Web Application Report

This report includes important security information about your web application.

安全報告

這份報告是由 HCL AppScan Standard 所建立 10.6.0
掃描開始時間： 2024/10/21 上午2:24:14

目錄

簡介

這份報告包含由 HCL AppScan Standard 執行 Web 應用程式安全掃描的結果。

中嚴重性問題：	8
報告中併入的安全問題總計：	8
掃描中探索到的安全問題總計：	23

一般資訊

掃描檔名：	2_wwwWEB
掃描開始時間：	2024/10/21 上午2:24:14
測試原則：	Default
CVSS 版本：	3.1
測試最佳化等級：	快速
主機	www.tyc.com.tw
埠	443
作業系統：	Unix
Web 伺服器：	Apache
應用程式伺服器：	任何

登入設定值

登入方法： 無

摘要

問題類型 6

目錄

	問題類型	問題數目
中	SameSite 屬性不安全、不適當或遺漏的 Cookie	1
中	不安全的第三方鏈結 (target="_blank")	1
中	主機標頭注入	1
中	加密的階段作業 (SSL) Cookie 中遺漏安全屬性	1
中	有弱點的元件	1
中	檢查是否有 SRI（子資源完整性）支援	3

有漏洞的 URL 3

目錄

	URL	問題數目
中	https://www.tyc.com.tw/	5
中	https://www.tyc.com.tw/admin/	2
中	https://www.tyc.com.tw/.admin/	1

修正建議 6

目錄

	補救作業	問題數目
中	將元件升級到最新穩定版本	1
中	將屬性 rel = "noopener noreferrer" 新增至 target="_blank" 的每一個鏈結元素	1
中	將每一個第三方 Script/鏈結元素支援新增至 SRI（子資源完整性）。	3
中	建構 HTTP 標頭時要很小心，避免使用未驗證/未消毒的輸入資料	1
中	新增 'Secure' 屬性至所有機密 Cookie	1
中	檢閱將 SameSite Cookie 屬性配置為建議值的可能解決方案	1

安全風險 6

目錄

風險	問題數目
中 將 Cookie 限制為第一方或相同網站環境定義以預防 Cookie 資訊洩漏。如果沒有設置額外的保護措施（如反 CSRF 記號），攻擊者可以延伸為偽造跨網站要求 (CSRF) 攻擊。	1
中 有可能說服無經驗而易受騙的使用者提供機密性資訊，如：使用者名稱、密碼、信用卡號碼、社會保險號碼等等	2
中 有可能透過 Web 快取毒害來破壞網站內容	1
中 有可能竊取在加密階段作業期間傳送的使用者和階段作業資訊 (Cookie)	1
中 攻擊者有可能使用 Web 伺服器來攻擊其他網站，讓其身分更加隱密	1
中 假設第三方伺服器已受損，網站的內容/行為會變更	3

原因 10

目錄

原因	問題數目
中 SameSite 屬性不適當、不安全或遺漏的機密 Cookie	1
連結元素中的 rel 屬性未設定為 "noopener noreferrer"。	0
中 以 target=_blank 鏈結所鏈結到的頁面可以透過 window.opener 物件部分存取鏈結頁面視窗物件	1
缺少輸入驗證和消毒	0
中 Web 應用程式會執行重新導向至外部網站	1
中 Web 應用程式會透過 SSL 傳送未受保護的 Cookie	1
測試應用程式中使用了一個有弱點的元件。	0
中 未安裝協力廠商產品的最新修補程式或緊急修復程式	1
不支援子資源完整性。	0
中 不支援 SRI（子資源完整性）	3

WASC 威脅分類

目錄

威脅	問題數目
伺服器配置錯誤	1
併入遠端檔案	3
資訊洩漏	1
濫用功能	3

依問題類型排列的問題

中 SameSite 屬性不安全、不適當或遺漏的 Cookie 1 目錄

問題 1 / 1 目錄

SameSite 屬性不安全、不適當或遺漏的 Cookie

嚴重性：	中
CVSS 評分：	4.7
CVSS 向量：	AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N/E:U/RL:O/RC:C/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL：	https://www.tyc.com.tw/
實體：	ci_session (Cookie)
風險：	將 Cookie 限制為第一方或相同網站環境定義以預防 Cookie 資訊洩漏。如果沒有設置額外的保護措施（如反 CSRF 記號），攻擊者可以延伸為偽造跨網站要求 (CSRF) 攻擊。
原因：	SameSite 屬性不適當、不安全或遺漏的機密 Cookie
修正：	檢閱將 SameSite Cookie 屬性配置為建議值的可能解決方案

差異：

推論： 回應包含 SameSite 屬性不安全、不適當或遺漏的機密 Cookie，這可能會導致 Cookie 資訊洩漏。如果沒有設置額外的保護措施，可能會衍生出偽造跨網站要求 (CSRF) 攻擊。

測試要求和回應：

```
GET / HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: www.tyc.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Date: Sun, 20 Oct 2024 18:27:54 GMT
Server: Apache/2.4.62 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
Set-Cookie: ci_session=thvip5ent6d6tl1jg4p2c0lqb7k67lof; expires=Sun, 20 Oct 2024 20:27:54 GMT; Max-Age=7200; path=/;
HttpOnly; SameSite=Lax
Set-Cookie: locale=en; expires=Sun, 20 Oct 2024 18:28:54 GMT; Max-Age=60
```

```
<!DOCTYPE html>
<html class='no-js' lang='zh-TW'>
<head>
    <!-- #BEGIN -->
    <!-- Google tag (gtag.js) -->
    <script async src="https://www.googletagmanager.com/gtag/js?id=G-BNNQ75MX9K"></script>
    <script>
    window.dataLayer = window.dataLayer || [];
    function gtag(){dataLayer.push(arguments);}
    gtag('js', new Date());

    gtag('config', 'G-BNNQ75MX9K');
    </script>
    <!-- Google tag (gtag.js) -->
    <!-- #END -->

    <meta charset='utf-8'>
    <title>TYC Brother Industrial Co., Ltd</title>
    <meta content='width=device-width, initial-scale=1.0' name='viewport'>
    <link href="https://www.tyc.com.tw/assets/stylesheets/fa-all.css" media="screen" rel="stylesheet" type="text/css"/> <!-
-2023.01.07 import font awesome css link-->
    <link href="https://www.tyc.com.tw/assets/stylesheets/all.css" media="screen" rel="stylesheet" type="text/css"/>
    <link href="https://www.tyc.com.tw/assets/stylesheets/all-2023.css?v=20230901" media="screen" rel="stylesheet"
type="text/css"/> <!--2023.01.18 2023 Renewal of website brand image-->
    <script src="https://www.tyc.com.tw/assets/javascripts/jquery.js" type="text/javascript"></script>
    <style>
        .goodbyeieeight { text-align: center; position: fixed; z-index: 9999; top: 0; right: 0; bottom: 0; left: 0;
background-color: #1f1f1f; color: #ffffff; padding-top: 120px; }
        .goodbyeieeight h1, .goodbyeieeight h2 { margin: 0 auto; width: 50%; }
        .goodbyeieeight p { margin: 20px auto; width: 50%; }
        .goodbyeieeight a { display: inline-block; color: #ffffff; width: 120px; }
        .goodbyeieeight img { display: block; width: 64px; margin: 0 auto; }

    </style>
    <!-- <link rel="shortcut icon" href="https://www.tyc.com.tw/assets/images/favicon.ico"> -->
    <link rel="apple-touch-icon" sizes="180x180" href="https://www.tyc.com.tw/assets/images/apple-touch-icon.png">
    <link rel="icon" type="image/png" sizes="32x32" href="https://www.tyc.com.tw/assets/images/favicon-32x32.png">
    <link rel="icon" type="image/png" sizes="16x16" href="https://www.tyc.com.tw/assets/images/favicon-16x16.png">
    <link rel="manifest" href="https://www.tyc.com.tw/assets/images/site.webmanifest">
    <link rel="mask-icon" href="https://www.tyc.com.tw/assets/images/safari-pinned-tab.svg" color="#5bbad5">
    <meta name="msapplication-TileColor" content="#da532c">
    <meta name="theme-color" content="#ffffff">

    <!-- SEO -->
    <meta property="og:image" content="https://www.tyc.com.tw/assets/images/SEO-cover.jpg"/>
    <meta property="og:image:url" content="https://www.tyc.com.tw/assets/images/SEO-cover.jpg"/>
    <meta property="og:image:secure_url" content="https://www.tyc.com.tw/assets/images/SEO-cover.jpg"/>
    <!-- SEO -->

</head>
<body>
<!--[if lt IE 9]>
<div class='goodbyeieeight'>
    <h1>您的瀏覽器版本太舊了！</h1>

    <h2>Your Browser is totally out of date !</h2>

    <p>請更新至 Internet Explorer 9 以上版本或選用更現代化的瀏覽器：</p>

    <p>We strongly recommend you at least upgrade your browser to Internet Explorer 9 by WindowsUpdate or try any modern
browsers below for the best web-surfing experiences.</p>

    <p>
        <a href='http://www.google.com/chrome/'><img src='https://www.tyc.com.tw/assets/images/chrome.png'>Google
Chrome</a>
        <a href='https://www.mozilla.org/en-US/firefox/new/'><img
src='https://www.tyc.com.tw/assets/images/firefox.png'>Mozilla Firefox</a>
        <a href='http://www.opera.com/zh-tw'><img src='https://www.tyc.com.tw/assets/images/opera.png'>OPERA</a>
        <a href='https://www.apple.com/tw/safari/'><img src='https://www.tyc.com.tw/assets/images/safari.png'>Safari</a>
    </p>
    </br>
    <h2>IE 8 以下瀏覽器請直接</h2>
    <h2><a href='http://notesweb.tyc.com.tw/public/scm.nsf/tyclink.xsp' target="_blank"><font color="#FFFF00">由此進入<font>
</a></h2>
    <p> </p>
</div>
<![endif]-->
<div id='sb-site'>
    <div id='wrapper'>
        <div id='sticker'>
    <nav class='restrict'>
        <div class='brand'>
          <a class='brand-icon-2023' href='https://www.tyc.com.tw/'></a>
        </div>
```

```
...
...
...
```

中 不安全的第三方鏈結 (target="_blank") 1

目錄

問題 1 / 1

目錄

不安全的第三方鏈結 (target="_blank")

嚴重性：	中
CVSS 評分：	5.3
CVSS 向量：	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL：	https://www.tyc.com.tw/
實體：	(Page)
風險：	有可能說服無經驗而易受騙的使用者提供機密性資訊，如：使用者名稱、密碼、信用卡號碼、社會保險號碼等等
原因：	以 target=_blank 鏈結所鏈結到的頁面可以透過 window.opener 物件部分存取鏈結頁面視窗物件
修正：	將屬性 rel = "noopener noreferrer" 新增至 target="_blank" 的每一個鏈結元素

差異：

推論： 具有 target="_blank" 屬性但沒有 rel="noopener noreferrer" 屬性的第三方鏈結可讓鏈結的頁面部分存取鏈結頁面視窗物件

測試要求和回應：

```
GET / HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: www.tyc.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Date: Sun, 20 Oct 2024 18:27:55 GMT
Server: Apache/2.4.62 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
Set-Cookie: ci_session=4dp1ou9vfg1tna86autpvqkjnq8fllrb; expires=Sun, 20 Oct 2024 20:27:55 GMT; Max-Age=7200; path=/;
HttpOnly; SameSite=Lax
Set-Cookie: locale=en; expires=Sun, 20 Oct 2024 18:28:55 GMT; Max-Age=60

<!DOCTYPE html>
<html class='no-js' lang='zh-TW'>
<head>
    <!-- #BEGIN -->
    <!-- Google tag (gtag.js) -->
    <script async src="https://www.googletagmanager.com/gtag/js?id=G-BNNQ75MX9K"></script>
    <script>
    window.dataLayer = window.dataLayer || [];
    function gtag(){dataLayer.push(arguments);}
    gtag('js', new Date());
```

```
    gtag('config', 'G-BNNQ75MX9K');
    </script>
    <!-- Google tag (gtag.js) -->
    <!-- #END -->

    <meta charset='utf-8'>
    <title>TYC Brother Industrial Co., Ltd</title>
    <meta content='width=device-width, initial-scale=1.0' name='viewport'>
    <link href="https://www.tyc.com.tw/assets/stylesheets/fa-all.css" media="screen" rel="stylesheet" type="text/css"/> <!-
-2023.01.07 import font awesome css link-->
    <link href="https://www.tyc.com.tw/assets/stylesheets/all.css" media="screen" rel="stylesheet" type="text/css"/>
    <link href="https://www.tyc.com.tw/assets/stylesheets/all-2023.css?v=20230901" media="screen" rel="stylesheet"
type="text/css"/> <!--2023.01.18 2023 Renewal of website brand image-->
    <script src="https://www.tyc.com.tw/assets/javascripts/jquery.js" type="text/javascript"></script>
    <style>
        .goodbyeieeight { text-align: center; position: fixed; z-index: 9999; top: 0; right: 0; bottom: 0; left: 0;
background-color: #1f1f1f; color: #ffffff; padding-top: 120px; }
        .goodbyeieeight h1, .goodbyeieeight h2 { margin: 0 auto; width: 50%; }
        .goodbyeieeight p { margin: 20px auto; width: 50%; }
        .goodbyeieeight a { display: inline-block; color: #ffffff; width: 120px; }
        .goodbyeieeight img { display: block; width: 64px; margin: 0 auto; }

    </style>
    <!-- <link rel="shortcut icon" href="https://www.tyc.com.tw/assets/images/favicon.ico"> -->
    <link rel="apple-touch-icon" sizes="180x180" href="https://www.tyc.com.tw/assets/images/apple-touch-icon.png">
    <link rel="icon" type="image/png" sizes="32x32" href="https://www.tyc.com.tw/assets/images/favicon-32x32.png">
    <link rel="icon" type="image/png" sizes="16x16" href="https://www.tyc.com.tw/assets/images/favicon-16x16.png">
    <link rel="manifest" href="https://www.tyc.com.tw/assets/images/site.webman
...
...
...

        <div class='copyrights restrict'>
          <div class='text grid g-6-12'>Copyright©2015 TYC Brother Industrial Co., Ltd. All rights reserved.</div>
          <div class='share grid g-6-12'>
          <div class="item">
          <a href='https://www.facebook.com/tyc.taiwan' target='_blank'>
          <span class="fa-layers fa-fw">
          <i class="fa-solid fa-square fa-2x" style="color:#939498; height:3em; width:3em;"></i>
          <i class="fa-brands fa-facebook-f fa-4x" data-fa-transform="right-7"></i>
          </span>
          </a>
          </div>
          <div class="item">
          <a href='https://www.youtube.com/@tyc9186' target='_blank'>
          <span class="fa-layers fa-fw">
          <i class="fa-solid fa-square fa-2x" style="color:#939498; height:3em; width:3em;"></i>
          <i class="fa-brands fa-youtube fa-3x" data-fa-transform="right-7"></i>
          </span>
...
...
...

          <a href='https://www.tyc.com.tw/investors/spokesperson'>Investor Relation Contacts</a>
          </li>
          <li>
          <a href='http://mops.twse.com.tw/mops/web/index' target='_blank'>Taiwan Stock Exchange Website</a>
          </li>
          </ul>
          </li>
          <li>
...
...
...
```

中 主機標頭注入 1 目錄

問題 1 / 1 目錄

主機標頭注入

嚴重性：	中
CVSS 評分：	5.3
CVSS 向量：	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL：	https://www.tyc.com.tw/
實體：	(Page)
風險：	有可能說服無經驗而易受騙的使用者提供機密性資訊，如：使用者名稱、密碼、信用卡號碼、社會保險號碼等等 有可能透過 Web 快取毒害來破壞網站內容
原因：	Web 應用程式會執行重新導向至外部網站
修正：	建構 HTTP 標頭時要很小心，避免使用未驗證/未消毒的輸入資料

差異： **標頭** `Host` 操作來源： `www.tyc.com.tw` 到： `appscanheaderinjection.com`

推論： AppScan 注入的值似乎已包含在回應中。

測試要求和回應：

```
GET / HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: appscanheaderinjection.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


...
...
...


    <meta charset='utf-8'>
    <title>TYC Brother Industrial Co., Ltd</title>
    <meta content='width=device-width, initial-scale=1.0' name='viewport'>
    <link href="https://appscanheaderinjection.com/assets/stylesheets/fa-all.css" media="screen" rel="stylesheet"
type="text/css"/> <!--2023.01.07 import font awesome css link-->
    <link href="https://appscanheaderinjection.com/assets/stylesheets/all.css" media="screen" rel="stylesheet"
type="text/css"/>
    <link href="https://appscanheaderinjection.com/assets/stylesheets/all-2023.css?v=20230901" media="screen"
rel="stylesheet" type="text/css"/> <!--2023.01.18 2023 Renewal of website brand image-->
    <script src="https://appscanheaderinjection.com/assets/javascripts/jquery.js" type="text/javascript"></script>
    <style>
        .goodbyeieeight { text-align: center; position: fixed; z-index: 9999; top: 0; right: 0; bottom: 0; left: 0;
background-color: #1f1f1f; color: #ffffff; padding-top: 120px; }
        .goodbyeieeight h1, .goodbyeieeight h2 { margin: 0 auto; width: 50%; }
        .goodbyeieeight p { margin: 20px auto; width: 50%; }
        .goodbyeieeight a { display: inline-block; color: #ffffff; width: 120px; }
        .goodbyeieeight img { display: block; width: 64px; margin: 0 auto; }

    </style>
    <!-- <link rel="shortcut icon" href="https://appscanheaderinjection.com/assets/images/favicon.ico"> -->
    <link rel="apple-touch-icon" sizes="180x180" href="https://appscanheaderinjection.com/assets/images/apple-touch-
icon.png">
    <link rel="icon" type="image/png" sizes="32x32" href="https://appscanheaderinjection.com/assets/images/favicon-
32x32.png">
    <link rel="icon" type="image/png" sizes="16x16" href="https://appscanheaderinjection.com/assets/images/favicon-
16x16.png">
    <link rel="manifest" href="https://appscanheaderinjection.com/assets/images/site.webmanifest">
    <link rel="mask-icon" href="https://appscanheaderinjection.com/assets/images/safari-pinned-tab.svg" color="#5bbad5">
    <meta name="msapplication-TileColor" content="#da532c">
    <meta name="theme-color" content="#ffffff">

    <!-- SEO -->
...
...
...


    <p>We strongly recommend you at least upgrade your browser to Internet Explorer 9 by WindowsUpdate or try any modern
browsers below for the best web-surfing experiences.</p>

    <p>
```

```
        <a href='http://www.google.com/chrome/'><img
src='https://appscanheaderinjection.com/assets/images/chrome.png'>Google Chrome</a>
        <a href='https://www.mozilla.org/en-US/firefox/new/'><img
src='https://appscanheaderinjection.com/assets/images/firefox.png'>Mozilla Firefox</a>
        <a href='http://www.opera.com/zh-tw'><img
src='https://appscanheaderinjection.com/assets/images/opera.png'>OPERA</a>
        <a href='https://www.apple.com/tw/safari/'><img
src='https://appscanheaderinjection.com/assets/images/safari.png'>Safari</a>
    </p>
    </br>
    <h2>IE 8 以下瀏覽器請直接</h2>
    <h2><a href='http://notesweb.tyc.com.tw/public/scm.nsf/tyclink.xsp' target="_blank"><font color="#FFFF00">由此進入<font>
</a></h2>
...
...
...

    <div id='wrapper'>
        <div id='sticker'>
    <nav class='restrict'>
        <div class='brand'>
          <a class='brand-icon-2023' href='https://appscanheaderinjection.com/'></a>
        </div>
        <div class='navigation'>

          <ul>
          <li>
          <a href='https://appscanheaderinjection.com/about'>ABOUT</a>
          </li>
          <li>
          <a href='https://appscanheaderinjection.com/products'>PRODUCTS</a>
          </li>

          <li>
          <a href='https://appscanheaderinjection.com/news'>NEWS</a>
          </li>

          <!-- Start 2022.12.07 CR:22002153 Add new button for ESG file -->
          <li>
          <a href='https://appscanheaderinjection.com/sustainable'>SUSTAINABILITY</a>
          </li>
          <!-- End 2022.12.07 CR:22002153 Add new button for ESG file -->


          <li class='toolbar-2023'>
          <a href='javascript:;'>CONTACT US</a>
          <ul>
          <li>
          <a href='https://appscanheaderinjection.com/stakeholders'>Contact Person</a>
          </li>

          <li>
          <a href='https://appscanheaderinjection.com/locations'>Locations</a>
          </li>

          <li>
          <a href='https://appscanheaderinjection.com/grievance'>Grievance Procedure</a>
          </li>


          </ul>
...
...
...

        <main>
          <section id='slider'>
          <div id='layerslider' style='width: 1600px; height: 560px;'>
          <div class='ls-slide' data-ls='slidedelay: 4000;'>
          <img class='ls-bg' src='https://appscanheaderinjection.com/assets/uploads/homepage/banner/banner1684991835.jpg'
style='width: 100%; height: 60%;'>

          <div class='description ls-l' style='left: 68%; top: 72%;'>
          <h1></h1>

...
...
...

          </div>
          </div>
          </div>
          <ul class='verbxslider'>
          <li><img src='https://appscanheaderinjection.com/assets/uploads/homepage/mobile/mobile1684992985.jpg'></li>
```

```
          </ul>
        </section>
        <section class='content-container centered highlights'>
        <div class='content-container-inner'>
...
...
...

    <!-- 2023 Cancel
          <section class='content-container background centered' style="background-image:
url('https://appscanheaderinjection.com/assets/uploads/news/banner1681711357.jpg');">
          <div class='content-container-inner'>
          <header>
          <h1><a href="https://appscanheaderinjection.com/news">New worlds, new technologies, new dreams.</a></h1>

          <div class='content'><p style='font-size: 1.2em; font-weight: bold;'></p></div>
          </header>
          </div>
...
...
...
```

中 加密的階段作業 (SSL) Cookie 中遺漏安全屬性 1

目錄

問題 1 / 1

目錄

加密的階段作業 (SSL) Cookie 中遺漏安全屬性

嚴重性：	中
CVSS 評分：	6.5
CVSS 向量：	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL：	https://www.tyc.com.tw/
實體：	ci_session (Cookie)
風險：	有可能竊取在加密階段作業期間傳送的使用者和階段作業資訊 (Cookie)
原因：	Web 應用程式會透過 SSL 傳送未受保護的 Cookie
修正：	新增 'Secure' 屬性至所有機密 Cookie

差異：

推論： AppScan 發現加密階段作業 (SSL) 使用不含 "secure" 屬性的 Cookie。

測試要求和回應：

```
GET / HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: www.tyc.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Date: Sun, 20 Oct 2024 18:27:55 GMT
Server: Apache/2.4.62 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
```

```
X-Frame-Options: SAMEORIGIN
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
Set-Cookie: ci_session=ld8p7f4k9aaghe92cf72b8kmgvemljee; expires=Sun, 20 Oct 2024 20:27:55 GMT; Max-Age=7200; path=/;
HttpOnly; SameSite=Lax
Set-Cookie: locale=en; expires=Sun, 20 Oct 2024 18:28:55 GMT; Max-Age=60

<!DOCTYPE html>
<html class='no-js' lang='zh-TW'>
<head>
    <!-- #BEGIN -->
    <!-- Google tag (gtag.js) -->
    <script async src="https://www.googletagmanager.com/gtag/js?id=G-BNNQ75MX9K"></script>
    <script>
    window.dataLayer = window.dataLayer || [];
    function gtag(){dataLayer.push(arguments);}
    gtag('js', new Date());

    gtag('config', 'G-BNNQ75MX9K');
    </script>
    <!-- Google tag (gtag.js) -->
    <!-- #END -->

    <meta charset='utf-8'>
    <title>TYC Brother Industrial Co., Ltd</title>
    <meta content='width=device-width, initial-scale=1.0' name='viewport'>
    <link href="https://www.tyc.com.tw/assets/stylesheets/fa-all.css" media="screen" rel="stylesheet" type="text/css"/> <!-
-2023.01.07 import font awesome css link-->
    <link href="https://www.tyc.com.tw/assets/stylesheets/all.css" media="screen" rel="stylesheet" type="text/css"/>
    <link href="https://www.tyc.com.tw/assets/stylesheets/all-2023.css?v=20230901" media="screen" rel="stylesheet"
type="text/css"/> <!--2023.01.18 2023 Renewal of website brand image-->
    <script src="https://www.tyc.com.tw/assets/javascripts/jquery.js" type="text/javascript"></script>
    <style>
        .goodbyeieeight { text-align: center; position: fixed; z-index: 9999; top: 0; right: 0; bottom: 0; left: 0;
background-color: #1f1f1f; color: #ffffff; padding-top: 120px; }
        .goodbyeieeight h1, .goodbyeieeight h2 { margin: 0 auto; width: 50%; }
        .goodbyeieeight p { margin: 20px auto; width: 50%; }
        .goodbyeieeight a { display: inline-block; color: #ffffff; width: 120px; }
        .goodbyeieeight img { display: block; width: 64px; margin: 0 auto; }

    </style>
    <!-- <link rel="shortcut icon" href="https://www.tyc.com.tw/assets/images/favicon.ico"> -->
    <link rel="apple-touch-icon" sizes="180x180" href="https://www.tyc.com.tw/assets/images/apple-touch-icon.png">
    <link rel="icon" type="image/png" sizes="32x32" href="https://www.tyc.com.tw/assets/images/favicon-32x32.png">
    <link rel="icon" type="image/png" sizes="16x16" href="https://www.tyc.com.tw/assets/images/favicon-16x16.png">
    <link rel="manifest" href="https://www.tyc.com.tw/assets/images/site.webmanifest">
    <link rel="mask-icon" href="https://www.tyc.com.tw/assets/images/safari-pinned-tab.svg" color="#5bbad5">
    <meta name="msapplication-TileColor" content="#da532c">
    <meta name="theme-color" content="#ffffff">

    <!-- SEO -->
    <meta property="og:image" content="https://www.tyc.com.tw/assets/images/SEO-cover.jpg"/>
    <meta property="og:image:url" content="https://www.tyc.com.tw/assets/images/SEO-cover.jpg"/>
    <meta property="og:image:secure_url" content="https://www.tyc.com.tw/assets/images/SEO-cover.jpg"/>
    <!-- SEO -->

</head>
<body>
<!--[if lt IE 9]>
<div class='goodbyeieeight'>
    <h1>您的瀏覽器版本太舊了！</h1>

    <h2>Your Browser is totally out of date !</h2>

    <p>請更新至 Internet Explorer 9 以上版本或選用更現代化的瀏覽器：</p>

    <p>We strongly recommend you at least upgrade your browser to Internet Explorer 9 by WindowsUpdate or try any modern
browsers below for the best web-surfing experiences.</p>

    <p>
        <a href='http://www.google.com/chrome/'><img src='https://www.tyc.com.tw/assets/images/chrome.png'>Google
Chrome</a>
        <a href='https://www.mozilla.org/en-US/firefox/new/'><img
src='https://www.tyc.com.tw/assets/images/firefox.png'>Mozilla Firefox</a>
        <a href='http://www.opera.com/zh-tw'><img src='https://www.tyc.com.tw/assets/images/opera.png'>OPERA</a>
        <a href='https://www.apple.com/tw/safari/'><img src='https://www.tyc.com.tw/assets/images/safari.png'>Safari</a>
    </p>
    </br>
    <h2>IE 8 以下瀏覽器請直接</h2>
    <h2><a href='http://notesweb.tyc.com.tw/public/scm.nsf/tyclink.xsp' target="_blank"><font color="#FFFF00">由此進入<font>
</a></h2>
    <p> </p>
</div>
<![endif]-->
```

```
<div id='sb-site'>
    <div id='wrapper'>
        <div id='sticker'>
    <nav class='restrict'>
        <div class='brand'>
          <a class='brand-icon-2023' href='https://www.tyc.com.tw/'></a>
        </div>

...
...
...
```

中 有弱點的元件 1

目錄

問題 1 / 1

目錄

有弱點的元件	
嚴重性：	中
CVSS 評分：	6.1
CVSS 向量：	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
CVE：	CVE-2020-11022
URL：	https://www.tyc.com.tw/admin/
實體：	jQuery 2.1.1 (Component)
風險：	攻擊者有可能使用 Web 伺服器來攻擊其他網站，讓其身分更加隱密
原因：	未安裝協力廠商產品的最新修補程式或緊急修復程式
修正：	將元件升級到最新穩定版本

差異：

推論：

測試要求和回應：

```
GET /admin/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: www.tyc.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Date: Sun, 20 Oct 2024 18:31:00 GMT
Server: Apache/2.4.62 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Content-Length: 7362
Content-Type: text/html; charset=UTF-8
Set-Cookie: ci_session=p9a05a2tu18msk1hie2d1qd5of47h2ko; expires=Sun, 20 Oct 2024 20:31:00 GMT; Max-Age=7200; path=/;
HttpOnly; SameSite=Lax

<!DOCTYPE html>
```

```
<html lang="en-us" id="extr-page">
<head>
    <meta charset="utf-8">
    <!--<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">-->
    <title> TYC - 後台管理系統 </title>
    <meta name="description" content="">
    <meta name="author" content="">
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
    <link rel="stylesheet" href="https://www.tyc.com.tw/assets/backend/css/bootstrap.min.css">
    <link rel="stylesheet" href="https://www.tyc.com.tw/assets/backend/css/font-awesome.min.css">
    <link rel="stylesheet" href="https://www.tyc.com.tw/assets/backend/css/smartadmin-production.min.css">
    <link rel="stylesheet" href="https://www.tyc.com.tw/assets/backend/css/smartadmin-skins.min.css">
    <link rel="shortcut icon" href="https://www.tyc.com.tw/assets/backend/img/favicon/favicon.ico" type="image/x-icon">
    <link rel="icon" href="https://www.tyc.com.tw/assets/backend/img/favicon/favicon.ico" type="image/x-icon">
    <link rel="stylesheet" href="http://fonts.googleapis.com/css?family=Open+Sans:400italic,700italic,300,400,700">
    <meta name="apple-mobile-web-app-capable" content="yes">
    <meta name="apple-mobile-web-app-status-bar-style" content="black">
    <style>
        .goodbyeieeight { text-align: center; position: fixed; z-index: 9999; top: 0; right: 0; bottom: 0; left: 0;
background-color: #1f1f1f; color: #ffffff; padding-top: 120px; }
        .goodbyeieeight h1, .goodbyeieeight h2 { margin: 0 auto; width: 50%; }
        .goodbyeieeight p { margin: 20px auto; width: 50%; }
        .goodbyeieeight a { display: inline-block; color: #ffffff; width: 120px; }
        .goodbyeieeight img { display: block; width: 64px; margin: 0 auto;}

    </style>
</head>
<body class="animated fadeInDown">

<!--[if lt IE 9]>
<div class='goodbyeieeight'>
    <h1>您的瀏覽器版本太舊了！</h1>

    <h2>Your Browser is totally out of date !</h2>

    <p>請更新至 Internet Explorer 9 以上版本或選用更現代化的瀏覽器：</p>

    <p>We strongly recommend you at least upgrade your browser to Internet Explorer 9 by WindowsUpdate or try any modern
browsers below for the best web-surfing experiences.</p>

    <p>
        <a href='http://www.google.com/chrome/'><img src='https://www.tyc.com.tw/assets/images/chrome.png'>Google
Chrome</a>
        <a href='https://www.mozilla.org/en-US/firefox/new/'><img
src='https://www.tyc.com.tw/assets/images/firefox.png'>Mozilla Firefox</a>
        <a href='http://www.opera.com/zh-tw'><img src='https://www.tyc.com.tw/assets/images/opera.png'>OPERA</a>
        <a href='https://www.apple.com/tw/safari/'><img src='https://www.tyc.com.tw/assets/images/safari.png'>Safari</a>
    </p>
</div>
<![endif]-->
<header id="header">
    <div id="logo-group">
        <span id="logo"> <img src="https://www.tyc.com.tw/assets/backend/img/tyc-logo.png" alt="TYC - 後台管理系統"></span>
    </div>
</header>
<div id="main" role="main">
    <!-- MAIN CONTENT -->
    <div id="content" class="container">
        <div class="row">
          <div class="col-xs-12 col-sm-12 col-md-7 col-lg-8 hidden-xs hidden-sm">
          <div class="hero">
          <div class="pull-left login-desc-box-l">
          <h4 class="paragraph-header"></h4>
          </div>
          <img src="" class="pull-right display-image" alt="" style="width:210px">
          </div>
          </div>
          <div class="col-xs-12 col-sm-12 col-md-5 col-lg-4">
          <div class="well no-padding">
          <form action="https://www.tyc.com.tw/backend/panel/logindo" class="smart-form client-form" id="login-form"
method="post" accept-charset="utf-8">
          <header>
          登入
          </header>
          <fieldset>
          <section>
          <label class="label">帳號</label>
          <label class="input"> <i class="icon-append fa fa-user"></i>
          <input type="text" name="username" value="" autofocus="autofocus">
          <b class="tooltip tooltip-top-right"><i class="fa fa-user txt-
...
...
...
```

問題 1 / 3

目錄

檢查是否有 SRI（子資源完整性）支援

嚴重性：	中
CVSS 評分：	5.3
CVSS 向量：	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL：	https://www.tyc.com.tw/
實體：	(Page)
風險：	假設第三方伺服器已受損，網站的內容/行為會變更
原因：	不支援 SRI（子資源完整性）
修正：	將每一個第三方 Script/鏈結元素支援新增至 SRI（子資源完整性）。

差異：

推論： 第三方鏈結/Script 沒有瀏覽器的完整性屬性，來確認它們未受損

測試要求和回應：

```
GET / HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: www.tyc.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Date: Sun, 20 Oct 2024 18:27:54 GMT
Server: Apache/2.4.62 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
Set-Cookie: ci_session=sib3uo4b7fd763g12bpfikkoe7skv40r; expires=Sun, 20 Oct 2024 20:27:54 GMT; Max-Age=7200; path=/;
HttpOnly; SameSite=Lax
Set-Cookie: locale=en; expires=Sun, 20 Oct 2024 18:28:54 GMT; Max-Age=60

<!DOCTYPE html>
<html class='no-js' lang='zh-TW'>
<head>
    <!-- #BEGIN -->
    <!-- Google tag (gtag.js) -->
    <script async src="https://www.googletagmanager.com/gtag/js?id=G-BNNQ75MX9K"></script>
    <script>
    window.dataLayer = window.dataLayer || [];
    function gtag(){dataLayer.push(arguments);}
    gtag('js', new Date());

    gtag('config', 'G-BNNQ75MX9K');
    </script>
    <!-- Google tag (gtag.js) -->
    <!-- #END -->
```

```
    <meta charset='utf-8'>
    <title>TYC Brother Industrial Co., Ltd</title>
    <meta content='width=device-width, initial-scale=1.0' name='viewport'>
    <link href="https://www.tyc.com.tw/assets/stylesheets/fa-all.css" media="screen" rel="stylesheet" type="text/css"/> <!-
-2023.01.07 import font awesome css link-->
    <link href="https://www.tyc.com.tw/assets/stylesheets/all.css" media="screen" rel="stylesheet" type="text/css"/>
    <link href="https://www.tyc.com.tw/assets/stylesheets/all-2023.css?v=20230901" media="screen" rel="stylesheet"
type="text/css"/> <!--2023.01.18 2023 Renewal of website brand image-->
    <script src="https://www.tyc.com.tw/assets/javascripts/jquery.js" type="text/javascript"></script>
    <style>
        .goodbyeieeight { text-align: center; position: fixed; z-index: 9999; top: 0; right: 0; bottom: 0; left: 0;
background-color: #1f1f1f; color: #ffffff; padding-top: 120px; }
        .goodbyeieeight h1, .goodbyeieeight h2 { margin: 0 auto; width: 50%; }
        .goodbyeieeight p { margin: 20px auto; width: 50%; }
        .goodbyeieeight a { display: inline-block; color: #ffffff; width: 120px; }
        .goodbyeieeight img { display: block; width: 64px; margin: 0 auto; }

    </style>
    <!-- <link rel="shortcut icon" href="https://www.tyc.com.tw/assets/images/favicon.ico"> -->
    <link rel="apple-touch-icon" sizes="180x180" href="https://www.tyc.com.tw/assets/images/apple-touch-icon.png">
    <link rel="icon" type="image/png" sizes="32x32" href="https://www.tyc.com.tw/assets/images/favicon-32x32.png">
    <link rel="icon" type="image/png" sizes="16x16" href="https://www.tyc.com.tw/assets/images/favicon-16x16.png">
    <link rel="manifest" href="https://www.tyc.com.tw/assets/images/site.webmanifest">
    <link rel="mask-icon" href="https://www.tyc.com.tw/assets/images/safari-pinned-tab.svg" color="#5bbad5">
    <meta name="msapplication-TileColor" content="#da532c">
    <meta name="theme-color" content="#ffffff">

    <!-- SEO -->
    <meta property="og:image" content="https://www.tyc.com.tw/assets/images/SEO-cover.jpg"/>
    <meta property="og:image:url" content="https://www.tyc.com.tw/assets/images/SEO-cover.jpg"/>
    <meta property="og:image:secure_url" content="https://www.tyc.com.tw/assets/images/SEO-cover.jpg"/>
    <!-- SEO -->

</head>
<body>
<!--[if lt IE 9]>
<div class='goodbyeieeight'>
    <h1>您的瀏覽器版本太舊了！</h1>

    <h2>Your Browser is totally out of date !</h2>

    <p>請更新至 Internet Explorer 9 以上版本或選用更現代化的瀏覽器：</p>

    <p>We strongly recommend you at least upgrade your browser to Internet Explorer 9 by WindowsUpdate or try any modern
browsers below for the best web-surfing experiences.</p>

    <p>
        <a href='http://www.google.com/chrome/'><img src='https://www.tyc.com.tw/assets/images/chrome.png'>Google
Chrome</a>
        <a href='https://www.mozilla.org/en-US/firefox/new/'><img
src='https://www.tyc.com.tw/assets/images/firefox.png'>Mozilla Firefox</a>
        <a href='http://www.opera.com/zh-tw'><img src='https://www.tyc.com.tw/assets/images/opera.png'>OPERA</a>
        <a href='https://www.apple.com/tw/safari/'><img src='https://www.tyc.com.tw/assets/images/safari.png'>Safari</a>
    </p>
    </br>
    <h2>IE 8 以下瀏覽器請直接</h2>
    <h2><a href='http://notesweb.tyc.com.tw/public/scm.nsf/tyclink.xsp' target="_blank"><font color="#FFFF00">由此進入<font>
</a></h2>
    <p> </p>
</div>
<![endif]-->
<div id='sb-site'>
    <div id='wrapper'>
        <div id='sticker'>
    <nav class='restrict'>
        <div class='brand'>
          <a class='brand-icon-2023' href='https://www.tyc.com.tw/'></a>
        </div>

...
...
...
```

檢查是否有 SRI（子資源完整性）支援

嚴重性：	中
CVSS 評分：	5.3
CVSS 向量：	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL：	https://www.tyc.com.tw/.admin/
實體：	(Page)
風險：	假設第三方伺服器已受損，網站的內容/行為會變更
原因：	不支援 SRI（子資源完整性）
修正：	將每一個第三方 Script/鏈結元素支援新增至 SRI（子資源完整性）。

差異：

推論： 第三方鏈結/Script 沒有瀏覽器的完整性屬性，來確認它們未受損

測試要求和回應：

```
GET /.admin/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: www.tyc.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Date: Sun, 20 Oct 2024 18:30:37 GMT
Server: Apache/2.4.62 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Content-Length: 7362
Content-Type: text/html; charset=UTF-8
Set-Cookie: ci_session=hsg0ojk1sog98llhu0rfeds77588meb0; expires=Sun, 20 Oct 2024 20:30:37 GMT; Max-Age=7200; path=/;
HttpOnly; SameSite=Lax

<!DOCTYPE html>
<html lang="en-us" id="extr-page">
<head>
    <meta charset="utf-8">
    <!--<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">-->
    <title> TYC - 後台管理系統 </title>
    <meta name="description" content="">
    <meta name="author" content="">
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
    <link rel="stylesheet" href="https://www.tyc.com.tw/assets/backend/css/bootstrap.min.css">
    <link rel="stylesheet" href="https://www.tyc.com.tw/assets/backend/css/font-awesome.min.css">
    <link rel="stylesheet" href="https://www.tyc.com.tw/assets/backend/css/smartadmin-production.min.css">
    <link rel="stylesheet" href="https://www.tyc.com.tw/assets/backend/css/smartadmin-skins.min.css">
    <link rel="shortcut icon" href="https://www.tyc.com.tw/assets/backend/img/favicon/favicon.ico" type="image/x-icon">
    <link rel="icon" href="https://www.tyc.com.tw/assets/backend/img/favicon/favicon.ico" type="image/x-icon">
    <link rel="stylesheet" href="http://fonts.googleapis.com/css?family=Open+Sans:400italic,700italic,300,400,700">
    <meta name="apple-mobile-web-app-capable" content="yes">
    <meta name="apple-mobile-web-app-status-bar-style" content="black">
    <style>
        .goodbyeieeight { text-align: center; position: fixed; z-index: 9999; top: 0; right: 0; bottom: 0; left: 0;
background-color: #1f1f1f; color: #ffffff; padding-top: 120px; }
        .goodbyeieeight h1, .goodbyeieeight h2 { margin: 0 auto; width: 50%; }
        .goodbyeieeight p { margin: 20px auto; width: 50%; }
        .goodbyeieeight a { display: inline-block; color: #ffffff; width: 120px; }
        .goodbyeieeight img { display: block; width: 64px; margin: 0 auto;}

    </style>
</head>
<body class="animated fadeInDown">

<!--[if lt IE 9]>
<div class='goodbyeieeight'>
    <h1>您的瀏覽器版本太舊了！</h1>

    <h2>Your Browser is totally out of date !</h2>
```

```
    <p>請更新至 Internet Explorer 9 以上版本或選用更現代化的瀏覽器：</p>

    <p>We strongly recommend you at least upgrade your browser to Internet Explorer 9 by WindowsUpdate or try any modern
browsers below for the best web-surfing experiences.</p>

    <p>
        <a href='http://www.google.com/chrome/'><img src='https://www.tyc.com.tw/assets/images/chrome.png'>Google
Chrome</a>
        <a href='https://www.mozilla.org/en-US/firefox/new/'><img
src='https://www.tyc.com.tw/assets/images/firefox.png'>Mozilla Firefox</a>
        <a href='http://www.opera.com/zh-tw'><img src='https://www.tyc.com.tw/assets/images/opera.png'>OPERA</a>
        <a href='https://www.apple.com/tw/safari/'><img src='https://www.tyc.com.tw/assets/images/safari.png'>Safari</a>
    </p>
</div>
<![endif]-->
<header id="header">
    <div id="logo-group">
        <span id="logo"> <img src="https://www.tyc.com.tw/assets/backend/img/tyc-logo.png" alt="TYC - 後台管理系統"></span>
    </div>
</header>
<div id="main" role="main">
    <!-- MAIN CONTENT -->
    <div id="content" class="container">
        <div class="row">
          <div class="col-xs-12 col-sm-12 col-md-7 col-lg-8 hidden-xs hidden-sm">
          <div class="hero">
          <div class="pull-left login-desc-box-l">
          <h4 class="paragraph-header"></h4>
          </div>
          <img src="" class="pull-right display-image" alt="" style="width:210px">
          </div>
          </div>
          <div class="col-xs-12 col-sm-12 col-md-5 col-lg-4">
          <div class="well no-padding">
          <form action="https://www.tyc.com.tw/backend/panel/logindo" class="smart-form client-form" id="login-form"
method="post" accept-charset="utf-8">
          <header>
          登入
          </header>
          <fieldset>
          <section>
          <label class="label">帳號</label>
          <label class="input"> <i class="icon-append fa fa-user"></i>
          <input type="text" name="username" value="" autofocus="autofocus">
          <b class="tooltip
...
...
...
```

問題 3 / 3

目錄

檢查是否有 SRI（子資源完整性）支援

嚴重性：	中
CVSS 評分：	5.3
CVSS 向量：	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL：	https://www.tyc.com.tw/admin/
實體：	(Page)
風險：	假設第三方伺服器已受損，網站的內容/行為會變更
原因：	不支援 SRI（子資源完整性）
修正：	將每一個第三方 Script/鏈結元素支援新增至 SRI（子資源完整性）。

差異：

推論： 第三方鏈結/Script 沒有瀏覽器的完整性屬性，來確認它們未受損

測試要求和回應：

```
GET /admin/ HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: www.tyc.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Date: Sun, 20 Oct 2024 18:30:37 GMT
Server: Apache/2.4.62 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Content-Length: 7362
Content-Type: text/html; charset=UTF-8
Set-Cookie: ci_session=0jskdehfsdcrosph7i5fdknt7r3gfmas; expires=Sun, 20 Oct 2024 20:30:37 GMT; Max-Age=7200; path=/;
HttpOnly; SameSite=Lax

<!DOCTYPE html>
<html lang="en-us" id="extr-page">
<head>
    <meta charset="utf-8">
    <!--<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">-->
    <title> TYC - 後台管理系統 </title>
    <meta name="description" content="">
    <meta name="author" content="">
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
    <link rel="stylesheet" href="https://www.tyc.com.tw/assets/backend/css/bootstrap.min.css">
    <link rel="stylesheet" href="https://www.tyc.com.tw/assets/backend/css/font-awesome.min.css">
    <link rel="stylesheet" href="https://www.tyc.com.tw/assets/backend/css/smartadmin-production.min.css">
    <link rel="stylesheet" href="https://www.tyc.com.tw/assets/backend/css/smartadmin-skins.min.css">
    <link rel="shortcut icon" href="https://www.tyc.com.tw/assets/backend/img/favicon/favicon.ico" type="image/x-icon">
    <link rel="icon" href="https://www.tyc.com.tw/assets/backend/img/favicon/favicon.ico" type="image/x-icon">
    <link rel="stylesheet" href="http://fonts.googleapis.com/css?family=Open+Sans:400italic,700italic,300,400,700">
    <meta name="apple-mobile-web-app-capable" content="yes">
    <meta name="apple-mobile-web-app-status-bar-style" content="black">
    <style>
        .goodbyeieeight { text-align: center; position: fixed; z-index: 9999; top: 0; right: 0; bottom: 0; left: 0;
background-color: #1f1f1f; color: #ffffff; padding-top: 120px; }
        .goodbyeieeight h1, .goodbyeieeight h2 { margin: 0 auto; width: 50%; }
        .goodbyeieeight p { margin: 20px auto; width: 50%; }
        .goodbyeieeight a { display: inline-block; color: #ffffff; width: 120px; }
        .goodbyeieeight img { display: block; width: 64px; margin: 0 auto;}

    </style>
</head>
<body class="animated fadeInDown">

<!--[if lt IE 9]>
<div class='goodbyeieeight'>
    <h1>您的瀏覽器版本太舊了！</h1>

    <h2>Your Browser is totally out of date !</h2>

    <p>請更新至 Internet Explorer 9 以上版本或選用更現代化的瀏覽器：</p>

    <p>We strongly recommend you at least upgrade your browser to Internet Explorer 9 by WindowsUpdate or try any modern
browsers below for the best web-surfing experiences.</p>

    <p>
        <a href='http://www.google.com/chrome/'><img src='https://www.tyc.com.tw/assets/images/chrome.png'>Google
Chrome</a>
        <a href='https://www.mozilla.org/en-US/firefox/new/'><img
src='https://www.tyc.com.tw/assets/images/firefox.png'>Mozilla Firefox</a>
        <a href='http://www.opera.com/zh-tw'><img src='https://www.tyc.com.tw/assets/images/opera.png'>OPERA</a>
        <a href='https://www.apple.com/tw/safari/'><img src='https://www.tyc.com.tw/assets/images/safari.png'>Safari</a>
    </p>
</div>
<![endif]-->
<header id="header">
    <div id="logo-group">
        <span id="logo"> <img src="https://www.tyc.com.tw/assets/backend/img/tyc-logo.png" alt="TYC - 後台管理系統"></span>
    </div>
</header>
<div id="main" role="main">
    <!-- MAIN CONTENT -->
    <div id="content" class="container">
```

```
        <div class="row">
          <div class="col-xs-12 col-sm-12 col-md-7 col-lg-8 hidden-xs hidden-sm">
          <div class="hero">
          <div class="pull-left login-desc-box-l">
          <h4 class="paragraph-header"></h4>
          </div>
          <img src="" class="pull-right display-image" alt="" style="width:210px">
          </div>
          </div>
          <div class="col-xs-12 col-sm-12 col-md-5 col-lg-4">
          <div class="well no-padding">
          <form action="https://www.tyc.com.tw/backend/panel/logindo" class="smart-form client-form" id="login-form"
method="post" accept-charset="utf-8">
          <header>
          登入
          </header>
          <fieldset>
          <section>
          <label class="label">帳號</label>
          <label class="input"> <i class="icon-append fa fa-user"></i>
          <input type="text" name="username" value="" autofocus="autofocus">
          <b class="tooltip
...
...
...
```

如何修正

SameSite 屬性不安全、不適當或遺漏的 Cookie

目錄

原因：

SameSite 屬性不適當、不安全或遺漏的機密 Cookie

風險：

將 Cookie 限制為第一方或相同網站環境定義，藉此預防 Cookie 資訊洩漏。
如果沒有設置額外的保護措施（如反 CSRF 記號），攻擊者可以延伸為偽造跨網站要求 (CSRF) 攻擊。
SameSite 屬性控制跨網域要求的 Cookie 傳送方式。
屬性的值有三個：「Lax」、「Strict」或「None」。如果您使用「None」，網站可以建立與其他網站之間的跨網域 POST HTTP 要求，而瀏覽器會自動將 Cookie 新增到該要求中。
如果沒有設置額外的保護措施（如反 CSRF 記號），可能會引發偽造跨網站要求 (CSRF) 攻擊。
模式與其用法：
「Lax」模式：Cookie 只會連同最上層 GET 要求一同傳送。
「Strict」模式：即使使用者遵循其他網站的鏈結，Cookie 也不會連同任何跨網站用法一同傳送。
「None」模式：Cookie 將連同跨網站要求一同傳送。
擁有「Lax」或「None」的屬性必須設定「Secure」旗標，而且必須透過 https 傳輸。
範例 - Set-Cookie: key=value; SameSite=Lax;Secure
建議選項是將屬性設定為「Strict」。
範例 - Set-Cookie: key=value; SameSite=Strict

受影響的產品：

此問題可能會影響各種類型的產品。

修正建議：

一般

[1] 檢閱將 SameSite Cookie 屬性配置為建議值的可能解決方案。[2] 將 Cookie 限制為第一方或相同網站環境定義。
[3] 將 Cookie 的 SameSite 屬性設定為 Strict 並加以驗證，確保 Cookie 只能在第一方環境定義中傳送。
[4] 或者，如果您想要放鬆第一方環境定義的限制，請將 Cookie 的 SameSite 屬性設定為 Lax 並啟用 Secure 旗標，再透過 HTTPS 傳輸，同時加以驗證。

CWE：

1275
284
923

外部參照：

WASC 威脅分類：資訊洩漏
SameSite Cookie

不安全的第三方鏈結 (target="_blank")

目錄

原因：

連結元素中的 rel 屬性未設定為 "noopener noreferrer"。

風險：

鏈結的頁面可以部分存取開啟的頁面視窗物件。
target="_blank" 屬性已新增至鏈結元素，使鏈結在新視窗中開啟。
這種類型的鏈結標籤（亦即具有 target="_blank" 屬性）會透過 window.opener 物件，將原始頁面的部分視窗物件暴露給鏈結的頁面。
如果鏈結的頁面是惡意的，則可以加以惡意探索以進行網路釣魚攻擊。
注意：如果鏈結可被使用者新增且傳播至其他使用者看得到的頁面，則應將此威脅視為「高」嚴重性處理

受影響的產品：

這個問題可能會影響不同類型的產品。

修正建議：

一般

將 rel="noopener noreferrer" 新增至包含不在您網域內之來源的每個連結標籤
在「諮詢參考資料與相關連結」中可以找到更詳細的修正建議事項

CWE：

1022
200

外部參照：

前所未有最被低估的弱點 - 說明、範例和修正建議事項

主機標頭注入

目錄

原因：

缺少輸入驗證和消毒

風險：

- 將要求發送給清單上的第一個虛擬主機 - 造成重新導向至由攻擊者控制的網域 - 執行 Web 快取毒害 - 操縱密碼重設功能
Web 伺服器常常在相同的 IP 位址上託管多個 Web 應用程式，透過虛擬主機指向每個應用程式。
Web 伺服器常常在傳入的 HTTP 要求中，根據主機或 X-Forwarded-Host 標頭所提供的值，將要求發送至目標虛擬主機。
惡意探索的例子：
GET /login.html HTTP/1.1
主機：evilhost.com

修正建議：

一般

適當地驗證並消毒使用者輸入的內容

CWE：

644
707
601

外部參照：

OWASP - WSTG 最新
實際的主機標頭攻擊

加密的階段作業 (SSL) Cookie 中遺漏安全屬性

目錄

原因：

Web 應用程式會透過 SSL 傳送未受保護的 Cookie

風險：

有可能竊取在加密階段作業期間傳送的使用者和階段作業資訊 (Cookie)
在應用程式測試期間，偵測到在加密階段作業中，所測試的 Web 應用程式設定了不含 "secure" 屬性的 Cookie。
由於這個 Cookie 未包含 "secure" 屬性，因此，也可能在未加密的階段作業期間將它傳給網站。
任何以明碼傳給伺服器的 Cookie、階段作業記號或使用者認證之類的資訊都可能被竊，稍後可用來盜用身分或使用者模擬。
此外，若干隱私權法規指出，使用者認證之類的機密性資訊一律以加密方式傳給網站

受影響的產品：

這個問題可能會影響不同類型的產品

修正建議：

一般

基本上，Cookie 的唯一必要屬性是 "name" 欄位。
常見的選用屬性如下："comment"、"domain"、"path"，等等。
"secure" 屬性必須相應地設定，才能防止以未加密的方式來傳送 Cookie。
如需如何設定安全旗標的相關資訊，請前往以下鏈結，並參閱 OWASP " 安全屬性 " 題要
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#secure-attribute
RFC 2965 指出：
「Secure 屬性（不含值）會指示使用者代理程式再次傳回這個 Cookie 時，都只用（未指定）安全方法來聯絡原始伺服器，以保護 Cookie 中之資訊的機密性與確實性。」
如需進一步的參照，請參閱「HTTP 狀態管理機制」RFC 2965，位置如下：
http://www.ietf.org/rfc/rfc2965.txt
如需使用「HTTP 狀態管理」的「最佳現行實務」，請參閱：
http://tools.ietf.org/html/rfc2964

CWE：

614
311
319

外部參照：

Financial Privacy: The Gramm-Leach Bliley Act
Health Insurance Portability and Accountability Act (HIPAA)
Sarbanes-Oxley Act
California SB1386

有弱點的元件

目錄

原因：

測試應用程式中使用了一個有弱點的元件。

風險：

有弱點的元件可能導致應用程式出現各種弱點

修正建議：

一般

升級到元件的最新版本。我們強烈建議聯絡此產品的供應商，以了解是否最近提供了修補程式或修正程式。

CWE：

1035

外部參照：

CERT 協調中心
常見弱點和暴露 (CVE)

檢查是否有 SRI（子資源完整性）支援

目錄

原因：

不支援子資源完整性。

風險：

使用者代理程式無法驗證來自協力廠商服務的 Script。 萬一協力廠商服務受到侵害，使用者將不受保護。
原始碼來自另一個網域的 Script 和鏈結標籤不支援完整性檢查。
如果含有這個 Script 的服務受到侵害，則這會遭到不當運用。
不支援 SRI 的範例 Script 元素：
<script src="https://example.com/example-framework.js" crossorigin="anonymous"></script>
支援 SRI 的範例 Script 元素：
<script src="https://example.com/example-framework.js" integrity="sha384-Li9vy3DqF8tnTXuiaAJuML3ky+er10rcgNR/VqsVpcw+ThHmYcwiB1pbOxEbzJr7" crossorigin="anonymous"></script>

受影響的產品：

這個問題可能會影響不同類型的產品。

修正建議：

一般

將「子資源完整性」新增至每一個 Script/鏈結（其原始碼不在您網域中）
W3C 子資源完整性：
https://www.w3.org/TR/SRI/
SRI 雜湊產生器：
https://srihash.org
不支援 SRI 的範例 Script 元素：
<script src="https://example.com/example-framework.js" crossorigin="anonymous"></script>
支援 SRI 的範例 Script 元素：
<script src="https://example.com/example-framework.js" integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC" crossorigin="anonymous"></script>

CWE：

829
669
830
354
345

外部參照：

FrontPage 伺服器延伸：安全考量
說明