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2:24:20

目錄

簡介

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

中嚴重性問題：	4
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：	23

一般資訊

掃描檔名：	1_webFTP
掃描開始時間：	2024/10/21 上午2:24:20
測試原則：	Default
CVSS 版本：	3.1
測試最佳化等級：	快速
主機	webftp.tyc.com.tw
埠	80
作業系統：	Win32
Web 伺服器：	IIS
應用程式伺服器：	ASP.NET

登入設定值

登入方法： 無

摘要

問題類型 4

目錄

	問題類型	問題數目
中	SameSite 屬性不安全、不適當或遺漏的 Cookie	1
中	啟用 TRACE 與 TRACK HTTP 方法	1
中	已啟用不安全的 "OPTIONS" HTTP 方法	1
中	有弱點的元件	3

有漏洞的 URL 1

目錄

	URL	問題數目
中	http://webftp.tyc.com.tw/	6

修正建議 4

目錄

	補救作業	問題數目
中	停用 WebDAV，或禁止不需要的 HTTP 方法	1
中	在 Web 伺服器中停用 HTTP TRACE 支援	1
中	將元件升級到最新穩定版本	1
中	檢閱將 SameSite Cookie 屬性配置為建議值的可能解決方案	1

安全風險 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。	1
中	有可能竊取或操作客戶階段作業和 Cookie，並可能用來假冒合法的使用者，讓駭客可以檢視或變更使用者記錄，以及用該使用者的身分來執行交易	1
中	有可能上傳、修改或刪除 Web 伺服器上的網頁、Script 和檔案	1
中	攻擊者有可能使用 Web 伺服器來攻擊其他網站，讓其身分更加隱密	1

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	1
中	使用不安全的方式配置 Web 伺服器或應用程式伺服器	2

	已使用不安全的方式配置 Web 伺服器或應用程式伺服器	0
	測試應用程式中使用了一個有弱點的元件。	0
中	未安裝協力廠商產品的最新修補程式或緊急修復程式	1

WASC 威脅分類

目錄

威脅	問題數目
內容盜用	1
伺服器配置錯誤	1
濫用功能	2

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://webftp.tyc.com.tw/
實體：	ASPSESSIONIDQQSAASBR (Cookie)
風險：	將 Cookie 限制為第一方或相同網站環境定義以預防 Cookie 資訊洩漏。如果沒有設置額外的保護措施（如反 CSRF 記號），攻擊者可以延伸為偽造跨網站要求 (CSRF) 攻擊。
原因：	SameSite 屬性不適當、不安全或遺漏的機密 Cookie
修正：	檢閱將 SameSite Cookie 屬性配置為建議值的可能解決方案

差異：

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

測試要求和回應：

```
GET / HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: webftp.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/1.1 302 Object moved
Server: Microsoft-IIS/5.0
Date: Sun, 20 Oct 2024 19:00:50 GMT
X-Powered-By: ASP.NET
Location: http://webftp.tyc.com.tw/gp02/frame.asp
Content-Length: 171
Content-Type: text/html
Cache-control: private
Set-Cookie: ASPSESSIONIDQQSAASBR=CCLDLNICLIGJIDBOGHJGIELJ; path=/

<head><title>Object moved</title></head>
<body><h1>Object Moved</h1>This object may be found <a HREF="http://webftp.tyc.com.tw/gp02/frame.asp"></a>找得到這個物件。
</body>
```

```
GET /gp02/frame.asp HTTP/1.1
Cookie: ASPSESSIONIDQQSAASBR=CCLDLNICLIGJIDBOGHJGIELJ
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://webftp.tyc.com.tw/
Host: webftp.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: Microsoft-IIS/5.0
Date: Sun, 20 Oct 2024 18:25:21 GMT
X-Powered-By: ASP.NET
Content-Length: 2182
Content-Type: text/html
Cache-control: private

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN" "http://www.w3.org/TR/html4/frameset.dtd">
<html>
<head>
<title>堤維西 WebFTP</title>
<meta http-equiv="Content-Type" content="text/html; charset=big5">
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>
<!-- 20230906 will add last mouse enter or leave datetime. -->
<script src="https://code.jquery.com/jquery-3.7.1.min.js" integrity="sha256-/JqT3SQfawRcv/BIHPThkBvs0OEvtFFmqPF/lYI/Cxo="
crossorigin="anonymous"></script>
<script>
 $(document).ready(function(){
         let temp = $("frame[name='topFrame']").contents().find("#active").val();
         $("frame").on("mouseleave", function(){
                 //console.log("leave");
                 if (window.XMLHttpRequest) { // IE7+, Firefox, Chrome, Opera, Safari
                         xhr = new XMLHttpRequest();
                 } else { // IE6, IE5
                         xhr = new ActiveXObject("Microsoft.XMLHTTP");
                        }
                 xhr.open("GET", "lastMouseLeave.asp?temp="+temp, true);
                 xhr.send();
         });
         $("frame").on("mouseenter", function(){
                 //console.log("enter");
                 if (window.XMLHttpRequest) { // IE7+, Firefox, Chrome, Opera, Safari
                         xhr = new XMLHttpRequest();
                 } else { // IE6, IE5
                         xhr = new ActiveXObject("Microsoft.XMLHTTP");
                        }
                 xhr.open("GET", "lastMouseEnter.asp?temp="+temp, true);
                 xhr.send();
         });
 });
</script>
</head>



<frameset rows="86,*" cols="*" framespacing="0" frameborder="NO" border="0">
  <frame src="top.asp" name="topFrame" scrolling="NO" noresize >
  <frameset rows="*" cols="180,*" framespacing="0" frameborder="NO" border="0">
    <frame src="left.asp" name="leftFrame" scrolling="no" noresize marginwidth="0" marginheight="0">
    <frame src="main.asp?lang=1&customer_id=169&name_id=1" name="mainFrame">
  </frameset>
</frameset>
<body>

</body>
</html>


GET /gp02/top.asp HTTP/1.1
Cookie: ASPSESSIONIDQQSAASBR=CCLDLNICLIGJIDBOGHJGIELJ
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://webftp.tyc.com.tw/gp02/frame.asp
```

```
Host: webftp.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: Microsoft-IIS/5.0
Date: Sun, 20 Oct 2024 18:25:21 GMT
X-Powered-By: ASP.NET
Content-Length: 1143
Content-Type: text/html
Cache-control: private

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>Untitled Document</title>
<meta http-equiv="Content-Type" content="text/html; charset=big5">

<script>
 function lastActive() {
         var xhr, temp = '';
         if (document.getElementById("active") !== null) {

                 temp = document.getElementById("active").value;
                 if (window.XMLHttpRequest) { // IE7+, Firefox, Chrome, Opera, Safari
                         xhr = new XMLHttpRequest();
                 } else { // IE6, IE5
                         xhr = new ActiveXObject("Microsoft.XMLHTTP");
                        }
                 xhr.open("GET", "lastActive.asp?temp="+temp, true);
                 xhr.send();

                 if (window.console && window.console.log) { //        避免在 IE9 以下的版本產生錯誤
                         console.log("check");
                        }
         }
        }
 var intervalID = setInterval(lastActive, 60000);
</script>
</head>

<body  leftmargin="0" topmargin="0" marginwidth="0" marginheight="0"
...
...
...
```

中 啟用 TRACE 與 TRACK HTTP 方法 1 目錄

問題 1 / 1 目錄

啟用 TRACE 與 TRACK HTTP 方法

嚴重性：	中
CVSS 評分：	5.3
CVSS 向量：	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL：	http://webftp.tyc.com.tw/
實體：	webftp.tyc.com.tw (Page)
風險：	有可能竊取或操作客戶階段作業和 Cookie，並可能用來假冒合法的使用者，讓駭客可以檢視或變更使用者記錄，以及用該使用者的身分來執行交易
原因：	使用不安全的方式配置 Web 伺服器或應用程式伺服器
修正：	在 Web 伺服器中停用 HTTP TRACE 支援

差異： **方法** 操作來源： `GET` 到： `TRACE`

推論： 回應的 HTTP 狀態 (200 OK) 或內容類型 (message/http) 以及回應正文中的測試回顯表示伺服器上啟用了 TRACE/TRACK 方法。

測試要求和回應：

```
TRACE / HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: webftp.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: Microsoft-IIS/5.0
Date: Sun, 20 Oct 2024 18:28:20 GMT
X-Powered-By: ASP.NET
Content-Type: message/http
Content-Length: 285

TRACE / HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: webftp.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
```

中 已啟用不安全的 "OPTIONS" HTTP 方法 1

目錄

問題 1 / 1

目錄

已啟用不安全的 "OPTIONS" HTTP 方法

嚴重性：	中
CVSS 評分：	5.3
CVSS 向量：	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL：	http://webftp.tyc.com.tw/
實體：	index.html (Page)
風險：	有可能上傳、修改或刪除 Web 伺服器上的網頁、Script 和檔案
原因：	使用不安全的方式配置 Web 伺服器或應用程式伺服器
修正：	停用 WebDAV，或禁止不需要的 HTTP 方法

差異： **路徑** 操作來源： `/` 到： `index.html`
方法 操作來源： `GET` 到： `OPTIONS`

推論： Allow 標頭顯示允許危險的「HTTP 選項」，表示伺服器已啟用 WebDAV。

測試要求和回應：

```
OPTIONS /index.html HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: webftp.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: Microsoft-IIS/5.0
Date: Sun, 20 Oct 2024 19:04:57 GMT
X-Powered-By: ASP.NET
MS-Author-Via: DAV
Content-Length: 0
Accept-Ranges: bytes
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, LOCK, UNLOCK
Cache-Control: private
```

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：	5.3
CVSS 向量：	AV:N/AC:L/PR:N/UI:N/S:U/C:N/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-2011-5279
URL：	http://webftp.tyc.com.tw/
實體：	IIS 5.0 (Component)
風險：	攻擊者有可能使用 Web 伺服器來攻擊其他網站，讓其身分更加隱密
原因：	未安裝協力廠商產品的最新修補程式或緊急修復程式
修正：	將元件升級到最新穩定版本

差異：

推論：

測試要求和回應：

```
GET / HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: webftp.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/1.1 302 Object moved
Server: Microsoft-IIS/5.0
Date: Sun, 20 Oct 2024 19:00:50 GMT
X-Powered-By: ASP.NET
Location: http://webftp.tyc.com.tw/gp02/frame.asp
Content-Length: 171
Content-Type: text/html
Cache-control: private
Set-Cookie: ASPSESSIONIDQQSAASBR=DCLDLNICJBKEAOKGOONJDKHK; path=/

<head><title>Object moved</title></head>
<body><h1>Object Moved</h1>This object may be found <a HREF="http://webftp.tyc.com.tw/gp02/frame.asp"></a>找得到這個物件。
</body>


GET /gp02/frame.asp HTTP/1.1
Cookie: ASPSESSIONIDQQSAASBR=DCLDLNICJBKEAOKGOONJDKHK
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://webftp.tyc.com.tw/
Host: webftp.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: Microsoft-IIS/5.0
Date: Sun, 20 Oct 2024 18:25:21 GMT
X-Powered-By: ASP.NET
Content-Length: 2182
Content-Type: text/html
Cache-control: private

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN" "http://www.w3.org/TR/html4/frameset.dtd">
<html>
<head>
<title>堤維西 WebFTP</title>
<meta http-equiv="Content-Type" content="text/html; charset=big5">
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
```

```
MM_reloadPage(true);
//-->
</script>
<!-- 20230906 will add last mouse enter or leave datetime. -->
<script src="https://code.jquery.com/jquery-3.7.1.min.js" integrity="sha256-/JqT3SQfawRcv/BIHPThkBvs0OEvtFFmqPF/lYI/Cxo="
crossorigin="anonymous"></script>
<script>
 $(document).ready(function(){
         let temp = $("frame[name='topFrame']").contents().find("#active").val();
         $("frame").on("mouseleave", function(){
                 //console.log("leave");
                 if (window.XMLHttpRequest) { // IE7+, Firefox, Chrome, Opera, Safari
                         xhr = new XMLHttpRequest();
                 } else { // IE6, IE5
                         xhr = new ActiveXObject("Microsoft.XMLHTTP");
                        }
                 xhr.open("GET", "lastMouseLeave.asp?temp="+temp, true);
                 xhr.send();
         });
         $("frame").on("mouseenter", function(){
                 //console.log("enter");
                 if (window.XMLHttpRequest) { // IE7+, Firefox, Chrome, Opera, Safari
                         xhr = new XMLHttpRequest();
                 } else { // IE6, IE5
                         xhr = new ActiveXObject("Microsoft.XMLHTTP");
                        }
                 xhr.open("GET", "lastMouseEnter.asp?temp="+temp, true);
                 xhr.send();
         });
 });
</script>
</head>



<frameset rows="86,*" cols="*" framespacing="0" frameborder="NO" border="0">
  <frame src="top.asp" name="topFrame" scrolling="NO" noresize >
  <frameset rows="*" cols="180,*" framespacing="0" frameborder="NO" border="0">
    <frame src="left.asp" name="leftFrame" scrolling="no" noresize marginwidth="0" marginheight="0">
    <frame src="main.asp?lang=1&customer_id=169&name_id=1" name="mainFrame">
  </frameset>
</frameset>
<body>

</body>
</html>


GET /gp02/top.asp HTTP/1.1
Cookie: ASPSESSIONIDQQSAASBR=DCLDLNICJBKEAOKGOONJDKHK
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://webftp.tyc.com.tw/gp02/frame.asp
Host: webftp.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: Microsoft-IIS/5.0
Date: Sun, 20 Oct 2024 18:25:21 GMT
X-Powered-By: ASP.NET
Content-Length: 1143
Content-Type: text/html
Cache-control: private

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>Untitled Document</title>
<meta http-equiv="Content-Type" content="text/html; charset=big5">

<script>
 function lastActive() {
         var xhr, temp = '';
         if (document.getElementById("active") !== null) {

                 temp = document.getElementById("active").value;
                 if (window.XMLHttpRequest) { // IE7+, Firefox, Chrome, Opera, Safari
                         xhr = new XMLHttpRequest();
                 } else { // IE6, IE5
                         xhr = new ActiveXObject("Microsoft.XMLHTTP");
                        }
                 xhr.open("GET", "lastActive.asp?temp="+temp, true);
```

```
                xhr.send();

                if (window.console && window.console.log) { //        避免在 IE9 以下的版本產生錯誤
                        console.log("check");
                       }
         }
        }
 var intervalID = setInterval(lastActive, 60000);
</script>
</head>

<body  leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">
<table width="100%" border="0" cellspacin
...
...
...
```

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

啟用 TRACE 與 TRACK HTTP 方法

目錄

原因：

使用不安全的方式配置 Web 伺服器或應用程式伺服器

風險：

有可能竊取或操作客戶階段作業和 Cookie，其可能用來假冒合法的使用者，讓駭客可以檢視或變更使用者記錄，以及以該使用者的身分來執行交易
RFC2616（第 9.8 節 - HTTP 'TRACE' 方法）：
「TRACE 方法用來呼叫要求訊息的遠端應用程式層迴圈。
要求的最終接受者應該以 200 (OK) 回應的實體主體向用戶端反映接回來的訊息...
TRACE 可讓用戶端查看要求鏈的另一端收到什麼，並將這項資料用於測試或診斷資訊...」如 RFC2616 所指定，完整的 HTTP 要求（包括 HTTP 標頭）是在 TACE 回應的主體中送回。
HTTP 標頭可包括階段作業記號、Cookie 或鑑別認證之類的機密性資訊。
由於 Script 程式碼可以透過 DOM（文件物件模型）介面來存取 TRACE 回應的主體，因此，攻擊者有可能濫用 Web 瀏覽器問題（跨網域問題）來讀取機密的標頭資訊，並略過 Microsoft Internet Explorer 6.0 SP1 所引進的 'HttpOnly' Cookie 屬性。

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

停用 Web 伺服器中的 HTTP TRACE 支援。
Apache Web Server 和 Microsoft IIS 可能的暫行解決方法如下：
- Apache HTTP Server：利用 Apache mod_rewrite 模組來拒絕 HTTP TRACE 要求，或只允許符合網站需求和原則的方法。
- Microsoft Internet Information Services (IIS)：利用 URLScan 工具來拒絕 HTTP TRACE 要求，或只允許符合網站需求和原則的方法。

CWE：

489
200

外部參照：

CERT 問題附註
XST 文章，來自 WhiteHat Security
RFC2616

已啟用不安全的 "OPTIONS" HTTP 方法

目錄

原因：

已使用不安全的方式配置 Web 伺服器或應用程式伺服器

風險：

有可能上傳、修改或刪除 Web 伺服器上的網頁、Script 和檔案
似乎 Web 伺服器配置成接受下列其中一個（或多個） HTTP 方法（動詞）：
- DELETE
- SEARCH
- COPY
- MOVE
- PROPFIND
- PROPPATCH
- MKCOL
- LOCK
- UNLOCK
- PUT

這些方法可能指出伺服器啟用了 WebDAV，並且可能會讓未獲授權的使用者加以不當運用。

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

如果伺服器不需要啟用 WebDAV，請務必停用它，或禁止不必要的 HTTP 方法（動詞）。

CWE：

749
200

外部參照：

WASC 威脅分類：內容盜用

有弱點的元件

目錄

原因：

測試應用程式中使用了一個有弱點的元件。

風險：

有弱點的元件可能導致應用程式出現各種弱點

修正建議：

一般

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

CWE：

1035

外部參照：

CERT 協調中心
常見弱點和暴露 (CVE)