 9. 啟用Microsoft ASP.NET除錯功能：

解決方式	於web.config中將debug屬性改為false: <pre>&lt;compilation debug="false" strict="false" explicit="true"&gt;</pre>
------	---

## 10. 網頁錯誤訊息洩漏機敏資訊：

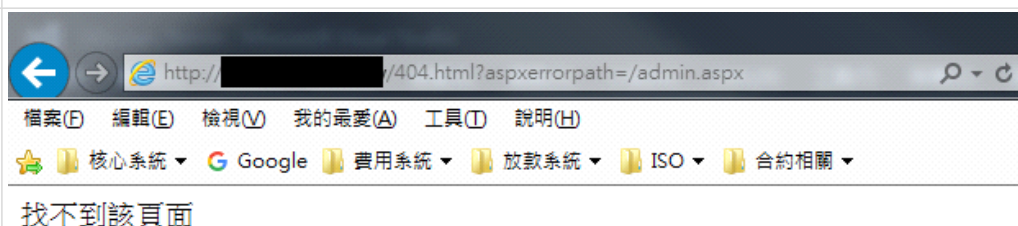
描述	檢測過程中，輸入「 <a href="http://xxx/admin.aspx">http://xxx/admin.aspx</a> 」，發現網頁錯誤訊息未關閉詳細錯誤訊息，導致攻擊者可透過錯誤訊息得知版本資訊，如下圖所示：
----	---



- 解決方式
- 1.新增錯誤訊息頁面(ex:404.html) , 上面顯示當錯誤發生要顯示的訊息。
  - 2.於web.config中增加以下程式, 定義當出現哪種訊息要跳到錯誤頁面。

```
<customErrors mode="On" defaultRedirect="404.html">
  <error statusCode="403" redirect="404.html" />
  <error statusCode="404" redirect="404.html" />
</customErrors>
```

結果



## 1.1. 網頁應用程式洩漏機敏資訊：

描述

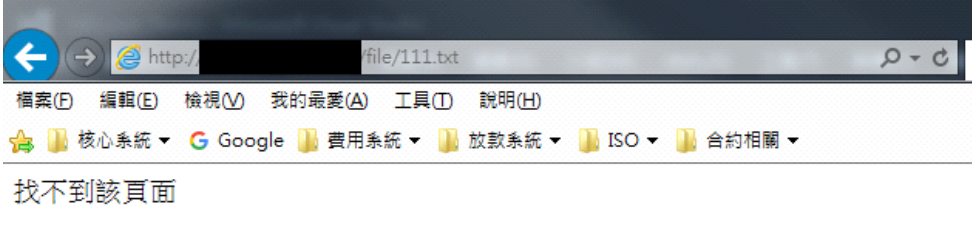
檢測過程中, 輸入「<http://xxx/file/111.txt>」, 發現網頁洩漏個人資料、地址、帳戶, 如下圖所示:



解決方式

於web.config中增加以下程式, 寫上不要顯示的副檔名。

```
<system.webServer>
<security>
  <requestFiltering>
    <fileExtensions>
      <add fileExtension=".csv" allowed="false" />
      <add fileExtension=".txt" allowed="false" />
      <add fileExtension=".xls" allowed="false" />
      <add fileExtension=".out" allowed="false" />
    </fileExtensions>
```

	<pre> &lt;/requestFiltering&gt; &lt;/security&gt; &lt;/system.webServer&gt; </pre>
結果	

## 1 2. 偵測到隱藏目錄：

解決方式	<p>於web.config中增加以下程式，將403錯誤訊息導頁至404.html中。</p> <pre> &lt;httpErrors errorMode="Custom"&gt;   &lt;remove statusCode="404" subStatusCode="-1" /&gt;   &lt;remove statusCode="403" subStatusCode="-1" /&gt;   &lt;error statusCode="404" prefixLanguageFilePath="" path="/404.html" responseMode="ExecuteURL"/&gt;   &lt;error statusCode="403" prefixLanguageFilePath="" path="/404.html" responseMode="ExecuteURL"/&gt; &lt;/httpErrors&gt; </pre>
結果	

## 排外處理

名稱	說明
Unencrypted connection	連線要透過HTTPS進行，但該系統為內部使用沒有對外，因此不須透過HTTPS。
Cookie(s) without Secure flag set	連線要透過HTTPS進行，但該系統為內部使用沒有對外，因此不須透過HTTPS。