P 447

可參考網址︰

<https://ithelp.ithome.com.tw/articles/10197916>

上面所說的，和 PDF 有出入。可能 PDF 已舊版。但我先看完PDF。

P 450 名詞解釋 (不是重點，也不是目錄)

|  |  |  |
| --- | --- | --- |
| Authentication | 驗証 | 使用 Credential 證明用戶是誰 |
| Authorization | 授權 | 用戶端是否有權限 |
| Impersonation | 模擬 | 使用**有驗証 +**  **權限的**用戶端來**執行**程式 |
| Delegation | 委派 | 更進階的**模擬**機制  以**模擬的**用戶端來**存取**遠端資源 |

這些設計，使ASP.NET 和 IIS 和 NTFS 檔案系統緊密整合。

NTFS (New Technology File System) 的維基︰<https://zh.wikipedia.org/wiki/NTFS>

ASP.NET的自介︰<https://dotnet.microsoft.com/apps/aspnet>

<https://dotnet.microsoft.com/learn/aspnet/what-is-aspnet>

Authentication驗証

(這個才是小主題們)

|  |  |  |  |
| --- | --- | --- | --- |
| None | Window | Forms | Passport |
| 不啓用ASP.NET  驗証服務 | 由作業系統檢視帳戶中的帳號和密碼。 | 由程式設計師來設計密碼驗証邏輯  將管理Cookie並且將使用者導向登入網頁。  通常要在IIS 中啓用匿名存取。 | 由 (下方網頁)  Passport Service <http://www.passport.com>  來進行密碼驗證  iis 7 不支援  iis 5 ,6 可支援 |

P452

也支援 Forms-Based Authentication ?

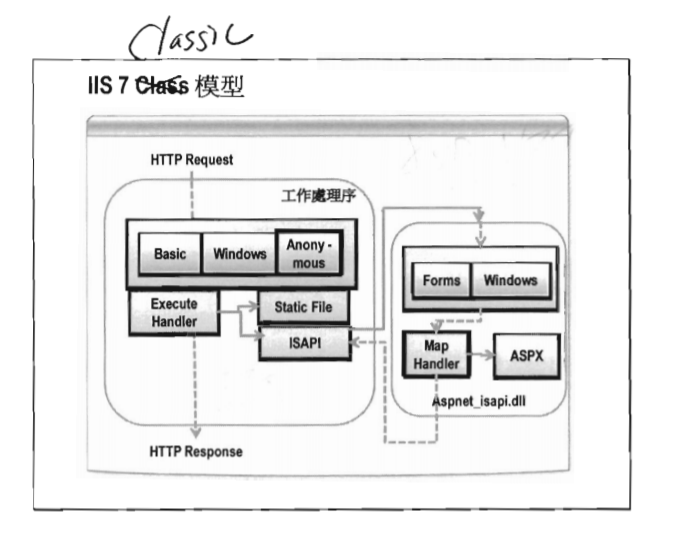
表單式驗証 使用 cookie 驗証者， 適合 Internet 應用程式？

None 略過不說。

##### P 453 Window 由作業系統檢視帳戶中的帳號和密碼。

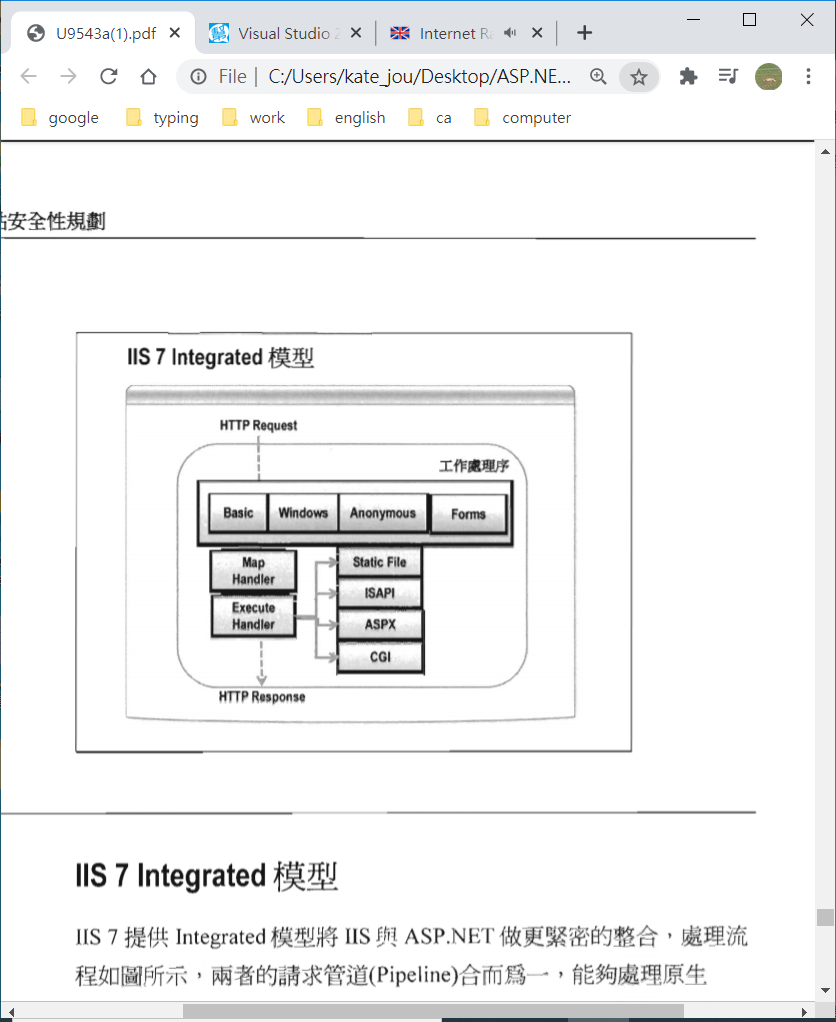
|  |  |  |
| --- | --- | --- |
| Anonymous Access | 匿名 | 不驗證 (預設) |
| Basic Authentication | 基本 | 工業標準  所有瀏覽器支援  帳號密碼以明碼傳？ |
| Digest Authentication | 摘要式 | 改良自基本  需目錄服務？  非所有瀏覽器支援  帳密不以明碼傳 |
| Integrated Window Security | 整合式 | 最安全機制 ?  使用目前登入身份作驗證。 |

P454 ( 還在說Window 嗎？怎麼突然說這個？ )



IIS7

|  |  |
| --- | --- |
| Classic模型 | Integrated 模型 |
| 運作和IIS 6一樣(具相容性)。  使用分離模型處理請求  =  處理 ASP.NET 請求時，  將IIS 和 ASP.NET 的 請求管道(pipelines) 分離。(如上圖)  ASP.NET 實作成 Server Application Programming Interface extension  (aspnet\_isapi.dll)  ISAPI ( Instance Server Application Programming Interface ?自己猜)  dll 就是一個 extension  aspnet\_isapi.dll以一個獨立的應用程式架構連接伺服器。  負責處理 ASPX﹑ASMX 等。  其他靜態檔案等，不歸他管。  分離模型的注意事項︰  1. 只處理有在 HTTP Handler 註冊的請求。  2. 某些動作重複發生?，如驗證 ?  3. 某些設定要在網站與IIS 重複設定?，如授權 ? | 使用整合模型處理請求  =  處理 ASP.NET 請求時，  IIS 和 ASP.NET 的 請求管道(pipelines) 合一。(如下圖)  能處理原生(Native)與Managed模組?  原生︰DLL (dynamic-link libraries)  Managed︰實作成.NET Framework類別？  整合模型好處︰   1. 能處理所有類型的Request   包括 原生﹑Managed 模組 和靜態檔案﹑CGI 等。  CGI ? 維基︰  <https://zh.wikipedia.org/wiki/CGI>   1. 減少 IIS 和 ASP.NET 重複執行動作，如驗證﹑URL 授權。 2. 集中管理設定 3. 易於使用ASP.NET Managed 模組來擴充IIS |

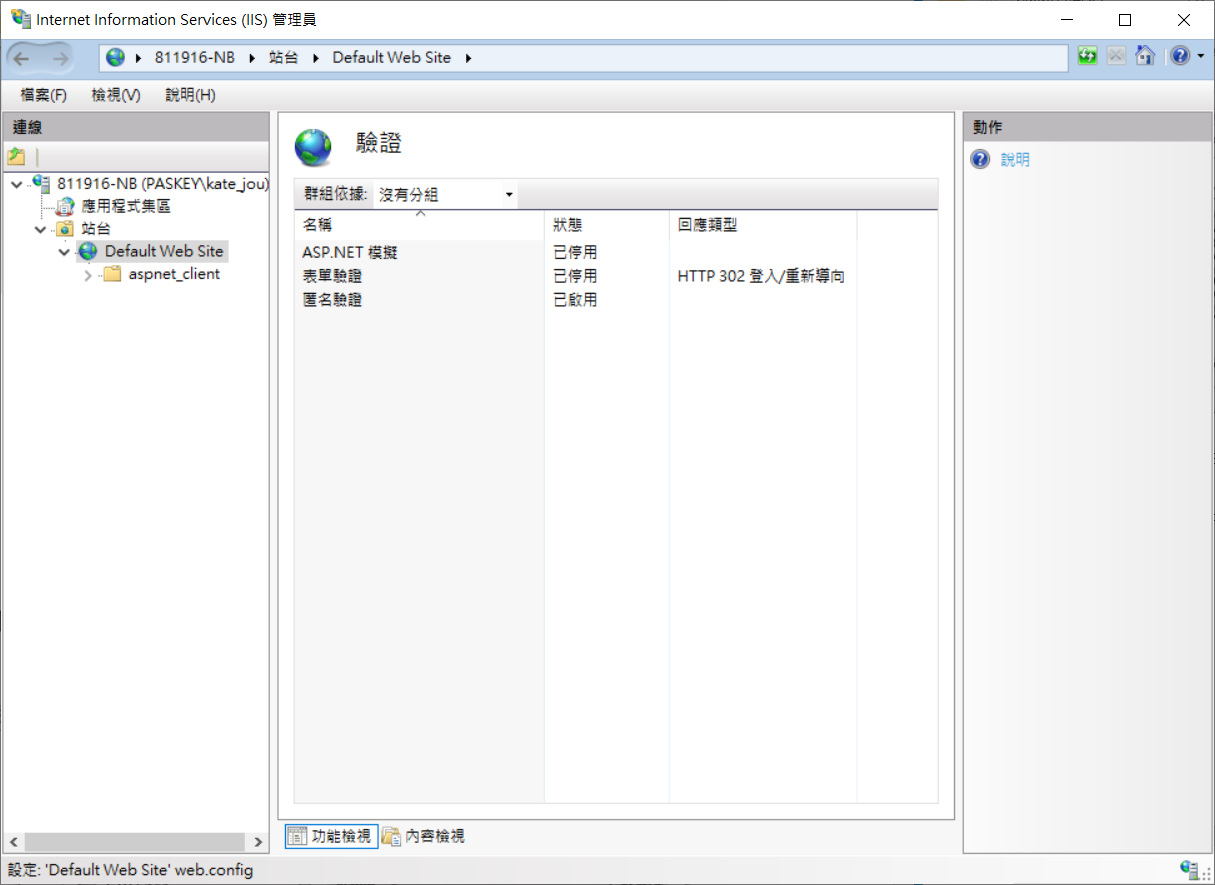


以上的兩個模型，是可以在哪裡，如何切換？

P 457 啓用或停用 Window 驗證

用 IIS > 找到 安全性 > 驗證 (Authentication)

在 Anonymous Authentication (匿名驗證) 右鍵 > Disable (停用)



預設的樣子。

P458 IUSR帳號

當網站設定為匿名驗證(預設)，

會以一個標準的Window 使用者帳號來執行程式，這就是IUSR帳號( I user ? )。

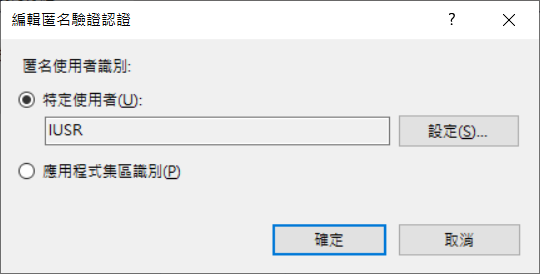
在安裝 IIS 時，就用自動建立了這個帳號。

可以用IIS 管理工具來變更改用別的帳號? How

例如指定特定帳號? How

或是使用應用程式集區的帳號(預設Network Service)? How

How : 右鍵 「匿名驗證」 > 編輯。



未實作，將實作看看是怎樣的結果。

P459 在 ASP.NET 網站設定 Windown驗證。 (終於說回來Window 了。)

在 Web.config 中設︰

<configuration>

<system.web>

<authentication mode="Windows"/>

</system.web>

</configuration>

預設以「非使用者」登入帳號執行，(🡨 以外人來登錄這個網站。)

如要以「使用者」來登錄這個網站︰

<identity impersonate="true" /> (這是放在system.web之中的)

這個「使用者身份」的掀涉到︰存取這個網站資源的權限。

Window驗證，可以用於內部網路，控管Window的使用者使用權限。

因為這個方法，結合了︰NTFS 的ACL (Access Control List)

這個內部網路，是所有的電腦都是用Window 系統的嗎？用Mac / Linux 的話，都不能用這個網絡了？

P 461 EX 13\_1

1. 實作 window 驗證，

2. 檢查使用者權限，

3. 顯示使用者帳號

4. 顯示驗證類型。

Step 1 :

開一頁空白的 Web Form ，前端放三個 Label 。

PageLoad 寫︰

Label1.Text = User.Identity.Name;

Label2.Text = User.Identity.AuthenticationType;

Label3.Text = System.Security.Principal.WindowsIdentity.GetCurrent().Name;

Web.Config 加︰

<authentication mode="Windows" />

在上文提過的位置。

F5開出來的結果︰

只有第三個 Label 會有顯示︰我現在在這個Window主機名和我的帳號名。

第一﹑二個 Label 都是空白，因為 IIS 啓用匿名存取。

第三個 Label 會顯示是因為它屬於︰ Network Service ?

Label1 = Name

Label2 = Authentication Type

Label3 = Window Identity

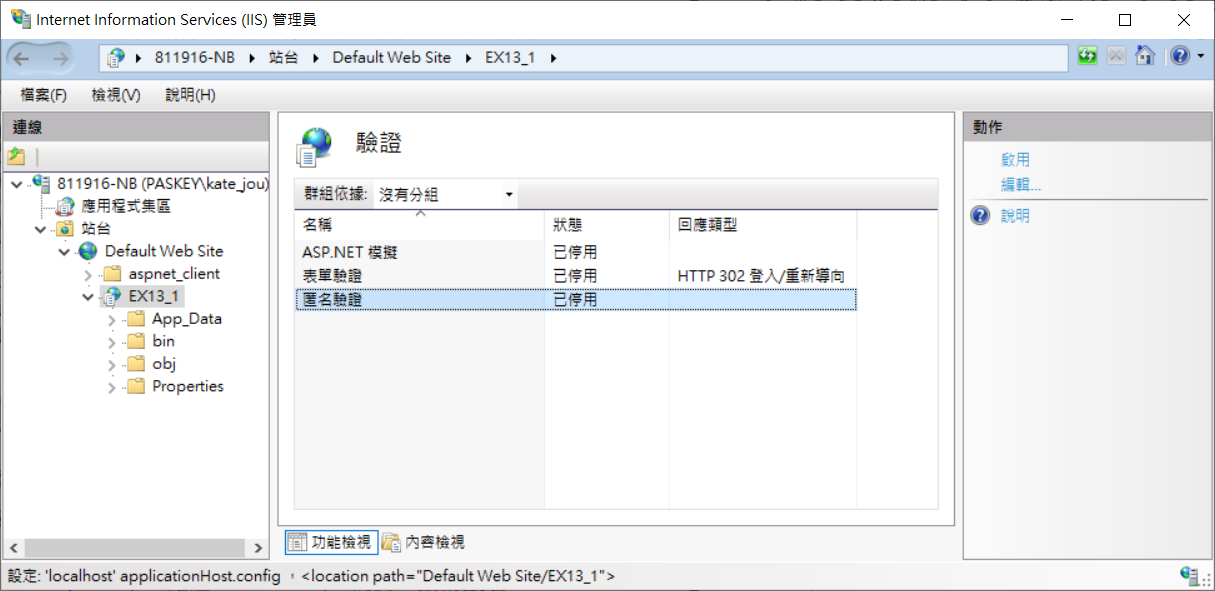
P463

Step 2 :

掛到 iis

匿名驗證 修改為「停用」，步驟如上所述。

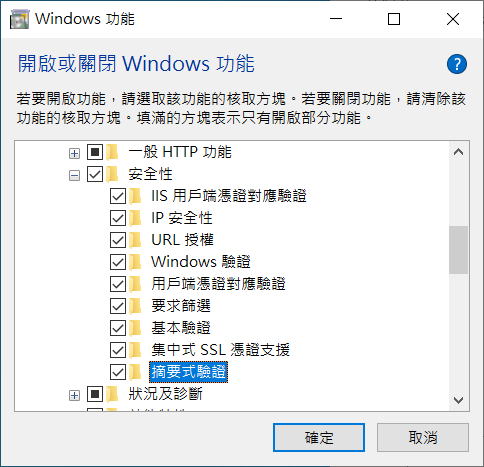
Windows Authentication 修改為「啟用」。 🡨 沒有這個選項



|  |
| --- |
| 引發一連串失敗的嘗試  和PDF裡不同，是因為舊版？︰    <https://blog.darkthread.net/blog/aspnet-and-iis-auth-setting/>  但是黑暗大的2019年版的教學卻有？  IIS 啟用停用匿名驗證、Windows 驗證的設定不是儲存在 web.config，而是在 C:\Windows\System32\inetsrv\config\applicationHost.config  我一層層的點開(用管理員權限，不能直貼路徑)，    結果如右圖。  <https://dotblogs.com.tw/DivingDon/2018/01/16/IISWindowsCertificate>  今天在Win Server 2016安裝了IIS後要使用Windows驗證，但IIS內找不到此驗證方式 ….  此時要回到伺服器管理員-->新增角色及功能-->網頁伺服器(IIS)-->安全性-->勾選Windows驗證  伺服器管理員 ?  <https://docs.microsoft.com/zh-tw/windows-server/administration/server-manager/server-manager>  伺服器管理員主控台隨附于 Windows 10 的[遠端伺服器管理工具](https://go.microsoft.com/fwlink/?LinkID=404281)。  請注意，當遠端伺服器管理工具安裝在用戶端電腦上時，  您無法使用伺服器管理員來管理本機電腦。  伺服器管理員不能用來管理執行 Windows 用戶端作業系統的電腦或裝置。  您只能使用伺服器管理員來管理以 Windows 為基礎的伺服器。  <https://www.microsoft.com/zh-tw/download/confirmation.aspx?id=45520>  我在這個網址上下載了[遠端伺服器管理工具](https://go.microsoft.com/fwlink/?LinkID=404281)。    在「開始」找到 Sever Manager > 按 新增角色及功能時︰  於是照做︰      結果確定後，沒有任何效果。  (Active Directory 可以掃到公司裡千台以上的電腦，但是不要用為好…)    沒有伺服器可以管理，它就不能打開 Windows Authentication ? |

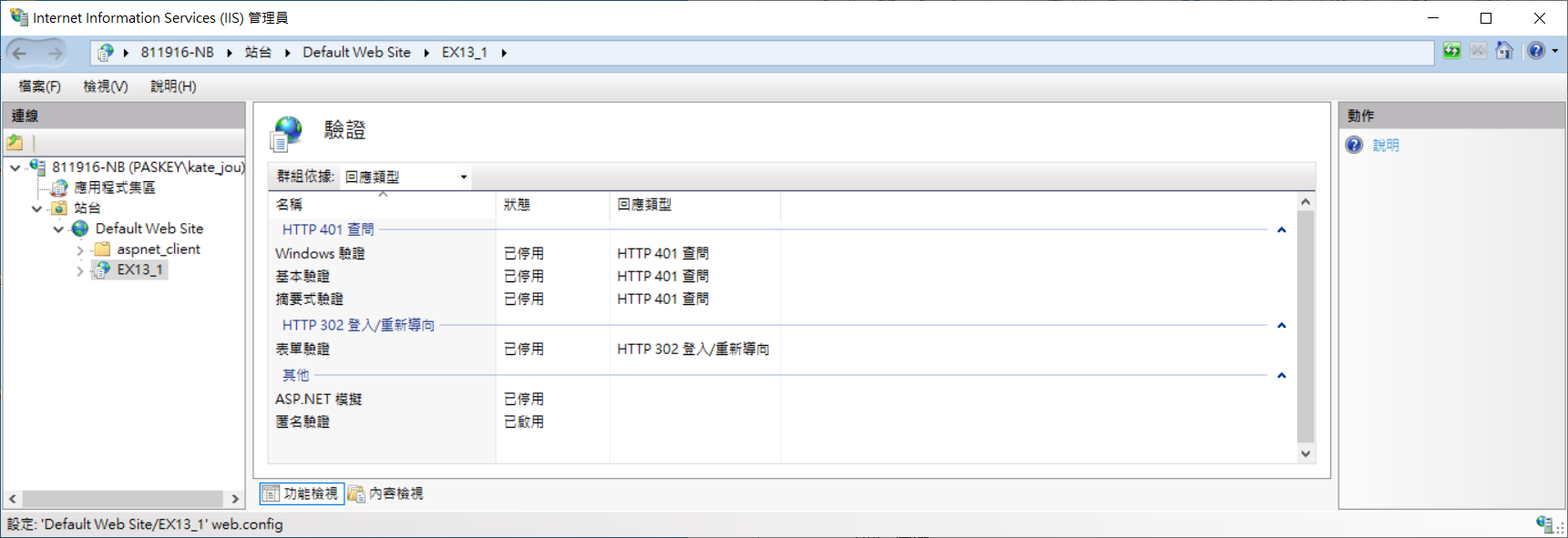
結果我去控制台>程式集>

開始或關閉 Window 功能 (參考學掛站的第一個網址)



勾開 Windows 驗證 和 之後好像會用到的 左鄰右里 等…

再開一次iis



有了。

我啟用Windows 驗證 ，停用其他。

但我還是看不到 Label1 和 2。

我懷疑是< identity impersonate="false" /> (PDF說這是預設)

這個自動出現在Web.config 的東東防礙了。結果我把它設為true︰

出現︰



最有可能的原因 :system.web/identity@impersonate 已設為 true。

解決方法 :

如果应用程序支持它，则禁用客户端模拟。

如果您确信可以忽略此错误，则可以通过将 system.webServer/validation@validateIntegratedModeConfiguration 设置为 false 来禁用它。

<https://stackoverflow.com/questions/4209999/an-asp-net-setting-has-been-detected-that-does-not-apply-in-integrated-managed-p>

<configuration>

<system.webServer>

<validation validateIntegratedModeConfiguration="false"/>

</system.webServer>

</configuration>

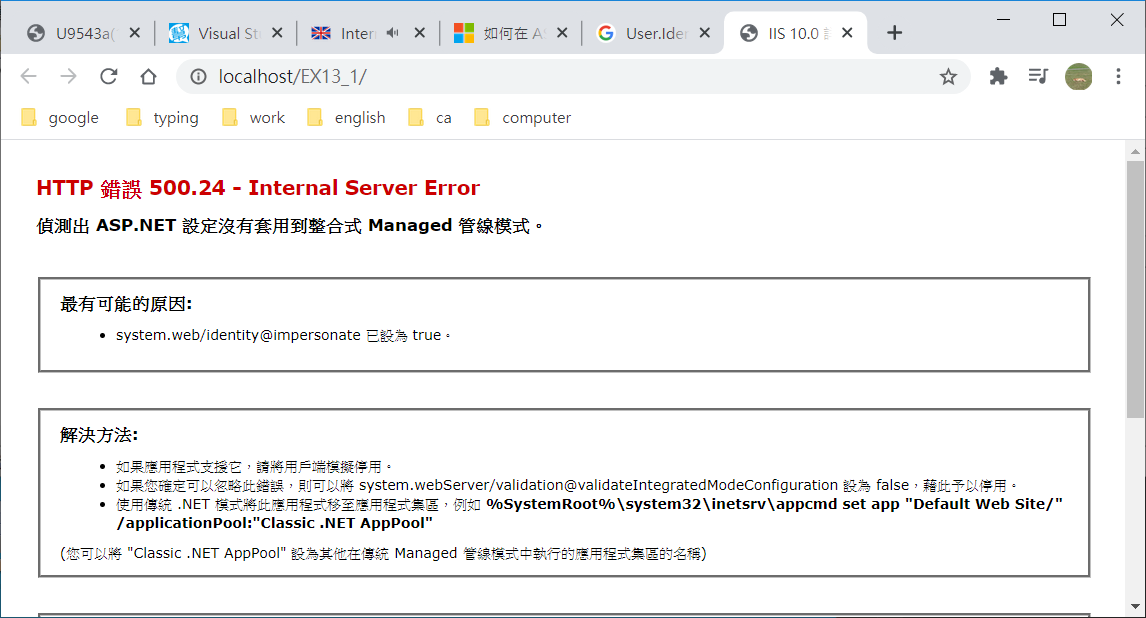
貼上看看。

結果︰ <identity impersonate="true"/> 可以開出了頁面，但是 Label 1,2 還是空白

<https://docs.microsoft.com/zh-tw/dotnet/api/system.security.principal.iidentity?view=netcore-3.1>

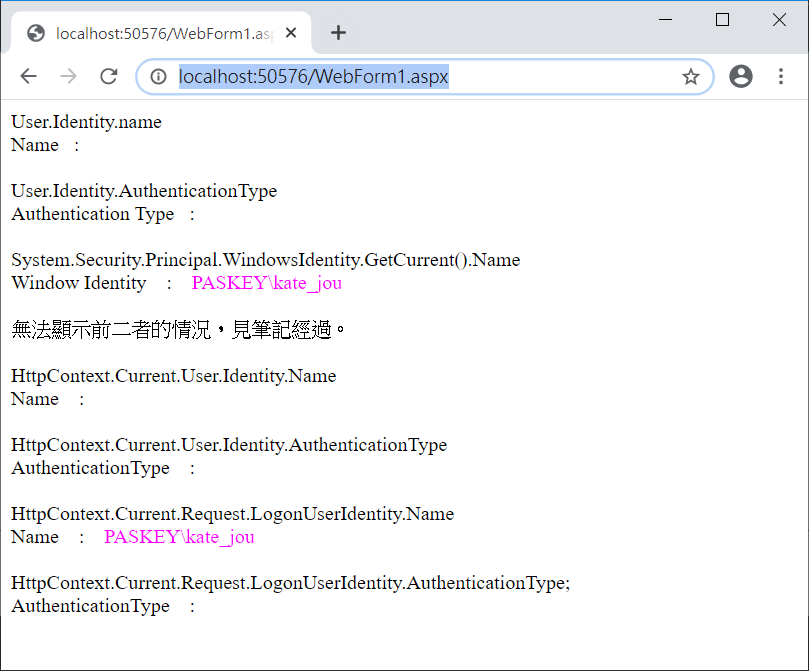
明明這個官網也說可以取得的…

在 IIS 開的話︰



算了，原地放棄。

網絡搜尋其他方法後︰



不過，掛了上iis ， 用 iis 開，按照了它的錯誤提醒︰我在 Web.config 改了一下︰

<configuration>

<system.web>

<compilation debug="true" targetFramework="4.7.2" />

<httpRuntime targetFramework="4.7.2" />

<authentication mode="Windows" />

<identity impersonate="false" />

</system.web>

<system.webServer>

<validation validateIntegratedModeConfiguration="true" />

<defaultDocument>

<files>

<add value="WebForm1.aspx" />

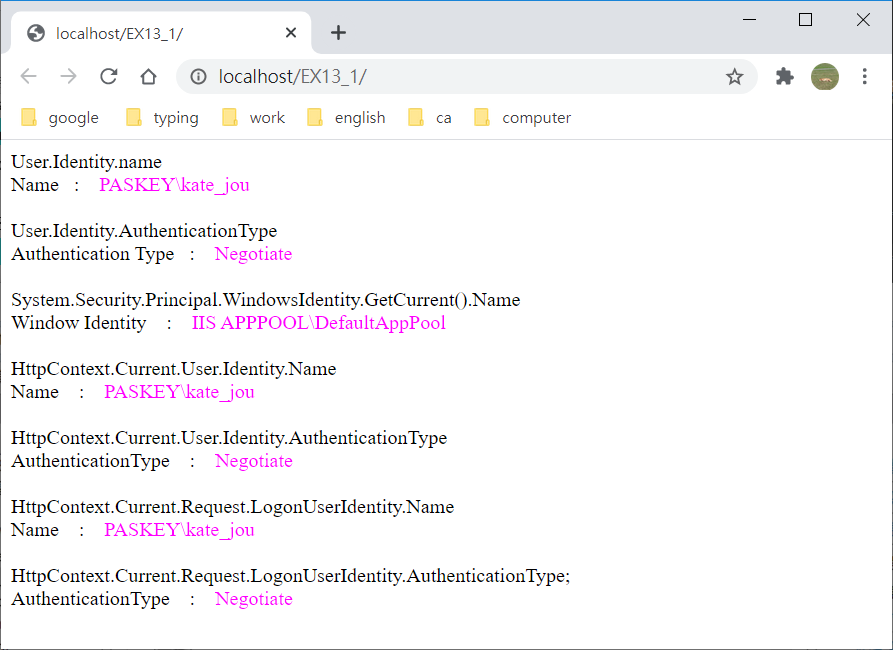
</files>

</defaultDocument>

</system.webServer>

</configuration>

在 iis 就可以開出以下的結果︰



P464

第 11 步︰

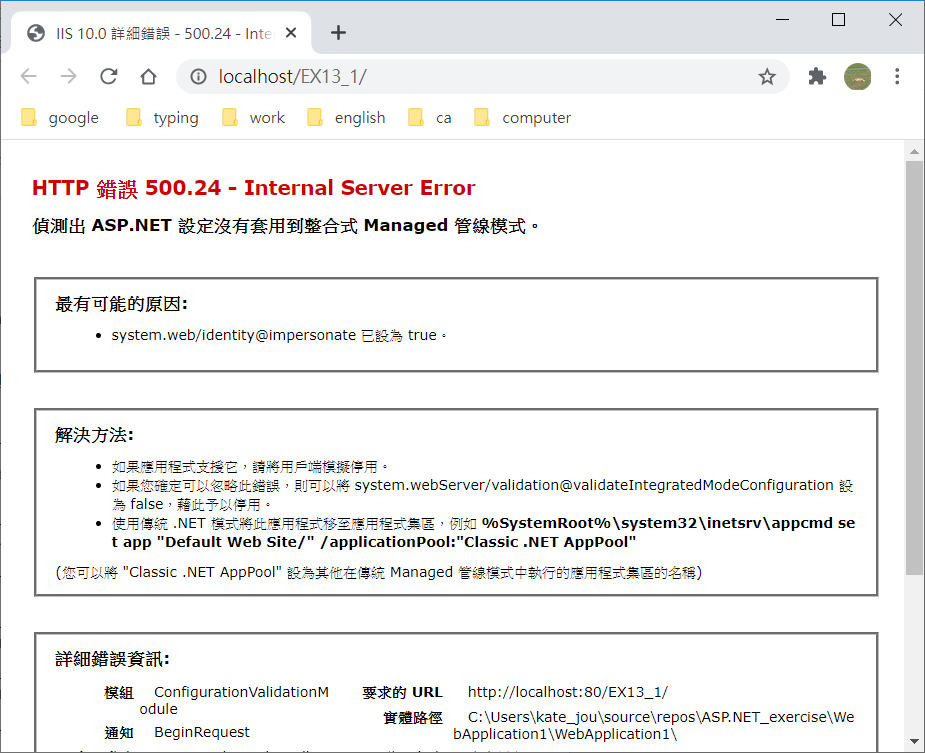
在 iis 上改 impersonation = Enable ? >「ASP.NET 模擬」 = 啟用

WindowsIdentity 會變得和 Name 一樣？

<https://anisv.pixnet.net/blog/post/36123043>

可以用下列的表格快速檢查一下ASP.NET 及 IIS 的設定是否有問題

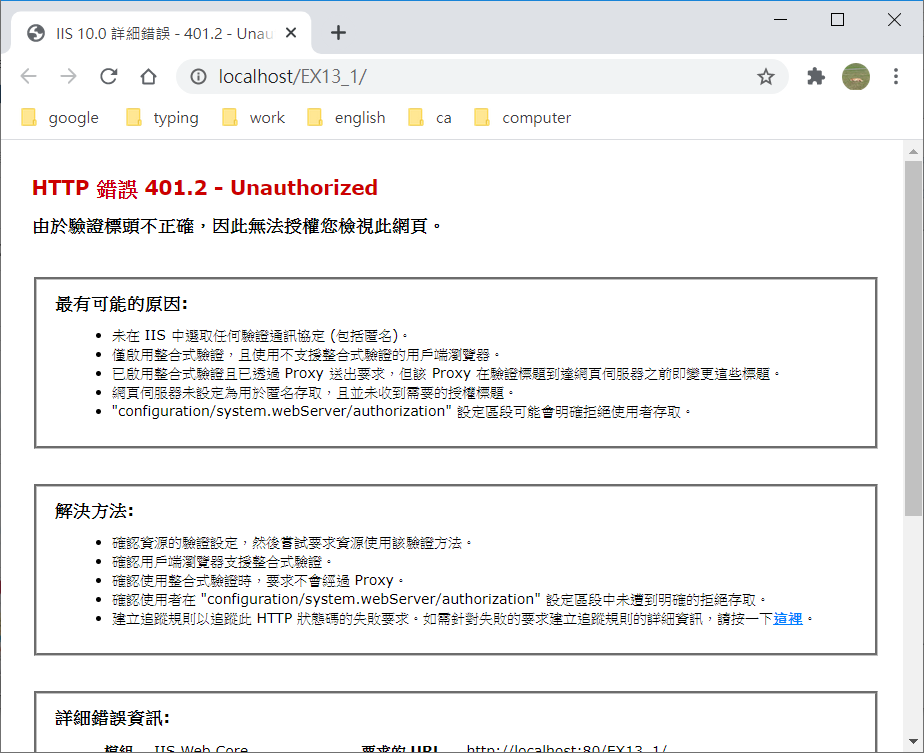
|  |  |  |  |
| --- | --- | --- | --- |
| Impersonation | Anonymous Access | WindowsIdentity.GetCurrent().Name | User.Identity.Name |
| Enabled | Enabled | IUSR\_<computer> | Empty string |
| Enabled | Disabled | ISV\Jacky | ISV\Jacky |
| Disabled | Enabled | NT Authority\Network Service | Empty string |
| Disabled | Disabled | NT Authority\Network Service | ISV\Jacky |



修 <identity impersonate="false" />

能開出，但沒有變化。

我去關了 Window 驗證看看︰



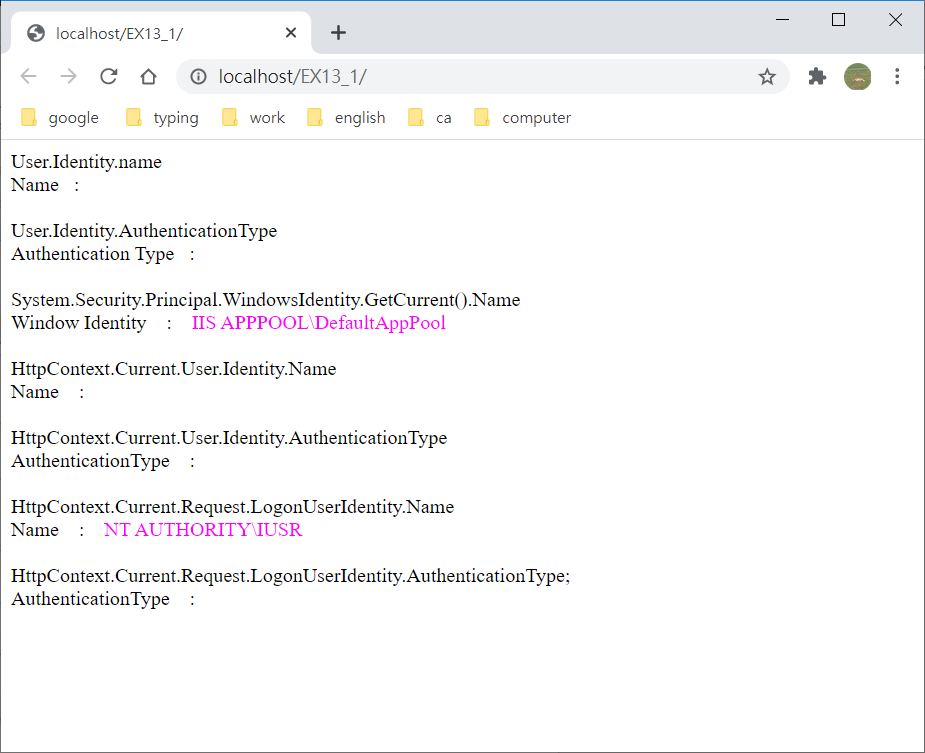
修 <identity impersonate="true" />

同上。

在亂試的時候 :

啟用匿名驗証 + <identity impersonate="false" />

開出以下的結果︰



IIS 7.5 Enabling ASP.Net Impersonation with Windows Authentication

<https://forums.iis.net/t/1228054.aspx>

沒有用。

亂試成功二︰

<configuration>

<system.web>

<compilation debug="true" targetFramework="4.7.2" />

<httpRuntime targetFramework="4.7.2" />

<authentication mode="Windows" />

<identity impersonate="true" />

</system.web>

<system.webServer>

<validation validateIntegratedModeConfiguration="false" />

<defaultDocument>

<files>

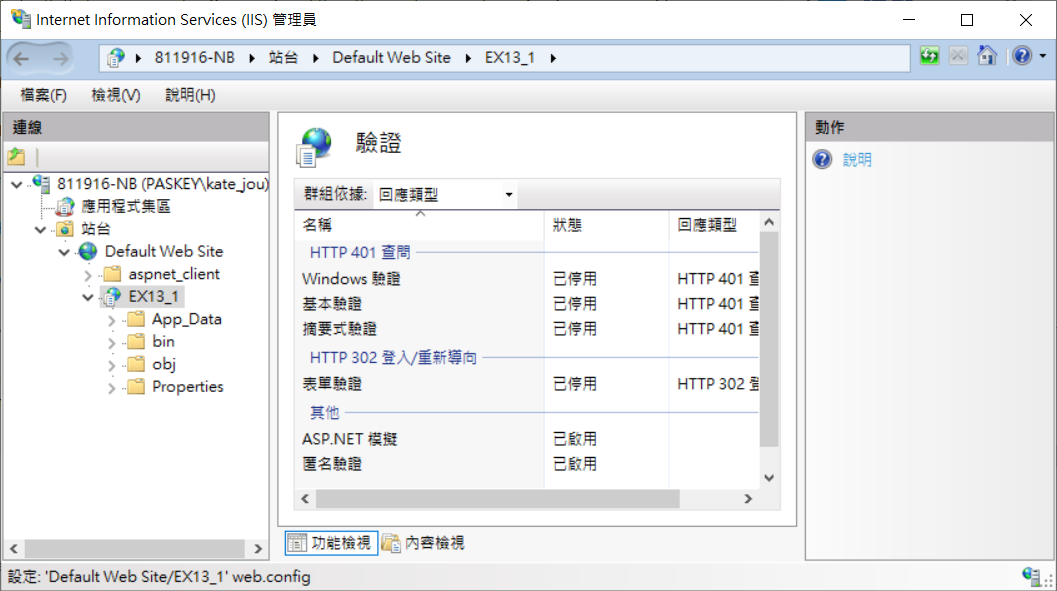
<add value="WebForm1.aspx" />

</files>

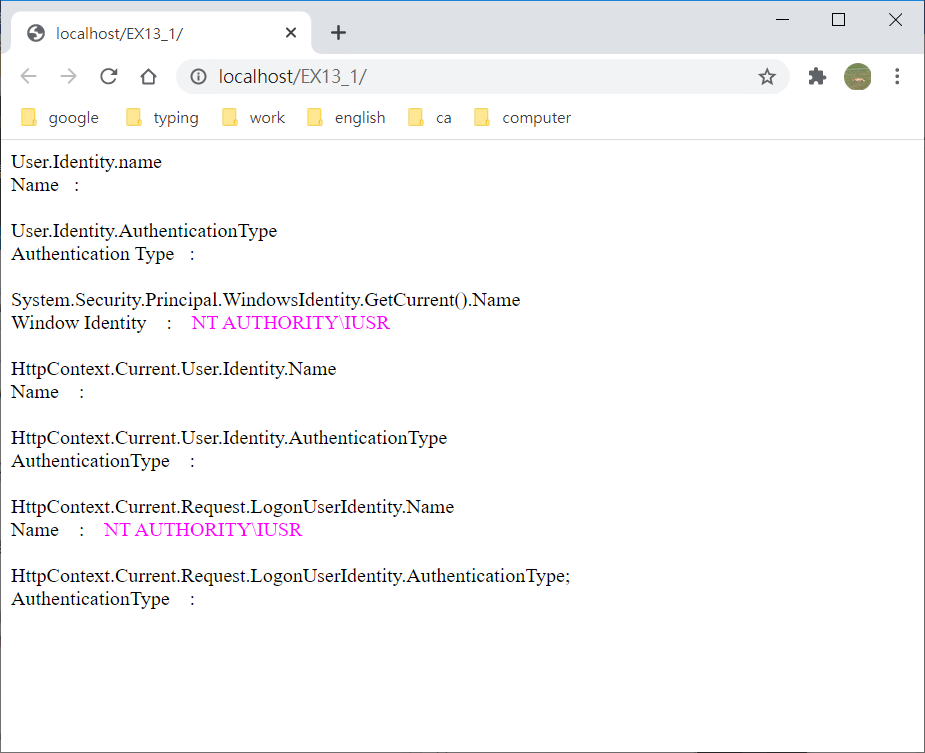
</defaultDocument>

</system.webServer>

</configuration>

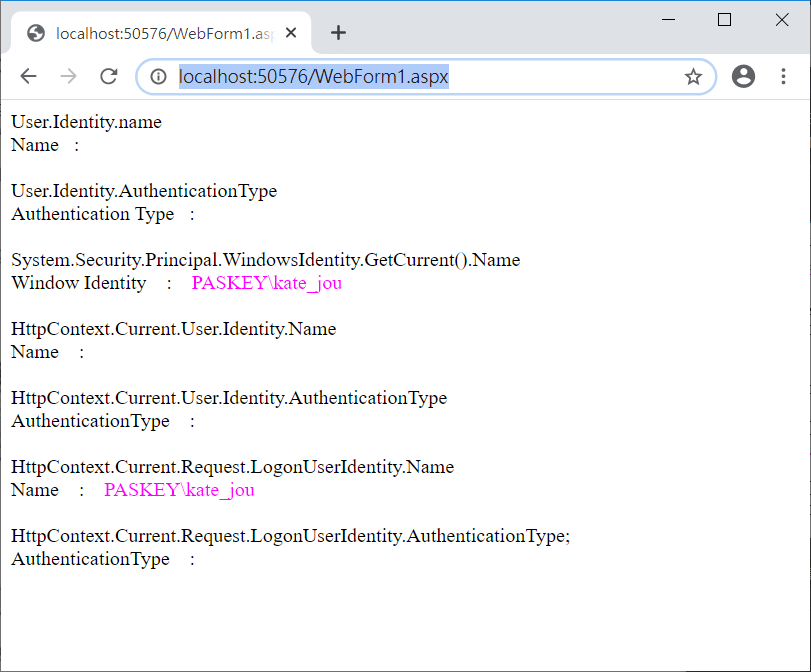


開出︰

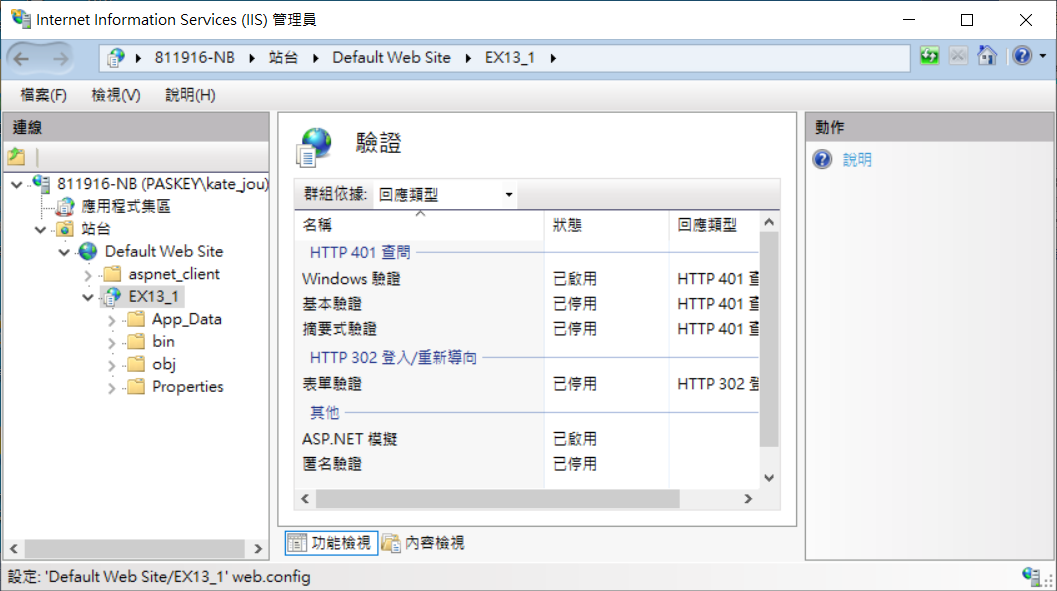


…. 總算是 一個 Name 和 Windows Identity 成功同步的例子？

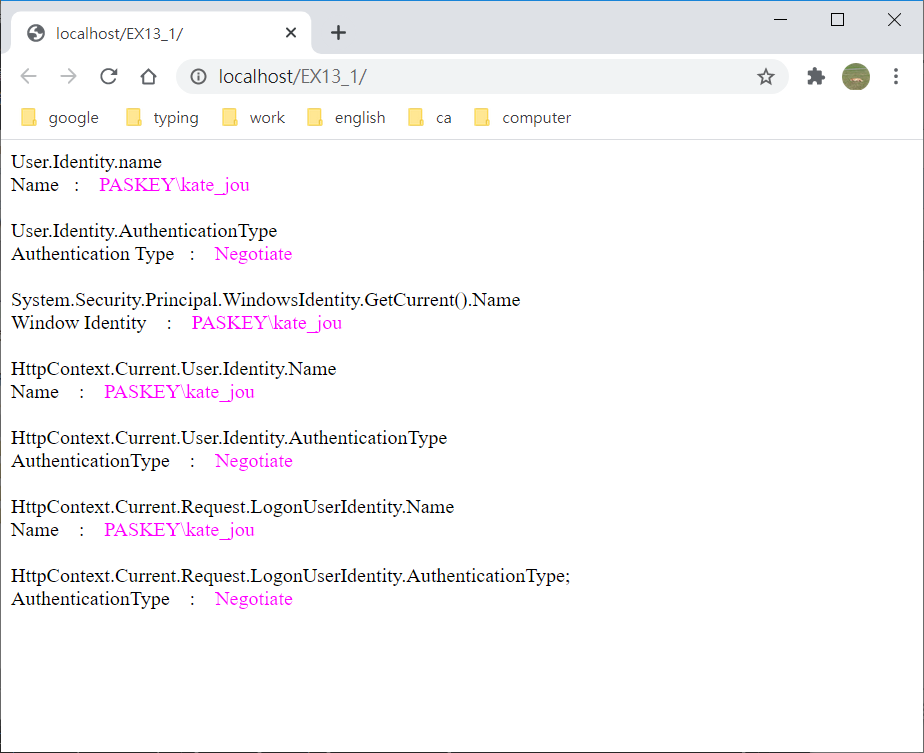
如果是 F5 出來的話，如下圖︰



在前文的 Web.config 不變下，只改這下面︰



終於成功了︰



其他補充︰

部署內部網站並使用 Windows 驗證登入的標準作業流程

<https://blog.miniasp.com/post/2014/01/12/Deployment-Intranet-Sites-using-Windows-Authentication-SOP>

使用windows驗證(Using Windows Authentication)

<https://www.itread01.com/content/1549113336.html>

##### P 465 Form 由程式設計師來設計密碼驗証邏輯

Window 驗證用於內部網絡，有易於管理使用者的長處 (我沒有實作過，PDF說的。)

網際網路的用Form 比較好。它將帳密存放在資料庫或文字檔再利用程式進行驗證。

使用 Forms 驗証︰

|  |
| --- |
| 1. IIS 要設為 匿名存取   驗証成功後，ASP.NET會將驗証Cookie寫入瀏覽器，因此   1. 用戶瀏覧器必需支授Cookie 的機制，或使用 Cookieless Sesson 2. From 驗証通過後，若用戶諯想要存取「受安全保護的資源」，必須再通過URL授權檢查。 |

-----

P466 啓用 Forms 驗證

在組態檔中設定，不動態改變。

Web.config 中 forms 常用的 屬性︰

|  |  |
| --- | --- |
| loginURL | 登入網頁所在的 URL |
| name | HTTP Cookie 的名稱。若多個應用程式(視窗頁面等)在「同一台」電腦上使用 Forms-base。各應用程式的Cookie 都要分開。  HOW ? |
| Timeout | Cookie 的逾期時間，以分鐘為單位。 |
| path | 已發行 Cookie 使用的路徑，預設為 / ? |

ASP.NET授權(Authorization)

|  |  |
| --- | --- |
| 授權 = | 用戶端是否有權限 (取後系統資源) |
| ASP.NET 支援 | ACL 授權 和 URL 授權 |
| URL 授權 = | 控制用戶端可否存取 URL 資源 ? |
| 做法 | 在Web.config 允許，某使用者或群組。 |

URL 授權 例子︰

|  |
| --- |
| 允許 George 以 Admins 群組存取，拒絕匿名。  「?」= 匿名 = 沒有通過驗証  「\*」= 所有使用者 (包不包括匿名？)  <configuration>  <system.web>  <authentication mode="Forms" />  <authorization>  <allow users="George" />  <allow roles="Admins" />  <deny users="?" />  </authorization>  </system.web>  </configuration>  ------------  多於一個使用者 :  <allow users="George,Mary" />  限制所有使用者不可以使用 GET 方法來存取 Web 應用程式︰  <deny VERB="GET" users="\*" /> |

P468 啓用 Forms 驗證步驟︰

|  |
| --- |
| 1. 將 IIS 設為匿名存取 ( 只enable 這個 ? )。 2. Web.config 設 (這個是設在 system.web 以外的？和上方不同？)   <configuration>  <authentication mode="Forms">  <forms  name=".ASPXCOOKIE" ??  loginUrl="login.aspx"  timeout="30"  path="/">  </forms>  </authentication>  </configuration>   1. Web.config 設 (這個是設在 system.web 以外的？和上方不同？)   <authorization>  <deny users="?" />  </authorization>   1. 建立 login.aspx login 通過之後，是會自動的跳去主頁？ |

P 469 撰寫登入網頁

在網頁(前端)中，滙入︰ 不用在前端，在後端using 就好

~~<%@ Import Namespace="System.Web.Security " %>~~

會多了FormsAuthentication.三個功能︰

1. Authenticate -- 將使用者輸入的帳密傳去驗證，回傳 bool

Authenticate 已過時

<https://docs.microsoft.com/zh-tw/dotnet/api/system.web.security.formsauthentication.authenticate?view=netframework-4.8>

1. RedirectFromLoginPage -- 導向要前往的網頁
2. SignOut -- 登出

P 470 EX 13.2 使用 Forms 驗證

在 Web.config 的 system.web 加入︰

<!--這個是在︰Form\_Authentication 去用的-->

<authentication mode="Forms">

<forms loginUrl="登入的網頁.aspx" />

</authentication>

<authorization>

<deny users="?" />

</authorization>

<identity impersonate="false"/>

<!--end-->

---------------------------

設計登入頁面，兩個 Textbox ，一個輸入帳號，一個輸入密碼 ….

P471

-----

using System.Web.Security;

登入的按鈕︰

protected void Button1\_Click(object sender, EventArgs e)

{

if (TextBox1.Text == "User" || TextBox2.Text == "PWD") {

FormsAuthentication.RedirectFromLoginPage(TextBox1.Text,false);

} else {

Label1.Text = "帳密有誤";

}

}

-------------------------------

FormsAuthentication.RedirectFromLoginPage(TextBox1.Text,false);

第一個參數通過驗證的使用者，第二個參數是︰

是否( 在伺服器 )產生 Cookie 去記錄登入者的機器

如果是 true ︰

使用者可以 ( 在同一台電腦 ) 使用多個瀏覽器，共享一個 Session (的 ID )

如果是 false ︰

使用者的電腦上，一個瀏覽器就是一個 Session (的 ID)

不同瀏覽器可以登入不同的帳戶

P472

設計登入後的歡迎頁面︰ 🡨 要設定為起始頁，成功登入後才會來到這裡。

using System.Web.Security;

PageLoad : Label1.Text = "歡迎 " + User.Identity.Name;

放入「登出」按鈕

protected void Button1\_Click(object sender, EventArgs e)

{

FormsAuthentication.SignOut();

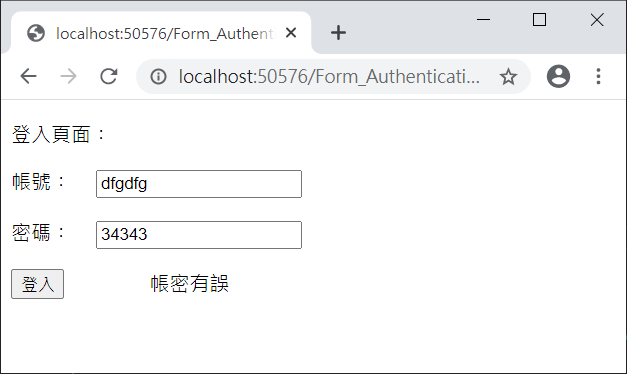
Response.Redirect("登入的那一頁.aspx");

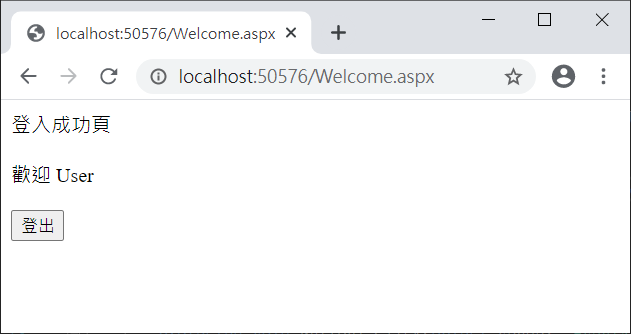
}

1. 因為 <forms loginUrl="XXX.aspx" />

XXX.aspx 成為了這個方案 ( /網站 ) 的首頁

2. Session 和 Cookie 的部份我沒有測。但用到再說。





P 474 使用安全管理工具 (暫略)

使用 ASP.NET 應用程式組態工具

建立使用者帳號及 使用者所屬角色。

P 467 的第三步已過時，跟不上。(好像是會開出一個網頁)

結果應該是可以建立 一個 ASPNETDB.MDF 檔案來存放使用者帳戶資料的。

P 478 使用安全性控制項

Tool box 中的控制項︰

Login : 登入的介面

LoginName : 顯示登入者名稱

LoginStatus : 顯示登入狀態

LoginView : 登入後，與登入前的不同畫面

PasswordRecovery : 提供密碼查詢/重設

ChangePassword : 變更密碼

CreateUserWizard : 建立使用者帳號

P 480 實作︰

??

使用 ASP.NET Identity （C#）進行帳戶確認和密碼復原

<https://docs.microsoft.com/zh-tw/aspnet/identity/overview/features-api/account-confirmation-and-password-recovery-with-aspnet-identity>