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 10.7.0
掃描開始時間： 2025/3/31 下午6:20:04

目錄

簡介

摘要

依問題類型分組的問題

如何修正

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：	5
低嚴重性問題：	5
參考資訊嚴重性問題：	1
報告中併入的安全問題總計：	11
掃描中探索到的安全問題總計：	11

一般資訊

掃描檔名：	1-11_台灣Pay QR code_正式
掃描開始時間：	2025/3/31 下午6:20:04
測試原則：	Default
CVSS 版本：	3.1
測試最佳化等級：	快速

主機	qgw.sunnybank.com.tw
埠	443
作業系統：	不明
Web 伺服器：	不明
應用程式伺服器：	JavaAppServer

登入設定值

登入方法：	無

摘要

問題類型 8

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	2
中	有弱點的元件	3
低	「Content-Security-Policy」中遺漏或包含不安全的「Style-src」或「Default-src」原則	1
低	「Content-Security-Policy」標頭中遺漏或包含不安全的「Object-Src」或「Default-src」原則	1
低	「Content-Security-Policy」標頭中遺漏或包含不安全的「Script-Src」或「Default-src」原則	1
低	遺漏「Content-Security-Policy」標頭	1
低	遺漏或不安全的 HTTP Strict-Transport-Security 標頭	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://qgw.sunnybank.com.tw/	8
中	https://qgw.sunnybank.com.tw/qgwBank/	3

修正建議 5

目錄

	補救作業	問題數目
中	將元件升級到最新穩定版本	3
中	檢閱將 SameSite Cookie 屬性配置為建議值的可能解決方案	2
低	使用長式 "max-age" 實作 HTTP Strict-Transport-Security 原則	1
低	配置伺服器利用安全原則使用 "Content-Security-Policy" 標頭	4
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 4

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。	2
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	3
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	6
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	6

原因 5

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	2
中	未安裝協力廠商產品的最新修補程式或緊急修復程式	3
低	不安全的 Web 應用程式設計或配置	6

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	6
濫用功能	3

依問題類型分組的問題

中 SameSite 屬性不安全、不適當或遺漏的 Cookie ②

目錄

問題 1 / 2

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://qgw.sunnybank.com.tw/
實體：	TS01e8aa5e (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：

```
POST /qgwBank/login HTTP/1.1
Host: qgw.sunnybank.com.tw
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
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
Content-Length: 14

userName=&dwp=

HTTP/1.1 302 Found
Date: Mon, 31 Mar 2025 10:34:37 GMT
```

```
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Security-Policy: default-src 'self' https:; img-src 'self' https: data:; style-src 'self' https: 'unsafe-inline';
script-src 'self' https: 'unsafe-inline' 'unsafe-eval'; connect-src 'self' https:; frame-ancestors 'self'
https://*.sunnybank.com.tw https://*.esunnybank.com.tw;object-src 'self';
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *; object-
src *; script-src * 'unsafe-inline' 'unsafe-eval'; style-src * 'unsafe-inline';
Referrer-Policy: no-referrer
Permissions-Policy: autoplay=(),camera=()
X-Download-Options: noopen
Access-Control-Allow-Origin: https://*.sunnybank.com.tw https://*.esunnybank.com.tw
X-Permitted-Cross-Domain-Policies: master-only
Location: https://qgw.sunnybank.com.tw/qgwBank/index
Content-Length: 0
Content-Language: en-US
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: JSESSIONID=HX3b_-eUnjlU3cv4JDlOCfGRAl3oNbX-uxhEkRqz.fiscqrcode-ap-p; path=/qgwBank; secure;
HttpOnly;HttpOnly;Secure;SameSite=Strict
Set-Cookie:
TS0134efca=0182d537af855acd5f05ec78199c823a84462d7b8e39de1a6140fce14f59bf04ba3bf9a998ccb6e5c92f6972bf10d2a74bdbe58cce;
Path=/; Secure; HttpOnly;
Set-Cookie:
TS01e8aa5e=0182d537af855acd5f05ec78199c823a84462d7b8e39de1a6140fce14f59bf04ba3bf9a998ccb6e5c92f6972bf10d2a74bdbe58cce;
path=/qgwBank; HttpOnly; Secure



GET /qgwBank/index HTTP/1.1
Cookie: JSESSIONID=HX3b_-eUnjlU3cv4JDlOCfGRAl3oNbX-uxhEkRqz.fiscqrcode-ap-p;
TS01e8aa5e=0182d537af855acd5f05ec78199c823a84462d7b8e39de1a6140fce14f59bf04ba3bf9a998ccb6e5c92f6972bf10d2a74bdbe58cce;
TS0134efca=0182d537af855acd5f05ec78199c823a84462d7b8e39de1a6140fce14f59bf04ba3bf9a998ccb6e5c92f6972bf10d2a74bdbe58cce
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://qgw.sunnybank.com.tw/qgwBank/login
Host: qgw.sunnybank.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: Mon, 31 Mar 2025 10:34:37 GMT
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Security-Policy: default-src 'self' https:; img-src 'self' https: data:; style-src 'self' https: 'unsafe-inline';
script-src 'self' https: 'unsafe-inline' 'unsafe-eval'; connect-src 'self' https:; frame-ancestors 'self'
https://*.sunnybank.com.tw https://*.esunnybank.com.tw;object-src 'self';
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *; object-
src *; script-src * 'unsafe-inline' 'unsafe-eval'; style-src * 'unsafe-inline';
Referrer-Policy: no-referrer
Permissions-Policy: autoplay=(),camera=()
X-Download-Options: noopen
Access-Control-Allow-Origin: https://*.sunnybank.com.tw https://*.esunnybank.com.tw
X-Permitted-Cross-Domain-Policies: master-only
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Pragma: no-cache
Cache-Control: no-cache,no-store,must-revalidate
Expires: 0
Transfer-Encoding: chunked

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
    <meta charset="UTF-8"/>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <title>QR Code Gateway 後台管理系統</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
 <meta http-equiv="Cache-control" content="no-store">
    <!-- Le HTML5 shim, for IE6-8 support of HTML elements -->
    <!--[if lt IE 9]>
    <script src="https://cdnjs.cloudflare.com/ajax/libs/html5shiv/3.7.3/html5shiv.min.js"></script>
    <![endif]-->
    <link href="/qgwBank/css/bootstrap.min.css" rel="stylesheet" type="text/css">
    <l
...
...
...
```

問題 2 / 2

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://qgw.sunnybank.com.tw/
實體：	TS0134efca (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：

```
POST /qgwBank/login HTTP/1.1
Host: qgw.sunnybank.com.tw
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
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
Content-Length: 14

userName=&dwp=

HTTP/1.1 302 Found
Date: Mon, 31 Mar 2025 10:34:36 GMT
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Security-Policy: default-src 'self' https:; img-src 'self' https: data:; style-src 'self' https: 'unsafe-inline';
script-src 'self' https: 'unsafe-inline' 'unsafe-eval'; connect-src 'self' https:; frame-ancestors 'self'
https://*.sunnybank.com.tw https://*.esunnybank.com.tw;object-src 'self';
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *; object-
src *; script-src * 'unsafe-inline' 'unsafe-eval'; style-src * 'unsafe-inline';
Referrer-Policy: no-referrer
```

```
Permissions-Policy: autoplay=(),camera=()
X-Download-Options: noopen
Access-Control-Allow-Origin: https://*.sunnybank.com.tw https://*.esunnybank.com.tw
X-Permitted-Cross-Domain-Policies: master-only
Location: https://qgw.sunnybank.com.tw/qgwBank/index
Content-Length: 0
Content-Language: en-US
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Set-Cookie: JSESSIONID=5AX6P4COJT6iUmYW7VwowZT0cPlFX9WBtN6cjWao.fiscqrcode-ap-p; path=/qgwBank; secure;
HttpOnly;HttpOnly;Secure;SameSite=Strict
Set-Cookie: 
TS0134efca=0182d537af2cecffb6c592a53cc2c89868633a76f308a76f85a8675b9a2cdd4025dd0e8ce13ec332ec71acac7b9164219c1f1effad; 
Path=/; Secure; HttpOnly;
Set-Cookie:
TS01e8aa5e=0182d537af2cecffb6c592a53cc2c89868633a76f308a76f85a8675b9a2cdd4025dd0e8ce13ec332ec71acac7b9164219c1f1effad;
path=/qgwBank; HttpOnly; Secure



GET /qgwBank/index HTTP/1.1
Cookie: JSESSIONID=5AX6P4COJT6iUmYW7VwowZT0cPlFX9WBtN6cjWao.fiscqrcode-ap-p;
TS01e8aa5e=0182d537af2cecffb6c592a53cc2c89868633a76f308a76f85a8675b9a2cdd4025dd0e8ce13ec332ec71acac7b9164219c1f1effad;
TS0134efca=0182d537af2cecffb6c592a53cc2c89868633a76f308a76f85a8675b9a2cdd4025dd0e8ce13ec332ec71acac7b9164219c1f1effad
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://qgw.sunnybank.com.tw/qgwBank/login
Host: qgw.sunnybank.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: Mon, 31 Mar 2025 10:34:37 GMT
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Security-Policy: default-src 'self' https:; img-src 'self' https: data:; style-src 'self' https: 'unsafe-inline';
script-src 'self' https: 'unsafe-inline' 'unsafe-eval'; connect-src 'self' https:; frame-ancestors 'self'
https://*.sunnybank.com.tw https://*.esunnybank.com.tw;object-src 'self';
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *; object-
src *; script-src * 'unsafe-inline' 'unsafe-eval'; style-src * 'unsafe-inline';
Referrer-Policy: no-referrer
Permissions-Policy: autoplay=(),camera=()
X-Download-Options: noopen
Access-Control-Allow-Origin: https://*.sunnybank.com.tw https://*.esunnybank.com.tw
X-Permitted-Cross-Domain-Policies: master-only
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Pragma: no-cache
Cache-Control: no-cache,no-store,must-revalidate
Expires: 0
Transfer-Encoding: chunked

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
    <meta charset="UTF-8"/>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <title>QR Code Gateway 後台管理系統</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
 <meta http-equiv="Cache-control" content="no-store">
    <!-- Le HTML5 shim, for IE6-8 support of HTML elements -->
    <!--[if lt IE 9]>
    <script src="https://cdnjs.cloudflare.com/ajax/libs/html5shiv/3.7.3/html5shiv.min.js"></script>
    <![endif]-->
    <link href="/qgwBank/css/bootstrap.min.css" rel="stylesheet" type="text/css">
    <l
...
...
...
```

中 有弱點的元件 3 目錄

問題 1 / 3

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-2012-6708
URL：	https://qgw.sunnybank.com.tw/qgwBank/
實體：	jQuery 1.8.3 (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： AppScan 發現有弱點的元件

測試要求和回應：

```
GET /qgwBank/ HTTP/1.1
Host: qgw.sunnybank.com.tw
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
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
Date: Mon, 31 Mar 2025 11:04:02 GMT
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Security-Policy: default-src 'self' https:; img-src 'self' https: data:; style-src 'self' https: 'unsafe-inline';
script-src 'self' https: 'unsafe-inline' 'unsafe-eval'; connect-src 'self' https:; frame-ancestors 'self'
https://*.sunnybank.com.tw https://*.esunnybank.com.tw;object-src 'self';
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *; object-
src *; script-src * 'unsafe-inline' 'unsafe-eval'; style-src * 'unsafe-inline';
Referrer-Policy: no-referrer
Permissions-Policy: autoplay=(),camera=()
X-Download-Options: noopen
Access-Control-Allow-Origin: https://*.sunnybank.com.tw https://*.esunnybank.com.tw
X-Permitted-Cross-Domain-Policies: master-only
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Pragma: no-cache
Cache-Control: no-cache,no-store,must-revalidate
Expires: 0
```

```
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
    <meta charset="UTF-8"/>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <title>QR Code Gateway 後台管理系統</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
 <meta http-equiv="Cache-control" content="no-store">
    <!-- Le HTML5 shim, for IE6-8 support of HTML elements -->
    <!--[if lt IE 9]>
    <script src="https://cdnjs.cloudflare.com/ajax/libs/html5shiv/3.7.3/html5shiv.min.js"></script>
    <![endif]-->
    <link href="/qgwBank/css/bootstrap.min.css" rel="stylesheet" type="text/css">
    <link href="/qgwBank/css/dcs.css" rel="stylesheet" type="text/css">
</head>
<body class="body-signIn">
<!-- Navigation bar -->
<div class="navbar navbar-fixed-top">
    <div class="navbar-inner">
        <div class="container" style="width: 98%">

                         <span>
                                 <img src="/qgwBank/images/logo/index_logo.png">&nbsp;&nbsp;
                                 <strong style="color: #04B404 "><b style="font-size:200%">QR Code Gateway        後台管理系
統</b></strong>
                         </span>
          <div class="nav-collapse collapse navbar-inverse-collapse">
          </div><!-- /.nav-collapse -->
        </div><!-- /container -->
    </div><!-- /navbar-inner -->
</div>
<!-- /navbar -->


<div class="container">
    <br><br><br><br><br>

    <form method="post" class="form-signIn" action="/qgwBank/login">
        <br>
        <div style="text-align:center">
          <b>員工編號: </b>
          <input type="text" style="width: 40%"
          placeholder="員編" id="userName" name="userName" value=""><br>
          <b>登入密碼: </b>
          <input type="password" style="width: 40%"
          placeholder="登入PC密碼" autocomplete="off" id="dwp" name="dwp" value=""><br>
          <br>
          <button class="btn btn-large btn-primary" type="submit">登入系統</button>
        </div>
    </form>


    <div>
                 <pre>
                                本系統僅提供電金部、資訊處人員進行操作。
                                若需要使用權限請洽詢以下聯絡窗口：

                                姓名:電金部 - 莊三輝
                                電話 (02)2820-8166分機877

                                姓名:資訊處 - 賴芳枝
                                電話：(02)2820-8166 分機:533</pre>
    </div>
</div>

<script src="/qgwBank/js/jquery-1.8.3.min.js"></script>
<script src="/qgwBank/js/bootstrap.min.js"></script>
<!--<script type="text/javascript">-->
    <!--if (window !== top) {-->
        <!--top.location.href = location.href;-->
    <!--}-->
<!--</script>-->
</body>
</html>
```

問題 2 / 3

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://qgw.sunnybank.com.tw/qgwBank/
實體：	jQuery 1.8.3 (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： AppScan 發現有弱點的元件

測試要求和回應：

```
GET /qgwBank/ HTTP/1.1
Host: qgw.sunnybank.com.tw
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
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
Date: Mon, 31 Mar 2025 11:04:02 GMT
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Security-Policy: default-src 'self' https:; img-src 'self' https: data:; style-src 'self' https: 'unsafe-inline';
script-src 'self' https: 'unsafe-inline' 'unsafe-eval'; connect-src 'self' https:; frame-ancestors 'self'
https://*.sunnybank.com.tw https://*.esunnybank.com.tw;object-src 'self';
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *; object-
src *; script-src * 'unsafe-inline' 'unsafe-eval'; style-src * 'unsafe-inline';
Referrer-Policy: no-referrer
Permissions-Policy: autoplay=(),camera=()
X-Download-Options: noopen
Access-Control-Allow-Origin: https://*.sunnybank.com.tw https://*.esunnybank.com.tw
X-Permitted-Cross-Domain-Policies: master-only
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Pragma: no-cache
Cache-Control: no-cache,no-store,must-revalidate
Expires: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
    <meta charset="UTF-8"/>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <title>QR Code Gateway 後台管理系統</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
 <meta http-equiv="Cache-control" content="no-store">
    <!-- Le HTML5 shim, for IE6-8 support of HTML elements -->
    <!--[if lt IE 9]>
    <script src="https://cdnjs.cloudflare.com/ajax/libs/html5shiv/3.7.3/html5shiv.min.js"></script>
    <![endif]-->
    <link href="/qgwBank/css/bootstrap.min.css" rel="stylesheet" type="text/css">
    <link href="/qgwBank/css/dcs.css" rel="stylesheet" type="text/css">
</head>
<body class="body-signIn">
<!-- Navigation bar -->
<div class="navbar navbar-fixed-top">
    <div class="navbar-inner">
        <div class="container" style="width: 98%">

                         <span>
                                 <img src="/qgwBank/images/logo/index_logo.png">&nbsp;&nbsp;
                                 <strong style="color: #04B404 "><b style="font-size:200%">QR Code Gateway        後台管理系
統</b></strong>
                         </span>
          <div class="nav-collapse collapse navbar-inverse-collapse">
          </div><!-- /.nav-collapse -->
        </div><!-- /container -->
    </div><!-- /navbar-inner -->
</div>
<!-- /navbar -->


<div class="container">
    <br><br><br><br><br>

    <form method="post" class="form-signIn" action="/qgwBank/login">
        <br>
        <div style="text-align:center">
          <b>員工編號: </b>
          <input type="text" style="width: 40%"
          placeholder="員編" id="userName" name="userName" value=""><br>
          <b>登入密碼: </b>
          <input type="password" style="width: 40%"
          placeholder="登入PC密碼" autocomplete="off" id="dwp" name="dwp" value=""><br>
          <br>
          <button class="btn btn-large btn-primary" type="submit">登入系統</button>
        </div>
    </form>


    <div>
                 <pre>
                                本系統僅提供電金部、資訊處人員進行操作。
                                若需要使用權限請洽詢以下聯絡窗口：

                                姓名:電金部 - 莊三輝
                                電話 (02)2820-8166分機877

                                姓名:資訊處 - 賴芳枝
                                電話：(02)2820-8166 分機:533</pre>
    </div>
</div>

<script src="/qgwBank/js/jquery-1.8.3.min.js"></script>
<script src="/qgwBank/js/bootstrap.min.js"></script>
<!--<script type="text/javascript">-->
    <!--if (window !== top) {-->
        <!--top.location.href = location.href;-->
    <!--}-->
<!--</script>-->
</body>
</html>
```

問題 3 / 3

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-2020-7656
URL：	https://qgw.sunnybank.com.tw/qgwBank/
實體：	jQuery 1.8.3 (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： AppScan 發現有弱點的元件

測試要求和回應：

```
GET /qgwBank/ HTTP/1.1
Host: qgw.sunnybank.com.tw
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
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
Date: Mon, 31 Mar 2025 11:04:02 GMT
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Security-Policy: default-src 'self' https:; img-src 'self' https: data:; style-src 'self' https: 'unsafe-inline';
script-src 'self' https: 'unsafe-inline' 'unsafe-eval'; connect-src 'self' https:; frame-ancestors 'self'
https://*.sunnybank.com.tw https://*.esunnybank.com.tw;object-src 'self';
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *; object-
src *; script-src * 'unsafe-inline' 'unsafe-eval'; style-src * 'unsafe-inline';
Referrer-Policy: no-referrer
Permissions-Policy: autoplay=(),camera=()
X-Download-Options: noopen
Access-Control-Allow-Origin: https://*.sunnybank.com.tw https://*.esunnybank.com.tw
X-Permitted-Cross-Domain-Policies: master-only
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Pragma: no-cache
Cache-Control: no-cache,no-store,must-revalidate
Expires: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
    <meta charset="UTF-8"/>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <title>QR Code Gateway 後台管理系統</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
 <meta http-equiv="Cache-control" content="no-store">
```

```
    <!-- Le HTML5 shim, for IE6-8 support of HTML elements -->
    <!--[if lt IE 9]>
    <script src="https://cdnjs.cloudflare.com/ajax/libs/html5shiv/3.7.3/html5shiv.min.js"></script>
    <![endif]-->
    <link href="/qgwBank/css/bootstrap.min.css" rel="stylesheet" type="text/css">
    <link href="/qgwBank/css/dcs.css" rel="stylesheet" type="text/css">
</head>
<body class="body-signIn">
<!-- Navigation bar -->
<div class="navbar navbar-fixed-top">
    <div class="navbar-inner">
        <div class="container" style="width: 98%">

                         <span>
                                 <img src="/qgwBank/images/logo/index_logo.png">&nbsp;&nbsp;
                                 <strong style="color: #04B404 "><b style="font-size:200%">QR Code Gateway        後台管理系
統</b></strong>
                         </span>
          <div class="nav-collapse collapse navbar-inverse-collapse">
          </div><!-- /.nav-collapse -->
        </div><!-- /container -->
    </div><!-- /navbar-inner -->
</div>
<!-- /navbar -->


<div class="container">
    <br><br><br><br><br>

    <form method="post" class="form-signIn" action="/qgwBank/login">
        <br>
        <div style="text-align:center">
          <b>員工編號: </b>
          <input type="text" style="width: 40%"
          placeholder="員編" id="userName" name="userName" value=""><br>
          <b>登入密碼: </b>
          <input type="password" style="width: 40%"
          placeholder="登入PC密碼" autocomplete="off" id="dwp" name="dwp" value=""><br>
          <br>
          <button class="btn btn-large btn-primary" type="submit">登入系統</button>
        </div>
    </form>


    <div>
                 <pre>
                                本系統僅提供電金部、資訊處人員進行操作。
                                若需要使用權限請洽詢以下聯絡窗口：

                                姓名:電金部 - 莊三輝
                                電話 (02)2820-8166分機877

                                姓名:資訊處 - 賴芳枝
                                電話：(02)2820-8166 分機:533</pre>
    </div>
</div>

<script src="/qgwBank/js/jquery-1.8.3.min.js"></script>
<script src="/qgwBank/js/bootstrap.min.js"></script>
<!--<script type="text/javascript">-->
    <!--if (window !== top) {-->
        <!--top.location.href = location.href;-->
    <!--}-->
<!--</script>-->
</body>
</html>
```

低 「Content-Security-Policy」中遺漏或包含不安全的「Style-src」或「Default-src」原則 1

目錄

問題 1 / 1

目錄

「Content-Security-Policy」中遺漏或包含不安全的「Style-src」或「Default-src」原則

嚴重性：	低
CVSS 評分：	3.7
CVSS 向量：	AV:N/AC:H/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://qgw.sunnybank.com.tw/
實體：	qgw.sunnybank.com.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

測試要求和回應：

```
GET /qgwBank/js/bootstrap.min.js HTTP/1.1
Host: qgw.sunnybank.com.tw
Connection: keep-alive
sec-ch-ua: "Not_A Brand";v="8", "Chromium";v="120"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Content-Length: 0


HTTP/1.1 200 OK
Date: Mon, 31 Mar 2025 10:37:23 GMT
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Security-Policy: default-src 'self' https:; img-src 'self' https: data:; style-src 'self' https: 'unsafe-inline';
script-src 'self' https: 'unsafe-inline' 'unsafe-eval'; connect-src 'self' https:; frame-ancestors 'self'
https://*.sunnybank.com.tw https://*.esunnybank.com.tw;object-src 'self';
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *; object-
src *; script-src * 'unsafe-inline' 'unsafe-eval'; style-src * 'unsafe-inline';
Referrer-Policy: no-referrer
Permissions-Policy: autoplay=(),camera=()
X-Download-Options: noopen
Access-Control-Allow-Origin: https://*.sunnybank.com.tw https://*.esunnybank.com.tw
X-Permitted-Cross-Domain-Policies: master-only
```

```
Accept-Ranges: bytes
Last-Modified: Fri, 04 Aug 2017 08:55:48 GMT
Content-Length: 31596
Content-Type: application/javascript; charset=UTF-8
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive

/*!
* Bootstrap.js by @fat & @mdo
* Copyright 2012 Twitter, Inc.
* http://www.apache.org/licenses/LICENSE-2.0.txt
*/
!function($){"use strict";$(function(){$.support.transition=function(){var transitionEnd=function(){var
name,el=document.createElement("bootstrap"),transEndEventNames=
{WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd
otransitionend",transition:"transitionend"};for(name in transEndEventNames)if(void 0!==el.style[name])return
transEndEventNames[name]}();return transitionEnd&&{end:transitionEnd}}()})}(window.jQuery),!function($){"use strict";var
dismiss='[data-dismiss="alert"]',Alert=function(el){$(el).on("click",dismiss,this.close)};Alert.prototype.close=function(e)
{function removeElement(){$parent.trigger("closed").remove()}var $parent,$this=$(this),selector=$this.attr("data-
target");selector||(selector=$this.attr("href"),selector=selector&&selector.replace(/.*(?=#
[^\s]*$)/,"")),$parent=$(selector),e&&e.preventDefault(),$parent.length||($parent=$this.hasClass("alert")?
$this:$this.parent()),$parent.trigger(e=$.Event("close")),e.isDefaultPrevented()||
($parent.removeClass("in"),$.support.transition&&$parent.hasClass("fade")?
$parent.on($.support.transition.end,removeElement):removeElement())};var old=$.fn.alert;$.fn.alert=function(option){return
this.each(function(){var $this=$(this),data=$this.data("alert");data||$this.data("alert",data=new
Alert(this)),"string"==typeof
option&&data[option].call($this)})},$.fn.alert.Constructor=Alert,$.fn.alert.noConflict=function(){return
$.fn.alert=old,this},$(document).on("click.alert.data-api",dismiss,Alert.prototype.close)}(window.jQuery),!function($){"use
strict";var Button=function(element,options)
{this.$element=$(element),this.options=$.extend({},$.fn.button.defaults,options)};Button.prototype.setState=function(state)
{var
d="disabled",$el=this.$element,data=$el.data(),val=$el.is("input")?"val":"html";state+="Text",data.resetText||$el.data("res
etText",$el[val]()),$el[val](data[state]||this.options[state]),setTimeout(function(){"loadingText"==state?
$el.addClass(d).attr(d,d):$el.removeClass(d).removeAttr(d)},0)},Button.prototype.toggle=function(){var
$parent=this.$element.closest('[data-toggle="buttons-
radio"]');$parent&&$parent.find(".active").removeClass("active"),this.$element.toggleClass("active")};var
old=$.fn.button;$.fn.button=function(option){return this.each(function(){var
$this=$(this),data=$this.data("button"),options="object"==typeof option&&option;data||$this.data("button",data=new
Button(this,options)),"toggle"==option?data.toggle():option&&data.setState(option)})},$.fn.button.defaults=
{loadingText:"loading..."},$.fn.button.Constructor=Button,$.fn.button.noConflict=function(){return
$.fn.button=old,this},$(document).on("click.button.data-api","[data-toggle^=button]",function(e){var
$btn=$(e.target);$btn.hasClass("btn")||($btn=$btn.closest(".btn")),$btn.button("toggle")})}(window.jQuery),!function($)
{"use strict";var Carousel=function(element,options)
{this.$element=$(element),this.options=options,"hover"==this.options.pause&&this.$element.on("mouseenter",$.proxy(this.paus
e,this)).on("mouseleave",$.proxy(this.cycle,this))};Carousel.prototype={cycle:function(e
...
...
...
```

低 「Content-Security-Policy」標頭中遺漏或包含不安全的「Object-Src」或「Default-src」原則 1

目錄

問題 1 / 1

目錄

「Content-Security-Policy」標頭中遺漏或包含不安全的「Object-Src」或「Default-src」原則

嚴重性：	低
CVSS 評分：	3.7
CVSS 向量：	AV:N/AC:H/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://qgw.sunnybank.com.tw/
實體：	qgw.sunnybank.com.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

測試要求和回應：

```
GET /qgwBank/js/bootstrap.min.js HTTP/1.1
Host: qgw.sunnybank.com.tw
Connection: keep-alive
sec-ch-ua: "Not_A Brand";v="8", "Chromium";v="120"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Content-Length: 0


HTTP/1.1 200 OK
Date: Mon, 31 Mar 2025 10:37:23 GMT
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Security-Policy: default-src 'self' https:; img-src 'self' https: data:; style-src 'self' https: 'unsafe-inline';
script-src 'self' https: 'unsafe-inline' 'unsafe-eval'; connect-src 'self' https:; frame-ancestors 'self'
https://*.sunnybank.com.tw https://*.esunnybank.com.tw;object-src 'self';
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *; object-
src *; script-src * 'unsafe-inline' 'unsafe-eval'; style-src * 'unsafe-inline';
Referrer-Policy: no-referrer
Permissions-Policy: autoplay=(),camera=()
X-Download-Options: noopen
Access-Control-Allow-Origin: https://*.sunnybank.com.tw https://*.esunnybank.com.tw
X-Permitted-Cross-Domain-Policies: master-only
Accept-Ranges: bytes
Last-Modified: Fri, 04 Aug 2017 08:55:48 GMT
Content-Length: 31596
Content-Type: application/javascript; charset=UTF-8
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive

/*!
* Bootstrap.js by @fat & @mdo
* Copyright 2012 Twitter, Inc.
* http://www.apache.org/licenses/LICENSE-2.0.txt
*/
!function($){"use strict";$(function(){$.support.transition=function(){var transitionEnd=function(){var
name,el=document.createElement("bootstrap"),transEndEventNames=
{WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd
otransitionend",transition:"transitionend"};for(name in transEndEventNames)if(void 0!==el.style[name])return
transEndEventNames[name]}();return transitionEnd&&{end:transitionEnd}}()})}(window.jQuery),!function($){"use strict";var
dismiss='[data-dismiss="alert"]',Alert=function(el){$(el).on("click",dismiss,this.close)};Alert.prototype.close=function(e)
{function removeElement(){$parent.trigger("closed").remove()}var $parent,$this=$(this),selector=$this.attr("data-
target");selector||(selector=$this.attr("href"),selector=selector&&selector.replace(/.*(?=#
[^\s]*$)/,"")),$parent=$(selector),e&&e.preventDefault(),$parent.length||($parent=$this.hasClass("alert")?
$this:$this.parent()),$parent.trigger(e=$.Event("close")),e.isDefaultPrevented()||
($parent.removeClass("in"),$.support.transition&&$parent.hasClass("fade")?
$parent.on($.support.transition.end,removeElement):removeElement())};var old=$.fn.alert;$.fn.alert=function(option){return
this.each(function(){var $this=$(this),data=$this.data("alert");data||$this.data("alert",data=new
Alert(this)),"string"==typeof
option&&data[option].call($this)})},$.fn.alert.Constructor=Alert,$.fn.alert.noConflict=function(){return
$.fn.alert=old,this},$(document).on("click.alert.data-api",dismiss,Alert.prototype.close)}(window.jQuery),!function($){"use
strict";var Button=function(element,options)
{this.$element=$(element),this.options=$.extend({},$.fn.button.defaults,options)};Button.prototype.setState=function(state)
{var
d="disabled",$el=this.$element,data=$el.data(),val=$el.is("input")?"val":"html";state+="Text",data.resetText||$el.data("res
etText",$el[val]()),$el[val](data[state]||this.options[state]),setTimeout(function(){"loadingText"==state?
$el.addClass(d).attr(d,d):$el.removeClass(d).removeAttr(d)},0)},Button.prototype.toggle=function(){var
$parent=this.$element.closest('[data-toggle="buttons-
radio"]');$parent&&$parent.find(".active").removeClass("active"),this.$element.toggleClass("active")};var
old=$.fn.button;$.fn.button=function(option){return this.each(function(){var
$this=$(this),data=$this.data("button"),options="object"==typeof option&&option;data||$this.data("button",data=new
Button(this,options)),"toggle"==option?data.toggle():option&&data.setState(option)})},$.fn.button.defaults=
{loadingText:"loading..."},$.fn.button.Constructor=Button,$.fn.button.noConflict=function(){return
$.fn.button=old,this},$(document).on("click.button.data-api","[data-toggle^=button]",function(e){var
$btn=$(e.target);$btn.hasClass("btn")||($btn=$btn.closest(".btn")),$btn.button("toggle")})}(window.jQuery),!function($)
{"use strict";var Carousel=function(element,options)
{this.$element=$(element),this.options=options,"hover"==this.options.pause&&this.$element.on("mouseenter",$.proxy(this.paus
e,this)).on("mouseleave",$.proxy(this.cycle,this))};Carousel.prototype={cycle:function(e
...
...
...
```

低 「Content-Security-Policy」標頭中遺漏或包含不安全的「Script-Src」或「Default-src」原則 1

目錄

問題 1 / 1

目錄

「Content-Security-Policy」標頭中遺漏或包含不安全的「Script-Src」或「Default-src」原則

嚴重性：	低
CVSS 評分：	3.7
CVSS 向量：	AV:N/AC:H/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://qgw.sunnybank.com.tw/
實體：	qgw.sunnybank.com.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

測試要求和回應：

```
GET /qgwBank/js/bootstrap.min.js HTTP/1.1
Host: qgw.sunnybank.com.tw
Connection: keep-alive
sec-ch-ua: "Not_A Brand";v="8", "Chromium";v="120"
```

```
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Content-Length: 0


HTTP/1.1 200 OK
Date: Mon, 31 Mar 2025 10:37:23 GMT
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Security-Policy: default-src 'self' https:; img-src 'self' https: data:; style-src 'self' https: 'unsafe-inline';
script-src 'self' https: 'unsafe-inline' 'unsafe-eval'; connect-src 'self' https:; frame-ancestors 'self'
https://*.sunnybank.com.tw https://*.esunnybank.com.tw;object-src 'self';
Content-Security-Policy: default-src 'self'; connect-src *; font-src *; frame-src *; img-src * data:; media-src *; object-
src *; script-src * 'unsafe-inline' 'unsafe-eval'; style-src * 'unsafe-inline';
Referrer-Policy: no-referrer
Permissions-Policy: autoplay=(),camera=()
X-Download-Options: noopen
Access-Control-Allow-Origin: https://*.sunnybank.com.tw https://*.esunnybank.com.tw
X-Permitted-Cross-Domain-Policies: master-only
Accept-Ranges: bytes
Last-Modified: Fri, 04 Aug 2017 08:55:48 GMT
Content-Length: 31596
Content-Type: application/javascript; charset=UTF-8
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive

/*!
* Bootstrap.js by @fat & @mdo
* Copyright 2012 Twitter, Inc.
* http://www.apache.org/licenses/LICENSE-2.0.txt
*/
!function($){"use strict";$(function(){$.support.transition=function(){var transitionEnd=function(){var
name,el=document.createElement("bootstrap"),transEndEventNames=
{WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd
otransitionend",transition:"transitionend"};for(name in transEndEventNames)if(void 0!==el.style[name])return
transEndEventNames[name]}();return transitionEnd&&{end:transitionEnd}}()})}(window.jQuery),!function($){"use strict";var
dismiss='[data-dismiss="alert"]',Alert=function(el){$(el).on("click",dismiss,this.close)};Alert.prototype.close=function(e)
{function removeElement(){$parent.trigger("closed").remove()}var $parent,$this=$(this),selector=$this.attr("data-
target");selector||(selector=$this.attr("href"),selector=selector&&selector.replace(/.*(?=#
[^\s]*$)/,"")),$parent=$(selector),e&&e.preventDefault(),$parent.length||($parent=$this.hasClass("alert")?
$this:$this.parent()),$parent.trigger(e=$.Event("close")),e.isDefaultPrevented()||
($parent.removeClass("in"),$.support.transition&&$parent.hasClass("fade")?
$parent.on($.support.transition.end,removeElement):removeElement())};var old=$.fn.alert;$.fn.alert=function(option){return
this.each(function(){var $this=$(this),data=$this.data("alert");data||$this.data("alert",data=new
Alert(this)),"string"==typeof
option&&data[option].call($this)})},$.fn.alert.Constructor=Alert,$.fn.alert.noConflict=function(){return
$.fn.alert=old,this},$(document).on("click.alert.data-api",dismiss,Alert.prototype.close)}(window.jQuery),!function($){"use
strict";var Button=function(element,options)
{this.$element=$(element),this.options=$.extend({},$.fn.button.defaults,options)};Button.prototype.setState=function(state)
{var
d="disabled",$el=this.$element,data=$el.data(),val=$el.is("input")?"val":"html";state+="Text",data.resetText||$el.data("res
etText",$el[val]()),$el[val](data[state]||this.options[state]),setTimeout(function(){"loadingText"==state?
$el.addClass(d).attr(d,d):$el.removeClass(d).removeAttr(d)},0)},Button.prototype.toggle=function(){var
$parent=this.$element.closest('[data-toggle="buttons-
radio"]');$parent&&$parent.find(".active").removeClass("active"),this.$element.toggleClass("active")};var
old=$.fn.button;$.fn.button=function(option){return this.each(function(){var
$this=$(this),data=$this.data("button"),options="object"==typeof option&&option;data||$this.data("button",data=new
Button(this,options)),"toggle"==option?data.toggle():option&&data.setState(option)})},$.fn.button.defaults=
{loadingText:"loading..."},$.fn.button.Constructor=Button,$.fn.button.noConflict=function(){return
$.fn.button=old,this},$(document).on("click.button.data-api","[data-toggle^=button]",function(e){var
$btn=$(e.target);$btn.hasClass("btn")||($btn=$btn.closest(".btn")),$btn.button("toggle")})}(window.jQuery),!function($)
{"use strict";var Carousel=function(element,options)
{this.$element=$(element),this.options=options,"hover"==this.options.pause&&this.$element.on("mouseenter",$.proxy(this.paus
e,this)).on("mouseleave",$.proxy(this.cycle,this))};Carousel.prototype={cycle:function(e
...
...
...
```

低 遺漏「Content-Security-Policy」標頭 1

目錄

問題 1 / 1

目錄

遺漏「Content-Security-Policy」標頭

嚴重性：	低
CVSS 評分：	3.7
CVSS 向量：	AV:N/AC:H/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://qgw.sunnybank.com.tw/
實體：	qgw.sunnybank.com.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

測試要求和回應：

```
GET /qgwBank/cfide/administrator/ HTTP/1.1
Host: qgw.sunnybank.com.tw
Connection: keep-alive
sec-ch-ua: "Not_A Brand";v="8", "Chromium";v="120"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Content-Length: 0


HTTP/1.1 200 OK
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Cache-Control: no-cache
Connection: close
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Content-Length: 2572

<!doctype html>
<!-- CSS only -->
<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.1/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-
F3w7mX95PdgyTmZZMECAngseQB83DfGTowi0iMjiWaeVhAn4FJkqJByhZMI3AhiU" crossorigin="anonymous">
<style type="text/css">



 #all { width: 850px; border:2px solid #006600; background-color: #FFFFFF;
            margin: 13% auto;}

 #logo {height: auto;  margin: 10px; }

 #center-content { border-top:1px solid #006600; }
 .content {
 width: 650px;
 font-family:"       微軟正黑體";
 text-decoration-color: #292421;
}

 .content-Location{ margin: auto; padding-top: 10px; padding-bottom: 10px;}
 .img- {width:845px; border: 0px}





body {
 background-color: #CCCCCC;
}
</style>
<html>
<head>
<meta charset="utf-8">
<title>無標題文件</title>


 <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.1/dist/js/bootstrap.bundle.min.js" integrity="sha384-
/bQdsTh/da6pkI1MST/rWKFNjaCP5gBSY4sEBT38Q/9RBh9AH40zEOg7Hlq2THRZ" crossorigin="anonymous"></script>



</head>

<body>


<div id="all">
 <div id="logo"><a href="https://www.sunnybank.com.tw/net/"><img style="border: 0px"
src="https://www.sunnybank.com.tw/images/logo-web.png"></a></div>
 <div id="center-content">
         <p><b><h1 class="content content-Location" style="color:#006600" align="center">       連線資料異常</h1></b></p>

         <div class="content content-Location">
         <p><font size="4">       親愛的客戶，您好:
很抱歉，由於未能與系統建立正常的連線服務，請將以下序號提供予本行客服人員，
將為您提供協助，敬請見諒!</font></p>
                 <p></p>
          <div class="content content-Location">
          <b style="color:#006600">查詢序號:
          <span><font size="6">15830642746004215122<br><br><a href='javascript:history.back();'></a></font><CENTER></span>
</b>
          </div>
         </div>

   </div>
 <span class="col font-weight-bold TileFont d-flex align-items-end" style="background-image: linear-gradient(to
right, white, rgba(255,255,255,1) 0%, rgba(252,255,130,1) 20%, rgba(41,154,11,1) 100%);">
         <span class="col-12 text-center" style="line-height:28px" >
                 <p></p>
                 <font size="3" color="006606">       分行營業時間 週一至週五  09:00~15:30  |  客服中心電話:(02)7736-6689</font>
<br>
                 <span class="col-12 text-center">
                         <font size="3" color="006606">©       陽信商業銀行 版權所有 SunnyBank. All Rights Reserved</font>
                 <p></p>
                 </span>
         </span>
     </span>
</div>

</body>
</html>
```

低 遺漏或不安全的 HTTP Strict-Transport-Security 標頭 1

目錄

目錄

遺漏或不安全的 HTTP Strict-Transport-Security 標頭

嚴重性：	低
CVSS 評分：	3.7
CVSS 向量：	AV:N/AC:H/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://qgw.sunnybank.com.tw/
實體：	qgw.sunnybank.com.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：	使用長式 "max-age" 實作 HTTP Strict-Transport-Security 原則

差異：

推論： AppScan 偵測到遺漏 HTTP Strict-Transport-Security 回應標頭或是 "max-age" 不足

測試要求和回應：

```
GET /qgwBank/sites/samples/ HTTP/1.1
Host: qgw.sunnybank.com.tw
Connection: keep-alive
sec-ch-ua: "Not_A Brand";v="8", "Chromium";v="120"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Content-Length: 0


HTTP/1.1 200 OK
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Cache-Control: no-cache
Connection: close
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Content-Length: 2572

<!doctype html>
<!-- CSS only -->
<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.1/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-
F3w7mX95PdgyTmZZMECAngseQB83DfGTowi0iMjiWaeVhAn4FJkqJByhZMI3AhiU" crossorigin="anonymous">
<style type="text/css">



 #all { width: 850px; border:2px solid #006600; background-color: #FFFFFF;
            margin: 13% auto;}

 #logo {height: auto;  margin: 10px; }

 #center-content { border-top:1px solid #006600; }

 .content {
 width: 650px;
 font-family:"       微軟正黑體";
 text-decoration-color: #292421;
}

 .content-Location{ margin: auto; padding-top: 10px; padding-bottom: 10px;}
 .img- {width:845px; border: 0px}
```

```
body {
 background-color: #CCCCCC;
}
</style>
<html>
<head>
<meta charset="utf-8">
<title>無標題文件</title>


 <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.1/dist/js/bootstrap.bundle.min.js" integrity="sha384-
/bQdsTh/da6pkI1MST/rWKFNjaCP5gBSY4sEBT38Q/9RBh9AH40zEOg7Hlq2THRZ" crossorigin="anonymous"></script>



</head>

<body>


<div id="all">
 <div id="logo"><a href="https://www.sunnybank.com.tw/net/"><img style="border: 0px"
src="https://www.sunnybank.com.tw/images/logo-web.png"></a></div>
 <div id="center-content">
         <p><b><h1 class="content content-Location" style="color:#006600" align="center">       連線資料異常</h1></b></p>

         <div class="content content-Location">
         <p><font size="4">       親愛的客戶，您好:
很抱歉，由於未能與系統建立正常的連線服務，請將以下序號提供予本行客服人員，
將為您提供協助，敬請見諒!</font></p>
                 <p></p>
          <div class="content content-Location">
          <b style="color:#006600">查詢序號:
          <span><font size="6">15830642746004212466<br><br><a href='javascript:history.back();'></a></font><CENTER></span>
</b>
          </div>
         </div>

  </div>
 <span class="col font-weight-bold TileFont d-flex align-items-end" style="background-image: linear-gradient(to
right, white, rgba(255,255,255,1) 0%, rgba(252,255,130,1) 20%, rgba(41,154,11,1) 100%);">
         <span class="col-12 text-center" style="line-height:28px" >
                 <p></p>
                 <font size="3" color="006606">       分行營業時間 週一至週五  09:00~15:30  ┃  客服中心電話:(02)7736-6689</font>
<br>
                 <span class="col-12 text-center">
                         <font size="3" color="006606">©       陽信商業銀行 版權所有 SunnyBank. All Rights Reserved</font>
                 <p></p>
                 </span>
         </span>
    </span>
</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
CVSS 向量：	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N/E:X/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://qgw.sunnybank.com.tw/
實體：	qgw.sunnybank.com.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

測試要求和回應：

```
GET /qgwBank/cfide/administrator/ HTTP/1.1
Host: qgw.sunnybank.com.tw
Connection: keep-alive
sec-ch-ua: "Not_A Brand";v="8", "Chromium";v="120"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
sec-ch-ua-platform: "Windows"
Accept: */*
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Content-Length: 0


HTTP/1.1 200 OK
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Cache-Control: no-cache
Connection: close
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Content-Length: 2572

<!doctype html>
<!-- CSS only -->
<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.1/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-
F3w7mX95PdgyTmZZMECAngseQB83DfGTowi0iMjiWaeVhAn4FJkqJByhZMI3AhiU" crossorigin="anonymous">
<style type="text/css">



 #all { width: 850px; border:2px solid #006600; background-color: #FFFFFF;
            margin: 13% auto;}
 #logo {height: auto;  margin: 10px; }

 #center-content { border-top:1px solid #006600; }

 .content {
 width: 650px;
 font-family:"        微軟正黑體";
 text-decoration-color: #292421;
}

 .content-Location{ margin: auto; padding-top: 10px; padding-bottom: 10px;}
 .img- {width:845px; border: 0px}





body {
 background-color: #CCCCCC;
}
</style>
<html>
<head>
<meta charset="utf-8">
<title>無標題文件</title>


 <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.1.1/dist/js/bootstrap.bundle.min.js" integrity="sha384-
/bQdsTh/da6pkI1MST/rWKFNjaCP5gBSY4sEBT38Q/9RBh9AH40zEOg7Hlq2THRZ" crossorigin="anonymous"></script>



</head>

<body>


<div id="all">
 <div id="logo"><a href="https://www.sunnybank.com.tw/net/"><img style="border: 0px"
src="https://www.sunnybank.com.tw/images/logo-web.png"></a></div>
 <div id="center-content">
         <p><b><h1 class="content content-Location" style="color:#006600" align="center">       連線資料異常</h1></b></p>

         <div class="content content-Location">
         <p><font size="4">       親愛的客戶，您好:
很抱歉，由於未能與系統建立正常的連線服務，請將以下序號提供予本行客服人員，
將為您提供協助，敬請見諒!</font></p>
                 <p></p>
          <div class="content content-Location">
          <b style="color:#006600">查詢序號:
          <span><font size="6">15830642746001449556<br><br><a href='javascript:history.back();'></a></font><CENTER></span>
</b>
          </div>
         </div>

  </div>
 <span class="col font-weight-bold TileFont d-flex align-items-end" style="background-image: linear-gradient(to
right, white, rgba(255,255,255,1) 0%, rgba(252,255,130,1) 20%, rgba(41,154,11,1) 100%);">
         <span class="col-12 text-center" style="line-height:28px" >
                 <p></p>
                 <font size="3" color="006606">       分行營業時間 週一至週五  09:00~15:30  ｜  客服中心電話:(02)7736-6689</font>
<br>
                 <span class="col-12 text-center">
                         <font size="3" color="006606">©        陽信商業銀行 版權所有 SunnyBank. All Rights Reserved</font>
                 <p></p>
                 </span>
         </span>
    </span>
</div>

</body>
</html>
```

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

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

升級到該組件的最新版本。如果該組件已達到其生命終結（EOL），請用最近支持的替代品替換該組件。我們強烈建議聯繫該產品的供應商，看看是否最近有補丁或修復可用。

CWE：

1035

外部參照：

CERT 協調中心
常見弱點和暴露 (CVE)

「Content-Security-Policy」中遺漏或包含不安全的「Style-src」或「Default-src」原則

目錄

原因：

不安全的 Web 應用程式設計或配置

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資訊，如：使用者名稱、密碼、信用卡號碼、社會保險號碼等等
缺少 style-src 指引 (CSP) 或不正確的值可能會導致 Web 應用程式更容易受到跨網站指令碼 的攻擊。
「Content-Security-Policy」標頭的目的在於修改瀏覽器呈現頁面的方式，進而預防各種跨網站注入攻擊，包括跨網站 Cross-Site Scripting。請務必設定正確的標頭值，避免網站運作不良。例如，如果將標頭設定為禁止執行行內 JavaScript，網站就不能在頁面中使用行內 JavaScript。
「style-src」內容安全原則 (CSP) 指令會保護 CSS 樣式和樣式表的載入和執行。
為了防止跨網站指令碼 (XSS)，請務必使用適當的值設定原則：
對 'style-src' 而言，不安全的值（例如：'*'、'data:'、'http:'、'https:'、'ws:'、'wss:'、'unsafe-inline' 或是 'unsafe-eval'）都應該避免。
如未明確設定 style-src 指引，請考慮使用 default-src，可充當包括 style-src 在內的多個指引之應變方案。
「default-src」指引也應該避免使用不安全的值。
如需詳細資訊，請參考以下連結。

受影響的產品：

此問題可能會影響不同類型的產品

修正建議：

一般

配置您的伺服器，以正確的「style-src」值傳送「Content-Security-Policy」標頭。
建議使用「self」或「none」等安全值來配置 style-src 指引，如有需要，您應將「unsafe-inline」或「unsafe-eval」與隨機數或雜湊演算法搭配使用。
如未明確設定 style-src 指引，請考慮使用 default-src 作為應變方案，並且也應避免在「default-src」指引中使用不安全的值。安全的「default-src」值包括「none」、「unsafe-inline」、「unsafe-eval」搭被隨機數或雜湊演算法。
如為 Apache，請參閱：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
如為 IIS，請參閱：
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
如為 nginx，請參閱：
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE：

1032
16
693
830

外部參照：

幾個實用且安全的標頭清單
內容安全原則 (Content Security Policy) 的簡介
MDN web 文件 - CSP: style-src

「Content-Security-Policy」標頭中遺漏或包含不安全的「Object-Src」或「Default-src」原則

目錄

原因：

不安全的 Web 應用程式設計或配置

風險：

有可能收集 Web 應用程式相關的機密資訊，例如：使用者名稱、密碼、機器名稱及/或機密檔案位置
有可能說服容易受騙的使用者提供機密資訊，例如使用者名稱、密碼、信用卡號碼、社會安全碼等等
缺少 object-src 指引 (CSP) 或包含不正確的值，可能會導致 Web 應用程式容易受到跨網站指令碼、跨網站 framing 等攻擊。
"Content-Security-Policy" 標頭的設計是用來修改瀏覽器顯示頁面的方式，藉此避免各種跨網站注入，包含跨網站指令碼 等等。請務必要將標頭值設定正確，避免影響網站的正常運作。
object-src 指引會限制可以載入外掛程式內容的 URL。若要避免發生跨網站指令碼 (XSS)，務必要使用適當的值設定原則，如下所示：
對 'object-src' 而言，不安全的值（例如：'*'、'data:'、'http:'、'https:'、'ws:'、'wss:'、'unsafe-inline' 或是 'unsafe-eval'）都應該避免。
如果 object-src 指引未明確設定，請考慮使用 default-src，作為許多指引（包括 object-src）的後援。
default-src 指引也應該避免使用不安全的值。
如需詳細資訊，請參考以下連結。
請注意，「Content-Security-Policy」包含四個不同的測試。有個一般測試會驗證「Content-Security-Policy」標頭是否正在使用中，其他三個測試會檢查「Frame-Ancestors」、「Object-Src」和「Script-Src」是否正確設定。

受影響的產品：

此問題可能會影響不同類型的產品

修正建議：

一般

設定您的伺服器以傳送「Content-Security-Policy」標頭，並帶有「object-src」和「default-src」指引適當的值
建議使用安全值設定 object-src 指引，例如 'self' 或 'none'。如果需要，您應該使用帶有 nonce 或 hash-algorithm 的 'unsafe-inline' 或 'unsafe-eval'
若為 Apache，請參閱：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
若為 IIS，請參閱：
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
若為 nginx，請參閱：
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE：

1032
16
79
693

外部參照：

幾個實用且安全的標頭清單
內容安全原則 (Content Security Policy) 的簡介
MDN web 文件 - CSP: object-src

「Content-Security-Policy」標頭中遺漏或包含不安全的「Script-Src」或「Default-src」原則

目錄

原因：

不安全的 Web 應用程式程式設計或設定

風險：

有可能收集有關 Web 應用程式的機密資訊，例如使用者名稱、密碼、機器名稱和/或機密檔案位置
有可能讓無經驗而易受騙的使用者信以為真而提供機密資訊，例如：使用者名稱、密碼、信用卡號碼、社會保險號碼等等
缺少 script-src 指引 (CSP) 或不正確的值，可能會導致 Web 應用程式容易受到跨網站指令碼、跨網站 framing 等攻擊。
「Content-Security-Policy」標頭的目的在於修改瀏覽器呈現頁面的方式，進而預防各種跨網站注入攻擊，包括跨網站指令碼。請務必設定正確的標頭值，避免網站運作不良。例如，如果將標頭設定為禁止執行行內 JavaScript，網站就不能在頁面中使用行內 JavaScript。
script-src 指引會限制 Script 可執行的位置。這不僅包括直接載入 Script 元素的 URL，也涵蓋會觸發 Script 執行的行內 Script 區塊以及 XSLT 樣式表 [XSLT] 等等。
為了防止跨網站指令碼 (XSS)，請務必使用適當的值設定原則：
對 'script-src' 而言，不安全的值（例如：'*'、'data:'、'http:'、'https:'、'ws:'、'wss:'、'unsafe-inline' 或是 'unsafe-eval'）都應該避免。
如果 script-src 指引未明確設定，請考慮使用 default-src 作為許多指引（包括 script-src）的後援。
'default-src' 指引也應該避免使用不安全的值。
可以使用 JSONP 端點來略過將 'script-src' 或 'default-src' 值設定為 "self"。列入白名單的網域可能包含 JSONP 端點，允許不安全的回呼方法，從而間接允許攻擊者執行 XSS。因此，建議遵循 API 最佳做法，並搭配合適的 Content-Security-Policy。
如需詳細資訊，請參考以下連結。
請注意，「Content-Security-Policy」包含四個不同的測試。有個一般測試會驗證「Content-Security-Policy」標頭是否正在使用中，其他三個測試會檢查「Frame-Ancestors」、「Object-Src」和「Script-Src」是否正確設定。

受影響的產品：

此問題可能會影響不同類型的產品

修正建議：

一般

設定您的伺服器以傳送「Content-Security-Policy」標頭，並帶有「script-src」和「default-src」指引適當的值
建議以安全值來設定 script-src 指引，例如「none」、「strict-dynamic」。或者若有需要，您應該使用帶有隨機值 (nonce) 或雜湊演算法 (hash-algorithm) 的「unsafe-inline」或「unsafe-eval」，而不是使用「self」設定「script-src」或「default-src」。
針對 Apache，請參閱：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
針對 IIS，請參閱：
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
針對 nginx，請參閱：
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE：

1032
16
830

外部參照：

幾個實用且安全的標頭清單
「內容安全原則 (Content Security Policy)」的簡介
MDN web 文件 - CSP: script-src

遺漏「Content-Security-Policy」標頭

目錄

原因：

不安全的 Web 應用程式設計或配置

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
有可能讓無經驗而易受騙的使用者信以為真而提供機密資訊，例如：使用者名稱、密碼、信用卡號碼、社會保險號碼等等
缺少 CSP 或設定不適當的值，可能會導致 Web 應用程式遭受 XSS、點擊劫持等攻擊。
「Content-Security-Policy」標頭的目的在於修改瀏覽器呈現頁面的方式，進而預防各種跨網站注入攻擊，包括跨網站 跨網站指令碼。請務必設定正確的標頭值，避免網站運作不良。例如，如果將標頭設定為禁止執行行內 JavaScript，網站就不能在頁面中使用行內 JavaScript。
為了抵禦跨網站指令碼、跨框架 Scripting 及點擊劫持，請務必設定以下原則並提供適當的值：
「default-src」和「frame-ancestors」原則兩者，*或*「script-src」、「object-src」及「frame-ancestors」原則三者。
對於「default-src」、「script-src」及「object-src」，請避免「*」、「data:」、「unsafe-inline」或「unsafe-eval」這類不安全的值。
對於「frame-ancestors」，請避免「*」或「data:」這類不安全的值。
此外，對於「script-src」和「default-src」（「script-src」的後援指引），一般認為「self」是不安全的，應避免使用。
如需詳細資訊，請參考以下鏈結。
請注意，「Content-Security-Policy」包含四個不同的測試。有個一般測試會驗證「Content-Security-Policy」標頭是否正在使用中，其他三個測試會檢查「Frame-Ancestors」、「Object-Src」和「Script-Src」是否正確設定。

受影響的產品：

此問題可能會影響不同類型的產品

修正建議：

一般

設定您的伺服器以傳送「Content-Security-Policy」標頭。
建議您將 Content-Security-Policy 標頭設定為其指引的安全值，如下所示：
對於「default-src」和「script-src」，安全值包括「none」或 https://any.example.com。
對於「frame-ancestors」和「object-src」，預期的安全值包括「self」、「none」或 https://any.example.com 等。
「unsafe-inline」和「unsafe-eval」絕不能使用。使用暫時 / 雜湊只能是短期替代方案。
若為 Apache 伺服器，請參閱：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
若為 IIS 伺服器，請參閱：
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
若為 nginx 伺服器，請參閱：
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE：

1032
79
693
830
1021

外部參照：

幾個安全的標頭清單
「內容安全原則 (Content Security Policy)」的簡介
MDN web docs - Content-Security-Policy

遺漏或不安全的 HTTP Strict-Transport-Security 標頭

目錄

原因：

不安全的 Web 應用程式設計或配置

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
HTTP Strict Transport Security (HSTS) 這個機制可保護安全的 (HTTPS) 網站不被降級到不安全的 HTTP。這個機制可以讓 Web 伺服器指示用戶端（Web 瀏覽器或其他使用者代理程式）在與伺服器互動時使用安全的 HTTPS 連線，並且永不使用不安全的 HTTP 通訊協定。
請務必將 'max-age' 設為夠高的值，以防止提前切換回不安全的連線。
HTTP Strict Transport Security 原則是由伺服器使用名為 "Strict-Transport-Security" 的回應標頭來與其用戶端通訊。此標頭的值是用戶端應該僅在 HTTPS 存取伺服器的時間。其他標頭屬性包含 "includeSubDomains" 和 "preload"。

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

藉由將 "Strict-Transport-Security" 回應標頭新增至 Web 應用程式回應，來實作 HTTP Strict Transport Security 原則。
如需相關資訊，請參閱
https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

CWE：

200
693

外部參照：

OWASP "HTTP Strict Transport Security"
HSTS 規格

遺漏「查閱者原則」安全標頭

目錄

原因：

不安全的 Web 應用程式程式設計或設定

風險：

有可能收集有關 Web 應用程式的機密資訊，例如使用者名稱、密碼、機器名稱和/或機密檔案位置
有可能說服天真的使用者提供機密資訊，例如使用者名稱、密碼、信用卡號碼、社會安全碼等等
查閱者原則的值缺少或不適當可能會導致 URL 洩漏，即使是 URL 中所含的機密資訊，都會向跨網站洩漏。
這是一部分的規則集，可檢查是否設有查閱者原則，若有的話可以測試其設定。「查閱者原則」標頭會在查閱者標頭中定義可提供的資料，並且在目的地的 (document.referrer) 定義導覽和 iframe。此標頭的設計是為了要修改瀏覽器呈現頁面的方式，藉此避免跨網域的查閱者洩漏。正確設定標頭值很重要，設定方式不要妨礙網站的正常運作。
查閱者標頭是一個要求標頭，可表示流量來自哪個網站。如果沒有設有適當的防護，URL 本身，甚至是包含在 URL 中的機密資訊，都會向跨網站洩漏。
「no-referrer-when-downgrade」和「unsafe-url」是會洩露第三方網站完整 URL 的原則。剩餘的原則為「no-referrer」、「origin」、「origin-when-cross-origin」、「same-origin」、「strict-origin」、「strict-origin-when-cross-origin」。
詳情請參閱下方連結。

受影響的產品：

此問題可能會影響不同類型的產品

修正建議：

一般

設定伺服器以傳送「查閱者原則」標頭。
建議透過查閱者原則標頭的目錄安全值，設定查閱者原則標頭。如下所示：
"strict-origin-when-cross-origin" 提供更高的隱私權。有了此原則，只有來源會在跨來源要求的查閱者標頭中傳送。
如果是 Google Chrome，請參閱：
https://developers.google.com/web/updates/2020/07/referrer-policy-new-chrome-default
如果是 Firefox，請參閱：
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy.

CWE：

200
664
668

外部參照：

MDN web 文件 - 查閱者原則