對外網站暨數位平台應用程式報告 (2024)

安全報告

這份報告是由 HCL AppScan Standard 所建立 10.4.0
掃描開始時間： 28/3/2024 11:01:04

目錄

簡介

- 一般資訊
- 登入設定值

摘要

- 問題類型
- 有漏洞的 URL
- 修正建議
- 安全風險
- 原因
- WASC 威脅分類

依問題類型排列的問題

- SameSite 屬性不安全、不適當或遺漏的 Cookie 1
- 偵測到隱藏目錄 2
- 找到可快取的 SSL 頁面 1
- 未停用密碼欄位的自動完成 HTML 屬性 1
- 未加密的 __VIEWSTATE 參數 1
- 查詢中接受了 Body 參數 1
- 遺漏「Content-Security-Policy」標頭 1
- 遺漏或不安全的 "X-Content-Type-Options" 標頭 1
- SameSite 屬性未受限制的 Cookie 1
- 找到電子郵件位址型樣 1
- 遺漏「查閱者原則」安全標頭 1

應用程式資料

- 造訪的 URL

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：	1
低嚴重性問題：	8
參考資訊嚴重性問題：	3
報告中併入的安全問題總計：	12
掃描中探索到的安全問題總計：	12

一般資訊

掃描檔名：	dd0239ff-d8c8-499b-bc06-79060ab6f508_2024_(frontend)_54_石油管線及儲油設施查核及檢測網站;(anonymous);p1;(CH0)
掃描開始時間：	28/3/2024 11:01:04
測試原則：	Default
CVSS 版本：	3.1
測試最佳化等級：	快速
主機	qilmms.itri.org.tw
埠	443
作業系統：	不明
Web 伺服器：	不明
應用程式伺服器：	任何

登入設定值

登入方法：	已記錄的登入
並行登入：	已啟用
階段作業內偵測：	已啟用
階段作業內型樣：	
已追蹤或階段作業 ID Cookies：	
已追蹤或階段作業 ID 參數：	
登入序列：	

摘要

問題類型 11

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
低	偵測到隱藏目錄	2
低	找到可快取的 SSL 頁面	1
低	未停用密碼欄位的自動完成 HTML 屬性	1
低	未加密的 __VIEWSTATE 參數	1
低	查詢中接受了 Body 參數	1
低	遺漏「Content-Security-Policy」標頭	1
低	遺漏或不安全的 "X-Content-Type-Options" 標頭	1
參	SameSite 屬性未受限制的 Cookie	1
參	找到電子郵件位址型樣	1
參	遺漏「查閱者原則」安全標頭	1

有漏洞的 URL 2

目錄

	URL	問題數目
中	https://qilmms.itri.org.tw/	7
低	https://qilmms.itri.org.tw/MainPage/Login.aspx	5

修正建議 10

目錄

	補救作業	問題數目
中	檢閱將 SameSite Cookie 屬性配置為建議值的可能解決方案	2
低	修改 Web.Config 檔來加密 VIEWSTATE 參數	1
低	在 SSL 頁面的回應中新增 "Cache-Control: no-store" 和 "Pragma: no-cache" 標頭，以防止快取 SSL 頁面。	1
低	對禁止的資源發出「404 - 找不到」回應狀態碼，或將其完全移除	2

低	從網站移除電子郵件位址	1
低	正確設定 "autocomplete" 屬性為 "off"	1
低	請勿接受查詢字串中傳送的 body 參數	1
低	配置伺服器利用 "nosniff" 值使用 "X-Content-Type-Options" 標頭	1
低	配置伺服器利用安全原則使用 "Content-Security-Policy" 標頭	1
低	配置您的伺服器，以搭配安全原則使用「查閱者原則」標頭	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
低	有可能擷取網站檔案系統結構的相關資訊，其可能會幫助攻擊者對映網站	2
低	有可能收集 Web 應用程式相關的機密性資訊，如：使用者名稱、密碼、機器名稱及/或機密檔案位置	7
低	有可能略過 Web 應用程式的鑑別機制	1
低	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	4
參	將 Cookie 限制為第一方，或是將相同網站環境定義設定為 Strict，藉此預防 Cookie 資訊洩漏。	1

原因 6

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
低	已使用不安全的方式配置 Web 伺服器或應用程式伺服器	2
低	瀏覽器可能已快取機密性資訊	1
低	不安全的 Web 應用程式設計或配置	6
參	SameSite 屬性與旗標未受限制的機密 Cookie	1
參	不安全的 Web 應用程式程式設計或設定	1

WASC 威脅分類

目錄

威脅	問題數目
伺服器配置錯誤	2
資訊洩漏	10

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
URL：	https://qilmms.itri.org.tw/
實體：	TS01b84bc8 (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。

原始回應

```
...


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000
Date: Thu, 28 Mar 2024 03:03:49 GMT
Content-Length: 5322
Set-Cookie: ASP.NET_SessionId=euz3xsruhceibd13nhlhqcw0; path=/; secure; HttpOnly; SameSite=Lax
Set-Cookie:
TS01b84bc8=01bba7060a1fe038eea24f9fdd1c6ed074fb36af9f4c52713b76579acca2a304ac944e3d237765ee53a5d381c092efc3d4aff51901;
Path=/; Secure; HTTPOnly



<!DOCTYPE html>
<html lang="zh">
<head>
    <!--<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />-->
    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />

...
```

低 偵測到隱藏目錄 2 目錄

問題 1 / 2

目錄

偵測到隱藏目錄

嚴重性：	低
CVSS 評分：	3.7
URL：	https://qilmms.itri.org.tw/
實體：	W3SVC11/ (Page)
風險：	有可能擷取網站檔案系統結構的相關資訊，其可能會幫助攻擊者對映網站
原因：	已使用不安全的方式配置 Web 伺服器或應用程式伺服器
修正：	對禁止的資源發出「404 - 找不到」回應狀態碼，或將其完全移除

差異： **路徑** 操作來源：`/MainPage/Login.aspx` 到：`/W3SVC11/`

推論： 測試已嘗試偵測伺服器上的隱藏目錄。「403 禁止」回應顯示目錄存在，即使不允許存取。

原始測試回應：

```
...

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Content-Length: 0


HTTP/1.1 403 Forbidden
Content-Type: text/html
Strict-Transport-Security: max-age=31536000
Date: Thu, 28 Mar 2024 03:09:28 GMT
Content-Length: 1233


...
```

問題 2 / 2

目錄

嚴重性：	低
CVSS 評分：	3.7
URL：	https://qilmms.itri.org.tw/
實體：	W3SVC91/ (Page)
風險：	有可能擷取網站檔案系統結構的相關資訊，其可能會幫助攻擊者對映網站
原因：	已使用不安全的方式配置 Web 伺服器或應用程式伺服器
修正：	對禁止的資源發出「404 - 找不到」回應狀態碼，或將其完全移除

差異： **路徑** 操作來源： `/MainPage/Login.aspx` 到： `/W3SVC91/`

推論： 測試已嘗試偵測伺服器上的隱藏目錄。「403 禁止」回應顯示目錄存在，即使不允許存取。

原始測試回應：

```
...

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Content-Length: 0


HTTP/1.1 403 Forbidden
Content-Type: text/html
Strict-Transport-Security: max-age=31536000
Date: Thu, 28 Mar 2024 03:09:28 GMT
Content-Length: 1233


...
```

低 找到可快取的 SSL 頁面 1

目錄

問題 1 / 1

目錄

找到可快取的 SSL 頁面

嚴重性：	低
CVSS 評分：	3.7
URL：	https://qilmms.itri.org.tw/MainPage/Login.aspx
實體：	Login.aspx (Page)
風險：	有可能收集 Web 應用程式相關的機密性資訊，如：使用者名稱、密碼、機器名稱及/或機密檔案位置
原因：	瀏覽器可能已快取機密性資訊
修正：	在 SSL 頁面的回應中新增 "Cache-Control: no-store" 和 "Pragma: no-cache" 標頭，以防止快取 SSL 頁面。

差異：

推論： 應用程式的回應指出系統應對頁面進行快取，但是您未設定快取控制項（您可以設定「Cache-Control: no-store」或「Cache-Control: no-cache」或「Pragma: no-cache」來阻止系統快取）。

原始測試回應：

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000
Date: Thu, 28 Mar 2024 03:03:49 GMT
Content-Length: 5322
Set-Cookie: ASP.NET_SessionId=o2xo4nbgrwecsfx1v4dk2ppl; path=/; secure; HttpOnly; SameSite=Lax
Set-Cookie:
TS01b84bc8=01bba7060a6f65b17982dc5d57bfe60ef2812d92313312639fd65c55d4e06d992babe9b2a4c0fca0a64061804b159f4cd0e99ae454;
Path=/; Secure; HTTPOnly



<!DOCTYPE html>
<html lang="zh">
<head>
    <!--<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />-->
    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />

...
```

低 未停用密碼欄位的自動完成 HTML 屬性 1

目錄

問題 1 / 1

目錄

未停用密碼欄位的自動完成 HTML 屬性

嚴重性：	低
CVSS 評分：	3.7
URL：	https://qilmms.itri.org.tw/MainPage/Login.aspx
實體：	Login.aspx (Page)
風險：	有可能略過 Web 應用程式的鑑別機制
原因：	不安全的 Web 應用程式設計或配置
修正：	正確設定 "autocomplete" 屬性為 "off"

差異：

推論： AppScan 發現，密碼欄位未施行停用自動完成功能。

原始測試回應：

```
...


<div>

 <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="A1DC5D2E" />
 <input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION"
value="/wEdAAWrCQjLGpKJPRtjj8e9C1kz7mZLWr84M0hwtHSgDJVxbM84QKZmnrxpBCrFktHK0/GinihG6d/Xh3PZm3b5AoMQg0tRkSbr/LcOznZlmYsJJgNX
ks6zAEkPy9oSjQBhptw6K0OwE6wPMGQmd/y/gGxg" />
</div>
          <div>帳號：<input name="tbxAccount" type="text" id="tbxAccount" tabindex="1" placeholder="請輸入帳號" size="25" />
          </div>
          <div>密碼：<input name="tbxPwd" type="password" id="tbxPwd" tabindex="2" placeholder="請輸入密碼" size="17" />

          <!--<input name="Login" type="submit" id="Login" value="登入" />-->

          <input type="submit" name="btnLogin" value="登入" id="btnLogin" tabindex="4" class="btn" />

          </div>
          <div class="flex">
          <div>驗證碼：<input name="tbxValidateCode" type="text" id="tbxValidateCode" tabindex="3" AUTOCOMPLETE="OFF"
size="7" />
          <img src="water_mark.ashx?type=login" id="vimg" alt="驗證碼" style="vertical-align: middle; height: 25px;" />

...
```

低 未加密的 __VIEWSTATE 參數 1

目錄

問題 1 / 1

目錄

未加密的 __VIEWSTATE 參數

嚴重性：	低
CVSS 評分：	3.7
URL：	https://qilmms.itri.org.tw/MainPage/Login.aspx
實體：	__VIEWSTATE (Parameter)
風險：	有可能收集 Web 應用程式相關的機密性資訊，如：使用者名稱、密碼、機器名稱及/或機密檔案位置
原因：	不安全的 Web 應用程式設計或配置
修正：	修改 Web.Config 檔來加密 VIEWSTATE 參數

差異：

推論： AppScan 已解碼 __VIEWSTATE 參數值，並發現其未加密。

原始要求

```
...

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://qilmms.itri.org.tw/MainPage/Login.aspx
Cookie: ASP.NET_SessionId=5rsd3n0sj3ydg4ibcaxviksl;
TS01b84bc8=01bba7060a1e875a75a8c1113b3f6eed2c2324626550592c4e9fc54c9cbbd73f13494fdda63ccec486fb45e4534dff637851695308

__VIEWSTATE=%2FwEPDwULLTIwNjE5MTg1NTAPFgIeB1ByZVBhZ2UFI0U6XFdlYkRhdGFcbWFpblxNYWluUGFnZVxMb2dpbi5hc3B4ZGS7lETxyuzNCY0Q5%2Be
7A6MMvjYy%2F%2FgU2MidjQx0P0aGDg%3D%3D&__VIEWSTATEGENERATOR=A1DC5D2E&__EVENTVALIDATION=%2FwEdAAWrCQjLGpKJPRtjj8e9C1kz7mZLWr8
4M0hwtHSgDJVxbM84QKZmnrxpBCrFktHK0%2FGinihG6d%2FXh3PZm3b5AoMQg0tRkSbr%2FLcOznZlmYsJJgNXks6zAEkPy9oSjQBhptw...

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000
Date: Thu, 28 Mar 2024 03:01:32 GMT

...
```

低 查詢中接受了 Body 參數 1

目錄

問題 1 / 1

目錄

查詢中接受了 Body 參數

嚴重性：	低
CVSS 評分：	3.7
URL：	https://qilmms.itri.org.tw/MainPage/Login.aspx
實體：	Login.aspx (Page)
風險：	有可能收集 Web 應用程式相關的機密性資訊，如：使用者名稱、密碼、機器名稱及/或機密檔案位置 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：	不安全的 Web 應用程式設計或配置
修正：	請勿接受查詢字串中傳送的 body 參數

差異： **內文參數** 已從要求中移除：

```
/wEPDwULLTIwNjE5MTg1NTAPFgIeB1ByZVBhZ2UFI0U6XFdlYkRhdGFcbWFpblxNYWluUGFnZVxMb2dpbi5hc3B4ZGS7lETxyuzNCY0Q5+e7A6MMvjYy//gU2MidjQx0P0aGDg==
```

查詢參數 已新增至要求：

```
/wEPDwULLTIwNjE5MTg1NTAPFgIeB1ByZVBhZ2UFI0U6XFdlYkRhdGFcbWFpblxNYWluUGFnZVxMb2dpbi5hc3B4ZGS7lETxyuzNCY0Q5+e7A6MMvjYy//gU2MidjQx0P0aGDg==
```

內文參數 已從要求中移除： `A1DC5D2E`

查詢參數 已新增至要求： `A1DC5D2E`

內文參數 已從要求中移除：

```
/wEdAAWrCQjLGpKJPRtjj8e9C1kz7mZLWr84M0hwtHSgDJVxbM84QKZmnrxpBCrFktHK0/GinihG6d/Xh3PZm3b5AoMQg0tRkSbr/LcOznZlmYsJJgNXks6zAEkPy9oSjQBhptw6K0OwE6wPMGQmd/y/gGxg
```

查詢參數 已新增至要求：

```
/wEdAAWrCQjLGpKJPRtjj8e9C1kz7mZLWr84M0hwtHSgDJVxbM84QKZmnrxpBCrFktHK0/GinihG6d/Xh3PZm3b5AoMQg0tRkSbr/LcOznZlmYsJJgNXks6zAEkPy9oSjQBhptw6K0OwE6wPMGQmd/y/gGxg
```

內文參數 已從要求中移除： `1234`

查詢參數 已新增至要求： `1234`

內文參數 已從要求中移除： —

查詢參數 已新增至要求： —

內文參數 已從要求中移除： `登入`

查詢參數 已新增至要求： `登入`

內文參數 已從要求中移除： —

查詢參數 已新增至要求： —

方法 操作來源： `POST` 到： `GET`

推論： 測試結果似乎指出有漏洞，因為「測試回應」與「原始回應」類似，表示應用程式已處理查詢中提交的主體參數。

原始回應

≈

測試回應

問題 1 / 1

目錄

遺漏「Content-Security-Policy」標頭

嚴重性：	低
CVSS 評分：	3.7
URL：	https://qilmms.itri.org.tw/
實體：	qilmms.itri.org.tw (Page)
風險：	有可能收集 Web 應用程式相關的機密性資訊，如：使用者名稱、密碼、機器名稱及/或機密檔案位置 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：	不安全的 Web 應用程式設計或配置
修正：	配置伺服器利用安全原則使用 "Content-Security-Policy" 標頭

差異：

推論： AppScan 偵測到遺漏 Content-Security-Policy 回應標頭或包含不安全的原則，這會增加各種跨網站注入攻擊的暴露風險

原始測試回應：

```
...

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Content-Length: 0


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000
Date: Thu, 28 Mar 2024 03:06:18 GMT
Content-Length: 5322
Set-Cookie: ASP.NET_SessionId=yzoc5gxf3rjhck3noemgcf0r; path=/; secure; HttpOnly; SameSite=Lax
Set-Cookie:
TS01b84bc8=01bba7060a05fa7a7aeea3c6110d35a8683f88335fcc0ce840b11c76286d9cd200b9cb38a02d822c5a897acd2df802cce94eb26a4e;
Path=/; Secure; HTTPOnly


...

...

Cache-Control: private
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000
Date: Thu, 28 Mar 2024 03:06:18 GMT
Content-Length: 5322
Set-Cookie: ASP.NET_SessionId=yzoc5gxf3rjhck3noemgcf0r; path=/; secure; HttpOnly; SameSite=Lax
Set-Cookie:
TS01b84bc8=01bba7060a05fa7a7aeea3c6110d35a8683f88335fcc0ce840b11c76286d9cd200b9cb38a02d822c5a897acd2df802cce94eb26a4e;
Path=/; Secure; HTTPOnly



<!DOCTYPE html>
```

```
<html lang="zh">
<head>
    <!--<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />-->
    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />


...
```

低 遺漏或不安全的 "X-Content-Type-Options" 標頭 1

目錄

問題 1 / 1

目錄

遺漏或不安全的 "X-Content-Type-Options" 標頭

嚴重性：	低
CVSS 評分：	3.7
URL：	https://qilmms.itri.org.tw/
實體：	qilmms.itri.org.tw (Page)
風險：	有可能收集 Web 應用程式相關的機密性資訊，如：使用者名稱、密碼、機器名稱及/或機密檔案位置 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：	不安全的 Web 應用程式設計或配置
修正：	配置伺服器利用 "nosniff" 值使用 "X-Content-Type-Options" 標頭

差異：

推論： AppScan 偵測到遺漏 X-Content-Type-Options 回應標頭或具有不安全的值，這會增加路過式下載攻擊的暴露風險

原始測試回應：

```
...

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Content-Length: 0


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000
Date: Thu, 28 Mar 2024 03:03:49 GMT
Content-Length: 5322
Set-Cookie: ASP.NET_SessionId=o2xo4nbgrwecsfx1v4dk2ppl; path=/; secure; HttpOnly; SameSite=Lax
Set-Cookie:
TS01b84bc8=01bba7060a6f65b17982dc5d57bfe60ef2812d92313312639fd65c55d4e06d992babe9b2a4c0fca0a64061804b159f4cd0e99ae454;
Path=/; Secure; HTTPOnly
```

```
...
...

Cache-Control: private
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000
Date: Thu, 28 Mar 2024 03:03:49 GMT
Content-Length: 5322
Set-Cookie: ASP.NET_SessionId=o2xo4nbgrwecsfx1v4dk2ppl; path=/; secure; HttpOnly; SameSite=Lax
Set-Cookie:
TS01b84bc8=01bba7060a6f65b17982dc5d57bfe60ef2812d92313312639fd65c55d4e06d992babe9b2a4c0fca0a64061804b159f4cd0e99ae454;
Path=/; Secure; HTTPOnly



<!DOCTYPE html>
<html lang="zh">
<head>
    <!--<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />-->
    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />


...
```

參 SameSite 屬性未受限制的 Cookie 1

目錄

問題 1 / 1

目錄

SameSite 屬性未受限制的 Cookie	
嚴重性：	參考資訊
CVSS 評分：	0.0
URL：	https://qilmms.itri.org.tw/
實體：	ASP.NET_SessionId (Cookie)
風險：	將 Cookie 限制為第一方，或是將相同網站環境定義設定為 Strict，藉此預防 Cookie 資訊洩漏。
原因：	SameSite 屬性與旗標未受限制的機密 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 屬性未受限制的機密 Cookie。如果可以的話，建議您將 SameSite 屬性設定為 Strict。不然的話，如果您避免使用 GET 要求，而且已設置完善的階段作業管理機制來徹底緩和 CSRF 風險，「Lax」值便已足夠。

原始回應

```
...


HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000
Date: Thu, 28 Mar 2024 03:03:49 GMT
Content-Length: 5322
Set-Cookie: ASP.NET_SessionId=thhvpe1ctwswtdle3dvvfcbm; path=/; secure; HttpOnly; SameSite=Lax
Set-Cookie:
TS01b84bc8=01bba7060ad9582924c6349dc1ba64e6542d5b4b9e4cf2284910b20c15373c1c3690f25aaf54a093beec9e13238e4af3e39eaab629;
Path=/; Secure; HTTPOnly


<!DOCTYPE html>
<html lang="zh">
<head>
    <!--<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />-->
    <meta charset="utf-8" />

...
```

參 找到電子郵件位址型樣 1

目錄

問題 1 / 1

目錄

找到電子郵件位址型樣

嚴重性：	參考資訊
CVSS 評分：	0.0
URL：	https://qilmms.itri.org.tw/MainPage/Login.aspx
實體：	Login.aspx (Page)
風險：	有可能收集 Web 應用程式相關的機密性資訊，如：使用者名稱、密碼、機器名稱及/或機密檔案位置
原因：	不安全的 Web 應用程式設計或配置
修正：	從網站移除電子郵件位址

差異：

推論： 回應包含可能是專用的電子郵件位址。

原始測試回應：

```
...

          <img src="water_mark.ashx?type=login" id="vimg" alt="驗證碼" style="vertical-align: middle; height: 25px;" />
           
          </div>
          <div><a href="#" onclick="change_code_login()" ><img style="padding-top:15px; padding-left:6px; width:30px;
height:30px;" src="../img/refresh40.png" alt="重新產生驗證碼" /></a></div>
          </div>
          </form>
          </div>
        </div>

        <!--<div class="Foot">聯絡人：    分機：12345    / e-mail：test@.com.tw</div>-->
    </div>
</body>
</html>

...
```

參 遺漏「查閱者原則」安全標頭 1

目錄

問題 1 / 1

目錄

遺漏「查閱者原則」安全標頭

嚴重性：	參考資訊
CVSS 評分：	0.0
URL：	https://qilmms.itri.org.tw/
實體：	qilmms.itri.org.tw (Page)
風險：	有可能收集 Web 應用程式相關的機密性資訊，如：使用者名稱、密碼、機器名稱及/或機密檔案位置 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：	不安全的 Web 應用程式程式設計或設定
修正：	配置您的伺服器，以搭配安全原則使用「查閱者原則」標頭

差異：

推論： AppScan 偵測到查閱者原則回應標頭遺漏或包含不安全的原則，這會增加各種跨網站注入攻擊的暴露風險

原始測試回應：

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000
Date: Thu, 28 Mar 2024 03:01:26 GMT
Content-Length: 5322
Set-Cookie: ASP.NET_SessionId=5rsd3n0sj3ydg4ibcaxviksl; path=/; secure; HttpOnly; SameSite=Lax
Set-Cookie:
TS01b84bc8=01bba7060a1e875a75a8c1113b3f6eed2c2324626550592c4e9fc54c9cbbd73f13494fdda63ccec486fb45e4534dff637851695308;
Path=/; Secure; HTTPOnly



<!DOCTYPE html>
<html lang="zh">
<head>
    <!--<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />-->
    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />

...
```

應用程式資料

造訪的 URL 2

目錄

URL
https://qilmms.itri.org.tw/MainPage/Login.aspx
https://qilmms.itri.org.tw/MainPage/Login.aspx