



臺灣大學網站弱點掃描報告

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 10.12.0
掃描開始時間：2026/9/10 下午2:32:14

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

依問題類型分組的問題

- 發現不存在網域的鏈結 ^❶
- SameSite 屬性不安全、不適當或遺漏的 Cookie ^❷
- 加密的階段作業 (SSL) Cookie 中遺漏安全屬性 ^❶

如何修正

- 發現不存在網域的鏈結
- SameSite 屬性不安全、不適當或遺漏的 Cookie
- 加密的階段作業 (SSL) Cookie 中遺漏安全屬性

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。

高嚴重性問題：1
中嚴重性問題：3
報告中併入的安全問題總計：4
掃描中探索到的安全問題總計：114

一般資訊

掃描檔名：網站弱點掃描_NTU-秘書室-校友中心_臺大校友中心官網_115-9-10
掃描開始時間：2026/9/10 下午2:32:14
測試原則：Default (已修改)
CVSS 版本：3.1
測試最佳化等級：快速

主機：www.alumni.ntu.edu.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：已停用
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 3

目錄

問題類型		問題數目
高	發現不存在網域的鏈結	1
中	SameSite 屬性不安全、不適當或遺漏的 Cookie	2
中	加密的階段作業 (SSL) Cookie 中遺漏安全屬性	1

有漏洞的 URL 2

目錄

URL		問題數目
高	https://www.alumni.ntu.edu.tw/AlumniReunion	1
中	https://www.alumni.ntu.edu.tw/	3

修正建議 3

目錄

補救作業		問題數目
高	請從網站移除不存在的網域	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	2

安全風險 3

目錄

風險		問題數目
高	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	1
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	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

原因 3

目錄

原因	問題數目
----	------

高	Web 應用程式包含不存在網域的鏈結	1	
中	SameSite 屬性不適當、不安全或遺漏的機密 Cookie	2	
中	Web 應用程式會透過 SSL 傳送未受保護的 Cookie	1	

WASC 威脅分類 3

[目錄](#)

威脅		問題數目	
高	URL 重新導向程式不當使用	1	
中	伺服器配置錯誤	2	
中	資訊洩漏	1	

依問題類型分組的問題

發現不存在網域的鏈結	
嚴重性：	高
狀態：	待解決
CVSS 3.1 向量：	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N
CVSS 3.1 評分：	8.2
CVSS 4.0 向量：	AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:N/SI:N/SA:N/E:X
CVSS 4.0 評分：	8.8
URL：	https://www.alumni.ntu.edu.tw/AlumniReunion
實體：	https://ntu1981.org/ (Link)
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：	Web 應用程式包含不存在網域的鏈結
修正：	請從網站移除不存在的網域

差異：

推論：AppScan 發現外部網站的鏈結，但無法解析它

測試要求和回應：

```
GET /AlumniReunion HTTP/1.1
Host: www.alumni.ntu.edu.tw
Connection: keep-alive
sec-ch-ua: "Chromium";v="149", "Not)A;Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
HeadlessChrome/149.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://www.alumni.ntu.edu.tw/Store/StoreList
Accept-Language: en-US
Cookie:
.AspNetCore.Antiforgery.FHLYmWbUJH8=CfDJ8OqUIrBc5rlEsYuyQKbdUw48WUcnYXQU3KtcC_EgaWQB2YgAu0nbQ03wTLIXdIxkmU_dG
O1_TNxIbOK-JQKS0lBz2MlSF85tl7ezH7QsFNL-S4d___ojP9wqL7QFylHO-6AAFSQmzlhJ-J0ZCvRghOY;
_cap=970E00F05BFC7E8CE8DC7808D2C9A4EB;
.AspNetCore.Mvc.CookieTempDataProvider=CfDJ8OqUIrBc5rlEsYuyQKbdUw5eNMFCv7esC3_3ExQqDy0jim2dw18cZvuk2xbtohd0ZA
fFzkircsYtqWgJJM10juPg5OXMIG-R0WHc9tE2JV_mk1Er6SqlFrJTclj7YjfyRCoELV8mCBkcLaC1hM9DJXAAs-
```

8CZpYjc2YRLsPTLD9RN9I009sAmNJAhh-xBKqNuabR_g_KdgVqmWUY0nkyppxx45DxfvX9ncPm0fOwMMXk33aK46AU54VTpAgzgChUxbg;
TS01037fe6=01087174e2e7cb9563f4153bf378afcf0ea50e95f505ec26a1a37f725964e6839cf3629be4cb2e74159337ffd79e312da0
37e43d631f4df6eb1d3de7487b9e37388813ec5048c11240f760df87a8808ce50885e3103e19c70b210d3b4952b72cf35c91dcaa
Content-Length: 0

HTTP/1.1 200 OK
Date: Thu, 10 Sep 2026 06:55:23 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Cache-Control: no-cache, no-store
Pragma: no-cache
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=2592000
Strict-Transport-Security: max-age=16070400; includeSubDomains
Cross-Origin-Embedder-Policy: credentialless
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(self), microphone=(), camera=()
X-XSS-Protection: 1; mode=block
Transfer-Encoding: chunked
Set-Cookie:
.AspNetCore.Mvc.CookieTempDataProvider=CfDJ80qUIrBc5rlEsYuyQKbdUw5iEq8fLCQKSLCEZWZ7Qwn2U2r3AUzLAZ2DfUpP_eaZ74
6hhL7AmlQ9tZrWxKfbPXnnDkx27kilLN0MVri-XDS2nRuFOoGb6zZU4YYmoMS3rENEP7Gg-tb-
f8piSLYLt8mPRSNzFnHa_RfJctonOECKlXbXhB4vcJOwpKQDd9dhYJ3T_XwU7HA_TQJHu6uJiOVNfYR8DqBjgfd9naGdVjqIeuourNo207R4
ERs29WjOA; path=/; Secure; SameSite=Lax; secure; samesite=lax; httponly
Set-Cookie:
TS01037fe6=01087174e2679a70bd5fd6862d991f0ce6ec7b9e8b19c27dc06ec47e69034613c4b7e961f3855656ba435b5b8c9clac843
849bb7bf7172546f6ef0a192df61a8c4c6162d4a6b9aa9ebd96687381b0dd36b0e58305994822e687bb31d1868f2d6cfa1e5aa11;
Path=/; Secure; HttpOnly; ; SameSite=None

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>臺大校友中心</title>

  <link rel="shortcut icon" type="image/x-icon" href="/areas/frontend/img/favicon.png?v=jMZq0Bg-mI0-
hYkMrMafjrJkhmQ98xl66BPRLX0jkuA">

  <link href="/areas/frontend/css/bootstrap.min.css?v=djO3wMl9GeaC_u6K-ic4Uj_LKhRUSlUFcsruzS7v5ms"
rel="stylesheet">
  <link href="/areas/fr
...
...
...
  <div class="accordion-item">
    <h2 class="accordion-header d-flex" id="headingOne_2022">
    <span class="acircle d-none d-md-block"></span>
    <span class="accordionDate d-none d-md-block">12/04</span>
    <a href="https://ntu1981.org/" target="_blank" rel="noreferrer noopener" title="(另開視窗)前往校友重聚的
網站連結" class="notaccordion">
      NTU B66 四十重聚
    </a>
    <span class="text-center reunionfile text-center d-flex align-items-center">
    </span>
...
...
...
  <div class="accordion-item">
    <h2 class="accordion-header d-flex" id="headingOne_2022">
    <span class="acircle d-none d-md-block"></span>
    <span class="accordionDate d-none d-md-block">05/22</span>
    <a href="https://ntu1981.org/" target="_blank" rel="noreferrer noopener" title="(另開視窗)前往校友重聚的
網站連結" class="notaccordion">
      NTU B66 四十重聚 (活動延期)
    </a>
    <span class="text-center reunionfile text-center d-flex align-items-center">
```


...

問題 1 / 2

目錄

SameSite 屬性不安全、不適當或遺漏的 Cookie

嚴重性：	中
狀態：	待解決
CVSS 3.1 向量：	AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N/E:U/RL:O/RC:C
CVSS 3.1 評分：	4.7
CVSS 4.0 向量：	AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:U
CVSS 4.0 評分：	1.3
URL：	https://www.alumni.ntu.edu.tw/
實體：	TS01037fe6 (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
Host: www.alumni.ntu.edu.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)
HeadlessChrome/149.0.0.0 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
sec-ch-ua: "Chromium";v="149", "Not)A;Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Language: en-US
Content-Length: 0

HTTP/1.1 200 OK
Date: Thu, 10 Sep 2026 07:00:36 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Cache-Control: no-cache, no-store
Pragma: no-cache
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
```

```
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=2592000
Strict-Transport-Security: max-age=16070400; includeSubDomains
Cross-Origin-Embedder-Policy: credentialless
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(self), microphone=(), camera=()
X-XSS-Protection: 1; mode=block
Transfer-Encoding: chunked
Set-Cookie:
.AspNetCore.Antiforgery.FHLYmWbUJH8=CfDJ80_wnXzCkStCuaIYoQAazEttdiy1lKhfoBxY7HEzu_Km0HLpJGHFPBLSyA6fVevNR0W3zH
WV18GRHgT-_7ho1F4z0BA9zS0-bVbrLw5CzcfLxrBy6ztQT1MFAzGaTU96AFhGQCv_gv-sFdFpLQ1j78A; path=/; Secure;
SameSite=Lax; secure; samesite=strict; httponly
Set-Cookie: .AspNetCore.Mvc.CookieTempDataProvider=; expires=Thu, 01 Jan 1970 00:00:00 GMT; path=/; Secure;
SameSite=Lax; secure; samesite=lax; httponly
Set-Cookie:
TS01037fe6=01087174e21da2dc84c92e7b5c744c3e02c7de207f473d9d3e43fdcbe30bc62efbee0be48f73d80fbc9e91f8551b6499c4
c429e9502e9a96fd8fd890f2644a24a5563a1a66731ca3f009565cd269ffb45aa600d5f3; Path=/; Secure; HttpOnly; ;
SameSite=None

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>臺大校友中心</title>

  <link rel="shortcut icon" type="image/x-icon" href="/areas/frontend/img/favicon.png?v=jMZq0Bg-mI0-
hYkMrMafjrJkhmQ98xl66BPRIx0jkuA">

  <link href="/areas/frontend/css/bootstrap.min.css?v=djO3wMl9GaeC_u6K-ic4Uj_LKhRUSlUFcsruzS7v5ms"
rel="stylesheet">
  <link href="/areas/frontend/fontawesome/css/all.css?v=8VXAaVxwnr35ta3m9zUWVyof2grVOiV3zWfCcwm107g"
rel="stylesheet">

  <link href="/areas/frontend/css/carousel.css?v=but07HzWroNJ74UBEIyz47bS7J3hHBjngJ7piCab0Uc"
rel="stylesheet">
  <link href="/areas/frontend/css/style.css?v=rduzr26RSWGUYEZRynaJjIrbBpE69qFPR1SdNyMelp0"
rel="stylesheet">

  <link href="/areas/frontend/css/animate.min.css?v=rDt4caIH9N3t5HmDH1WroMQQPnj58v2EfrWR1F4aRmY"
rel="stylesheet">

  <link href="/lib/Parsley/v2.9.2/dist/parsley.css?v=qYCT6My33sawnvLU35_jTZNJfkazZnUyTxK3WxR9gbQ"
rel="stylesheet" />

  <link href="/lib/daterangepicker/v3.1/daterangepicker.css?v=9e9MfmRHWQmp4yMV-R9cxXU6-ZjzB2x-YcE4Z1Kmuag"
rel="stylesheet" />

  <!-- fileupload -->
  <link href="/lib/bootstrap-fileinput/v5.2.7/css/fileinput.min.css" rel="stylesheet" />
  <link rel="stylesheet" href="/css/bootstrap-icons.min.css">
  <link href="/lib/cdnjs/select2/v3.5.0/select2.min.css" rel="stylesheet" />

  <!-- toastr -->
  <link href="/lib/toastr/dist/toastr.min.css" rel="stylesheet">

  <link href="/areas/frontend/css/custom.css?v=SZ5svTjY6S-Zr3S7ubULGMAEcK18ek7dEOZBzLjfiQ"
rel="stylesheet" />

</head>
<body>
  <a id="gotopbutton"></a>

  <div class="Cta-btn">
    <a href="#" onclick="ShowLoginModal()">
      
      <p>校友登入</p>
    </a>

    <a href="/AlumniCard">
```

```

        
        <p>校友證</p>
    </a>
</div>

<header id="myHeader">
    <div class="small-header d-none d-lg-block" id="small-header">
        <div class="container">
            <div class="row justify-content-between align-items-center">
                <div class="col-3">
                    <form action="/SiteSearch" autocomplete="off" class="d-flex searchBar" method="post" onsubmit="return
                    checkData()">
                        <input type="text" id="Search_keyword" name="Search.Keyword" class="form-control bg-
                        gray" placeholder="全站搜尋" title="輸入關鍵字搜尋">
                        <button type="submit" class="btn btn-tgreen"><i class="fa-solid fa-magnifying-glass"></i></button>
                    <input name="__X-XSRFVerificationToken" type="hidden" value="CfDJ8O_wnXzCkStCuaIYoQAazEsAFdoN_Lqlte-
                    jvirIcn8hF7hs9wpsWfMteF-5C4S12MQYJpVVdDJifgSyCL_NGyGNb-
                    G6kZItxxbYn70EIgrTb60G1Tcxqp46f60sdkvdzXzan3q09aTdlyNqyoMP-fk" /></form>
                    <div class=
                </div>
            </div>
        </div>
    </div>
    ...
    ...
    ...

```

問題 2 / 2

目錄

SameSite 屬性不安全、不適當或遺漏的 Cookie

嚴重性：	中
狀態：	待解決
CVSS 3.1 向量：	AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N/E:U/RL:O/RC:C
CVSS 3.1 評分：	4.7
CVSS 4.0 向量：	AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:U
CVSS 4.0 評分：	1.3
URL：	https://www.alumni.ntu.edu.tw/
實體：	TSb5eff440027 (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 /News/NewsDetail/NN00000324 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://www.alumni.ntu.edu.tw/
Host: www.alumni.ntu.edu.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
Cookie:
.AspNetCore.Antiforgery.FHLYmWbUJH8=CfDJ8OqUIrBc5rlEsYuyQKbdUw48WUcnYXQU3KtcC_EgaWQB2YgAu0nbQ03wTLIXdIxkmU_dG
O1_TNxIbOK-JQKS01Bz2M1SF85t17ezH7QsFNL-S4d_ojP9wqL7QFylHO-6AAFSQmzlhJ-J0ZCvRghOY;
TS01037fe6=01087174e232bd9671d7dfaad56996bf0e22ccc87405ec26a1a37f725964e6839cf3629be4cb2e74159337ffd79e312da0
37e43d631f4df6eb1d3de7487b9e37388813ec5003167ada538ee93bcc55d8298b5d0fa1
Content-Length: 0

```

```
HTTP/1.1 200 OK
Date: Thu, 10 Sep 2026 07:00:36 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Cache-Control: no-cache, no-store
Pragma: no-cache
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=2592000
Strict-Transport-Security: max-age=16070400; includeSubDomains
Cross-Origin-Embedder-Policy: credentialless
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(self), microphone=(), camera=()
X-XSS-Protection: 1; mode=block
Transfer-Encoding: chunked
Set-Cookie:
.AspNetCore.Antiforgery.FHLYmWbUJH8=CfDJ8O_wnXzCkStCuaIYoQAazEsvG_YtIwJ20WFWc45K_qkYqdQgHBvaKHiVDk-
2XuAO0r0WLLhwxGJNzbwgDupjXzSRE8DmIGQXTHeg8sE4xE0KU4EtIBFg8YLV0ynlc1P7ohmdy8aD5Em4uiX_fyDgLKI; path=/; Secure;
SameSite=Lax; secure; samesite=strict; httponly
Set-Cookie: .AspNetCore.Mvc.CookieTempDataProvider=; expires=Thu, 01 Jan 1970 00:00:00 GMT; path=/; Secure;
SameSite=Lax; secure; samesite=lax; httponly
Set-Cookie:
TS01037fe6=01087174e2e07272e7106bf85bda185f30d686bc00657ac2adf561125beea54c8c17ea1476703937fcc58bf77ac350a4f2
94000075f9dbf5efa7ed9505cf9fcb3725aadfaf2f8556c3914adb7788e47e6c5dad83b8; Path=/; Secure; HttpOnly; ;
SameSite=None
Set-Cookie:
TSb5eff440027=0822b7c44eab20004861de714a411857ed22a3bd37a907582759c2b6cb00957cc47dacda7385fff408ce94eade11300
09c534567e6c5626f0eca50c3023cffe7c8752bcad77e84b047298ddc4d8c0415a46c2cd8868d5c90c905b71cebd2a0e1; Path=/

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>臺大校友中心</title>

  <link rel="shortcut icon" type="image/x-icon" href="/areas/frontend/img/favicon.png?v=jMZq0Bg-mI0-
hYkMrMafjrJkhmQ98xl66BPRIx0jkuA">

  <link href="/areas/frontend/css/bootstrap.min.css?v=djO3wMl9GeaC_u6K-ic4Uj_LKhRUSlUFcsruzS7v5ms"
rel="stylesheet">
  <link href="/areas/frontend/fontawesome/css/all.css?v=8VXAaVxwnr35ta3m9zUWVyof2grVOiV3zWfCcwm107g"
rel="stylesheet">

  <link href="/areas/frontend/css/carousel.css?v=but07HzWroNJ74UBEIyz47bS7J3hHBjngJ7piCab0Uc"
rel="stylesheet">
  <link href="/areas/frontend/css/style.css?v=rduzr26RSWGYUEZRynaJjIrbBpE69qFPR1SdNyMelp0"
rel="stylesheet">

  <link href="/areas/frontend/css/animate.min.css?v=rDt4caIH9N3t5HmDH1WroMQQPnj58v2EfrWR1F4aRmY"
rel="stylesheet">

  <link href="/lib/Parsley/v2.9.2/dist/parsley.css?v=qYCT6My33sawnvLU35_jTZNJfkazZnUyTxK3WxR9gbQ"
rel="stylesheet" />

  <link href="/lib/daterangepicker/v3.1/daterangepicker.css?v=9e9MfmRHWQmp4yMV-R9cxXU6-ZjzB2x-YcE4Z1Kmuag"
rel="stylesheet" />

  <!-- fileupload -->
  <link href="/lib/bootstrap-fileinput/v5.2.7/css/fileinput.min.css" rel="stylesheet" />
  <link rel="stylesheet" href="/css/bootstrap-icons.min.css">
  <link href="/lib/cdnjs/select2/v3.5.0/select2.min.css" rel="stylesheet" />

  <!-- toastr -->
  <link href="/lib/toastr/dist/toastr.min.css" rel="stylesheet">

  <link href="/areas/frontend/css/custom.css?v=SZ5svTjY6S-Zr3S7ubULGMAEcK18ek7dEOZBzLjf_iQ">
```

```

rel="stylesheet" />

</head>
<body>
  <a id="gotopbutton"></a>

  <div class="Cta-btn">
    <a href="#" onclick="ShowLoginModal()">
      
      <p>校友登入</p>
    </a>

    <a href="/AlumniCard">
      
      <p>校友證</p>
    </a>
  </div>

  <header id="myHeader">
    <div class="small-header d-none d-lg-block" id="small-header">
      <div class="container">
        <div class="row justify-content-between align-items-center">
          <div class="col-3">
            <form action="/SiteSearch" autocomplete="off" class="d-flex searchBar" method="post" onsubmit="return
            checkData()">
              <input type="text" id="Search_keyword" name="Search.Keyword" class="form-control bg-
              gray" placeholder="全站搜尋" title="輸入關鍵字搜尋">
              <button type="submit" class="btn b
            ...
            ...
            ...

```

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
狀態：	待解決
CVSS 3.1 向量：	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS 3.1 評分：	6.5
CVSS 4.0 向量：	AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:X
CVSS 4.0 評分：	6.9
URL：	https://www.alumni.ntu.edu.tw/
實體：	TSb5eff440027 (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 /News/NewsDetail/NN00000324 HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://www.alumni.ntu.edu.tw/
Host: www.alumni.ntu.edu.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
Cookie:
.AspNetCore.Antiforgery.FHLYmWbUJH8=CfDJ80qUIrBc5r1EsYuyQKbdUw48WUcnYXQU3KtcC_EgaWQB2YgAu0nbQ03wTLIXdIxkmU_dG
01_TNxIbOK-JQKS01Bz2M1SF85t17ezH7QsFNL-S4d____ojP9wqL7QFylHO-6AAFSQmzlhJ-J0ZCvRghOY;
TS01037fe6=01087174e232bd9671d7dfaad56996bf0e22ccc87405ec26a1a37f725964e6839cf3629be4cb2e74159337ffd79e312da0
37e43d631f4df6eb1d3de7487b9e37388813ec5003167ada538ee93bcc55d8298b5d0fa1
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 10 Sep 2026 07:00:36 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Cache-Control: no-cache, no-store
Pragma: no-cache
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=2592000
Strict-Transport-Security: max-age=16070400; includeSubDomains
Cross-Origin-Embedder-Policy: credentialless
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(self), microphone=(), camera=()
X-XSS-Protection: 1; mode=block
Transfer-Encoding: chunked
Set-Cookie:
.AspNetCore.Antiforgery.FHLYmWbUJH8=CfDJ80_wnXzCkStCuaIYoQAazEtflX9c7jPX3Y7Kzem5oRQ1WmIGRkSGODamnp5x2CttxpUZDE
whZLFroA3aqP3Ap28ThoG6kwwVMY8N8MZx2rxliPZMmlgX2INctyqjsPjY2M99yH40E_Hk0JmngfVvk21IQ; path=/; Secure;
SameSite=Lax; secure; samesite=strict; httponly
Set-Cookie: .AspNetCore.Mvc.CookieTempDataProvider=; expires=Thu, 01 Jan 1970 00:00:00 GMT; path=/; Secure;
SameSite=Lax; secure; samesite=lax; httponly
Set-Cookie:
TS01037fe6=01087174e21b7fcf04247ff2c35ffadb837aae1ea88a0d51529a8fa00b3affdbfd8a6af71fa0ca5cc579012e23946c03ef
c442349d528cc8519d0ad1564d699a4bd6bd6e801b7fdb253a08e9323d758427272130d3; Path=/; Secure; HttpOnly; ;
SameSite=None
Set-Cookie:
TSb5efff440027=0822b7c44eab200041f579c99fdd296ae2d09fb04074287b9392ef7a9f24854889683129def88340087c6a576c11300
0a422517bd04ea3fc0eca50c3023cffe7c6025235b1ce821b3f3772524e96b0515d0b756758295b6f241da0891dfb45e5; Path=/
```

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>臺大校友中心</title>

  <link rel="shortcut icon" type="image/x-icon" href="/areas/frontend/img/favicon.png?v=jMZq0Bg-mI0-
hYkMrMafjrJkhmQ98xl66BPRLX0jkuA">

  <link href="/areas/frontend/css/bootstrap.min.css?v=djO3wMl9GeaC_u6K-ic4Uj_LKhRUSlUFcsruzS7v5ms"
rel="stylesheet">
  <link href="/areas/frontend/fontawesome/css/all.css?v=8VXAaVxwnr35ta3m9zUWVyof2grVOiV3zWfCcwm107g"
rel="stylesheet">

  <link href="/areas/frontend/css/carousel.css?v=but07HzWroNJ74UBEIyz47bS7J3hHBjngJ7piCab0Uc"
rel="stylesheet">
  <link href="/areas/frontend/css/style.css?v=rduzr26RSWGYUEZRynaJjIrbBpE69qFPR1SdNyMelp0"
rel="stylesheet">

  <link href="/areas/frontend/css/animate.min.css?v=rDt4caIH9N3t5HmDH1WroMQQPnj58v2EfrWR1F4aRmY"
rel="stylesheet">

  <link href="/lib/Parsley/v2.9.2/dist/parsley.css?v=qYCT6My33sawnvLU35_jTZNJfkazZnUyTxK3WxR9gbQ"
rel="stylesheet" />
```

```

<link href="/lib/daterangepicker/v3.1/daterangepicker.css?v=9e9MfmRHWQmp4yMV-R9cxXU6-ZjzB2x-YcE4Z1Kmuag"
rel="stylesheet" />

<!-- fileupload -->
<link href="/lib/bootstrap-fileinput/v5.2.7/css/fileinput.min.css" rel="stylesheet" />
<link rel="stylesheet" href="/css/bootstrap-icons.min.css">
<link href="/lib/cdnjs/select2/v3.5.0/select2.min.css" rel="stylesheet" />

<!-- toastr -->
<link href="/lib/toastr/dist/toastr.min.css" rel="stylesheet">

<link href="/areas/frontend/css/custom.css?v=SZ5svTjY6S-Zr3S7ubULGMAEcK18ek7dEOZBzLjf_iQ"
rel="stylesheet" />

</head>
<body>
  <a id="gotopbutton"></a>

  <div class="Cta-btn">
    <a href="#" onclick="ShowLoginModal()">
      
      <p>校友登入</p>
    </a>

    <a href="/AlumniCard">
      
      <p>校友證</p>
    </a>
  </div>

  <header id="myHeader">
    <div class="small-header d-none d-lg-block" id="small-header">
      <div class="container">
        <div class="row justify-content-between align-items-center">
          <div class="col-3">
            <form action="/SiteSearch" autocomplete="off" class="d-flex searchBar" method="post" onsubmit="return
            checkData()">
              <input type="text" id="Search_keyword" name="Search.Keyword" class="form-control bg-
              gray" placeholder="全站搜尋" title="輸入關鍵字搜尋">
              <button type="submit" class="btn b
            ...
            ...
            ...

```

如何修正

發現不存在網域的鏈結

目錄

原因：

Web 應用程式包含不存在網域的鏈結

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、社會保險號碼等等網站包含不存在網域的鏈結。

攻擊者可以運用這個情境來登錄此不存在的網域，以啟動網路釣魚攻擊。

無經驗而易受騙的使用者可能會瀏覽至該鏈結，以為其位於原始網站內，但事實上是在瀏覽攻擊者網站。

這個狀況可能會導致機密性資訊洩漏，因為使用者信任該惡意網站。

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

建議您移除所有不存在網域的鏈結。此外，請定期檢查外部網站鏈結的有效性。

CWE：

601

610

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

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認證之類的資訊都可能被竊，稍後可用來盜用身分或使用模擬。

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

外部参照：

Financial Privacy: The Gramm-Leach Bliley Act

Health Insurance Portability and Accountability Act (HIPAA)

Sarbanes-Oxley Act

California SB1386