Web Application Report

This report includes important security information about your web application.

安全報告

這份報告是由 HCL AppScan Standard 所建立 10.6.0
掃描開始時間： 2024/10/21 上午2:24:32

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

如何修正

- SameSite 屬性不安全、不適當或遺漏的 Cookie

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
報告中併入的安全問題總計：	1
掃描中探索到的安全問題總計：	4

一般資訊

掃描檔名：	3_Note
掃描開始時間：	2024/10/21 上午2:24:32
測試原則：	Default
CVSS 版本：	3.1
測試最佳化等級：	快速
主機	notesweb.tyc.com.tw
埠	80
作業系統：	不明
Web 伺服器：	Lotus-Domino
應用程式伺服器：	任何

登入設定值

登入方法： 無

摘要

問題類型 1

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

有漏洞的 URL 1

目錄

	URL	問題數目
中	http://notesweb.tyc.com.tw/	1

修正建議 1

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	1

安全風險 1

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

原因 1

目錄

	原因	問題數目

WASC 威脅分類

目錄

威脅	問題數目
伺服器配置錯誤	1

依問題類型排列的問題

中 SameSite 屬性不安全、不適當或遺漏的 Cookie 1 目錄

問題 1 / 1 目錄

SameSite 屬性不安全、不適當或遺漏的 Cookie

嚴重性：	中
CVSS 評分：	4.7
CVSS 向量：	AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N/E:U/RL:O/RC:C/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL：	http://notesweb.tyc.com.tw/
實體：	SessionID (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 /public/scm.nsf HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: notesweb.tyc.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: Lotus-Domino
Date: Sun, 20 Oct 2024 18:27:28 GMT
Content-Type: text/html;charset=UTF-8
Expires: -1
Content-Length: 8095
Set-Cookie: SessionID=H11DTY60QW; path=/

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html lang="en">
<head>
<script
type="text/javascript">if(!navigator.cookieEnabled)window.location.href='http://notesweb.tyc.com.tw/public/scm.nsf/index.xs
p?SessionID=H11DTY60QW';</script>
```

```
<title>TYC&#21332;&#21516;&#20316;&#26989;&#20837;&#21475;&#32178;</title>
<link rel="stylesheet" type="text/css"
href="/xsp/.ibmxspres/.mini/css/2Ojcore.css&amp;2Ojdojo.css&amp;2OldefaultTheme.css&amp;2OldojoTheme.css&amp;@Da&amp;@Ib&amp;@Th&amp;@Ti&amp;2TgxspSF.css.css">
<script type="text/javascript" src="/xsp/.ibmxspres/dojoroot-1.6.1/dojo/dojo.js" djConfig="locale: 'en-us'"></script>
<script type="text/javascript" src="/xsp/.ibmxspres/.mini/dojo/.en-us/@Iq.js"></script>
</head>
<body class="xsp lotusui tundra">
<form id="view:_id1" method="post" action="/public/scm.nsf/index.xsp" class="lotusForm" enctype="multipart/form-data">
<table style="width:100%"><tr><td style="width:70%"><a id="view:_id1:_id2:link1" href="http://www.tyc.com.tw"
class="xspLink"><img id="view:_id1:_id2:image1" src="/public/scm.nsf/tyclogo.gif" alt="" class="xspImage"></a> <span
id="view:_id1:_id2:label1" style="font-family:&#33775;&#24247;&#29305;&#31895;&#26999;&#39636;;font-
size:24pt;color:rgb(0,64,128);padding-top:10.0px;width:203.0px"
class="xspTextLabel">&#21332;&#21516;&#20316;&#26989;&#24179;&#21488;</span> <span id="view:_id1:_id2:computedField2"
style="font-family:&#26032;&#32048;&#26126;&#39636;;font-size:12pt;color:rgb(128,0,128);font-weight:bold"
class="xspTextComputedField"></span></td>
<td style="width:50.0%"><br>
<span id="view:_id1:_id2:computedField1" style="font-family:&#26032;&#32048;&#26126;&#39636;;font-size:11pt;font-
weight:bold;color:rgb(0,0,255)" class="xspTextComputedField"></span></td>
</tr>
</table>
<div class="lotusFrame" id="view:_id1:_id2:applicationLayout1">
<div class="lotusBanner" role="banner">
<div class="lotusRightCorner">
<div class="lotusInner">
<a href="#lotusMainContent" accesskey="S" class="lotusAccess"><img src="/oneuiv2.1/images/blank.gif" alt="Skip to main
content link. Accesskey S"></a><span style="float:left;vertical-align:middle;margin-right: 5px;"></span>

<ul id="view:_id1:_id2:applicationLayout1_al" style="float: left" class="lotusInlinelist lotusLinks">
<li style="font-family:&#26032;&#32048;&#26126;&#39636;;font-size:12pt;font-weight:bold" class="lotusFirst lotusFirst"><a
href="/public/scm.nsf/?opendatabase&amp;login" style="text-decoration:none">&#30331;&#20837;Login</a></li>
<li style="font-family:&#26032;&#32048;&#26126;&#39636;;font-size:12pt"><a
href="http://notesweb.tyc.com.tw/public/scm.nsf/xpg03.xsp" style="text-decoration:none">&#24536;&#35352;&#23494;&#30908;
(Forgot Password)</a></li>
<li style="font-family:&#26032;&#32048;&#26126;&#39636;;font-size:12pt"><a
href="http://notesweb.tyc.com.tw/public/scm_acl.nsf/xpg01.xsp" style="text-
decoration:none">&#24115;&#34399;&#30003;&#35531;</a></li>
</ul>

</div>
</div>
</div>
<div class="lotusMain">
<a id="lotusMainContent" name="lotusMainContent"></a><div class="lotusContent" role="main"><div
id="view:_id1:_id2:facetMiddle">
<div style="height:500.0px">
<table id="view:_id1:_id2:facetMiddle:viewPanel1_OUTER_TABLE" cellspacing="0" cellpadding="0" style="width:100%;border-
color:rgb(192,192,192);border-style:solid;border-width:thin" class="xspDataTableViewPanel">
<tr>

<td class="xspDataTableViewPanelHeaderStart">
 
</td><td class="xspDataTableViewPanelHeaderMiddle"><table style="width:100%; height:100%;"><tr><td style="white-
space:nowrap"><span style="xspPagerContainer"><span style="xspPagerLeft"><span
id="view:_id1:_id2:facetMiddle:viewPanel1:viewTitle1" style="font-family:&#26032;&#32048;&#26126;&#39636;;font-
size:12pt;font-weight:bold" class="xspTextViewTitle">&#9678; &#31995;&#32113;&#20844;&#21578;</span></span></span></td><td
style="white-space:nowrap"><div class="xspPagerContainer"><div class="xspPagerRight"
id="view:_id1:_id2:facetMiddle:viewPanel1:pager1"><span class="xspPagerNav"
id="view:_id1:_id2:facetMiddle:viewPanel1:pager1__FirstImage"><img src="/domjava/xsp/theme/common/images/PagerArrowhead2-
L_d.png" alt=""></span><span class="xspPagerNav" id="view:_id1:_id2:facetMiddle:viewPanel1:pager1__PreviousImage"><img
src="/domjava/xsp/theme/common/images/PagerArrowhead-L_d.png" alt=""></span><span class="xspPagerNav">Page</span><span
class="xspPagerNav xspGroup" id="view:_id1:_id2:facetMiddle
...
...
...
```

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