

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

- SQL 注入 ❷
- 未加密的登入要求 ❸
- 查詢中的 Password 參數 ❶
- 不適當地封鎖帳戶 ❶
- 未更新階段作業 ID ❶
- 偽造跨網站要求 ❷
- 登入錯誤訊息認證列舉 ❶
- SameSite 屬性不安全、不適當或遺漏的 Cookie ❶
- 未停用密碼欄位的自動完成 HTML 屬性 ❷
- 在階段作業 Cookie 中遺漏 HttpOnly 屬性 ❶
- 找到資料庫錯誤型樣 ❸
- 偵測到隱藏目錄 ❶
- 遺漏「Content-Security-Policy」標頭 ❶
- 遺漏或不安全的 "X-Content-Type-Options" 標頭 ❶
- 遺漏或不安全的 "X-XSS-Protection" 標頭 ❶
- 遺漏或不安全的跨頁框 Scripting 防禦 ❶
- 應用程式中找到不必要的 HTTP 回應標頭 ❶
- 檢查是否有 SRI（子資源完整性）支援 ❹
- 找到可能的伺服器路徑揭露型樣 ❶
- 遺漏「查閱者原則」安全標頭 ❶
- 應用程式錯誤 ❶

修正建議

- 傳送機密性資訊時，一律使用 **SSL** 和 **POST**（主體）參數。
- 檢查危險字元注入可能的解決方案
- 在數次登入嘗試失敗之後，強制封鎖帳戶
- 登入後變更階段作業 ID 值
- 對每一個錯誤的登入嘗試發出相同的錯誤訊息
- 請驗證 **"Referer"** 標頭的值，並對每一個提交的表單使用 **one-time-nonce**
- 正確設定 **"autocomplete"** 屬性為 **"off"**
- 配置伺服器利用 **"nosniff"** 值使用 **"X-Content-Type-Options"** 標頭
- 配置伺服器利用 **DENY** 或 **SAMEORIGIN** 值使用 **"X-Frame-Options"** 標頭
- 配置伺服器利用安全原則使用 **"Content-Security-Policy"** 標頭
- 配置伺服器利用值 **'1'** (已啟用) 使用 **"X-XSS-Protection"** 標頭
- 配置您的伺服器，以搭配安全原則使用「查閱者原則」標頭
- 將每一個第三方 **Script**/鏈結元素支援新增至 **SRI**（子資源完整性）。
- 新增 **'HttpOnly'** 屬性至所有階段作業 **Cookie**
- 對禁止的資源發出「**404 - 找不到**」回應狀態碼，或將其完全移除
- 請下載您的 **Web** 伺服器或 **Web** 應用程式的相關安全修補程式。
- 請勿容許機密性資訊洩漏。
- 請驗證參數值是在預期的範圍內且為預期的類型。請勿輸出除錯錯誤訊息和異常狀況
- 檢閱將 **SameSite Cookie** 屬性配置為建議值的可能解決方案

諮詢

- **SQL** 注入
- 未加密的登入要求
- 查詢中的 **Password** 參數
- 不適當地封鎖帳戶
- 未更新階段作業 ID
- 偽造跨網站要求
- 登入錯誤訊息認證列舉
- **SameSite** 屬性不安全、不適當或遺漏的 **Cookie**
- 未停用密碼欄位的自動完成 **HTML** 屬性
- 在階段作業 **Cookie** 中遺漏 **HttpOnly** 屬性
- 找到資料庫錯誤型樣
- 偵測到隱藏目錄
- 遺漏「**Content-Security-Policy**」標頭
- 遺漏或不安全的 **"X-Content-Type-Options"** 標頭
- 遺漏或不安全的 **"X-XSS-Protection"** 標頭
- 遺漏或不安全的跨頁框 **Scripting** 防禦
- 應用程式中找到不必要的 **HTTP** 回應標頭
- 檢查是否有 **SRI**（子資源完整性）支援
- 找到可能的伺服器路徑揭露型樣
- 遺漏「查閱者原則」安全標頭
- 應用程式錯誤

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：	6
中嚴重性問題：	5
低嚴重性問題：	17
參考資訊嚴重性問題：	3
報告中併入的安全問題總計：	31
掃描中探索到的安全問題總計：	31

一般資訊

掃描檔名：	20210727014_kit.geohealth.tw_人社中心彭逸帆0728
掃描開始時間：	2021/7/28 下午 06:18:36
測試原則：	Default
測試最佳化等級：	快速
主機	kit.geohealth.tw
埠	80
作業系統：	Win32
Web 伺服器：	IIS
應用程式伺服器：	PHP

登入設定值

登入方法：	已記錄的登入
並行登入：	已啟用
階段作業內偵測：	已啟用
階段作業內型樣：	200\s+OK
已追蹤或階段作業 ID Cookies：	PHPSESSID
已追蹤或階段作業 ID 參數：	
登入序列：	http://kit.geohealth.tw/ http://kit.geohealth.tw/ http://kit.geohealth.tw/main.php http://kit.geohealth.tw/main.php

摘要

問題類型 21

目錄

問題類型		問題數目	
高	SQL 注入	2	<div><div></div></div>
高	未加密的登入要求	3	<div><div></div></div>
高	查詢中的 Password 參數	1	<div><div></div></div>
中	不適當地封鎖帳戶	1	<div><div></div></div>
中	未更新階段作業 ID	1	<div><div></div></div>
中	偽造跨網站要求	2	<div><div></div></div>
中	登入錯誤訊息認證列舉	1	<div><div></div></div>
低	SameSite 屬性不安全、不適當或遺漏的 Cookie	1	<div><div></div></div>
低	未停用密碼欄位的自動完成 HTML 屬性	2	<div><div></div></div>
低	在階段作業 Cookie 中遺漏 HttpOnly 屬性	1	<div><div></div></div>
低	找到資料庫錯誤型樣	3	<div><div></div></div>
低	偵測到隱藏目錄	1	<div><div></div></div>
低	遺漏「Content-Security-Policy」標頭	1	<div><div></div></div>
低	遺漏或不安全的 "X-Content-Type-Options" 標頭	1	<div><div></div></div>
低	遺漏或不安全的 "X-XSS-Protection" 標頭	1	<div><div></div></div>
低	遺漏或不安全的跨頁框 Scripting 防禦	1	<div><div></div></div>
低	應用程式中找到不必要的 HTTP 回應標頭	1	<div><div></div></div>
低	檢查是否有 SRI（子資源完整性）支援	4	<div><div></div></div>
參	找到可能的伺服器路徑揭露型樣	1	<div><div></div></div>
參	遺漏「查閱者原則」安全標頭	1	<div><div></div></div>
參	應用程式錯誤	1	<div><div></div></div>

有漏洞的 URL 5

目錄

URL		問題數目	
高	http://kit.geohealth.tw/	18	<div><div></div><div></div><div></div><div></div></div>
高	http://kit.geohealth.tw/main.php	7	<div><div></div><div></div><div></div><div></div></div>
高	http://kit.geohealth.tw/index.php	4	<div><div></div><div></div><div></div><div></div></div>
中	http://kit.geohealth.tw/logout.php	1	<div><div></div></div>

低	http://kit.geohealth.tw/preview.php	1	
---	-------------------------------------	---	--

修正建議 19

目錄

補救作業		問題數目	
高	傳送機密性資訊時，一律使用 SSL 和 POST （主體）參數。	4	<div></div>
高	檢查危險字元注入可能的解決方案	5	<div></div>
中	在數次登入嘗試失敗之後，強制封鎖帳戶	1	<div></div>
中	登入後變更階段作業 ID 值	1	<div></div>
中	對每一個錯誤的登入嘗試發出相同的錯誤訊息	1	<div></div>
中	請驗證 "Referer" 標頭的值，並對每一個提交的表單使用 one-time-nonce	2	<div></div>
低	正確設定 "autocomplete" 屬性為 "off"	2	<div></div>
低	配置伺服器利用 "nosniff" 值使用 "X-Content-Type-Options" 標頭	1	<div></div>
低	配置伺服器利用 DENY 或 SAMEORIGIN 值使用 "X-Frame-Options" 標頭	1	<div></div>
低	配置伺服器利用安全原則使用 "Content-Security-Policy" 標頭	1	<div></div>
低	配置伺服器利用值 '1' (已啟用) 使用 "X-XSS-Protection" 標頭	1	<div></div>
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	<div></div>
低	將每一個第三方 Script/鏈結元素支援新增至 SRI（子資源完整性）。	4	<div></div>
低	新增 'HttpOnly' 屬性至所有階段作業 Cookie	1	<div></div>
低	對禁止的資源發出「404 - 找不到」回應狀態碼，或將其完全移除	1	<div></div>
低	請下載您的 Web 伺服器或 Web 應用程式的相關安全修補程式。	1	<div></div>
低	請勿容許機密性資訊洩漏。	1	<div></div>
低	請驗證參數值是在預期的範圍內且為預期的類型。請勿輸出除錯錯誤訊息和異常狀況	1	<div></div>
低	檢閱將 SameSite Cookie 屬性配置為建議值的可能解決方案	1	<div></div>

安全風險 13

目錄

風險		問題數目	
高	有可能檢視、修改或刪除資料庫項目和表格	5	<div></div>
高	有可能竊取以未加密方式傳送的使用者登入資訊，如：使用者名稱和密碼	3	<div></div>
高	有可能竊取查詢字串中傳送的機密資料，如：使用者名稱和密碼	1	<div></div>
中	有可能透過 Web 應用程式升級使用者專用權及取得管理許可權	2	<div></div>
中	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	4	<div></div>
低	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	<div></div>
低	有可能略過 Web 應用程式的鑑別機制	2	<div></div>
低	有可能擷取網站檔案系統結構的相關資訊，其可能會幫助攻擊者對映網站	1	<div></div>
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	<div></div>

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	5	<div><div></div><div></div></div>
低	假設第三方伺服器已受損，網站的內容/行為會變更	4	<div><div></div><div></div></div>
參	有可能擷取 Web 伺服器安裝架構的絕對路徑，其可能會幫助攻擊者展開進一步攻擊，以及取得 Web 應用程式之檔案系統結構的相關資訊	1	<div><div></div><div></div></div>
參	有可能收集機密性除錯資訊	1	<div><div></div><div></div></div>

原因 13

目錄

原因	問題數目
高 未正確地消毒使用者所輸入的危險字元	5 <div><div></div><div></div></div>
高 機密性輸入欄位（如：使用者名稱、密碼和信用卡號碼）傳遞時未加密	3 <div><div></div></div>
高 查詢字串中傳遞了機密性輸入欄位（如：使用者名稱、密碼和信用卡號碼）	1 <div><div></div></div>
中 不安全的 Web 應用程式設計或配置	10 <div><div></div><div></div><div></div></div>
中 應用程式所使用的鑑別方法不足	2 <div><div></div></div>
中 已向使用者顯示可能含有機密性除錯資訊的異常狀況和錯誤訊息	1 <div><div></div></div>
低 SameSite 屬性不適當、不安全或遺漏的機密 Cookie	1 <div><div></div></div>
低 Web 應用程式設定的階段作業 Cookie 不含 HttpOnly 屬性	1 <div><div></div></div>
低 使用不安全的方式配置 Web 伺服器或應用程式伺服器	1 <div><div></div></div>
低 不支援 SRI（子資源完整性）	4 <div><div></div></div>
參 未安裝協力廠商產品最新的修補程式或緊急修復程式	1 <div><div></div></div>
參 未對送入的參數值執行適當的範圍檢查	1 <div><div></div></div>
參 未執行驗證，以確定使用者輸入符合預期的資料類型	1 <div><div></div></div>

WASC 威脅分類

目錄

威脅	問題數目	
SQL 注入	5	<div></div>
伺服器配置錯誤	1	<div></div>
併入遠端檔案	4	<div></div>
偽造跨網站要求	2	<div></div>
強制入侵	2	<div></div>
階段作業固定	1	<div></div>
傳輸層保護不足	3	<div></div>
資訊洩漏	13	<div></div>

依問題類型排列的問題

SQL 注入	
嚴重性：	高
CVSS 評分：	9.7
URL：	http://kit.geohealth.tw/
實體：	username (Parameter)
風險：	有可能檢視、修改或刪除資料庫項目和表格
原因：	未正確地消毒使用者所輸入的危險字元
修正：	檢查危險字元注入可能的解決方案

推論： 測試結果似乎指出有漏洞，因為回應包含 **SQL Server** 錯誤。這暗示受管理的測試已透過注入危險的字元來滲透應用程式，並呼叫到 **SQL** 查詢本身。

測試要求和回應：

```
POST / HTTP/1.1
Content-Length: 67
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

username=admin%40localhost%a5'%20having%201=1--%20&password1=**CONFIDENTIAL 0**

HTTP/1.1 200 OK
Content-Length: 469
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=ih73js3ctt90unpr8nm2pv2v34; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:28:04 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate

<br />
<b>Fatal error</b>: Uncaught PDOException: SQLSTATE[HY000]: General error: 1267 Illegal mix of collations
(utf8mb4_general_ci,IMPLICIT) and (utf8_general_ci,COERCIBLE) for operation '=' in
C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\index.php:12
```

```
Stack trace:
#0 C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\index.php(12): PDOStatement->execute()
#1 {main}
  thrown in <b>C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\index.php</b> on line <b>12</b><br />
```

問題 2 / 2

目錄

SQL 注入

嚴重性：**高**

CVSS 評分：9.7

URL：<http://kit.geohealth.tw/main.php>

實體：search (Parameter)

風險：有可能檢視、修改或刪除資料庫項目和表格

原因：未正確地消毒使用者所輸入的危險字元

修正：檢查危險字元注入可能的解決方案

推論： 測試結果似乎指出有漏洞，因為回應包含 **SQL Server** 錯誤。這暗示受管理的測試已透過注入危險的字元來滲透應用程式，並呼叫到 **SQL** 查詢本身。

測試要求和回應：

```
POST /main.php HTTP/1.1
Content-Length: 48
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
Cookie: PHPSESSID=nv04crtbcdldvqrqasn7h9ee81
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/main.php
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

searchProject=1&search=1%a5'%20having%201=1--%20

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 469
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:27:46 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8

<br />
<b>Fatal error</b>: Uncaught PDOException: SQLSTATE[HY000]: General error: 1267 Illegal mix of collations
(utf8mb4_general_ci,IMPLICIT) and (utf8_general_ci,COERCIBLE) for operation 'like' in
C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\main.php:62
Stack trace:
#0 C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\main.php(62): PDOStatement->execute()
#1 {main}
  thrown in <b>C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\main.php</b> on line <b>62</b><br />
```

高 未加密的登入要求 3

目錄

未加密的登入要求

嚴重性：

CVSS 評分： 8.5

URL：<http://kit.geohealth.tw/>

實體： (Page)

風險： 有可能竊取以未加密方式傳送的使用者登入資訊，如：使用者名稱和密碼

原因： 機密性輸入欄位（如：使用者名稱、密碼和信用卡號碼）傳遞時未加密

修正： 傳送機密性資訊時，一律使用 **SSL** 和 **POST**（主體）參數。**推論：** AppScan 指出未透過 SSL 傳送登入要求。**測試要求和回應：**

```

POST / HTTP/1.1
Content-Length: 43
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
Cookie: PHPSESSID=u5bos330rbfk32ja6hq49oud41
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

username=admin%40localhost&password1=**CONFIDENTIAL 0**

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 0
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:19:00 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8

```

未加密的登入要求

嚴重性：**高**

CVSS 評分：8.5

URL：<http://kit.geohealth.tw/>

實體：password1 (Parameter)

風險：有可能竊取以未加密方式傳送的使用者登入資訊，如：使用者名稱和密碼

原因：機密性輸入欄位（如：使用者名稱、密碼和信用卡號碼）傳遞時未加密

修正：傳送機密性資訊時，一律使用 **SSL** 和 **POST**（主體）參數。

推論：AppScan 指出未透過 SSL 傳送密碼參數。

測試要求和回應：

```
POST / HTTP/1.1
Content-Length: 43
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
Cookie: PHPSESSID=u5bos330rbfk32ja6hq49oud41
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

username=admin%40localhost&password1=**CONFIDENTIAL 0**

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 0
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:19:00 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
```

問題 3 / 3

目錄

未加密的登入要求

嚴重性：**高**

CVSS 評分：8.5

URL：<http://kit.geohealth.tw/index.php>

實體：password1 (Parameter)

風險：有可能竊取以未加密方式傳送的使用者登入資訊，如：使用者名稱和密碼

原因：機密性輸入欄位（如：使用者名稱、密碼和信用卡號碼）傳遞時未加密

修正：傳送機密性資訊時，一律使用 **SSL** 和 **POST**（主體）參數。

推論：AppScan 指出未透過 SSL 傳送密碼參數。

測試要求和回應：

```
GET /index.php?username=admin%40localhost&password1=**CONFIDENTIAL 0** HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Referer: http://kit.geohealth.tw/index.php
Cookie: PHPSESSID=af6chl22gtf10c2uk381vfv531
Host: kit.geohealth.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 8321
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:18:56 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
```

```
<!DOCTYPE html>
<html>
<head>
<title>      幼兒點日記管理</title>
<meta http-equiv="Content-Type" content="text/html" charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="cache-control" content="no-cache">

<!-- Bootstrap 4 CDN -->
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
<script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FggCb/KJQLLNF0u91ta32o/NM2xltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
<script src="https://cdn.jsdelivr.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-
UO2eT0CpHqdSjQ6hJty5KVphtPhzWj9W01clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgyd0p3pXBlrRibZUAYoIIy6OrQ6VrjIEaFf/nJGzIxFDsf4x0xIM+B07jRM" crossorigin="anonymous"></script>

<!-- Fontawesome CDN -->
<link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">

<!-- JQuery-Confirm -->
<link rel="stylesheet" href="https://cdn.jsdelivr.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
<script src="https://cdn.jsdelivr.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

<style>
/* BASIC */
html, body{
  height: 100%; letter-spacing: 0.05em;
  font-family: Microsoft JhengHei;
}

/* STRUCTURE */
.container{
  height: 100%;
}

.wrapper{
  min-height: 100%; width: 100%;
  display: flex; flex-direction: column; justify-content: center; align-items: center;
}

#formContent{
  width: 40%; padding: 2em 2em 1.5em 2em;
  background-color: #FFFFFF;
  position: relative; text-align: center;
  -webkit-box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); -webkit-border-
radius: 15px; border-radius: 15px;
}

/* DETAILED */
.form-group{
  justify-content: center;
}

hr{
  height: 0.05em;
  background-color: #2E317C;
}

.input-group-prepend, input{
  margin: 0.25em 0;
}
```

```

input{
  width: 75%; height: 2.5em; border: 0;
  background-color: #F0F5E5;
  text-align: center; display: inline-block;
  -webkit-border-radius: 5px; border-radius: 5px;
}

input:focus{
  border: 2.5px solid #2E317C;
}

#signIn{
  margin: -0.25em;
}

.icon{
  width: 7.5em; height: 5em;
}

/* ANIMATIONS */
@-webkit-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@-moz-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@keyframes fadeIn{from{opacity:0;}to{opacity:1;}}

.fadeIn{
  opacity:0;
  -webkit-animation:fadeIn ease-in 1; -moz-animation:fadeIn ease-in 1; animation:fadeIn ease-in 1;
  -webkit-animation-duration: 1s; -moz-animation-duration: 1s; animation-duration: 1s;
  -webkit-animation-fill-mode: forwards; -moz-animation-fill-mode: forwards; animation-fill-mode: forwards;
}

.fadeIn.first{
  -webkit-animation-delay: 0.1s; -moz-animation-delay: 0.1s; animation-delay: 0.1s;
}

.fadeIn.second{
  -webkit-animation-delay: 0.3s; -moz-animation-delay: 0.3s; animation-delay: 0.3s;
}

.fadeIn.third{
  -webkit-animation-delay: 0.5s; -moz-animation-delay: 0.5s; animation-delay: 0.5s;
}

.fadeIn.fourth{
  -webkit-animation-delay: 0.7s; -moz-animation-delay: 0.7s; animation-delay: 0.7s;
}

/* RESPONSIVE */
@media screen and (max-width: 800px){
  #formContent{
    width: 85%;
    font-size: 0.8em;
  }
}

...
...
...

```

高

查詢中的 Password 參數 ①

目錄

問題 1 / 1

目錄

查詢中的 Password 參數

嚴重性：**高**

CVSS 評分：8.5

URL：<http://kit.geohealth.tw/index.php>

實體：password1 (Parameter)

風險：有可能竊取查詢字串中傳送的機密資料，如：使用者名稱和密碼

原因：查詢字串中傳遞了機密性輸入欄位（如：使用者名稱、密碼和信用卡號碼）

修正：傳送機密性資訊時，一律使用 SSL 和 POST（主體）參數。

推論：AppScan 指出查詢字串中收到 password 參數

測試要求和回應：

```
GET /index.php?username=admin%40localhost&password1=**CONFIDENTIAL 0** HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Referer: http://kit.geohealth.tw/index.php
Cookie: PHPSESSID=af6chl22gtf10c2uk381vfv531
Host: kit.geohealth.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 8321
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:18:56 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<title>    幼兒點日記管理</title>
<meta http-equiv="Content-Type" content="text/html" charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="cache-control" content="no-cache">

<!-- Bootstrap 4 CDN -->
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
<script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FgpCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
<script src="https://cdn.jsdelivr.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-
U02eT0CpHqdsJQ6hJty5KVphtPhzWj9WO1clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgyd0p3pXb1rRibZUAYoIIy6OrQ6VrjIEaFF/nGzIxFDsf4x0IM+B07jRM" crossorigin="anonymous"></script>

<!-- Fontawesome CDN -->
<link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvItY8vEf7N7fWAU" crossorigin="anonymous">

<!-- JQuery-Confirm -->
<link rel="stylesheet" href="https://cdn.jsdelivr.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
<script src="https://cdn.jsdelivr.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

<style>
/* BASIC */
html, body{
    height: 100%; letter-spacing: 0.05em;
    font-family: Microsoft JhengHei;
}

/* STRUCTURE */
.container{
    height: 100%;
}

.wrapper{
    min-height: 100%; width: 100%;
```

```

        display: flex; flex-direction: column; justify-content: center; align-items: center;
    }

    #formContent{
        width: 40%; padding: 2em 2em 1.5em 2em;
        background-color: #FFFFFF;
        position: relative; text-align: center;
        -webkit-box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); -webkit-border-
radius: 15px; border-radius: 15px;
    }

    /* DETAILED */
    .form-group{
        justify-content: center;
    }

    hr{
        height: 0.05em;
        background-color: #2E317C;
    }

    .input-group-prepend, input{
        margin: 0.25em 0;
    }

    input{
        width: 75%; height: 2.5em; border: 0;
        background-color: #F0F5E5;
        text-align: center; display: inline-block;
        -webkit-border-radius: 5px; border-radius: 5px;
    }

    input:focus{
        border: 2.5px solid #2E317C;
    }

    #signIn{
        margin: -0.25em;
    }

    .icon{
        width: 7.5em; height: 5em;
    }

    /* ANIMATIONS */
    @-webkit-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
    @-moz-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
    @keyframes fadeIn{from{opacity:0;}to{opacity:1;}}

    .fadeIn{
        opacity:0;
        -webkit-animation:fadeIn ease-in 1; -moz-animation:fadeIn ease-in 1; animation:fadeIn ease-in 1;
        -webkit-animation-duration: 1s; -moz-animation-duration: 1s; animation-duration: 1s;
        -webkit-animation-fill-mode: forwards; -moz-animation-fill-mode: forwards; animation-fill-mode: forwards;
    }

    .fadeIn.first{
        -webkit-animation-delay: 0.1s; -moz-animation-delay: 0.1s; animation-delay: 0.1s;
    }
    .fadeIn.second{
        -webkit-animation-delay: 0.3s; -moz-animation-delay: 0.3s; animation-delay: 0.3s;
    }
    .fadeIn.third{
        -webkit-animation-delay: 0.5s; -moz-animation-delay: 0.5s; animation-delay: 0.5s;
    }
    .fadeIn.fourth{
        -webkit-animation-delay: 0.7s; -moz-animation-delay: 0.7s; animation-delay: 0.7s;
    }

    /* RESPONSIVE */
    @media screen and (max-width: 800px){
        #formContent{
            width: 85%;
            font-size: 0.8em;
        }
    }

    ...
    ...
    ...

```

問題 1 / 1

目錄

不適當地封鎖帳戶

嚴重性： 中

CVSS 評分： 6.4

URL： <http://kit.geohealth.tw/>

實體： password1 (Parameter)

風險： 有可能透過 Web 應用程式升級使用者專用權及取得管理許可權

原因： 不安全的 Web 應用程式設計或配置

修正： 在數次登入嘗試失敗之後，強制封鎖帳戶

推論： 已嘗試傳送兩個合法的登入，期間有幾個失敗的登入嘗試。最後一個回應與第一個回應相同。這表示帳戶強制封鎖的方式不適當，而允許對登入頁面進行強制入侵攻擊。（即使第一個回應不是成功的登入頁面，這也是正確的。）

測試要求和回應：

```
POST / HTTP/1.1
Content-Length: 43
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

username=admin%40localhost&password1=**CONFIDENTIAL 0**
```

```
HTTP/1.1 200 OK
Content-Length: 0
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=jd25g2fge8ubvbqsvu7r29ijf5; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:28:08 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
```

```
POST / HTTP/1.1
Content-Length: 44
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

username=admin%40localhost&password1=4ppSc4n
```

HTTP/1.1 200 OK
Content-Length: 14
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=87cglg4mttb8t1ldgk4jthaun2; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:28:08 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate

Wrong Password

POST / HTTP/1.1
Content-Length: 44
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

username=admin%40localhost&password1=4ppSc4n

HTTP/1.1 200 OK
Content-Length: 14
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=dee8oqbn72rultqrjlp2i6sil3; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:28:08 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate

Wrong Password

POST / HTTP/1.1
Content-Length: 44
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

username=admin%40localhost&password1=4ppSc4n

HTTP/1.1 200 OK
Content-Length: 14
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=i0hnathlsslne84eibv6likmk2; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:28:08 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate

Wrong Password

POST / HTTP/1.1
Content-Length: 44
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

username=admin%40localhost&password1=4ppSc4n

HTTP/1.1 200 OK
Content-Length: 14
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=hf4fd59nqk5gfjb6u2ufidcf51; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27


```

Date: Wed, 28 Jul 2021 10:28:08 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate

Wrong Password

POST / HTTP/1.1
Content-Length: 44
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

username=admin%40localhost&password1=4ppSc4n

HTTP/1.1 200 OK
Content-Length: 14
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=qtjeuo2oeca0j1mlgfsp15g3k5; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:28:08 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate

Wrong Password

POST / HTTP/1.1
Content-Length: 44
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
X-Requested-With: XMLHttpRequest
Connection: keep-alive
...
...
...

```

問題 1 / 1

目錄

未更新階段作業 ID

嚴重性：	中
CVSS 評分：	6.4
URL：	http://kit.geohealth.tw/
實體：	(Page)
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
原因：	不安全的 Web 應用程式設計或配置
修正：	登入後變更階段作業 ID 值

推論： 測試結果似乎指出有漏洞，因為「原始要求」與「回應」中的階段作業 ID 相同。它們應該會在回應中被更新。

測試要求和回應：

```
POST / HTTP/1.1
Content-Length: 43
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
Cookie: PHPSESSID=u5bos330rbfk32ja6hq49oud41
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

username=admin%40localhost&password1=**CONFIDENTIAL 0**

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 0
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:19:00 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
```

中

偽造跨網站要求 ②

目錄

問題 1 / 2

目錄

偽造跨網站要求

嚴重性： **中**

CVSS 評分： 6.4

URL： <http://kit.geohealth.tw/main.php>

實體： main.php (Page)

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

原因： 應用程式所使用的鑑別方法不足

修正： 請驗證 "Referer" 標頭的值，並對每一個提交的表單使用 one-time-nonce

推論： 測試結果似乎指出有漏洞，因為「測試回應」與「原始回應」相同，表示即使包含虛構的「參照位址」標頭，但是「偽造跨網站要求」嘗試已成功。

測試要求和回應：

```
GET /main.php?project_id=1234 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Referer: https://bogus.referer.hcl.com
Cookie: PHPSESSID=nv04crtbcdldvrqtasn7h9ee81
Host: kit.geohealth.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Origin: https://bogus.origin.hcl.com
Accept-Language: en-US
```

```

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 62487
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:26:34 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
  <title>      總覽儀表板</title>
  <meta http-equiv="Content-Type" content="text/html" charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta http-equiv="cache-control" content="no-cache">

  <!-- Bootstrap 4 CDN -->
  <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
  <script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FgpCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
  <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-
UO2eT0CpHqdsJQ6hJty5KVphtPhzWj9WO1clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
  <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgyd0p3pXB1rRibZUAYoIIy6OrQ6VrjIEaFf/njGzIxFdsf4x0xIM+B07jRM" crossorigin="anonymous"></script>

  <!-- Fontawesome CDN -->
  <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">

  <!-- JQuery-Confirm -->
  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
  <script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

  <!-- loadash -->
  <script src="https://cdn.jsdelivr.net/npm/lodash@4.17.10/lodash.min.js"></script>

<style>
  html{
    min-height: 100%;
    font-family: Microsoft JhengHei; position: relative;
  }

  body{
    padding-top: 100px; padding-bottom: 125px;
  }

  .wrap{
    width: 100%; margin: 20px auto;
    display: inline-block; position: relative; text-align: center;
  }

  .title{
    width: 100%; top: 15%; letter-spacing: 0.05em;
    color: #2E317C;
    font-size: 1.75em; text-align: center; position: absolute;
  }

  .modal{
    width: 30%; left: 35%; top: 20%
  }

  .row{
    width: 80%; margin: 0px auto;
  }

  .btn, .input-group-text{
    font-size: 0.95em;
  }

  .icon{
    width: 7.5em;
  }

  .container{
    width: 75%; margin: 10px auto; letter-spacing: 0.05em;
    font-size: 0.8em; align-content: center;
  }

  td{
    line-height: 2.5em;

```

```

        vertical-align: middle;
    }
</style>

<script>
$(document).ready(function(){
$.ajax({
    type: "POST",
    dataType: "json",
    url: "",
    data: {fetchProject: 1},
    success: function(data){
        console.log(data);

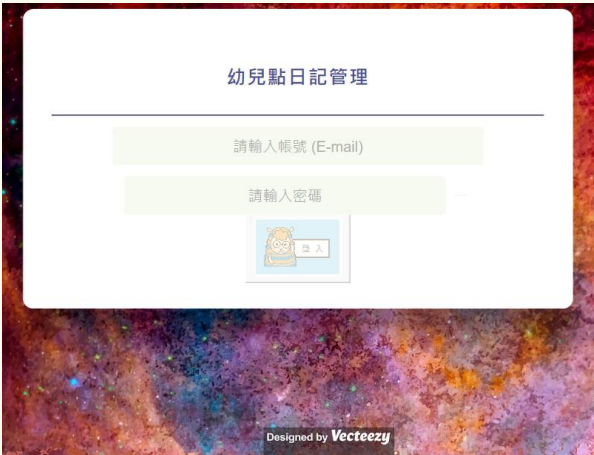
        for($i=0; $i<data.length; $i++){
            var row_n=document.getElementById("project_list").rows.length-1;
            var append_row=document.getElementById("project_list").insertRow(row_n);

            append_row.insertCell(0).innerHTML=data[$i]["project_id"];
            append_row.insertCell(1).innerHTML=data[$i]["project_name"];
            append_row.insertCell(2).innerHTML=data[$i]["name"];
            append_row.insertCell(3).innerHTML=data[$i]["sample_size"];

            if(data[$i].active==0){
                append_row.insertCell(4).innerHTML="<span style='padding: 10%; color: #FFFFFF; background-color: #003B83; border-radius: 5px'><b>D 關閉</b></span>";
            }else if(data[$i].active==1){
                append_row.insertCell(4).innerHTML="<span style='padding: 10%; color: #FFFFFF; background-color: orange; border-radius: 5px'><b>A 開啟</b></span>";
            }
        }
    }
});

```


原始回應



幼兒點日記管理

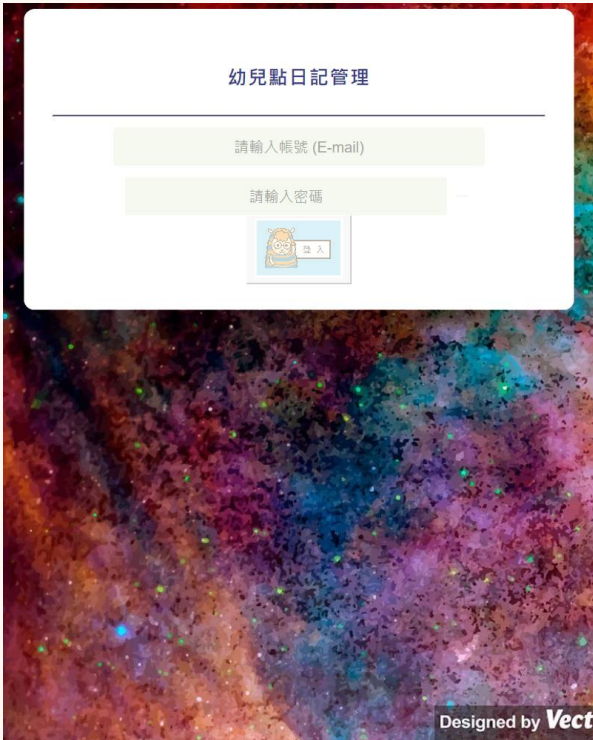
請輸入帳號 (E-mail)

請輸入密碼

 登入

Designed by Vecteezy


測試回應



幼兒點日記管理

請輸入帳號 (E-mail)

請輸入密碼

 登入

Designed by Vect

偽造跨網站要求

嚴重性： 中

CVSS 評分： 6.4

URL： <http://kit.geohealth.tw/logout.php>

實體： logout.php (Page)

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

原因： 應用程式所使用的鑑別方法不足

修正： 請驗證 "Referer" 標頭的值，並對每一個提交的表單使用 one-time-nonce

推論： 測試結果似乎指出有漏洞，因為「測試回應」與「原始回應」相同，表示即使包含虛構的「參照位址」標頭，但是「偽造跨網站要求」嘗試已成功。

測試要求和回應：

```
GET /logout.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Referer: https://bogus.referer.hcl.com
Cookie: PHPSESSID=brnr7dsatcn3mpffmabmnhugl4
Host: kit.geohealth.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Origin: https://bogus.origin.hcl.com
Accept-Language: en-US
```

```
HTTP/1.1 302 Found
Location: ./index.php
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 134
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:28:30 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8

<head><title>文件已移動</title></head>
<body><h1>物件已移動</h1>此文件可能是在<a href="./index.php">這裡</a></body>
```

```
GET /index.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Referer: http://kit.geohealth.tw/logout.php
Cookie: PHPSESSID=brnr7dsatcn3mpffmabmnhugl4
Host: kit.geohealth.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 8321
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:18:56 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
```

```
<!DOCTYPE html>
<html>
<head>
<title> 幼兒點日記管理</title>
<meta http-equiv="Content-Type" content="text/html" charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="cache-control" content="no-cache">

<!-- Bootstrap 4 CDN -->
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css">
```

```

integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
<script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FgpCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-
UO2eT0CpHqdsJQ6hJty5KVphtPhzWj9WO1clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgyd0p3pXB1rRibZUAYoIIy6OrQ6VrjIEaFF/nJGzIxFDsf4x0xIM+B07jRM" crossorigin="anonymous"></script>

<!-- Fontawesome CDN -->
<link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsq01SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">

<!-- JQuery-Confirm -->
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

<style>
/* BASIC */
html, body{
  height: 100%; letter-spacing: 0.05em;
  font-family: Microsoft JhengHei;
}

/* STRUCTURE */
.container{
  height: 100%;
}

.wrapper{
  min-height: 100%; width: 100%;
  display: flex; flex-direction: column; justify-content: center; align-items: center;
}

#formContent{
  width: 40%; padding: 2em 2em 1.5em 2em;
  background-color: #FFFFFF;
  position: relative; text-align: center;
  -webkit-box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); -webkit-border-
radius: 15px; border-radius: 15px;
}

/* DETAILED */
.form-group{
  justify-content: center;
}

hr{
  height: 0.05em;
  background-color: #2E317C;
}

.input-group-prepend, input{
  margin: 0.25em 0;
}

input{
  width: 75%; height: 2.5em; border: 0;
  background-color: #F0F5E5;
  text-align: center; display: inline-block;
  -webkit-border-radius: 5px; border-radius: 5px;
}

input:focus{
  border: 2.5px solid #2E317C;
}

#signIn{
  margin: -0.25em;
}

.icon{
  width: 7.5em; height: 5em;
}

/* ANIMATIONS */
@-webkit-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@-moz-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@keyframes fadeIn{from{opacity:0;}to{opacity:1;}}

.fadeIn{
  opacity:0;
  -webkit-animation:fadeIn ease-in 1; -moz-animation:fadeIn ease-in 1; animation:fadeIn ease-in 1;
  -webkit-animation-duration: 1s; -moz-animation-duration: 1s; animation-duration: 1s;
}

```

...

問題 1 / 1

目錄

登入錯誤訊息認證列舉

嚴重性：	中
CVSS 評分：	6.4
URL：	http://kit.geohealth.tw/
實體：	(Page)
風險：	有可能透過 Web 應用程式升級使用者專用權及取得管理許可權
原因：	已向使用者顯示可能含有機密性除錯資訊的異常狀況和錯誤訊息
修正：	對每一個錯誤的登入嘗試發出相同的錯誤訊息

推論： 測試發現應用程式在使用者名稱欄位無效時，發出一個錯誤訊息，並在密碼欄位無效時，發出不同的錯誤訊息。這個行為可能會使攻擊者利用強制入侵技術來列舉有效的使用者名稱和密碼。

測試要求和回應：

```
POST / HTTP/1.1
Content-Length: 57
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

username=aadmin%40localhostWithSomeChars&passwordl=**CONFIDENTIAL 0**

HTTP/1.1 200 OK
Content-Length: 16
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=uqdmg5pokscmiblk47vq3d7on4; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:28:04 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate

Invalid Username

POST / HTTP/1.1
Content-Length: 57
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US
```

```
username=admin%40localhost&password1=a**CONFIDENTIAL 0**WithSomeChars
```

```
HTTP/1.1 200 OK
Content-Length: 14
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=7qsjrej9sca3fa61rvlblaiao6; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:28:04 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
```

Wrong Password

```
POST / HTTP/1.1
Content-Length: 57
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US
```

```
username=aadmin%40localhostWithSomeChars&password1=**CONFIDENTIAL 0**
```

```
HTTP/1.1 200 OK
Content-Length: 16
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=u3ogg9gte4gb6u2adig0a30s93; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:28:04 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
```

Invalid Username

測試回應

Invalid Username

問題 1 / 1

目錄

SameSite 屬性不安全、不適當或遺漏的 Cookie

嚴重性： 低

CVSS 評分： 4.1

URL： <http://kit.geohealth.tw/>

實體： PHPSESSID (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](#)

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
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Connection: keep-alive
Host: kit.geohealth.tw
Upgrade-Insecure-Requests: 1
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=0.9
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Content-Length: 8321
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=tdihdkqp4kben783o4945g1m26; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:26:34 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
```

```
<!DOCTYPE html>
<html>
<head>
<title> 幼兒點日記管理</title>
<meta http-equiv="Content-Type" content="text/html" charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="cache-control" content="no-cache">

<!-- Bootstrap 4 CDN -->
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
<script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FggCb/KJQ1LNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
<script src="https://cdn.jsdelivr.net/npm/popper.js@1.14.7/umd/popper.min.js" integrity="sha384-
```

```

U02eT0CpHqdsJQ6hJty5KVphtPhzWj9W01clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgyd0p3pXB1rRibZUAYoIIy6OrQ6VrjIEaFf/njGzIxFdsf4x0xIM+B07jRM" crossorigin="anonymous"></script>

<!-- Fontawesome CDN -->
<link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">

<!-- JQuery-Confirm -->
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

<style>
/* BASIC */
html, body{
  height: 100%; letter-spacing: 0.05em;
  font-family: Microsoft JhengHei;
}

/* STRUCTURE */
.container{
  height: 100%;
}

.wrapper{
  min-height: 100%; width: 100%;
  display: flex; flex-direction: column; justify-content: center; align-items: center;
}

#formContent{
  width: 40%; padding: 2em 2em 1.5em 2em;
  background-color: #FFFFFF;
  position: relative; text-align: center;
  -webkit-box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); -webkit-border-
radius: 15px; border-radius: 15px;
}

/* DETAILED */
.form-group{
  justify-content: center;
}

hr{
  height: 0.05em;
  background-color: #2E317C;
}

.input-group-prepend, input{
  margin: 0.25em 0;
}

input{
  width: 75%; height: 2.5em; border: 0;
  background-color: #F0F5E5;
  text-align: center; display: inline-block;
  -webkit-border-radius: 5px; border-radius: 5px;
}

input:focus{
  border: 2.5px solid #2E317C;
}

#signIn{
  margin: -0.25em;
}

.icon{
  width: 7.5em; height: 5em;
}

/* ANIMATIONS */
@-webkit-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@-moz-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@keyframes fadeIn{from{opacity:0;}to{opacity:1;}}

.fadeIn{
  opacity:0;
  -webkit-animation:fadeIn ease-in 1; -moz-animation:fadeIn ease-in 1; animation:fadeIn ease-in 1;
  -webkit-animation-duration: 1s; -moz-animation-duration: 1s; animation-duration: 1s;
  -webkit-animation-fill-mode: forwards; -moz-animation-fill-mode: forwards; animation-fill-mode: forwards;
}

.fadeIn.first{
  -webkit-animation-delay: 0.1s; -moz-animation-delay: 0.1s; animation-delay: 0.1s;
}

```

```

    }
    .fadeIn.second{
        -webkit-animation-delay: 0.3s; -moz-animation-delay: 0.3s; animation-delay: 0.3s;
    }
    .fadeIn.third{
        -webkit-animation-delay: 0.5s; -moz-animation-delay: 0.5s; animation-delay: 0.5s;
    }
    .fadeIn.fourth{
        -webkit-animation-delay: 0.7s; -moz-animation-delay: 0.7s; animation-delay: 0.7s;
    }
}

/* RESPONSIVE */
@media screen and (max-width: 800px){
    #formContent{
        width: 85%;
    }
}
...
...
...

```

低

未停用密碼欄位的自動完成 HTML 屬性 2

目錄

問題 1 / 2

目錄

未停用密碼欄位的自動完成 HTML 屬性

嚴重性：

低

CVSS 評分： 5.0

URL：<http://kit.geohealth.tw/>

實體： (Page)

風險： 有可能略過 Web 應用程式的鑑別機制

原因： 不安全的 Web 應用程式設計或配置

修正： 正確設定 "autocomplete" 屬性為 "off"

推論： AppScan 發現，密碼欄位未施行停用自動完成功能。

測試要求和回應：

```

GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Connection: keep-alive
Host: kit.geohealth.tw
Upgrade-Insecure-Requests: 1
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=0.9
Accept-Language: en-US

HTTP/1.1 200 OK
Content-Length: 8321
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=ujle7u50p0tvm9t95nc57tqfm2; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:26:34 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate

```

```

<!DOCTYPE html>
<html>
<head>
<title>        幼兒點日記管理</title>
<meta http-equiv="Content-Type" content="text/html" charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="cache-control" content="no-cache">

<!-- Bootstrap 4 CDN -->
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MDdH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
<script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FgpCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-
UO2eT0CpHgdsJQ6hJty5KVphtPhzWj9W01clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgyd0p3pXB1rRibZUAYoIIy60Rq6VrjIEaFf/nJGzIxFdsf4x0xIM+B07jRM" crossorigin="anonymous"></script>

<!-- Fontawesome CDN -->
<link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mrzmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">

<!-- JQuery-Confirm -->
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

<style>
/* BASIC */
html, body{
height: 100%; letter-spacing: 0.05em;
font-family: Microsoft JhengHei;
}

/* STRUCTURE */
.container{
height: 100%;
}

.wrapper{
min-height: 100%; width: 100%;
display: flex; flex-direction: column; justify-content: center; align-items: center;
}

#formContent{
width: 40%; padding: 2em 2em 1.5em 2em;
background-color: #FFFFFF;
position: relative; text-align: center;
-webkit-box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); -webkit-border-
radius: 15px; border-radius: 15px;
}

/* DETAILED */
.form-group{
justify-content: center;
}

hr{
height: 0.05em;
background-color: #2E317C;
}

.input-group-prepend, input{
margin: 0.25em 0;
}

input{
width: 75%; height: 2.5em; border: 0;
background-color: #F0F5E5;
text-align: center; display: inline-block;
-webkit-border-radius: 5px; border-radius: 5px;
}

input:focus{
border: 2.5px solid #2E317C;
}

#signIn{
margin: -0.25em;
}

.icon{
width: 7.5em; height: 5em;

```

```

    }

    /* ANIMATIONS */
    @-webkit-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
    @-moz-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
    @keyframes fadeIn{from{opacit

...
...
...

    $("#eye2").on("click", function(event){
        event.preventDefault();
        var password2=$("#password2").val();
        $("#password2").replaceWith(`<input id="password1" name="password1" type="password"
value=$("#password2)" style="width: 65%">`);
        $("#eye1").show();
        $("#eye2").hide();
    })

...
...
...

    <div class="input-group form-group fadeIn second">
    <div class="input-group-prepend">
    <span class="input-group-text"><i class="fas fa-key"></i></span>
    </div>
    <input id="password1" name="password1" type="password" placeholder="請輸入密碼" required style="width: 65%">
    <button id="eye1" style="margin: 1%; border: 0"><i class="fas fa-eye"></i></button>
    <button id="eye2" style="margin: 1%; border: 0; display: none"><i class="fas fa-eye-slash"></i></button>
    </div>

...
...
...

```

問題 2 / 2

目錄

未停用密碼欄位的自動完成 HTML 屬性

嚴重性： 低

CVSS 評分： 5.0

URL： <http://kit.geohealth.tw/index.php>

實體： index.php (Page)

風險： 有可能略過 Web 應用程式的鑑別機制

原因： 不安全的 Web 應用程式設計或配置

修正： 正確設定 "autocomplete" 屬性為 "off"

推論： AppScan 發現，密碼欄位未施行停用自動完成功能。

測試要求和回應：

```

GET /index.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Referer: http://kit.geohealth.tw/main.php?project_id3=1234&end_date=2019-01-01
Cookie: PHPSESSID=nv04crtbcdldvrqtasn7h9ee81
Host: kit.geohealth.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 8321

```

Cache-Control: no-store, no-cache, must-revalidate

X-Powered-By: PHP/7.0.27

Date: Wed, 28 Jul 2021 10:26:34 GMT

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Content-Type: text/html; charset=UTF-8

```
<!DOCTYPE html>
<html>
<head>
  <title>      幼兒點日記管理</title>
  <meta http-equiv="Content-Type" content="text/html" charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta http-equiv="cache-control" content="no-cache">

  <!-- Bootstrap 4 CDN -->
  <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MDdH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
  <script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FgpCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
  <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-
UO2eT0CpHqdSjQ6hJty5KVphtPhzWj9W01clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
  <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgy0p3pXBlrRibZUAYoIIy6OrQ6VrjIEaFf/nJGzIxFDsf4x0xIM+B07jRM" crossorigin="anonymous"></script>

  <!-- Fontawesome CDN -->
  <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">

  <!-- JQuery-Confirm -->
  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
  <script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

<style>
  /* BASIC */
  html, body{
    height: 100%; letter-spacing: 0.05em;
    font-family: Microsoft JhengHei;
  }

  /* STRUCTURE */
  .container{
    height: 100%;
  }

  .wrapper{
    min-height: 100%; width: 100%;
    display: flex; flex-direction: column; justify-content: center; align-items: center;
  }

  #formContent{
    width: 40%; padding: 2em 2em 1.5em 2em;
    background-color: #FFFFFF;
    position: relative; text-align: center;
    -webkit-box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); -webkit-border-
radius: 15px; border-radius: 15px;
  }

  /* DETAILED */
  .form-group{
    justify-content: center;
  }

  hr{
    height: 0.05em;
    background-color: #2E317C;
  }

  .input-group-prepend, input{
    margin: 0.25em 0;
  }

  input{
    width: 75%; height: 2.5em; border: 0;
    background-color: #F0F5E5;
    text-align: center; display: inline-block;
    -webkit-border-radius: 5px; border-radius: 5px;
  }

  input:focus{
    border: 2.5px solid #2E317C;
  }

  #signIn{
```

```

        margin: -0.25em;
    }

    .icon{
        width: 7.5em; height: 5em;
    }

    /* ANIMATIONS */
    @-webkit-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
    @-moz-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
    @keyframes fadeIn{from{opacity:0;}to{opacity:1;}}

    .fadeIn{
    ...
    ...
    ...

        $("#eye2").on("click", function(event){
            event.preventDefault();
            var password2=$("#password2").val();
            $("#password2").replaceWith(`
            <input id="password1" name="password1" type="password"
            value="${password2}" style="width: 65%">`);
            $("#eye1").show();
            $("#eye2").hide();
        })

    ...
    ...
    ...

        <div class="input-group form-group fadeIn second">
        <div class="input-group-prepend">
        <span class="input-group-text"><i class="fas fa-key"></i></span>
        </div>
        <input id="password1" name="password1" type="password" placeholder="請輸入密碼" required style="width: 65%">
        <button id="eye1" style="margin: 1%; border: 0"><i class="fas fa-eye"></i></button>
        <button id="eye2" style="margin: 1%; border: 0; display: none"><i class="fas fa-eye-slash"></i></button>
        </div>

    ...
    ...
    ...

```

低 在階段作業 Cookie 中遺漏 HttpOnly 屬性 ①

目錄

問題 1 / 1

目錄

在階段作業 Cookie 中遺漏 HttpOnly 屬性

嚴重性： 低

CVSS 評分： 5.0

URL： <http://kit.geohealth.tw/>

實體： PHPSESSID (Cookie)

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

原因： Web 應用程式設定的階段作業 Cookie 不含 HttpOnly 屬性

修正： 新增 'HttpOnly' 屬性至所有階段作業 Cookie

推論：AppScan 發現階段作業 Cookie 使用時不含 "HttpOnly" 屬性。

測試要求和回應：

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Connection: keep-alive
Host: kit.geohealth.tw
Upgrade-Insecure-Requests: 1
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=0.9
Accept-Language: en-US

HTTP/1.1 200 OK
Content-Length: 8321
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=8oqtpuenqeed6iij3vq3icjjg0; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:26:34 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate

<!DOCTYPE html>
<html>
<head>
<title>        幼兒點日記管理</title>
<meta http-equiv="Content-Type" content="text/html" charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="cache-control" content="no-cache">

<!-- Bootstrap 4 CDN -->
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MDdH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
<script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FgpCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-
UO2eT0CpHqdsSJK6hJty5KVphtPhzWj9W01clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgYdOp3pXB1rRibZUAYoIIy6OrQ6VrjIEaFf/nJGzIxFDsf4x0xIM+B07jRM" crossorigin="anonymous"></script>

<!-- Fontawesome CDN -->
<link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvItY8vEf7N7fWAU" crossorigin="anonymous">

<!-- JQuery-Confirm -->
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

<style>
/* BASIC */
html, body{
height: 100%; letter-spacing: 0.05em;
font-family: Microsoft JhengHei;
}

/* STRUCTURE */
.container{
height: 100%;
}

.wrapper{
min-height: 100%; width: 100%;
display: flex; flex-direction: column; justify-content: center; align-items: center;
}

#formContent{
width: 40%; padding: 2em 2em 1.5em 2em;
background-color: #FFFFFF;
position: relative; text-align: center;
-webkit-box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); -webkit-border-
radius: 15px; border-radius: 15px;
}

/* DETAILED */
.form-group{
justify-content: center;
}
```

```

hr{
  height: 0.05em;
  background-color: #2E317C;
}

.input-group-prepend, input{
  margin: 0.25em 0;
}

input{
  width: 75%; height: 2.5em; border: 0;
  background-color: #F0F5E5;
  text-align: center; display: inline-block;
  -webkit-border-radius: 5px; border-radius: 5px;
}

input:focus{
  border: 2.5px solid #2E317C;
}

#signIn{
  margin: -0.25em;
}

.icon{
  width: 7.5em; height: 5em;
}

/* ANIMATIONS */
@-webkit-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@-moz-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@keyframes fadeIn{from{opacity:0;}to{opacity:1;}}

.fadeIn{
  opacity:0;
  -webkit-animation:fadeIn ease-in 1; -moz-animation:fadeIn ease-in 1; animation:fadeIn ease-in 1;
  -webkit-animation-duration: 1s; -moz-animation-duration: 1s; animation-duration: 1s;
  -webkit-animation-fill-mode: forwards; -moz-animation-fill-mode: forwards; animation-fill-mode: forwards;
}

.fadeIn.first{
  -webkit-animation-delay: 0.1s; -moz-animation-delay: 0.1s; animation-delay: 0.1s;
}
.fadeIn.second{
  -webkit-animation-delay: 0.3s; -moz-animation-delay: 0.3s; animation-delay: 0.3s;
}
.fadeIn.third{
  -webkit-animation-delay: 0.5s; -moz-animation-delay: 0.5s; animation-delay: 0.5s;
}
.fadeIn.fourth{
  -webkit-animation-delay: 0.7s; -moz-animation-delay: 0.7s; animation-delay: 0.7s;
}

/* RESPONSIVE */
@media screen and (max-width: 800px){
  #formContent{
    width: 85%;
  }

```

...
...
...

低

找到資料庫錯誤型樣 ③

目錄

問題 1 / 3

目錄

找到資料庫錯誤型樣

嚴重性： **低**

CVSS 評分： 5.0

URL： <http://kit.geohealth.tw/>

實體： username (Global)

風險： 有可能檢視、修改或刪除資料庫項目和表格

原因： 未正確地消毒使用者所輸入的危險字元

修正： [檢查危險字元注入可能的解決方案](#)

推論： 測試結果似乎指出有漏洞，因為回應包含 **SQL Server** 錯誤。這暗示受管理的測試已透過注入危險的字元來滲透應用程式，並呼叫到 **SQL** 查詢本身。

測試要求和回應：

```
POST / HTTP/1.1
Content-Length: 207
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

username=%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/%c0%ae%c0%ae/winnt/win.ini%c0%80.html&password1=**CONFIDENTIAL 0**

HTTP/1.1 200 OK
Content-Length: 469
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=749rcfmpn6qk3n33neud3ok5i0; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:28:06 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate

<br />
<b>Fatal error</b>: Uncaught PDOException: SQLSTATE[HY000]: General error: 1267 Illegal mix of collations (utf8mb4_general_ci,IMPLICIT) and (utf8_general_ci,COERCIBLE) for operation '=' in C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\index.php:12
Stack trace:
#0 C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\index.php(12): PDOStatement->execute()
#1 {main}
  thrown in C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\index.php on line 12</b><br />
```

找到資料庫錯誤型樣

嚴重性： **低**

CVSS 評分： 5.0

URL： <http://kit.geohealth.tw/main.php>

實體： search (Global)

風險： 有可能檢視、修改或刪除資料庫項目和表格

原因： 未正確地消毒使用者所輸入的危險字元

修正： 檢查危險字元注入可能的解決方案

推論： 測試結果似乎指出有漏洞，因為回應包含 **SQL Server** 錯誤。這暗示受管理的測試已透過注入危險的字元來滲透應用程式，並呼叫到 **SQL** 查詢本身。

測試要求和回應：

```
POST /main.php HTTP/1.1
Content-Length: 49
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
Cookie: PHPSESSID=nv04crtbcdldvrqtasn7h9ee81
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/main.php
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

searchProject=1&search=1WFXSSProbe%27%22%29%2F%3E

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 536
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:27:45 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8

<br />
<b>Fatal error</b>: Uncaught PDOException: SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in
your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near
')/>%'' at line 1 in C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\main.php:62
Stack trace:
#0 C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\main.php(62): PDOStatement->execute()
#1 {main}
  thrown in C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\main.php on line 62</b></b><br />
```

找到資料庫錯誤型樣

嚴重性： **低**

CVSS 評分： 5.0

URL： <http://kit.geohealth.tw/main.php>

實體： main.php (Global)

風險： 有可能檢視、修改或刪除資料庫項目和表格

原因： 未正確地消毒使用者所輸入的危險字元

修正： 檢查危險字元注入可能的解決方案

推論： 測試結果似乎指出有漏洞，因為回應包含 **SQL Server** 錯誤。這暗示受管理的測試已透過注入危險的字元來滲透應用程式，並呼叫到 **SQL** 查詢本身。

測試要求和回應：

```
POST /main.php HTTP/1.1
Content-Length: 128
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
Cookie: PHPSESSID=nv04crtbcdldvrqtasn7h9ee81
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/main.php
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

searchProject=%3E%22%27%3E%3Cscript%3Ealert%28489%29%3C%2Fscript%3E&search=%3E%22%27%3E%3Cscript%3Ealert%28489%29%3C%2Fscript%3E

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 641
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:27:43 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8

<br />
<b>Fatal error</b>: Uncaught PDOException: SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '<script>alert(489)</script>' or name LIKE '>'</script>alert(489)</script>' at line 1 in C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\main.php:62
Stack trace:
#0 C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\main.php(62): PDOStatement->execute()
#1 {main}
  thrown in C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\main.php on line 62<br />
```

低 偵測到隱藏目錄 ①

目錄

問題 1 / 1

目錄

偵測到隱藏目錄

嚴重性： **低**

CVSS 評分： 5.0

URL： <http://kit.geohealth.tw/>

實體： uploads/ (Page)

風險： 有可能擷取網站檔案系統結構的相關資訊，其可能會幫助攻擊者對映網站

原因： 使用不安全的方式配置 Web 伺服器或應用程式伺服器

修正： 對禁止的資源發出「404 - 找不到」回應狀態碼，或將其完全移除

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

測試要求和回應：

```
GET /uploads/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Connection: keep-alive
Host: kit.geohealth.tw
Upgrade-Insecure-Requests: 1
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=0.9
Accept-Language: en-US
```

```
HTTP/1.1 403 Forbidden
Server: Microsoft-IIS/8.5
Content-Length: 1147
Date: Wed, 28 Jul 2021 10:27:02 GMT
Content-Type: text/html
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=big5"/>
<title>403 - 禁止: 拒絕存取。</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:**CONFIDENTIAL 0**;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:9px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>伺服器錯誤</h1></div>
<div id="content">
<div class="content-container"><fieldset>
<h2>403 - 禁止: 拒絕存取。</h2>
<h3>使用您提供的認證，沒有權限檢視此目錄或網頁。</h3>
</fieldset></div>
</div>
</body>
</html>
```

低 遺漏「Content-Security-Policy」標頭 1

目錄

遺漏「Content-Security-Policy」標頭

嚴重性： 低

CVSS 評分： 5.0

URL： <http://kit.geohealth.tw/>

實體： kit.geohealth.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

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 / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Connection: keep-alive
Host: kit.geohealth.tw
Upgrade-Insecure-Requests: 1
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=0.9
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Content-Length: 8321
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=u5bos330rbfk32ja6hq49oud41; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:18:51 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
```

```
<!DOCTYPE html>
<html>
<head>
<title> 幼兒點日記管理</title>
<meta http-equiv="Content-Type" content="text/html" charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="cache-control" content="no-cache">

<!-- Bootstrap 4 CDN -->
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
<script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FgpCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-
U02eT0CpHqdsJQ6hJty5KVphtPhzWj9WO1clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgyd0p3pXb1rRibZUAYoIIy6OrQ6VrjIEaFf/nJGzIxFDsf4x0xIM+B07jRM" crossorigin="anonymous"></script>

<!-- Fontawesome CDN -->
<link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvItY8vEf7N7fWAU" crossorigin="anonymous">

<!-- JQuery-Confirm -->
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

<style>
/* BASIC */
html, body{
```

```

        height: 100%; letter-spacing: 0.05em;
        font-family: Microsoft JhengHei;
    }

    /* STRUCTURE */
    .container{
        height: 100%;
    }

    .wrapper{
        min-height: 100%; width: 100%;
        display: flex; flex-direction: column; justify-content: center; align-items: center;
    }

    #formContent{
        width: 40%; padding: 2em 2em 1.5em 2em;
        background-color: #FFFFFF;
        position: relative; text-align: center;
        -webkit-box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); -webkit-border-
radius: 15px; border-radius: 15px;
    }

    /* DETAILED */
    .form-group{
        justify-content: center;
    }

    hr{
        height: 0.05em;
        background-color: #2E317C;
    }

    .input-group-prepend, input{
        margin: 0.25em 0;
    }

    input{
        width: 75%; height: 2.5em; border: 0;
        background-color: #F0F5E5;
        text-align: center; display: inline-block;
        -webkit-border-radius: 5px; border-radius: 5px;
    }

    input:focus{
        border: 2.5px solid #2E317C;
    }

    #signIn{
        margin: -0.25em;
    }

    .icon{
        width: 7.5em; height: 5em;
    }

    /* ANIMATIONS */
    @-webkit-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
    @-moz-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
    @keyframes fadeIn{from{opacity:0;}to{opacity:1;}}

    .fadeIn{
        opacity:0;
        -webkit-animation:fadeIn ease-in 1; -moz-animation:fadeIn ease-in 1; animation:fadeIn ease-in 1;
        -webkit-animation-duration: 1s; -moz-animation-duration: 1s; animation-duration: 1s;
        -webkit-animation-fill-mode: forwards; -moz-animation-fill-mode: forwards; animation-fill-mode: forwards;
    }

    .fadeIn.first{
        -webkit-animation-delay: 0.1s; -moz-animation-delay: 0.1s; animation-delay: 0.1s;
    }
    .fadeIn.second{
        -webkit-animation-delay: 0.3s; -moz-animation-delay: 0.3s; animation-delay: 0.3s;
    }
    .fadeIn.third{
        -webkit-animation-delay: 0.5s; -moz-animation-delay: 0.5s; animation-delay: 0.5s;
    }
    .fadeIn.fourth{
        -webkit-animation-delay: 0.7s; -moz-animation-delay: 0.7s; animation-delay: 0.7s;
    }

    /* RESPONSIVE */
    @media screen and (max-width: 800px){
        #formContent{
            width: 85%;

```



```
font-size: 0.8em;
}
```

...

低

遺漏或不安全的 "X-Content-Type-Options" 標頭 ①

目錄

問題 1 / 1

目錄

遺漏或不安全的 "X-Content-Type-Options" 標頭

嚴重性：

低

CVSS 評分： 5.0

URL：<http://kit.geohealth.tw/>

實體：[kit.geohealth.tw \(Page\)](#)

風險：有可能收集 Web 應用程式相關的機密性資訊，如：使用者名稱、密碼、機器名稱及/或機密檔案位置
有可能說服無經驗而易受騙的使用者提供機密性資訊，如：使用者名稱、密碼、信用卡號碼、社會保險號碼等等

原因：不安全的 Web 應用程式設計或配置

修正：[配置伺服器利用 "nosniff" 值使用 "X-Content-Type-Options" 標頭](#)

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

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Connection: keep-alive
Host: kit.geohealth.tw
Upgrade-Insecure-Requests: 1
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=0.9
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Content-Length: 8321
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=lpmoaae5i348ua5fjanc4q85v2; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:26:34 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
```

```
<!DOCTYPE html>
<html>
<head>
<title>        幼兒點日記管理</title>
<meta http-equiv="Content-Type" content="text/html" charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="cache-control" content="no-cache">

<!-- Bootstrap 4 CDN -->
```

```

<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQV3Xipma34MDdH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
<script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FgpCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-
UO2eT0CpHgdsJQ6hJty5KVphtPhzWj9W01clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgyd0p3pXB1rRibZUAYoIIy6OrQ6VrjIEaFF/nJGzIxFDsf4x0xIM+B07jRM" crossorigin="anonymous"></script>

<!-- Fontawesome CDN -->
<link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">

<!-- JQuery-Confirm -->
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

<style>
  /* BASIC */
  html, body{
    height: 100%; letter-spacing: 0.05em;
    font-family: Microsoft JhengHei;
  }

  /* STRUCTURE */
  .container{
    height: 100%;
  }

  .wrapper{
    min-height: 100%; width: 100%;
    display: flex; flex-direction: column; justify-content: center; align-items: center;
  }

  #formContent{
    width: 40%; padding: 2em 2em 1.5em 2em;
    background-color: #FFFFFF;
    position: relative; text-align: center;
    -webkit-box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); -webkit-border-
radius: 15px; border-radius: 15px;
  }

  /* DETAILED */
  .form-group{
    justify-content: center;
  }

  hr{
    height: 0.05em;
    background-color: #2E317C;
  }

  .input-group-prepend, input{
    margin: 0.25em 0;
  }

  input{
    width: 75%; height: 2.5em; border: 0;
    background-color: #F0F5E5;
    text-align: center; display: inline-block;
    -webkit-border-radius: 5px; border-radius: 5px;
  }

  input:focus{
    border: 2.5px solid #2E317C;
  }

  #signIn{
    margin: -0.25em;
  }

  .icon{
    width: 7.5em; height: 5em;
  }

  /* ANIMATIONS */
  @-webkit-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
  @-moz-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
  @keyframes fadeIn{from{opacity:0;}to{opacity:1;}}

  .fadeIn{
    opacity:0;
    -webkit-animation:fadeIn ease-in 1; -moz-animation:fadeIn ease-in 1; animation:fadeIn ease-in 1;
    -webkit-animation-duration: 1s; -moz-animation-duration: 1s; animation-duration: 1s;
  }

```

```

        -webkit-animation-fill-mode: forwards; -moz-animation-fill-mode: forwards; animation-fill-mode: forwards;
    }

    .fadeIn.first{
        -webkit-animation-delay: 0.1s; -moz-animation-delay: 0.1s; animation-delay: 0.1s;
    }
    .fadeIn.second{
        -webkit-animation-delay: 0.3s; -moz-animation-delay: 0.3s; animation-delay: 0.3s;
    }
    .fadeIn.third{
        -webkit-animation-delay: 0.5s; -moz-animation-delay: 0.5s; animation-delay: 0.5s;
    }
    .fadeIn.fourth{
        -webkit-animation-delay: 0.7s; -moz-animation-delay: 0.7s; animation-delay: 0.7s;
    }

    /* RESPONSIVE */
    @media screen and (max-width: 800px){
        #formContent{
            width: 85%;
        }
    }
    ...
    ...
    ...

```

低 遺漏或不安全的 "X-XSS-Protection" 標頭 ①

目錄

問題 1 / 1

目錄

遺漏或不安全的 "X-XSS-Protection" 標頭

嚴重性： **低**

CVSS 評分： 5.0

URL： <http://kit.geohealth.tw/>

實體： kit.geohealth.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： 配置伺服器利用值 '1' (已啟用) 使用 "X-XSS-Protection" 標頭

推論： AppScan 偵測到遺漏 X-XSS-Protection 回應標頭或包含不安全的值，這可能會容許「跨網站 Scripting」攻擊
測試要求和回應：

```

GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Connection: keep-alive
Host: kit.geohealth.tw
Upgrade-Insecure-Requests: 1
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=0.9
Accept-Language: en-US

HTTP/1.1 200 OK
Content-Length: 8321
Server: Microsoft-IIS/8.5

```

Set-Cookie: PHPSESSID=lpmoaae5i348ua5fjanc4q85v2; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:26:34 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate

```
<!DOCTYPE html>
<html>
<head>
<title>        幼兒點日記管理</title>
<meta http-equiv="Content-Type" content="text/html" charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="cache-control" content="no-cache">

<!-- Bootstrap 4 CDN -->
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MDdH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
<script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FgpCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-
UO2eT0CpHqdSjQ6hJty5KVphtPhzWj9W01clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgyd0p3pXBlrRibZUAYoIIy6OrQ6VrjIEaFf/nJGzIxFdsf4x0xIM+B07jRM" crossorigin="anonymous"></script>

<!-- Fontawesome CDN -->
<link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">

<!-- JQuery-Confirm -->
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

<style>
/* BASIC */
html, body{
    height: 100%; letter-spacing: 0.05em;
    font-family: Microsoft JhengHei;
}

/* STRUCTURE */
.container{
    height: 100%;
}

.wrapper{
    min-height: 100%; width: 100%;
    display: flex; flex-direction: column; justify-content: center; align-items: center;
}

#formContent{
    width: 40%; padding: 2em 2em 1.5em 2em;
    background-color: #FFFFFF;
    position: relative; text-align: center;
    -webkit-box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); -webkit-border-
radius: 15px; border-radius: 15px;
}

/* DETAILED */
.form-group{
    justify-content: center;
}

hr{
    height: 0.05em;
    background-color: #2E317C;
}

.input-group-prepend, input{
    margin: 0.25em 0;
}

input{
    width: 75%; height: 2.5em; border: 0;
    background-color: #F0F5E5;
    text-align: center; display: inline-block;
    -webkit-border-radius: 5px; border-radius: 5px;
}

input:focus{
    border: 2.5px solid #2E317C;
}
```

```

#signIn{
  margin: -0.25em;
}

.icon{
  width: 7.5em; height: 5em;
}

/* ANIMATIONS */
@-webkit-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@-moz-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@keyframes fadeIn{from{opacity:0;}to{opacity:1;}}

.fadeIn{
  opacity:0;
  -webkit-animation:fadeIn ease-in 1; -moz-animation:fadeIn ease-in 1; animation:fadeIn ease-in 1;
  -webkit-animation-duration: 1s; -moz-animation-duration: 1s; animation-duration: 1s;
  -webkit-animation-fill-mode: forwards; -moz-animation-fill-mode: forwards; animation-fill-mode: forwards;
}

.fadeIn.first{
  -webkit-animation-delay: 0.1s; -moz-animation-delay: 0.1s; animation-delay: 0.1s;
}
.fadeIn.second{
  -webkit-animation-delay: 0.3s; -moz-animation-delay: 0.3s; animation-delay: 0.3s;
}
.fadeIn.third{
  -webkit-animation-delay: 0.5s; -moz-animation-delay: 0.5s; animation-delay: 0.5s;
}
.fadeIn.fourth{
  -webkit-animation-delay: 0.7s; -moz-animation-delay: 0.7s; animation-delay: 0.7s;
}

/* RESPONSIVE */
@media screen and (max-width: 800px){
  #formContent{
    width: 85%;
  }
}
...
...
...

```

低 遺漏或不安全的跨頁框 Scripting 防禦 ①

目錄

問題 1 / 1

目錄

遺漏或不安全的跨頁框 Scripting 防禦

嚴重性：	低
CVSS 評分：	5.0
URL：	http://kit.geohealth.tw/
實體：	kit.geohealth.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 DENY 或 SAMEORIGIN 值使用 "X-Frame-Options" 標頭

推論： AppScan 偵測到遺漏 X-Frame-Options 回應或包含不安全的值，這會容許跨頁框 Scripting 攻擊

測試要求和回應：

```
GET /main.php?project_id1=1234 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Referer: http://kit.geohealth.tw/main.php
Cookie: PHPSESSID=nv04crtbcdldvrqtasn7h9ee81
Host: kit.geohealth.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 62487
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:26:34 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
```

```
<!DOCTYPE html>
<html>
<head>
  <title>          總覽儀表板</title>
  <meta http-equiv="Content-Type" content="text/html" charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta http-equiv="cache-control" content="no-cache">

  <!-- Bootstrap 4 CDN -->
  <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
  integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
  <script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
  FgppCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
  <script src="https://cdn.jsdelivr.net/npm/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-
  UO2eT0CpHgdsJQ6hJty5KVphtPhzWj9WO1clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
  <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
  JjSmVgyd0p3pXB1rRibZUAYoIIy6OrQ6VrjIEaFF/nJGzIxFSdF4x0xIM+B07jRM" crossorigin="anonymous"></script>

  <!-- Fontawesome CDN -->
  <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
  mZrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">

  <!-- JQuery-Confirm -->
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/jquery-confirm/3.2.2/jquery-confirm.min.css">
  <script src="https://cdn.jsdelivr.net/npm/jquery-confirm/3.2.2/jquery-confirm.min.js"></script>

  <!-- loadash -->
  <script src="https://cdn.jsdelivr.net/npm/lodash@4.17.10/lodash.min.js"></script>

  <style>
    html{
      min-height: 100%;
      font-family: Microsoft JhengHei; position: relative;
    }

    body{
      padding-top: 100px; padding-bottom: 125px;
    }

    .wrap{
      width: 100%; margin: 20px auto;
      display: inline-block; position: relative; text-align: center;
    }

    .title{
      width: 100%; top: 15%; letter-spacing: 0.05em;
      color: #2E317C;
      font-size: 1.75em; text-align: center; position: absolute;
    }

    .modal{
      width: 30%; left: 35%; top: 20%
    }

    .row{
      width: 80%; margin: 0px auto;
    }

    .btn, .input-group-text{
      font-size: 0.95em;
    }
  </style>
```

```

.icon{
    width: 7.5em;
}

.container{
    width: 75%; margin: 10px auto; letter-spacing: 0.05em;
    font-size: 0.8em; align-content: center;
}

td{
    line-height: 2.5em;
    vertical-align: middle;
}
</style>

<script>
$(document).ready(function(){
    $.ajax({
        type: "POST",
        dataType: "json",
        url: "",
        data: {fetchProject: 1},
        success: function(data){
            console.log(data);

            for($i=0; $i<data.length; $i++){
                var row_n=document.getElementById("project_list").rows.length-1;
                var append_row=document.getElementById("project_list").insertRow(row_n);

                append_row.insertCell(0).innerHTML=data[$i]["project_id"];
                append_row.insertCell(1).innerHTML=data[$i]["project_name"];
                append_row.insertCell(2).innerHTML=data[$i]["name"];
                append_row.insertCell(3).innerHTML=data[$i]["sample_size"];

                if(data[$i].active==0){
                    append_row.insertCell(4).innerHTML="<span style='padding: 10%; color: #FFFFFF; background-color: #003B83; border-
radius: 5px'><b>D 關閉</b></span>";
                }else if(data[$i].active==1){
                    append_row.insertCell(4).innerHTML="<span style='padding: 10%; color: #FFFFFF; background-color: orange; border-
radius: 5px'><b>A 開啟</b></span>";
                }else if(data[$i].active==2){

            ...
            ...
            ...

```

低 應用程式中找到不必要的 HTTP 回應標頭 ①

目錄

問題 1 / 1

目錄

應用程式中找到不必要的 HTTP 回應標頭

嚴重性： **低**

CVSS 評分： 5.0

URL： <http://kit.geohealth.tw/>

實體： / (Page)

風險： 有可能收集 Web 應用程式相關的機密性資訊，如：使用者名稱、密碼、機器名稱及/或機密檔案位置

原因： 不安全的 Web 應用程式設計或配置

修正： 請勿容許機密性資訊洩漏。

推論： 回應包含不必要的標頭，這可能協助攻擊者規劃進一步的攻擊。

測試要求和回應：

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Connection: keep-alive
Host: kit.geohealth.tw
Upgrade-Insecure-Requests: 1
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=0.9
Accept-Language: en-US

HTTP/1.1 200 OK
Content-Length: 8321
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=0g2507e04n5p6vkdt7crt4521; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:26:52 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate

<!DOCTYPE html>
<html>
<head>
<title>      幼兒點日記管理</title>
<meta http-equiv="Content-Type" content="text/html" charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="cache-control" content="no-cache">

<!-- Bootstrap 4 CDN -->
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MDdH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
<script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FgpCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-
UO2eT0CpHgdS3Q6hJty5KvphtPhzWj9W01clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgdy0p3pXBlrRibZUAYoIIy6OrQ6VrjIEaFf/nJGzIxFdsf4x0xIM+B07jRM" crossorigin="anonymous"></script>

<!-- Fontawesome CDN -->
<link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">

<!-- JQuery-Confirm -->
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

<style>
/* BASIC */
html, body{
height: 100%; letter-spacing: 0.05em;
font-family: Microsoft JhengHei;
}

/* STRUCTURE */
.container{
height: 100%;
}

.wrapper{
min-height: 100%; width: 100%;
display: flex; flex-direction: column; justify-content: center; align-items: center;
}

#formContent{
width: 40%; padding: 2em 2em 1.5em 2em;
background-color: #FFFFFF;
position: relative; text-align: center;
-webkit-box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); -webkit-border-
radius: 15px; border-radius: 15px;
}

/* DETAILED */
.form-group{
justify-content: center;
}
```



```

hr{
  height: 0.05em;
  background-color: #2E317C;
}

.input-group-prepend, input{
  margin: 0.25em 0;
}

input{
  width: 75%; height: 2.5em; border: 0;
  background-color: #F0F5E5;
  text-align: center; display: inline-block;
  -webkit-border-radius: 5px; border-radius: 5px;
}

input:focus{
  border: 2.5px solid #2E317C;
}

#signIn{
  margin: -0.25em;
}

.icon{
  width: 7.5em; height: 5em;
}

/* ANIMATIONS */
@-webkit-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@-moz-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@keyframes fadeIn{from{opacity:0;}to{opacity:1;}}

.fadeIn{
  opacity:0;
  -webkit-animation:fadeIn ease-in 1; -moz-animation:fadeIn ease-in 1; animation:fadeIn ease-in 1;
  -webkit-animation-duration: 1s; -moz-animation-duration: 1s; animation-duration: 1s;
  -webkit-animation-fill-mode: forwards; -moz-animation-fill-mode: forwards; animation-fill-mode: forwards;
}

.fadeIn.first{
  -webkit-animation-delay: 0.1s; -moz-animation-delay: 0.1s; animation-delay: 0.1s;
}
.fadeIn.second{
  -webkit-animation-delay: 0.3s; -moz-animation-delay: 0.3s; animation-delay: 0.3s;
}
.fadeIn.third{
  -webkit-animation-delay: 0.5s; -moz-animation-delay: 0.5s; animation-delay: 0.5s;
}
.fadeIn.fourth{
  -webkit-animation-delay: 0.7s; -moz-animation-delay: 0.7s; animation-delay: 0.7s;
}

/* RESPONSIVE */
@media screen and (max-width: 800px){
  #formConte
...
...
...

```

低

檢查是否有 SRI（子資源完整性）支援 ④

目錄

問題 1 / 4

目錄

檢查是否有 SRI（子資源完整性）支援

嚴重性：**低**

CVSS 評分：5.0

URL：<http://kit.geohealth.tw/>

實體：(Page)

風險：假設第三方伺服器已受損，網站的內容/行為會變更

原因：不支援 SRI（子資源完整性）

修正：將每一個第三方 Script/鏈結元素支援新增至 SRI（子資源完整性）。

推論： 第三方鏈結/Script 沒有瀏覽器的完整性屬性，來確認它們未受損

測試要求和回應：

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Connection: keep-alive
Host: kit.geohealth.tw
Upgrade-Insecure-Requests: 1
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=0.9
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Content-Length: 8321
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=3nbdsenbp1j6s4e64onuok6l07; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:26:34 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
```

```
<!DOCTYPE html>
<html>
<head>
<title> 幼兒點日記管理</title>
<meta http-equiv="Content-Type" content="text/html" charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="cache-control" content="no-cache">
```

```
<!-- Bootstrap 4 CDN -->
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
<script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FgpCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-
UO2eT0CpHqdSjQ6hJty5KVphtPhzWj9W01clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgy0p3pXBlrRibZUAYoIIy6OrQ6VrjIEaFf/nJGzIxFdsf4x0xIM+B07jRM" crossorigin="anonymous"></script>
```

```
<!-- Fontawesome CDN -->
<link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">
```

```
<!-- Jquery-Confirm -->
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>
```

```
<style>
/* BASIC */
html, body{
height: 100%; letter-spacing: 0.05em;
font-family: Microsoft JhengHei;
}

/* STRUCTURE */
.container{
height: 100%;
}
```

```

.wrapper{
  min-height: 100%; width: 100%;
  display: flex; flex-direction: column; justify-content: center; align-items: center;
}

#formContent{
  width: 40%; padding: 2em 2em 1.5em 2em;
  background-color: #FFFFFF;
  position: relative; text-align: center;
  -webkit-box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); -webkit-border-
radius: 15px; border-radius: 15px;
}

/* DETAILED */
.form-group{
  justify-content: center;
}

hr{
  height: 0.05em;
  background-color: #2E317C;
}

.input-group-prepend, input{
  margin: 0.25em 0;
}

input{
  width: 75%; height: 2.5em; border: 0;
  background-color: #F0F5E5;
  text-align: center; display: inline-block;
  -webkit-border-radius: 5px; border-radius: 5px;
}

input:focus{
  border: 2.5px solid #2E317C;
}

#signIn{
  margin: -0.25em;
}

.icon{
  width: 7.5em; height: 5em;
}

/* ANIMATIONS */
@-webkit-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@-moz-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@keyframes fadeIn{from{opacity:0;}to{opacity:1;}}

.fadeIn{
  opacity:0;
  -webkit-animation:fadeIn ease-in 1; -moz-animation:fadeIn ease-in 1; animation:fadeIn ease-in 1;
  -webkit-animation-duration: 1s; -moz-animation-duration: 1s; animation-duration: 1s;
  -webkit-animation-fill-mode: forwards; -moz-animation-fill-mode: forwards; animation-fill-mode: forwards;
}

.fadeIn.first{
  -webkit-animation-delay: 0.1s; -moz-animation-delay: 0.1s; animation-delay: 0.1s;
}

.fadeIn.second{
  -webkit-animation-delay: 0.3s; -moz-animation-delay: 0.3s; animation-delay: 0.3s;
}

.fadeIn.third{
  -webkit-animation-delay: 0.5s; -moz-animation-delay: 0.5s; animation-delay: 0.5s;
}

.fadeIn.fourth{
  -webkit-animation-delay: 0.7s; -moz-animation-delay: 0.7s; animation-delay: 0.7s;
}

/* RESPONSIVE */
@media screen and (max-width: 800px){
  #formConte
...
...
...

```

檢查是否有 SRI（子資源完整性）支援

嚴重性：	低
CVSS 評分：	5.0
URL：	http://kit.geohealth.tw/main.php
實體：	main.php (Page)
風險：	假設第三方伺服器已受損，網站的內容/行為會變更
原因：	不支援 SRI（子資源完整性）
修正：	將每一個第三方 Script/鏈結元素支援新增至 SRI（子資源完整性）。

推論： 第三方鏈結/Script 沒有瀏覽器的完整性屬性，來確認它們未受損
測試要求和回應：

```
GET /main.php?project_id=1234 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Referer: http://kit.geohealth.tw/main.php
Cookie: PHPSESSID=nv04crtbcdldvrtasn7h9ee81
Host: kit.geohealth.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 62487
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:26:34 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
  <title>      總覽儀表板</title>
  <meta http-equiv="Content-Type" content="text/html" charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta http-equiv="cache-control" content="no-cache">

  <!-- Bootstrap 4 CDN -->
  <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
  <script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FggCb/KJQ1LNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
  <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-
UO2eT0CpHqdsJQ6hJty5KVphtPhzWj9WO1clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
  <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgyd0p3pXb1rRibZUAYoIIy6OrQ6VrjIEaFf/njGzIxFdsf4x0xIM+B07jRM" crossorigin="anonymous"></script>

  <!-- Fontawesome CDN -->
  <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">

  <!-- JQuery-Confirm -->
  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
  <script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

  <!-- loadash -->
  <script src="https://cdn.jsdelivr.net/npm/lodash@4.17.10/lodash.min.js"></script>

<style>
  html{
    min-height: 100%;
    font-family: Microsoft JhengHei; position: relative;
  }
}
```

```

body{
  padding-top: 100px; padding-bottom: 125px;
}

.wrap{
  width: 100%; margin: 20px auto;
  display: inline-block; position: relative; text-align: center;
}

.title{
  width: 100%; top: 15%; letter-spacing: 0.05em;
  color: #2E317C;
  font-size: 1.75em; text-align: center; position: absolute;
}

.modal{
  width: 30%; left: 35%; top: 20%
}

.row{
  width: 80%; margin: 0px auto;
}

.btn, .input-group-text{
  font-size: 0.95em;
}

.icon{
  width: 7.5em;
}

.container{
  width: 75%; margin: 10px auto; letter-spacing: 0.05em;
  font-size: 0.8em; align-content: center;
}

td{
  line-height: 2.5em;
  vertical-align: middle;
}
</style>

<script>
$(document).ready(function(){
  $.ajax({
    type: "POST",
    dataType: "json",
    url: "",
    data: {fetchProject: 1},
    success: function(data){
      console.log(data);

      for($i=0; $i<data.length; $i++){
        var row_n=document.getElementById("project_list").rows.length-1;
        var append_row=document.getElementById("project_list").insertRow(row_n);

        append_row.insertCell(0).innerHTML=data[$i]["project_id"];
        append_row.insertCell(1).innerHTML=data[$i]["project_name"];
        append_row.insertCell(2).innerHTML=data[$i]["name"];
        append_row.insertCell(3).innerHTML=data[$i]["sample_size"];

        if(data[$i].active==0){
          append_row.insertCell(4).innerHTML="<span style='padding: 10%; color: #FFFFFF; background-color: #003B83; border-
radius: 5px'><b>D 關閉</b></span>";
        }else if(data[$i].active==1){
          append_row.insertCell(4).innerHTML="<span style='padding: 10%; color: #FFFFFF; background-color: orange; border-
radius: 5px'><b>
...
...
...

```

檢查是否有 SRI (子資源完整性) 支援

嚴重性： **低**

CVSS 評分： 5.0

URL： <http://kit.geohealth.tw/preview.php>

實體： preview.php (Page)

風險： 假設第三方伺服器已受損，網站的內容/行為會變更

原因： 不支援 SRI (子資源完整性)

修正： 將每一個第三方 Script/鏈結元素支援新增至 SRI (子資源完整性)。

推論： 第三方鏈結/Script 沒有瀏覽器的完整性屬性，來確認它們未受損

測試要求和回應：

```
GET /preview.php?project_id=110017 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Referer: http://kit.geohealth.tw/main.php
Cookie: PHPSESSID=nv04crtbcdldvrgtasn7h9ee81
Connection: keep-alive
Host: kit.geohealth.tw
Upgrade-Insecure-Requests: 1
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=0.9
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 53172
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:27:42 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8
```

```
<!DOCTYPE html>
<html>
<head>
  <title>專案預覽</title>
  <meta http-equiv="Content-Type" content="text/html" charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta http-equiv="cache-control" content="no-cache">

  <!-- Bootstrap 4 CDN -->
  <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
  <script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FggCb/KJQlLnFou91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
  <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-
UO2eT0CpHqdsJQ6hJty5KVphtPhzWj9W01clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
  <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgyd0p3pXB1rRibZUAYoIIy60Rq6VrjIEaFf/njGzIxFdsf4x0xIM+B07jRM" crossorigin="anonymous"></script>

  <!-- Fontawesome CDN -->
  <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">

  <!-- JQuery-Confirm -->
  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
  <script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

  <!-- loadash -->
  <script src="https://cdn.jsdelivr.net/npm/lodash@4.17.10/lodash.min.js"></script>
  <!-- Dexie -->
  <script src="https://capi.geohealth.tw/js/dexie.js"></script>

<style>
  html{
    min-height: 100%;
    font-family: Microsoft JhengHei; position: relative;
  }
```

```

body{
  padding-top: 100px; padding-bottom: 125px;
}

.wrap{
  width: 100%; margin: 20px auto;
  display: inline-block; position: relative; text-align: center;
}

#title{
  width: 12.5%;
}

.title{
  width: 100%; top: 15%; letter-spacing: 0.05em;
  color: #2E317C;
  font-size: 1.75em; text-align: center; position: absolute;
}

.infobar{
  letter-spacing: 0.1em; padding-bottom: 2em;
  font-size: 0.9em; text-align: right;
}

.container{
  width: 60%; margin: 20px auto;
  align-content: center;
}

.card{
  background-color: #FFFFBB;
}

.card-body{
  line-height: 1.75em; letter-spacing: 0.05em; padding: 2.5em 5% 0 5%;
  text-align: left;
}

.icon{
  width: 8.5em;
}

/* RESPONSIVE */
@media screen and (max-width: 800px){
  body{
    padding-bottom: 150px;
  }

  .wrap{
    margin: auto;
  }

  #title{
    width: 7.5em;
  }

  .title{
    font-size: 1.15em;
  }

  .container{
    width: 100%; margin: auto; margin-top: 6.25%;
  }

  .infobar{
    font-size: 0.6em;
  }

  .card-body{
    margin-top: 5%; padding: 2.5%;
    font-size: 0.6em;
  }

  .input-group-text{
    padding-left: 2.5%;
  }

  .row{
    width: 90%; margin-bottom: 1.5em;
  }

  .icon{
    width: 6em;
  }

```

```

    }
  }
</style>

<script>
  $(document).ready(function() {
    $.ajax({
      type: "POST",
      dataType: "json",
      url: "",
      data: {fetchProject: 1},
      success: function(da
...
...
...

```

問題 4 / 4

目錄

檢查是否有 SRI (子資源完整性) 支援

嚴重性：	低
CVSS 評分：	5.0
URL：	http://kit.geohealth.tw/index.php
實體：	index.php (Page)
風險：	假設第三方伺服器已受損，網站的內容/行為會變更
原因：	不支援 SRI (子資源完整性)
修正：	將每一個第三方 Script/鏈結元素支援新增至 SRI (子資源完整性)。

推論： 第三方鏈結/Script 沒有瀏覽器的完整性屬性，來確認它們未受損

測試要求和回應：

```

GET /index.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Referer: http://kit.geohealth.tw/main.php?project_id3=1234&end_date=2019-01-01
Cookie: PHPSESSID=nv04crtbcdldvrqtasn7h9ee81
Host: kit.geohealth.tw
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US

```

```

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 8321
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:26:34 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8

```

```

<!DOCTYPE html>
<html>
<head>
  <title>        幼兒點日記管理</title>
  <meta http-equiv="Content-Type" content="text/html" charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta http-equiv="cache-control" content="no-cache">

  <!-- Bootstrap 4 CDN -->
  <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
  <script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FgPcb/KJQILNfOu91ta32o/NMZxltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
  <script src="https://cdn.jsdelivr.net/npm/popper.js/1.14.7/umd/popper.min.js" integrity="sha384-

```



```

U02eT0CpHqdsJQ6hJty5KVphtPhzWj9W01clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgyd0p3pXB1rRibZUAYoIIy60rQ6VrjIEaFf/nJGzIxFDsf4x0xIM+B07jRM" crossorigin="anonymous"></script>

<!-- Fontawesome CDN -->
<link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">

<!-- JQuery-Confirm -->
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

<style>
/* BASIC */
html, body{
  height: 100%; letter-spacing: 0.05em;
  font-family: Microsoft JhengHei;
}

/* STRUCTURE */
.container{
  height: 100%;
}

.wrapper{
  min-height: 100%; width: 100%;
  display: flex; flex-direction: column; justify-content: center; align-items: center;
}

#formContent{
  width: 40%; padding: 2em 2em 1.5em 2em;
  background-color: #FFFFFF;
  position: relative; text-align: center;
  -webkit-box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); -webkit-border-
radius: 15px; border-radius: 15px;
}

/* DETAILED */
.form-group{
  justify-content: center;
}

hr{
  height: 0.05em;
  background-color: #2E317C;
}

.input-group-prepend, input{
  margin: 0.25em 0;
}

input{
  width: 75%; height: 2.5em; border: 0;
  background-color: #F0F5E5;
  text-align: center; display: inline-block;
  -webkit-border-radius: 5px; border-radius: 5px;
}

input:focus{
  border: 2.5px solid #2E317C;
}

#signIn{
  margin: -0.25em;
}

.icon{
  width: 7.5em; height: 5em;
}

/* ANIMATIONS */
@-webkit-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@-moz-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
@keyframes fadeIn{from{opacity:0;}to{opacity:1;}}

.fadeIn{
  opacity:0;
  -webkit-animation:fadeIn ease-in 1; -moz-animation:fadeIn ease-in 1; animation:fadeIn ease-in 1;
  -webkit-animation-duration: 1s; -moz-animation-duration: 1s; animation-duration: 1s;
  -webkit-animation-fill-mode: forwards; -moz-animation-fill-mode: forwards; animation-fill-mode: forwards;
}

.fadeIn.first{
  -webkit-animation-delay: 0.1s; -moz-animation-delay: 0.1s; animation-delay: 0.1s;
}

```

```
    }  
    .fadeIn.second{  
      -webkit-animation-delay: 0.3s; -moz-animation-delay: 0.3s; animation-delay: 0.3s;  
    }  
    .fadeIn.third{  
      -webkit-animation-delay: 0.5s; -moz-animation-delay: 0.5s; animation-delay: 0.5s;  
    }  
    .fadeIn.fourth{  
      -webkit-animation-delay: 0.7s; -moz-animation-delay: 0.7s; animation-delay: 0.7s;  
    }  
  
    /* RESPONSIVE */  
    @media screen and (max-width: 800px){  
      #formContent{  
        width: 85%;  
      }  
    }  
  }  
}
```

```
...  
...  
...
```

問題 1 / 1

目錄

找到可能的伺服器路徑揭露型樣

嚴重性：	參考資訊
CVSS 評分：	0.0
URL：	http://kit.geohealth.tw/main.php
實體：	main.php (Page)
風險：	有可能擷取 Web 伺服器安裝架構的絕對路徑，其可能會幫助攻擊者展開進一步攻擊，以及取得 Web 應用程式之檔案系統結構的相關資訊
原因：	未安裝協力廠商產品最新的修補程式或緊急修復程式
修正：	請下載您的 Web 伺服器或 Web 應用程式的相關安全修補程式。

推論： 回應包含伺服器上的絕對路徑及/或檔名。

測試要求和回應：

```
POST /main.php HTTP/1.1
Content-Length: 44
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
Cookie: PHPSESSID=nv04crtbcdldvrgtasn7h9ee81
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/main.php
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

project_name=1234&id=&sample_size=9876543210

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 444
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:27:41 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8

<br />
<b>Fatal error</b>: Uncaught PDOException: SQLSTATE[22007]: Invalid datetime format: 1366 Incorrect integer value: '' for column `children`.`project`.`id` at row 1 in C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\main.php:42
Stack trace:
#0 C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\main.php(42): PDOStatement->execute()
#1 {main}
  thrown in C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\main.php on line 42</b><br />
```

問題 1 / 1

目錄

遺漏「查閱者原則」安全標頭

嚴重性：[參考資訊](#)

CVSS 評分： 0.0

URL：<http://kit.geohealth.tw/>

實體： kit.geohealth.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](#)

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则，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 / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Connection: keep-alive
Host: kit.geohealth.tw
Upgrade-Insecure-Requests: 1
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=0.9
Accept-Language: en-US

HTTP/1.1 200 OK
Content-Length: 8321
Server: Microsoft-IIS/8.5
Set-Cookie: PHPSESSID=u5bos330rbfk32ja6hq49oud41; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:18:51 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate

<!DOCTYPE html>
<html>
<head>
<title>        幼兒點日記管理</title>
<meta http-equiv="Content-Type" content="text/html" charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="cache-control" content="no-cache">

<!-- Bootstrap 4 CDN -->
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T" crossorigin="anonymous">
<script src="https://code.jquery.com/jquery-3.3.1.min.js" integrity="sha256-
FgpCb/KJQlLNfOu91ta32o/NM2xltwRo8QtmkMRdAu8=" crossorigin="anonymous"></script>
<script src="https://cdn.jsdelivr.net/npm/popper.js@1.14.7/umd/popper.min.js" integrity="sha384-
UO2eT0CpHqdSJK6hJty5KVphtPhzWj9WO1clHTMGa3JDZwrnQq4sF86dIHNDz0W1" crossorigin="anonymous"></script>
<script src="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js" integrity="sha384-
JjSmVgyd0p3pXBlrRibZUAYoIIy6OrQ6VrjIEaFf/nJGzIxFdsf4x0xIM+B07jRM" crossorigin="anonymous"></script>

<!-- Fontawesome CDN -->
<link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.3.1/css/all.css" integrity="sha384-
mzrmE5qonljUremFsqc01SB46JvROS7bZs3IO2EmfFsd15uHvIt+Y8vEf7N7fWAU" crossorigin="anonymous">

<!-- JQuery-Confirm -->
```

```

<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.css">
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-confirm/3.3.2/jquery-confirm.min.js"></script>

<style>
  /* BASIC */
  html, body{
    height: 100%; letter-spacing: 0.05em;
    font-family: Microsoft JhengHei;
  }

  /* STRUCTURE */
  .container{
    height: 100%;
  }

  .wrapper{
    min-height: 100%; width: 100%;
    display: flex; flex-direction: column; justify-content: center; align-items: center;
  }

  #formContent{
    width: 40%; padding: 2em 2em 1.5em 2em;
    background-color: #FFFFFF;
    position: relative; text-align: center;
    -webkit-box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); box-shadow: 0 30px 60px 0 rgba(0,0,0,0.3); -webkit-border-
radius: 15px; border-radius: 15px;
  }

  /* DETAILED */
  .form-group{
    justify-content: center;
  }

  hr{
    height: 0.05em;
    background-color: #2E317C;
  }

  .input-group-prepend, input{
    margin: 0.25em 0;
  }

  input{
    width: 75%; height: 2.5em; border: 0;
    background-color: #F0F5E5;
    text-align: center; display: inline-block;
    -webkit-border-radius: 5px; border-radius: 5px;
  }

  input:focus{
    border: 2.5px solid #2E317C;
  }

  #signIn{
    margin: -0.25em;
  }

  .icon{
    width: 7.5em; height: 5em;
  }

  /* ANIMATIONS */
  @-webkit-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
  @-moz-keyframes fadeIn{from{opacity:0;}to{opacity:1;}}
  @keyframes fadeIn{from{opacity:0;}to{opacity:1;}}

  .fadeIn{
    opacity:0;
    -webkit-animation:fadeIn ease-in 1; -moz-animation:fadeIn ease-in 1; animation:fadeIn ease-in 1;
    -webkit-animation-duration: 1s; -moz-animation-duration: 1s; animation-duration: 1s;
    -webkit-animation-fill-mode: forwards; -moz-animation-fill-mode: forwards; animation-fill-mode: forwards;
  }

  .fadeIn.first{
    -webkit-animation-delay: 0.1s; -moz-animation-delay: 0.1s; animation-delay: 0.1s;
  }
  .fadeIn.second{
    -webkit-animation-delay: 0.3s; -moz-animation-delay: 0.3s; animation-delay: 0.3s;
  }
  .fadeIn.third{
    -webkit-animation-delay: 0.5s; -moz-animation-delay: 0.5s; animation-delay: 0.5s;
  }
  .fadeIn.fourth{
    -webkit-animation-delay: 0.7s; -moz-animation-delay: 0.7s; animation-delay: 0.7s;
  }

```

```

    }

    /* RESPONSIVE */
    @media screen and (max-width: 800px){
        #formContent{
            width: 85%;
            font-size: 0.8em;
        }
    }

```

...

應用程式錯誤 ①

目錄

問題 1 / 1

目錄

應用程式錯誤

嚴重性：[參考資訊](#)

CVSS 評分： 0.0

URL：<http://kit.geohealth.tw/main.php>

實體： search (Parameter)

風險： 有可能收集機密性除錯資訊

原因： 未對送入的參數值執行適當的範圍檢查
未執行驗證，以確定使用者輸入符合預期的資料類型

修正： 請驗證參數值是在預期的範圍內且為預期的類型。請勿輸出除錯錯誤訊息和異常狀況

推論： 應用程式已回應錯誤訊息，指出有未定義的狀態可能會顯現機密性資訊。

測試要求和回應：

```

POST /main.php HTTP/1.1
Content-Length: 26
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
Host: kit.geohealth.tw
Cookie: PHPSESSID=nv04crtbcdldvrqtasn7h9ee81
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://kit.geohealth.tw/main.php
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

searchProject=1&search=%27

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Pragma: no-cache
Content-Length: 549
Cache-Control: no-store, no-cache, must-revalidate
X-Powered-By: PHP/7.0.27
Date: Wed, 28 Jul 2021 10:27:53 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: text/html; charset=UTF-8

<br />
<b>Fatal error</b>: Uncaught PDOException: SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in

```

```
your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '%' or
name LIKE '%'' at line 1 in C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\main.php:62
Stack trace:
#0 C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\main.php(62): PDOStatement->execute()
#1 {main}
  thrown in <b>C:\inetpub\wwwroot\00_domain\kit.geohealth.tw\main.php</b> on line <b>62</b><br />
```

修正建議

高 傳送機密性資訊時，一律使用 SSL 和 POST（主體）參數。

目錄

此作業所修正的問題類型

- 未加密的登入要求
- 查詢中的 Password 參數

一般

未加密的登入要求

在登入頁面或任何用來傳輸使用者認證或其他敏感性資訊的頁面上強制實施 SSL。即使整個網站不使用 SSL，也必須使用 SSL 進行登入。此外，若要協助防止網路釣魚攻擊，請確定該登入頁面使用 SSL。SSL 會允許使用者向其連線的伺服器驗證其伺服器的身分。如果登入頁面使用 SSL，使用者即可確定他們是與正確的后端系統交談。網路釣魚攻擊一般會將使用者重新導向至未具備由獲授權供應商發出之有效受信任伺服器憑證的網站。

查詢中的 Password 參數

在登入頁面或任何用來傳輸使用者認證或其他敏感性資訊的頁面上強制實施 SSL。即使整個網站不使用 SSL，也必須使用 SSL 進行登入。此外，若要協助防止網路釣魚攻擊，請確定該登入頁面使用 SSL。SSL 會允許使用者向其連線的伺服器驗證其伺服器的身分。如果登入頁面使用 SSL，使用者即可確定他們是與正確的后端系統交談。網路釣魚攻擊一般會將使用者重新導向至未具備由獲授權供應商發出之有效受信任伺服器憑證的網站。

高 檢查危險字元注入可能的解決方案

目錄

此作業所修正的問題類型

- SQL 注入
- 找到資料庫錯誤型樣

一般

SQL 注入

搭配使用預存程序與參數以防止在資料中注入 SQL 指令，或至少搭配使用預存程序與不容許注入程式碼的參數化資料庫呼叫。請勿在預存程序中包括任何動態 SQL 執行。

甚至更好的解決方案是使用「休眠」或「實體架構」這類 ORM（與物件相關的對映）架構（若您的平台上有的話）。

確定已驗證和過濾伺服器端上的所有使用者輸入，這不只是禁止單引號 (') 和雙引號s (") 這類不正確字元，而是只容許安全字元。根據要求中參數的預期值，來縮小定義安全字元集。

在所有使用者輸入上使用跳出函數。

配置完成必要作業所需之最低資料庫專用權的應用程式身分。強化資料庫伺服器來停用任何不需要的功能，例如 Shell 指令。

找到資料庫錯誤型樣

以下是幾種減輕風險的技巧：

[1] 策略：程式庫或架構

使用檢查過且不容許發生此弱點的程式庫或架構，或提供使其更容易避免的建構項。

[2] 策略：參數化

如果可行，請使用結構化機制來自動強制分開資料與程式碼。這些機制可能可以自動提供相關的引用、編碼和驗證，而不會在每次產生輸出時，都依賴開發人員來提供這項功能。

[3] 策略：環境強化 使用完成必要作業所需的最低專用權，來執行程式碼。

[4] 策略：輸出編碼

如果儘管有風險，您還是需要使用動態產生的查詢字串或指令，適當地括住引數且避免在這些引數內使用任何特殊字元。

[5] 策略：輸入驗證

假設所有輸入都是惡意的。請使用「接受已知良好」輸入驗證策略：嚴格符合規格的可接受輸入白名單。拒絕未嚴格符合規格的任何輸入，或將其轉換成嚴格符合規格者。請勿只靠排除惡意或形態異常的輸入。不過，在偵測潛在攻擊或判斷哪些輸入因形態異常而應該斷然拒絕時，黑名單就很有用。

以下是保護 Web 應用程式免於遭受 SQL 注入攻擊的兩種可能方式：

[1] 使用儲存程序，而不用動態建置的 SQL 查詢字串。

參數傳給 SQL Server 儲存程序的方式，會防止使用單引號和連字號。

如何在 ASP.NET 中使用儲存程序的範例如下：

```
' Visual Basic example Dim DS As DataSet Dim MyConnection As SqlConnection Dim MyCommand As SqlCommand Dim SelectCommand As String = "select * from users where username = @username" ... MyCommand.SelectCommand.Parameters.Add(New SqlParameter("@username", SqlDbType.NVarChar, 20)) MyCommand.SelectCommand.Parameters("@username").Value = UserNameField.Value // C# example String selectCmd = "select * from Authors where state = @username"; SqlConnection myConnection = new SqlConnection("server=..."); SqlDataAdapter myCommand = new SqlDataAdapter(selectCmd, myConnection); myCommand.SelectCommand.Parameters.Add(new SqlParameter("@username", SqlDbType.NVarChar, 20)); myCommand.SelectCommand.Parameters["@username"].Value = UserNameField.Value;
```

[2] 您可以利用驗證控制項，將輸入驗證新增到「Web 表單」頁面中。驗證控制項提供適用於標準驗證之所有一般類型的簡易使用機制（例如：測試日期是否有效，或值是否在範圍內），以及用來提供自訂編寫驗證的方式。

此外，驗證控制項也可讓您完整自訂向使用者顯示錯誤資訊的方式。驗證控制項可以搭配「Web 表單」頁面類別檔所處理的任何控制項來使用，其中包括 HTML 和 Web 伺服器控制項。

如果要確定使用者輸入只包含有效值，您可以使用下列其中一個驗證控制項：

a. "RangeValidator"：檢查使用者的輸入（值）是否在指定的上下界限之間。

您可以檢查數字、英文字母和日期之配對內的範圍。

b. "RegularExpressionValidator"：檢查輸入是否符合正規表示式所定義的型樣。

這類型的驗證可讓您檢查可預期的字元序列，例如：社會保險號碼、電子郵件位址、電話號碼、郵遞區號等等中的字元序列。

重要注意事項：驗證控制項不會封鎖使用者輸入，或變更頁面處理流程；它們只會設定錯誤狀態，以及產生錯誤訊息。在執行進一步的應用程式專屬動作之前，程式設計師負責測試程式碼中的控制項狀態。

檢查使用者輸入有效性有兩種方式：

1. 測試一般錯誤狀態：

在您的程式碼中，測試頁面的 IsValid 內容。

這個內容會累積頁面上所有驗證控制項的 IsValid 內容值（使用邏輯 AND）。如果其中一個驗證控制項設為無效，頁面內容便會傳回 False。

2. 測試個別控制項的錯誤狀態：

在迴圈中處理頁面的驗證器集合，集合中含有指向所有驗證控制項的參照。

之後，您便可以檢查每個驗證控制項的 IsValid 內容。

** 備妥陳述式：

保護您的應用程式免於遭受 SQL 注入（亦即，惡意竄改 SQL 參數）有三種可能的方式。

請利用下列方式，而非動態建置 SQL 陳述式：

[1] PreparedStatement，經過前置編譯而存放在 PreparedStatement 物件儲存區中。

PreparedStatement 定義用來登錄輸入參數的設定元，輸入參數相容於支援的 JDBC SQL 資料類型。

例如，setString 應該用於 VARCHAR 或 LONGVARCHAR 類型的輸入參數（請參閱 Java API，以取得進一步的詳細資料）。

這個設定輸入參數的方式，可以防止攻擊者注入不正確的字元（如單引號）來操作 SQL 陳述式。

如何使用 J2EE 中之 PreparedStatement 的範例：

```
// J2EE PreparedStatement Example // Get a connection to the database Connection myConnection; if (isDataSourceEnabled()) { // using the
```

DataSource to get a managed connection Context ctx = new InitialContext(); myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword); } else { try { // using the DriverManager to get a JDBC connection Class.forName(jdbcDriverClassName); myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword); } catch (ClassNotFoundException e) { ... } ... try { PreparedStatement myStatement = myConnection.prepareStatement("select * from users where username = ?"); myStatement.setString(1, userNameField); ResultSet rs = myStatement.executeQuery(); ... rs.close(); } catch (SQLException sqlException) { ... } finally { myStatement.close(); myConnection.close(); }

[2] CallableStatement，延伸 PreparedStatement 來執行資料庫 SQL 儲存程序。

這個類別繼承 PreparedStatement 的輸入設定元（請參閱上面的 [1]）。

下列範例假設已建立好這個資料庫儲存程序：

```
CREATE PROCEDURE select_user (@username varchar(20))
```

```
AS SELECT * FROM USERS WHERE USERNAME = @username;
```

如何利用 J2EE 中的 CallableStatement 來執行上述儲存程序的範例：

```
// J2EE PreparedStatement Example // Get a connection to the database Connection myConnection; if (isDataSourceEnabled()) { // using the DataSource to get a managed connection Context ctx = new InitialContext(); myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword); } else { try { // using the DriverManager to get a JDBC connection Class.forName(jdbcDriverClassName); myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword); } catch (ClassNotFoundException e) { ... } ... try { PreparedStatement myStatement = myConnection.prepareStatement("select * from users where username = ?"); myStatement.setString(1, userNameField); myStatement.registerOutParameter(1, Types.VARCHAR); ResultSet rs = myStatement.executeQuery(); ... rs.close(); } catch (SQLException sqlException) { ... } finally { myStatement.close(); myConnection.close(); }
```

[3] Entity Bean，在持續性儲存庫機制中代表 EJB 商業物件。

Entity Bean 有兩種類型：Bean 管理和儲存器管理。

當使用 Bean 管理的持續性時，開發人員負責撰寫存取資料庫的 SQL 程式碼（請參閱上述 [1] 和 [2] 區段）。

當使用儲存器管理的持續性時，EJB 儲存器會自動產生 SQL 程式碼。

因此，儲存器要負責防止惡意嘗試竄改產生的 SQL 程式碼。

如何使用 J2EE 中之 Entity Bean 的範例：

```
// J2EE EJB Example try { // lookup the User home interface UserHome userHome = (UserHome)context.lookup(User.class); // find the User remote interface User = userHome.findByPrimaryKey(new UserKey(userNameField)); ... } catch (Exception e) { ... }
```

建議的 Java 工具

N/A

參照

<https://docs.oracle.com/javase/7/docs/api/java/sql/PreparedStatement.html>

<https://docs.oracle.com/javase/7/docs/api/java/sql/CallableStatement.html>

** 驗證輸入資料：

雖然為了使用者的方便，可以在用戶端層提供資料驗證，但必須利用 Servlet，在伺服器層執行資料驗證。

用戶端驗證原本就不安全，因為它們可以輕易略過，例如：停用 JavaScript。

好的設計通常需要 Web 應用程式架構提供伺服器端公用程式常式來驗證下列項目：

[1] 必要欄位

[2] 欄位資料類型（依預設，所有 HTTP 要求參數都是 String）

[3] 欄位長度

[4] 欄位範圍

[5] 欄位選項

[6] 欄位型樣

[7] Cookie 值

[8] HTTP 回應

在實務中，好的做法是在 "Validator" 公用程式類別中將上述常式當作靜態方法來實作。下列各節說明範例驗證器類別

[1] 必要欄位

一律檢查確認欄位不是空值，欄位長度大於零，且不含在前端及尾端的空格。

如何驗證必要欄位的範例：

```
// Java example to validate required fields public Class Validator { ... public static boolean validateRequired(String value) { boolean isFieldValid = false; if (value != null && value.trim().length() > 0) { isFieldValid = true; } return isFieldValid; } ... } ... String fieldValue = request.getParameter("fieldName"); if (Validator.validateRequired(fieldValue)) { // fieldValue is valid, continue processing request ... }
```

[2] 欄位資料類型

在 Web 應用程式中，所輸入的輸入參數設定不良。例如，所有 HTTP 要求參數或 Cookie 值都是 String 類型。開發人員負責確認輸入的資料類型正確。

請利用 Java 基本封套類別來檢查欄位值是否能安全轉換成所需要的基本資料類型。

如何驗證數值欄位（int 類型）的範例：

```
// Java example to validate that a field is an int number public Class Validator { ... public static boolean validateInt(String value) { boolean isFieldValid = false; try { Integer.parseInt(value); isFieldValid = true; } catch (Exception e) { isFieldValid = false; } return isFieldValid; } ... } ... // check if the HTTP request parameter is of type int String fieldValue = request.getParameter("fieldName"); if (Validator.validateInt(fieldValue)) { // fieldValue is valid, continue processing request ... }
```

在實務中，好的做法是將所有 HTTP 要求參數轉換成它們的相關資料類型。例如，開發人員應該將要求參數的 "integerValue" 儲存在要求屬性中，再依照下列範例所示來使用它：

```
// Example to convert the HTTP request parameter to a primitive wrapper data type // and store this value in a request attribute for further processing String fieldValue = request.getParameter("fieldName"); if (Validator.validateInt(fieldValue)) { // convert fieldValue to an Integer Integer integerValue = Integer.getInteger(fieldValue); // store integerValue in a request attribute request.setAttribute("fieldName", integerValue); } ... // Use the request attribute for further processing Integer integerValue = (Integer)request.getAttribute("fieldName"); ...
```

- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

一律確定輸入參數（HTTP 要求參數或 Cookie 值）在長度下限及/或長度上限的範圍內。

```
// Example to validate the field length public Class Validator { ... public static boolean validateLength(String value, int minLength, int maxLength)
{ String validatedValue = value; if (!validateRequired(value)) { validatedValue = ""; } return (validatedValue.length() >= minLength &&
validatedValue.length() <= maxLength); } ... } ... String userName = request.getParameter("userName"); if
(Validator.validateRequired(userName)) { if (Validator.validateLength(userName, 8, 20)) { // userName is valid, continue further processing ... } }
```

一律確定輸入參數在函數需求定義的範圍內。

```
// Example to validate the field range public Class Validator { ... public static boolean validateRange(int value, int min, int max) { return (value >= min && value <= max); } ... } ... String fieldValue = request.getParameter("numberOfChoices"); if (Validator.validateRequired(fieldValue)) { if (Validator.validateInt(fieldValue)) { int numberOfChoices = Integer.parseInt(fieldValue); if (Validator.validateRange(numberOfChoices, 10, 20)) { // numberOfChoices is valid, continue processing request ... } } }
```

Web 應用程式通常會向使用者呈現一組可供選擇的選項（例如：使用 **SELECT HTML** 標籤），但無法執行伺服器端驗證來確保所選的值是容許的選項之一。請記住，惡意的使用者可以輕易修改任何選項值。請一律對照函數需求所定義容許的選項來驗證所選的使用者值。

```
// Example to validate user selection against a list of options
public Class Validator { ...
    public static boolean validateOption(Object[] options,
    Object value) {
        boolean isValidValue = false;
        try {
            List list = Arrays.asList(options);
            if (list != null) {
                isValidValue = list.contains(value);
            }
        } catch (Exception e) {}
        return isValidValue;
    } ... }

// Allowed options
String[] options = {"option1", "option2", "option3"};

// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request ...
}
```

一律檢查使用者輸入是否符合功能需求所定義的型樣。比方說，如果 `userName` 欄位只應接受英數字元，且不區分大小寫，請使用下列正規表示式：`^[a-zA-Z0-9]*$`

```
// Example to validate that a given value matches a specified pattern // using the Apache regular expression package import
org.apache.regexp.RE; import org.apache.regexp.RESyntaxException; public Class Validator { ... public static boolean matchPattern(String
value, String expression) { boolean match = false; if (validateRequired(expression)) { RE r = new RE(expression); match = r.match(value); }
return match; } ... } // Verify that the userName request parameter is alpha-numeric String userName = request.getParameter("userName"); if
(Validator.matchPattern(userName, "[a-zA-Z0-9]*$")) { // userName is valid, continue processing request ... }
```

```
// Example to validate that a given value matches a specified pattern // using the Java 1.4 regular expression package import
java.util.regex.Pattern; import java.util.regex.Matcher; public Class Validator { ... public static boolean matchPattern(String value, String
expression) { boolean match = false; if (validateRequired(expression)) { match = Pattern.matches(expression, value); } return match; } ... }
```

請利用 `javax.servlet.http.Cookie` 物件來驗證 `Cookie` 值。依應用程式需求而定，相同的驗證規則（說明如上）也適用於 `Cookie` 值，例如：驗證必要的值、驗證長度，等等。

```
// Example to validate a required cookie value // First retrieve all available cookies submitted in the HTTP request Cookie[] cookies =
request.getCookies(); if (cookies != null) { // find the "user" cookie for (int i=0; i<cookies.length; ++i) { if (cookies[i].getName().equals("user")) { //
validate the cookie value if (Validator.validateRequired(cookies[i].getValue()) { // valid cookie value, continue processing request ... } } } }
```

[8-1] 過濾使用者輸入

< > " ' % ;) (& +

```
// Example to filter sensitive data to prevent cross-site scripting public Class Validator { ... public static String filter(String value) { if (value == null) { return null; } StringBuffer result = new StringBuffer(value.length()); for (int i=0; i<value.length(); ++i) { switch (value.charAt(i)) { case '<': result.append("&lt;"); break; case '>': result.append("&gt;"); break; case '"': result.append("&quot;"); break; case ''': result.append("&apos;"); break; case '%': result.append("%"); break; case '\\': result.append("\\"); break; case '(': result.append("("); break; case ')': result.append(")"); break; case '&': result.append("&"); break; case '+': result.append("+"); break; default: result.append(value.charAt(i)); break; } return result; } ... } // Filter the HTTP response using Validator.filter PrintWriter out = response.getWriter(); // set output response out.write(Validator.filter(response)); out.close();
```

利用「Servlet 過濾器」，以 Validator.filter 來消毒回應的範例：

```
// Example to filter all sensitive characters in the HTTP response using a Java Filter. // This example is for illustration purposes since it will filter
all content in the response, including HTML tags! public class SensitiveCharsFilter implements Filter { ... public void doFilter(ServletRequest
request, ServletResponse response, FilterChain chain) throws IOException, ServletException { PrintWriter out = response.getWriter();
ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response); chain.doFilter(request, wrapper); CharArrayWriter caw
= new CharArrayWriter(); caw.write(Validator.filter(wrapper.toString())); response.setContentType("text/html");
response.setContentLength(caw.toString().length()); out.write(caw.toString()); out.close(); } ... public class CharResponseWrapper extends
HttpServletResponseWrapper { private CharArrayWriter output; public String toString() { return output.toString(); } public
CharResponseWrapper(HttpServletResponse response){ super(response); output = new CharArrayWriter(); } public PrintWriter getWriter(){
return new PrintWriter(output); } } }
```

[8-2] 維護 Cookie 安全

當機密資料儲存在 Cookie 中，請務必利用 `Cookie.setSecure`（布林旗標），在 HTTP 回應中設定 Cookie 的安全旗標，以指示瀏覽器利用 HTTPS 或 SSL 之類的安全通訊協定來傳送 Cookie。

維護 "user" Cookie 安全的範例：

```
// Example to secure a cookie, i.e. instruct the browser to // send the cookie using a secure protocol Cookie cookie = new Cookie("user",
"sensitive"); cookie.setSecure(true); response.addCookie(cookie);
```

建議的 Java 工具

適用於伺服器端驗證的兩個主要的 Java 架構如下：

[1] Jakarta 一般驗證器（整合 Struts 1.1）

「Jakarta 一般驗證器」實作上述所有資料驗證需求，是一個功能強大的架構。這些規則配置在定義表單欄位輸入驗證規則的 XML 檔中。依預設，Struts 支援在利用 Struts 'bean:write' 標籤撰寫的所有資料上，過濾 [8] HTTP 回應中輸出的危險字元。設定 'filter=false' 旗標可以停用這個過濾。

Struts 定義下列基本輸入驗證器，但也可以定義自訂驗證器：

required：如果欄位含有空格以外的任何字元，便告成功。

mask：如果值符合 **mask** 屬性給定的正規表示式，便告成功。

range：如果值在 **min** 和 **max** 屬性給定的值範圍內（(value >= min) 且 (value <= max)），便告成功。

maxLength：如果欄位長度小於或等於 **max** 屬性，便告成功。

minLength：如果欄位長度大於或等於 **min** 屬性，便告成功。

byte、**short**、**integer**、**long**、**float**、**double**：如果值可以轉換成對應的基本類型，便告成功。

date：如果值代表有效日期，便告成功。可提供日期型樣。

creditCard：如果值可能是有效的信用卡號碼，便告成功。

e-mail：如果值可能是有效的電子郵件位址，便告成功。

利用「Struts 驗證器」驗證 loginForm 之 userName 欄位的範例：

```
<form-validation> <global> ... <validator name="required" classname="org.apache.struts.validator.FieldChecks" method="validateRequired"
msg="errors.required"> </validator> <validator name="mask" classname="org.apache.struts.validator.FieldChecks" method="validateMask"
msg="errors.invalid"> </validator> ... </global> <formset> <form name="loginForm"> <!-- userName is required and is alpha-numeric case
insensitive --> <field property="userName" depends="required,mask"> <!-- message resource key to display if validation fails --> <msg
name="mask" key="login.userName.maskmsg"/> <arg0 key="login.userName.displayName"/> <var> <var-name>mask</var-name> <var-
value>^[a-zA-Z0-9]*$</var-value> </var> </field> ... </form> ... </formset> </form-validation>
```

[2] JavaServer Faces 技術

「JavaServer Faces 技術」是一組代表使用者介面元件、管理元件狀態、處理事件及輸入驗證的 Java API (JSR 127)。

JavaServer Faces API 實作下列基本驗證器，但可以定義自訂驗證器：

validate_doublerange：登錄元件的 `DoubleRangeValidator`

validate_length：登錄元件的 `LengthValidator`

validate_longrange：登錄元件的 `LongRangeValidator`

validate_required：登錄元件的 `RequiredValidator`

validate_stringrange：登錄元件的 `StringRangeValidator`

validator：登錄元件的自訂 `Validator`

JavaServer Faces API 定義下列 UIInput 和 UIOutput 展現器（標籤）：

input_date：接受以 `java.text.Date` 實例格式化的 `java.util.Date`

output_date：顯示以 `java.text.Date` 實例格式化的 `java.util.Date`

input_datetime：接受以 `java.text.Time` 實例格式化的 `java.util.Date`

output_datetime：顯示以 `java.text.Time` 實例格式化的 `java.util.Date`

input_number：顯示以 `java.text.NumberFormat` 格式化的數值資料類型（`java.lang.Number` 或基本資料類型）

output_number：顯示以 `java.text.NumberFormat` 格式化的數值資料類型（`java.lang.Number` 或基本資料類型）

input_text：接受單行字串。

output_text：顯示單行字串。

input_time：接受以 `java.text.DateFormat` 時間實例格式化的 `java.util.Date`

output_time：顯示以 `java.text.DateFormat` 時間實例格式化的 `java.util.Date`

input_hidden：可讓頁面作者將隱藏變數併入頁面

input_secret：接受不含空格的單行文字，輸入之時，將它顯示成一組星號

input_textarea：接受多行文字

output_errors：顯示整個頁面的錯誤訊息，或指定之用戶端 ID 的相關錯誤訊息

output_label：將巢狀元件顯示為指定輸入欄位的標籤

output_message：顯示本地化訊息

利用 JavaServer Faces 驗證 loginForm 之 userName 欄位的範例：

```
<%@ taglib uri="https://docs.oracle.com/javaee/6/tutorial/doc/glxce.html" prefix="h" %> <%@ taglib uri="http://mrbool.com/how-to-create-a-
```



```
login-validation-with-jsf-java-server-faces/27046" prefix="f" %> ... <jsp:useBean id="UserBean" class="myApplication.UserBean"
scope="session" /> <f:use_faces> <h:form formName="loginForm" > <h:input_text id="userName" size="20"
modelReference="UserBean.userName"> <f:validate_required/> <f:validate_length minimum="8" maximum="20"/> </h:input_text> <!-- display
errors if present --> <h:output_errors id="loginErrors" clientId="userName"/> <h:command_button id="submit" label="Submit"
commandName="submit" /><p> </h:form> </f:use_faces>
```

參照

Java API 1.3 -

<https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html>

Java API 1.4 -

<https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html>

Java Servlet API 2.3 -

<https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api>

Java 正規表示式套件 -

<http://jakarta.apache.org/regexp/>

Jakarta 驗證器 -

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技術 -

<http://www.javaserverfaces.org/>

**** 錯誤處理：**

許多 J2EE Web 應用程式架構都遵循「模型視圖控制器 (MVC)」型樣。在這個型樣中，Servlet 扮演控制器的角色。Servlet 將應用程式處理程序委派給 JavaBean，例如，EJB Session Bean（模型）。之後，Servlet 再將要求轉遞給 JSP（視圖）來呈現處理結果。Servlet 應該檢查所有輸入、輸出、回覆碼、錯誤碼及已知的異常狀況，以確保會實際進行預期的處理程序。

資料驗證可以保護應用程式免於遭受惡意的資料竄改，有效的錯誤處理策略則是防止應用程式意外揭露內部錯誤訊息（例如：異常狀況堆疊追蹤）所不可或缺。好的錯誤處理策略會處理下列項目：

[1] 定義錯誤

[2] 報告錯誤

[3] 呈現錯誤

[4] 錯誤對映

[1] 定義錯誤

應該避免將錯誤訊息寫在應用程式層（例如：Servlet）。相反地，應用程式應該使用對映至已知之應用程式失敗的錯誤索引鍵。在實務中，好的做法是定義錯誤索引鍵來對映至 HTML 表單欄位或其他 Bean 內容的驗證規則。比方說，如果需要 "user_name" 欄位，它必須是英數字元，且在資料庫中必須是唯一，便應該定義下列錯誤索引鍵：

(a) ERROR_USERNAME_REQUIRED：這個錯誤索引鍵用來顯示一則訊息，通知使用者需要 "user_name" 欄位；

(b) ERROR_USERNAME_ALPHANUMERIC：這個錯誤索引鍵用來顯示一則訊息，通知使用者 "user_name" 欄位應該是英數字元；

(c) ERROR_USERNAME_DUPLICATE：這個錯誤索引鍵用來顯示一則訊息，通知使用者 "user_name" 值在資料庫中重複；

(d) ERROR_USERNAME_INVALID：這個錯誤索引鍵用來顯示一則一般訊息，通知使用者 "user_name" 值無效；

在實務中，好的做法是定義下列架構 Java 類別來儲存及報告應用程式錯誤：

- ErrorKeys：定義所有錯誤索引鍵

```
// Example: ErrorKeys defining the following error keys: // - ERROR_USERNAME_REQUIRED // - ERROR_USERNAME_ALPHANUMERIC // -
ERROR_USERNAME_DUPLICATE // - ERROR_USERNAME_INVALID // ... public Class ErrorKeys { public static final String
ERROR_USERNAME_REQUIRED = "error.username.required"; public static final String ERROR_USERNAME_ALPHANUMERIC =
"error.username.alphanumeric"; public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate"; public static final
String ERROR_USERNAME_INVALID = "error.username.invalid"; ... }
```

- Error：封裝個別錯誤

```
// Example: Error encapsulates an error key. // Error is serializable to support code executing in multiple JVMs. public Class Error implements
Serializable { // Constructor given a specified error key public Error(String key) { this(key, null); } // Constructor given a specified error key and
array of placeholder objects public Error(String key, Object[] values) { this.key = key; this.values = values; } // Returns the error key public String
getKey() { return this.key; } // Returns the placeholder values public Object[] getValues() { return this.values; } private String key = null; private
Object[] values = null; }
```

- Errors：封裝錯誤的集合

```
// Example: Errors encapsulates the Error objects being reported to the presentation layer. // Errors are stored in a HashMap where the key is
the bean property name and value is an // ArrayList of Error objects. public Class Errors implements Serializable { // Adds an Error object to the
Collection of errors for the specified bean property. public void addError(String property, Error error) { ArrayList propertyErrors =
(ArrayList)errors.get(property); if (propertyErrors == null) { propertyErrors = new ArrayList(); errors.put(property, propertyErrors); }
propertyErrors.put(error); } // Returns true if there are any errors public boolean hasErrors() { return (errors.size > 0); } // Returns the Errors for
the specified property public ArrayList getErrors(String property) { return (ArrayList)errors.get(property); } private HashMap errors = new
HashMap(); }
```

以下是利用上述架構類別來處理 "user_name" 欄位驗證錯誤的範例：

```
// Example to process validation errors of the "user_name" field. Errors errors = new Errors(); String userName =
request.getParameter("user_name"); // (a) Required validation rule if (!Validator.validateRequired(userName)) { errors.addError("user_name",
new Error(ErrorKeys.ERROR_USERNAME_REQUIRED)); } // (b) Alpha-numeric validation rule else if (!Validator.matchPattern(userName, "^[a-
zA-Z0-9]*$")) { errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC)); } else { // (c) Duplicate check
validation rule // We assume that there is an existing UserValidationEJB session bean that implements // a checkIfDuplicate() method to verify if
the user already exists in the database. try { ... if (UserValidationEJB.checkIfDuplicate(userName)) { errors.addError("user_name", new
Error(ErrorKeys.ERROR_USERNAME_DUPLICATE)); } } catch (RemoteException e) { // log the error logger.error("Could not validate user for
specified userName: " + userName); errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE)); } } // set the
```

errors object in a request attribute called "errors" request.setAttribute("errors", errors); ...

[2] 報告錯誤

報告 Web 層應用程式錯誤的方式有兩種：

(a) Servlet 錯誤機制

(b) JSP 錯誤機制

[2-a] Servlet 錯誤機制

Servlet 報告錯誤的可能方式如下：

- 轉遞至輸入 JSP（已將錯誤儲存在要求屬性中），或
- 利用 HTTP 錯誤碼引數來呼叫 response.sendError，或
- 擲出異常狀況

在實務中，好的做法是處理所有已知的應用程式錯誤（依照 [1] 區段所說明），將它們儲存在要求屬性中，再轉遞給輸入 JSP。輸入 JSP 應該顯示錯誤訊息，並提示使用者重新輸入資料。下列範例說明如何轉遞到輸入 JSP (userInput.jsp)：

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd =
getServletContext().getRequestDispatcher("/user/userInput.jsp"); if (rd != null) { rd.forward(request, response); }
```

如果 Servlet 無法轉遞到已知的 JSP 頁面，第二個選項是利用 response.sendError 方法，設定 HttpServletResponse.SC_INTERNAL_SERVER_ERROR 引數（狀態碼 500）來報告錯誤。

請參閱 javax.servlet.http.HttpServletResponse javadoc，以取得各種 HTTP 狀態碼的詳細資訊。

傳回 HTTP 錯誤的範例：

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp"); if (rd == null) {
// messages is a resource bundle with all message keys and values
response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID)); }
```

作為最後的手段，Servlet 可以擲出異常狀況，它必須是下列類別之一的子類別：

- RuntimeException
- ServletException
- IOException

[2-b] JSP 錯誤機制 JSP 頁面依照下列範例所示來定義 errorPage 指引，從而提供了執行時期異常狀況的處理機制：

```
<%@ page errorPage="/errors/userValidation.jsp" %>
```

未捕捉的 JSP 異常狀況是轉遞到指定的 errorPage，而原始異常狀況則設在稱為 javax.servlet.jsp.jspException 的要求參數中。錯誤頁面必須包含 isErrorPage 指引，如下所示：

```
<%@ page isErrorPage="true" %>
```

isErrorPage 指引會使 "exception" 變數起始設定為所擲出的異常狀況物件。

[3] 呈現錯誤

J2SE Internationalization API 提供用來提出應用程式資源以及將訊息格式化的公用程式類別，其中包括：

(a) 資源組

(b) 訊息格式化

[3-a] 資源組

資源組會將本地化的資料與使用它的原始碼分開，從而支援國際化。每個資源組都會儲存特定語言環境之鍵值配對的對映。

通常是利用或延伸 java.util.PropertyResourceBundle，它會將內容儲存在外部內容檔中，如下列範例所示：

```
##### # ErrorMessages.properties
##### # required user name error message
error.username.required=User name field is required
# invalid user name format
error.username.alphanumeric=User name must be alphanumeric
# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one ...
```

定義多重資源可以支援不同的語言環境（因此稱為資源組）。例如，定義 ErrorMessages_fr.properties 可以支援資源組系列的法國成員。如果要求之語言環境的資源成員不存在，便會使用預設成員。在上述範例中，預設資源是 ErrorMessages.properties。依使用者的語言環境而定，應用程式（JSP 或 Servlet）會從適當的資源擷取內容。

[3-b] 訊息格式化

J2SE 標準類別 java.util.MessageFormat 提供以取代位置保留元來建立訊息的一般方式。MessageFormat 物件包含內嵌了格式指定元的型樣字串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1]; args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

以下是利用 ResourceBundle 和 MessageFormat 來呈現錯誤訊息的更綜合性的範例：

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public Class ErrorMessageResource { // Returns the error message for the specified error key in the environment locale
public String getErrorMessage(String errorKey) { return getErrorMessage(errorKey, defaultLocale); } // Returns the error message for the specified error key in the specified locale
public String getErrorMessage(String errorKey, Locale locale) { return getErrorMessage(errorKey, null, locale); } // Returns a formatted error message for the specified error key in the specified locale
public String getErrorMessage(String errorKey, Object[] args, Locale locale) { // Get localized ErrorMessageResource
ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale); // Get localized error message
String errorMessage = errorMessageResource.getString(errorKey); if (args != null) { // Format the message using the specified placeholders
args return MessageFormat.format(errorMessage, args); } else { return errorMessage; } } // default environment locale
private Locale defaultLocale = Locale.getDefaultLocale(); } ... // Get the user's locale
Locale userLocale = request.getLocale(); // Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors"); if (errors != null && errors.hasErrors()) { // iterate through errors and output error messages corresponding to the "user_name" property
ArrayList userNameErrors = errors.getErrors("user_name"); ListIterator iterator = userNameErrors.iterator(); while (iterator.hasNext()) { // Get the next error object
Error error = (Error)iterator.next(); String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale); output.write(errorMessage
```

```
+ "\r\n"); }}
```

建議您定義自訂 JSP 標籤（如 `displayErrors`）來疊代處理及呈現錯誤訊息，如上述範例所示。

[4] 錯誤對映

一般而言，「Servlet 儲存器」會傳回對應於回應狀態碼或異常狀況的預設錯誤頁面。您可以利用自訂錯誤頁面來指定狀態碼或異常狀況與 Web 資源之間的對映。

在實務中，好的做法是開發不揭露內部錯誤狀態的靜態錯誤頁面（依預設，大部分 Servlet 儲存器都會報告內部錯誤訊息）。這項對映是依照下列範例所指定，配置在「Web 部署描述子 (`web.xml`)」中：

```
<!-- Mapping of HTTP error codes and application exceptions to error pages --> <error-page> <exception-  
type>UserValidationException</exception-type> <location>/errors/validationError.html</error-page> </error-page> <error-page> <error-  
code>500</error-code> <location>/errors/internalError.html</error-page> </error-page> ... </error-page> ...
```

建議的 Java 工具

適用於伺服器端驗證的兩個主要的 Java 架構如下：

[1] Jakarta 一般驗證器（整合 Struts 1.1）

「Jakarta 一般驗證器」是依照上述說明來定義錯誤處理機制的 Java 架構。驗證規則配置在 XML 檔中，檔案定義了表單欄位的輸入驗證規則以及對應的驗證錯誤索引鍵。Struts 提供國際化支援，供您利用資源組和訊息格式化來建置本地化應用程式。

利用「Struts 驗證器」驗證 `loginForm` 之 `userName` 欄位的範例：

```
<form-validation> <global> ... <validator name="required" classname="org.apache.struts.validator.FieldChecks" method="validateRequired"  
msg="errors.required"> </validator> <validator name="mask" classname="org.apache.struts.validator.FieldChecks" method="validateMask"  
msg="errors.invalid"> </validator> ... </global> <formset> <form name="loginForm"> <!-- userName is required and is alpha-numeric case  
insensitive --> <field property="userName" depends="required,mask"> <!-- message resource key to display if validation fails --> <msg  
name="mask" key="login.userName.maskmsg"/> <arg0 key="login.userName.displayName"/> <var> <var-name>mask</var-name> <var-  
value>^[a-zA-Z0-9]*$</var-value> </var> </field> ... </formset> </form-validation>
```

Struts JSP 標籤庫定義了有條件地顯示一組累計錯誤訊息的 "errors" 標籤，如下列範例所示：

```
<%@ page language="java" %> <%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %> <%@ taglib uri="/WEB-INF/struts-bean.tld"  
prefix="bean" %> <html:html> <head> <body> <html:form action="/logon.do"> <table border="0" width="100%"> <tr> <th align="right">  
<html:errors property="username"/> <bean:message key="prompt.username"/> </th> <td align="left"> <html:text property="username"  
size="16"/> </td> </tr> <tr> <td align="right"> <html:submit><bean:message key="button.submit"/></html:submit> </td> <td align="right">  
<html:reset><bean:message key="button.reset"/></html:reset> </td> </tr> </table> </html:form> </body> </html:html>
```

[2] JavaServer Faces 技術

「JavaServer Faces 技術」是一組代表使用者介面元件、管理元件狀態、處理事件、驗證輸入，以及支援國際化的 Java API (JSR 127)。

JavaServer Faces API 定義了 "output_errors" UIOutput 展現器，以顯示整個頁面的錯誤訊息，或指定之用戶端 ID 的相關錯誤訊息。

利用 JavaServer Faces 驗證 `loginForm` 之 `userName` 欄位的範例：

```
<%@ taglib uri="https://docs.oracle.com/javaee/6/tutorial/doc/glxce.html" prefix="h" %> <%@ taglib uri="http://mrbool.com/how-to-create-a-  
login-validation-with-jsf-java-server-faces/27046" prefix="f" %> ... <jsp:useBean id="UserBean" class="myApplication.UserBean"  
scope="session" /> <f:use_faces> <h:form formName="loginForm"> <h:input_text id="userName" size="20"  
modelReference="UserBean.userName"> <f:validate_required/> <f:validate_length minimum="8" maximum="20"/> </h:input_text> <!-- display  
errors if present --> <h:output_errors id="loginErrors" clientId="userName"/> <h:command_button id="submit" label="Submit"  
commandName="submit" /><p> </h:form> </f:use_faces>
```

參照

Java API 1.3 -

<https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html>

Java API 1.4 -

<https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html>

Java Servlet API 2.3 -

<https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api>

Java 正規表示式套件 -

<http://jakarta.apache.org/regexp/>

Jakarta 驗證器 -

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技術 -

<http://www.javaserverfaces.org/>

** 過濾使用者輸入

將任何資料傳給 SQL 查詢之前，一律應該先利用白名單技術來適當過濾。這無論如何強調都不為過。

過濾使用者輸入可讓許多注入缺失，在抵達資料庫之前便得到更正。

** 引用使用者輸入

不論任何資料類型，只要資料庫允許，使用單引號括住所有使用者資料，始終是好的觀念。

MySQL 接受這個格式化技術。

** 跳出資料值

如果您使用 MySQL 4.3.0 或更新的版本，您應該用 `mysql_real_escape_string()` 來跳出所有字串。

如果使用舊版的 MySQL，便應該使用 `mysql_escape_string()` 函數。

如果未使用 MySQL，您可以選擇使用特定資料庫的特定跳出函數。

如果不知道跳出函數，您可以選擇使用較一般的跳出函數，例如，`addslashes()`。

如果使用 PEAR DB 資料庫抽象層，您可以使用 `DB::quote()` 方法或使用 `?` 之類的查詢位置保留元，它會自動跳出取代位置保留元的值。

參照

http://ca3.php.net/mysql_real_escape_string

http://ca.php.net/mysql_escape_string

<http://ca.php.net/addslashes>

<http://pear.php.net/package-info.php?package=DB>

**** 驗證輸入資料：**

雖然為了使用者的方便，可以在用戶端層提供資料驗證，但一律必須在伺服器層執行資料驗證。用戶端驗證原本就不安全，因為它們可以輕易略過，例如：停用 JavaScript。

好的設計通常需要 Web 應用程式架構提供伺服器端公用程式來驗證下列項目：

- [1] 必要欄位
- [2] 欄位資料類型（依預設，所有 HTTP 要求參數都是 String）
- [3] 欄位長度
- [4] 欄位範圍
- [5] 欄位選項
- [6] 欄位型樣
- [7] Cookie 值
- [8] HTTP 回應

在實務中，好的做法是實作一或多個驗證各個應用程式參數的函數。下列各節說明一些檢查範例。

- [1] 必要欄位
- 一律檢查確認欄位不是空值，欄位長度大於零，且不含在前端及尾端的空格。

如何驗證必要欄位的範例：

```
// PHP example to validate required fields function validateRequired($input) { ... $pass = false; if (strlen(trim($input))>0){ $pass = true; } return $pass; ... } ... if (validateRequired($fieldName)) { // fieldName is valid, continue processing request ... }
```

- [2] 欄位資料類型

在 Web 應用程式中，所輸入的輸入參數設定不良。例如，所有 HTTP 要求參數或 Cookie 值都是 String 類型。開發人員負責確認輸入的資料類型正確。

- [3] 欄位長度
- 一律確定輸入參數（HTTP 要求參數或 Cookie 值）在長度下限及/或長度上限的範圍內。

- [4] 欄位範圍
- 一律確定輸入參數在函數需求定義的範圍內。

- [5] 欄位選項
- Web 應用程式通常會向使用者呈現一組可供選擇的選項（例如：使用 SELECT HTML 標籤），但無法執行伺服器端驗證來確保所選的值是容許的選項之一。請記住，惡意的使用者可以輕易修改任何選項值。請一律對照函數需求所定義容許的選項來驗證所選的使用者值。

- [6] 欄位型樣
- 一律檢查使用者輸入是否符合功能需求所定義的型樣。比方說，如果 userName 欄位只應接受英數字元，且不區分大小寫，請使用下列正規表示式：

```
^[a-zA-Z0-9]+$
```

- [7] Cookie 值

依應用程式需求而定，相同的驗證規則（說明如上）也適用於 Cookie 值，例如：驗證必要的值、驗證長度，等等。

- [8] HTTP 回應

- [8-1] 過濾使用者輸入

如果要保護應用程式免於遭受跨網站 Scripting，開發人員應該將機密字元轉換成對應的字元實體來消毒 HTML。以下是 HTML 區分字元：

```
<>"'%;)( & +
```

PHP 包括一些 htmlentities() 之類的自動化消毒公用程式函數：

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

此外，為了避免「跨網站 Scripting」的 UTF-7 變式，您應該明確定義回應的 Content-Type 標頭，例如：

```
<?php header('Content-Type: text/html; charset=UTF-8'); ?>
```

- [8-2] 維護 Cookie 安全

當機密資料儲存在 Cookie 中，且透過 SSL 來傳輸它時，請務必先在 HTTP 回應中設定 Cookie 的安全旗標。這會指示瀏覽器只透過 SSL 連線來使用這個 Cookie。

您可以利用下列程式碼範例來維護 Cookie 安全：

```
<$php $value = "some_value"; $time = time()+3600; $path = "/application/"; $domain = ".example.com"; $secure = 1; setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE); ?>
```

此外，我們建議您使用 HttpOnly 旗標。當 HttpOnly 旗標設為 TRUE 時，只能透過 HTTP 通訊協定來存取 Cookie。這表示無法用 JavaScript 之類的 Scripting 語言存取 Cookie。這個設定有助於實際減少透過 XSS 攻擊來盜用身分的情況（不過，並非所有瀏覽器都支援）。

PHP 5.2.0 新增 HttpOnly 旗標。

參照

- [1] 利用「HTTP 專用 Cookie」緩和「跨網站 Scripting」：

<http://msdn2.microsoft.com/en-us/library/ms533046.aspx>

- [2] PHP 安全聯盟：

<http://phpsec.org/>

- [3] PHP & Web 應用程式安全部落格 (Chris Shiflett)：

<http://shiflett.org/>

此作業所修正的問題類型

- 不適當封鎖帳戶

一般

請決定容許的登入嘗試次數（通常是 3-5 次），確定超出允許的嘗試次數之後，便鎖定帳戶。

為了避免真正的使用者因需要啟用鎖定的帳戶而發出不必要的支援呼叫，可以只是暫停帳戶活動，過了特定時段之後，便加以啟用。帳戶鎖定大約 10 分鐘，通常便足以封鎖強制入侵攻擊。

此作業所修正的問題類型

- 未更新階段作業 ID

一般

不讓使用者能夠操作階段作業 ID。

請勿接受使用者瀏覽器登入時所提供的階段作業 ID；一律產生新的階段作業，供使用者順利鑑別時登入。

在授權新的使用者階段作業之前，先使任何現有的階段作業 ID 失效。

針對不會產生新的階段作業 ID Cookie 值的平台（如 ASP），請使用次要 Cookie。在這種作法中，請在使用者的瀏覽器中將次要 Cookie 設為隨機值，並將某個階段作業變數設為相同的值。如果該階段作業變數和 Cookie 值不符，則使該階段作業失效，並強制使用者重新登入。

此作業所修正的問題類型

- 登入錯誤訊息認證列舉

一般

每次試圖登入失敗時，不論是哪個欄位發生錯誤（特別是使用者名稱或密碼欄位錯誤時），都會發出相同的錯誤訊息。

此作業所修正的問題類型

- 偽造跨網站要求

一般

設定所有階段作業和鑑別 Cookie 以包括 `SameSite` 屬性，並將此屬性設定為 `Strict` 或 `Lax`。將此屬性設定為 `Lax` 時，請確定依據 HTTP 標準，不能透過 `GET` 要求執行機密動作。

使用平台或架構所提供的內建 CSRF 保護，而且不論在配置或程式碼中，都請務必適當地予以啟動。

如果您的平台未提供內建反 CSRF 機制，請考慮整合進行過良好檢查的程式庫來實作保護，例如 OWASP CSRFGuard。

請避免建置自訂反 CSRF 實作，因為此作業很複雜而難以正確達成，不容許輕易略過。如果您因缺乏標準程式庫支援而絕對需要這麼做，則應該在伺服器上產生安全、隨機且不可預測的記號（例如 GUID v4），並將它內嵌於每個 HTML 表單，同時將它連結至使用者的階段作業。收到提交的表單時，請驗證包括的表單記號是否符合先前連結至使用者的記號。您也可以將 CSRF 記號內嵌於指定的 Cookie（重複提交的 Cookie），或者最好使用自訂要求標頭；伺服器同時收到這些項目與提交的表單記號時，只需要驗證它們是否相符（而非儲存於使用者的階段作業中）。

替代方式是使用者需要重新鑑別特定動作，以確定使用者的主動確認。請注意，這會持續影響使用者體驗，因此應該盡量不要使用，且應僅特別用於機密動作。

驗證 `Origin` 標頭（若存在）或至少驗證 `Referer` 標頭，以確認要求的來源。請捨棄源自不同網站的機密要求。

此作業所修正的問題類型

- 未停用密碼欄位的自動完成 HTML 屬性

一般

如果在 "input" 元素的 "password" 欄位中遺漏了 "autocomplete" 屬性，請新增它並設定為 "off"。如果 "autocomplete" 屬性設定為 "on"，請變更為 "off"。

例如：

有漏洞的網站：

```
<form action="AppScan.html" method="get"> Username: <input type="text" name="firstname" /><br /> Password: <input type="password" name="lastname" /> <input type="submit" value="Submit" /> </form>
```

無漏洞的網站：

```
<form action="AppScan.html" method="get"> Username: <input type="text" name="firstname" /><br /> Password: <input type="password" name="lastname" autocomplete="off"/> <input type="submit" value="Submit" /> </form>
```

此作業所修正的問題類型

- 遺漏或不安全的 "X-Content-Type-Options" 標頭

一般

配置您的伺服器，在所有送出的要求上使用值為 "nosniff" 的 "X-Content-Type-Options" 標頭。

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/nginx_headers_module.html

低 配置伺服器利用 DENY 或 SAMEORIGIN 值使用 "X-Frame-Options" 標頭

目錄

此作業所修正的問題類型

- 遺漏或不安全的跨頁框 Scripting 防禦

一般

使用 X-Frame-Options 來避免（或限制）頁面內嵌在 iFrames 中。對於舊版瀏覽器，請在不應嵌入框架的每個頁面中併入 "frame-breaker" Script。

低 配置伺服器利用安全原則使用 "Content-Security-Policy" 標頭

目錄

此作業所修正的問題類型

- 遺漏「Content-Security-Policy」標頭

一般

配置您的伺服器以傳送「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」、「script-src」及「object-src」，預期的安全值包括「none」、「self」、「https://any.example.com」，以及「unsafe-inline」或「unsafe-eval」搭配 nonce 或雜湊演算法等。

對於「frame-ancestors」，預期的安全值包括「self」、「none」或 https://any.example.com 等。

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/nginx_headers_module.html

此作業所修正的問題類型

- 遺漏或不安全的 "X-XSS-Protection" 標頭

一般

將您的伺服器配置為在所有送出的要求中，傳送值為 1 的 X-XSS-Protection 標頭（即「已啟用」）。

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

此作業所修正的問題類型

- 遺漏「查閱者原則」安全標頭

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>

此作業所修正的問題類型

- 檢查是否有 SRI（子資源完整性）支援

一般

將「子資源完整性」新增至每一個 Script/鏈結（其原始碼不在您網域中）

W3C 子資源完整性：

<https://www.w3.org/TR/SRI/>

SRI 雜湊產生器：

<https://srihash.org>

不支援 SRI 的範例 Script 元素：

```
<script src="https://example.com/example-framework.js" crossorigin="anonymous"></script>
```

支援 SRI 的範例 Script 元素：

```
<script src="https://example.com/example-framework.js" integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQIGYI1kPzQho1wx4JwY8wC" crossorigin="anonymous"></script>
```

低

新增 'HttpOnly' 屬性至所有階段作業 Cookie

目錄

此作業所修正的問題類型

- 在階段作業 Cookie 中遺漏 HttpOnly 屬性

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。

"HttpOnly" 屬性必須相應地設定，才能防止 Script 存取階段作業 Cookie。

低

對禁止的資源發出「404 - 找不到」回應狀態碼，或將其完全移除

目錄

此作業所修正的問題類型

- 偵測到隱藏目錄

一般

如果不需要禁止的資源，請將它從網站中移除。

可能的話，請發出「404 - 找不到」回應狀態碼，而不是「403 - 禁止」。

這項變更會將網站的目錄模糊化，可以防止洩漏網站結構。

低

請下載您的 Web 伺服器或 Web 應用程式的相關安全修補程式。

目錄

此作業所修正的問題類型

- 找到可能的伺服器路徑揭露型樣

一般

以下方法能降低風險：

[1] 若應用程式本身含有漏洞，請修正伺服器程式碼，使輸出值中不含有檔案位置。

[2] 若應用程式位於協力廠商產品內，請根據您在 **Web** 伺服器或 **Web** 應用程式所使用的協力廠商產品，下載相關安全修補程式。

低

請勿容許機密性資訊洩漏。

目錄

此作業所修正的問題類型

- 應用程式中找到不必要的 HTTP 回應標頭

一般

配置伺服器以移除預設的 "Server" 標頭，以免傳送到所有送出的請求。

IIS

連結：設定 IIS 回應標頭

針對 nginx，請參閱：

連結：設定 nginx 回應標頭

針對 Weblogic，請參閱：

連結：設定 Weblogic 回應標頭

針對 Apache，請參閱：

連結：設定 Apache 回應標頭

低

請驗證參數值是在預期的範圍內且為預期的類型。請勿輸出除錯錯誤訊息和異常狀況

目錄

此作業所修正的問題類型

- 應用程式錯誤

一般

[1] 檢查送入要求，以瞭解所有預期的參數和值是否存在。

當遺漏參數時，便發出適當的錯誤訊息，或使用預設值。

[2] 應用程式應該驗證它的輸入是否由有效字元組成（解碼之後）。

例如，含有空值位元組的輸入值（編碼為 %00）、單引號、引號等，都應該予以拒絕。

[3] 施行符合預期範圍和類型的值。

如果您的應用程式預期特定參數有特定值集中的值，應用程式應該確定它接收的值確實屬於這個值集。比方說，如果您的應用程式預期 10..99 範

圍內的值，它應該確定值確實是數值，且在 10..99 範圍內。

[4] 確認資料屬於提供給用戶端的資料集。

[5] 不在正式作業環境中，輸出除錯錯誤訊息和異常狀況。

如果要在 ASP.NET 中停用除錯，請編輯您的 web.config 檔，使它含有下列內容：

```
<compilation
debug="false"
/>
```

如需相關資訊，請參閱「如何：停用 ASP.NET 應用程式除錯」，位置如下：

<http://support.microsoft.com/default.aspx?scid=kb;en-us;815157>

您可以利用驗證控制項，將輸入驗證新增到「Web 表單」頁面中。

驗證控制項提供適用於標準驗證之所有一般類型的簡易使用機制（例如：測試日期是否有效，或值是否在範圍內），以及用來提供自訂編寫驗證的方式。此外，驗證控制項也可讓您完整自訂向使用者顯示錯誤資訊的方式。驗證控制項可以搭配「Web 表單」頁面類別檔所處理的任何控制項來使用，其中包括 HTML 和 Web 伺服器控制項。

如果要確定要求含有所有必要的參數，請使用 "RequiredFieldValidator" 驗證控制項。

這個控制項可確保使用者未跳過 Web 表單中的任何項目。如果要確定使用者輸入只包含有效值，您可以使用下列其中一個驗證控制項：

[1] "RangeValidator"：檢查使用者的輸入（值）是否在指定的上下界限之間。您可以檢查數字、英文字母和日期之配對內的範圍。[2]

"RegularExpressionValidator"：檢查輸入是否符合正規表示式所定義的型樣。這類型的驗證可讓您檢查可預期的字元序列，例如：社會保險號碼、電子郵件位址、電話號碼、郵遞區號等等中的字元序列。

重要注意事項：驗證控制項不會封鎖使用者輸入，或變更頁面處理流程；它們只會設定錯誤狀態，以及產生錯誤訊息。在執行進一步的應用程式專屬動作之前，程式設計師負責測試程式碼中的控制項狀態。

檢查使用者輸入有效性有兩種方式：

1. 測試一般錯誤狀態：

在您的程式碼中，測試頁面的 IsValid 內容。

這個內容會累積頁面上所有驗證控制項的 IsValid 內容值（使用邏輯 AND）。如果其中一個驗證控制項設為無效，頁面內容便會傳回 False。

2. 測試個別控制項的錯誤狀態：

在迴圈中處理頁面的驗證器集合，集合中含有指向所有驗證控制項的參照。

之後，您便可以檢查每個驗證控制項的 IsValid 內容。

** 驗證輸入資料：

雖然為了使用者的方便，可以在用戶端層提供資料驗證，但必須利用 Servlet，在伺服器層執行資料驗證。

用戶端驗證原本就不安全，因為它們可以輕易略過，例如：停用 JavaScript。

好的設計通常需要 Web 應用程式架構提供伺服器端公用程式常式來驗證下列項目：

[1] 必要欄位

[2] 欄位資料類型（依預設，所有 HTTP 要求參數都是 String）

[3] 欄位長度

[4] 欄位範圍

[5] 欄位選項

[6] 欄位型樣

[7] Cookie 值

[8] HTTP 回應

在實務中，好的做法是在 "Validator" 公用程式類別中將上述常式當作靜態方法來實作。下列各節說明範例驗證器類別

[1] 必要欄位

一律檢查確認欄位不是空值，欄位長度大於零，且不含在前端及尾端的空格。

如何驗證必要欄位的範例：

```
// Java example to validate required fields public Class Validator { ... public static boolean validateRequired(String value) { boolean isFieldValid = false; if (value != null && value.trim().length() > 0) { isFieldValid = true; } return isFieldValid; } ... } ... String fieldValue = request.getParameter("fieldName"); if (Validator.validateRequired(fieldValue)) { // fieldValue is valid, continue processing request ... }
```

[2] 欄位資料類型

在 Web 應用程式中，所輸入的輸入參數設定不良。例如，所有 HTTP 要求參數或 Cookie 值都是 String 類型。開發人員負責確認輸入的資料類型正確。

請利用 Java 基本封套類別來檢查欄位值是否能安全轉換成所需要的基本資料類型。

如何驗證數值欄位（int 類型）的範例：

```
// Java example to validate that a field is an int number public Class Validator { ... public static boolean validateInt(String value) { boolean isFieldValid = false; try { Integer.parseInt(value); isFieldValid = true; } catch (Exception e) { isFieldValid = false; } return isFieldValid; } ... } ... // check if the HTTP request parameter is of type int String fieldValue = request.getParameter("fieldName"); if (Validator.validateInt(fieldValue)) { // fieldValue is valid, continue processing request ... }
```

在實務中，好的做法是將所有 HTTP 要求參數轉換成它們的相關資料類型。例如，將要求參數的 "integerValue" 儲存在要求屬性中，再依照下列範例所示來使用它：

```
// Example to convert the HTTP request parameter to a primitive wrapper data type // and store this value in a request attribute for further processing String fieldValue = request.getParameter("fieldName"); if (Validator.validateInt(fieldValue)) { // convert fieldValue to an Integer Integer integerValue = Integer.getInteger(fieldValue); // store integerValue in a request attribute request.setAttribute("fieldName", integerValue); } ... // Use the request attribute for further processing Integer integerValue = (Integer)request.getAttribute("fieldName"); ...
```

應用程式應該處理的主要 Java 資料類型：

- Byte
- Short
- Integer
- Long

- Float
- Double
- Date

[3] 欄位長度

一律確定輸入參數（HTTP 要求參數或 Cookie 值）在長度下限及/或長度上限的範圍內。

驗證 `userName` 欄位的長度是否在 8-20 個字元之間的範例：

```
// Example to validate the field length public Class Validator { ... public static boolean validateLength(String value, int minLength, int maxLength)
{ String validatedValue = value; if (!validateRequired(value)) { validatedValue = ""; } return (validatedValue.length() >= minLength &&
validatedValue.length() <= maxLength); } ... } ... String userName = request.getParameter("userName"); if
(Validator.validateRequired(userName)) { if (Validator.validateLength(userName, 8, 20)) { // userName is valid, continue further processing ... } }
```

[4] 欄位範圍

一律確定輸入參數在函數需求定義的範圍內。驗證輸入 `numberOfChoices` 是否在 10-20 之間的範例：

```
// Example to validate the field range public Class Validator { ... public static boolean validateRange(int value, int min, int max) { return (value >=
min && value <= max); } ... } ... String fieldValue = request.getParameter("numberOfChoices"); if (Validator.validateRequired(fieldValue)) { if
(Validator.validateInt(fieldValue)) { int numberOfChoices = Integer.parseInt(fieldValue); if (Validator.validateRange(numberOfChoices, 10, 20)) {
// numberOfChoices is valid, continue processing request ... } }
```

[5] 欄位選項

Web 應用程式通常會向使用者呈現一組可供選擇的選項（例如：使用 `SELECT` HTML 標籤），但無法執行伺服器端驗證來確保所選的值是容許的選項之一。請記住，惡意的使用者可以輕易修改任何選項值。一律檢查使用者輸入是否符合功能需求所定義的型樣。

對照容許的選項清單來驗證使用者選項的範例：

```
// Example to validate user selection against a list of options public Class Validator { ... public static boolean validateOption(Object[] options,
Object value) { boolean isValidValue = false; try { List list = Arrays.asList(options); if (list != null) { isValidValue = list.contains(value); } } catch
(Exception e) { } return isValidValue; } ... } ... // Allowed options String[] options = {"option1", "option2", "option3"}; // Verify that the user selection
is one of the allowed options String userSelection = request.getParameter("userSelection"); if (Validator.validateOption(options, userSelection)) {
// valid user selection, continue processing request ... }
```

[6] 欄位型樣

一律檢查使用者輸入是否符合功能需求所定義的型樣。比方說，如果 `userName` 欄位只應接受英數字元，且不區分大小寫，請使用下列正規表示式：

`^[a-zA-Z0-9]*$`

Java 1.3 或更早的版本不包括任何正規表示式套件。建議搭配 Java 1.3 來使用「Apache 正規表示式套件」（請參閱下列「資源」），以解決這項支援欠缺。

執行正規表示式驗證的範例：

```
// Example to validate that a given value matches a specified pattern // using the Apache regular expression package import
org.apache.regexp.RE; import org.apache.regexp.RESyntaxException; public Class Validator { ... public static boolean matchPattern(String
value, String expression) { boolean match = false; if (validateRequired(expression)) { RE r = new RE(expression); match = r.match(value); }
return match; } ... } ... // Verify that the userName request parameter is alpha-numeric String userName = request.getParameter("userName"); if
(Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) { // userName is valid, continue processing request ... }
```

Java 1.4 引進了新的正規表示式套件（`java.util.regex`）。以下是 `Validator.matchPattern` 的修正版，使用新的 Java 1.4 正規表示式套件：

```
// Example to validate that a given value matches a specified pattern // using the Java 1.4 regular expression package import
java.util.regex.Pattern; import java.util.regex.Matcher; public Class Validator { ... public static boolean matchPattern(String value, String
expression) { boolean match = false; if (validateRequired(expression)) { match = Pattern.matches(expression, value); } return match; } ... }
```

[7] Cookie 值

請利用 `javax.servlet.http.Cookie` 物件來驗證 Cookie 值。依應用程式需求而定，相同的驗證規則（說明如上）也適用於 Cookie 值，例如：驗證必要的值、驗證長度，等等。

驗證必要 Cookie 值的範例：

```
// Example to validate a required cookie value // First retrieve all available cookies submitted in the HTTP request Cookie[] cookies =
request.getCookies(); if (cookies != null) { // find the "user" cookie for (int i=0; i<cookies.length; ++i) { if (cookies[i].getName().equals("user")) { //
validate the cookie value if (Validator.validateRequired(cookies[i].getValue()) { // valid cookie value, continue processing request ... } } }
```

[8] HTTP 回應

[8-1] 過濾使用者輸入

如果要保護應用程式免於遭受跨網站 Scripting，請將機密字元轉換成對應的字元實體來消毒 HTML。以下是 HTML 區分字元：

`<>"'%;)(& +`

將機密字元轉換成對應的字元實體來過濾指定字串的範例：

```
// Example to filter sensitive data to prevent cross-site scripting public Class Validator { ... public static String filter(String value) { if (value == null)
{ return null; } StringBuffer result = new StringBuffer(value.length()); for (int i=0; i<value.length(); ++i) { switch (value.charAt(i)) { case '<':
result.append("<"); break; case '>': result.append(">"); break; case '"': result.append("""); break; case ''': result.append("'"); break; case '%':
result.append("%"); break; case ';': result.append(";"); break; case '(': result.append("("); break; case ')': result.append(")"); break; case '&':
result.append("&"); break; case '+': result.append("+"); break; default: result.append(value.charAt(i)); break; } } return result; } ... } ... // Filter the
HTTP response using Validator.filter PrintWriter out = response.getWriter(); // set output response out.write(Validator.filter(response));
out.close();
```

Java Servlet API 2.3 引進了「過濾器」，它支援截取及轉換 HTTP 要求或回應。

利用「Servlet 過濾器」，以 `Validator.filter` 來消毒回應的範例：

```
// Example to filter all sensitive characters in the HTTP response using a Java Filter. // This example is for illustration purposes since it will filter
all content in the response, including HTML tags! public class SensitiveCharsFilter implements Filter { ... public void doFilter(ServletRequest
request, ServletResponse response, FilterChain chain) throws IOException, ServletException { PrintWriter out = response.getWriter();
ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response); chain.doFilter(request, wrapper); CharArrayWriter caw
```



```
= new CharArrayWriter(); caw.write(Validator.filter(wrapper.toString())); response.setContentType("text/html");
response.setContentLength(caw.toString().length()); out.write(caw.toString()); out.close(); } ... public class CharResponseWrapper extends
HttpServletResponseWrapper { private CharArrayWriter output; public String toString() { return output.toString(); } public
CharResponseWrapper(HttpServletResponse response){ super(response); output = new CharArrayWriter(); } public PrintWriter getWriter(){
return new PrintWriter(output); } } }
```

[8-2] 維護 Cookie 安全

當機密資料儲存在 Cookie 中，請務必利用 `Cookie.setSecure(boolean flag)`，在 HTTP 回應中設定 Cookie 的安全旗標，以指示瀏覽器利用 HTTPS 或 SSL 之類的安全通訊協定來傳送 Cookie。

維護 "user" Cookie 安全的範例：

```
// Example to secure a cookie, i.e. instruct the browser to // send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);
```

建議的 Java 工具

適用於伺服器端驗證的兩個主要的 Java 架構如下：

[1] Jakarta 一般驗證器（整合 Struts 1.1）

「Jakarta 一般驗證器」實作上述所有資料驗證需求，是一個功能強大的架構。這些規則配置在定義表單欄位輸入驗證規則的 XML 檔中。依預設，Struts 支援在利用 Struts 'bean:write' 標籤撰寫的所有資料上，過濾 [8] HTTP 回應中輸出的危險字元。

設定 'filter=false' 旗標可以停用這個過濾。

Struts 定義下列基本輸入驗證器，但也可以定義自訂驗證器：

required：如果欄位含有空格以外的任何字元，便告成功。

mask：如果值符合 **mask** 屬性給定的正規表示式，便告成功。

range：如果值在 **min** 和 **max** 屬性給定的值範圍內（(value >= min) 且 (value <= max)），便告成功。

maxLength：如果欄位長度小於或等於 **max** 屬性，便告成功。

minLength：如果欄位長度大於或等於 **min** 屬性，便告成功。

byte、**short**、**integer**、**long**、**float**、**double**：如果值可以轉換成對應的基本類型，便告成功。

date：如果值代表有效日期，便告成功。

可提供日期型樣。

creditCard：如果值可能是有效的信用卡號碼，便告成功。

e-mail：如果值可能是有效的電子郵件位址，便告成功。

利用「Struts 驗證器」驗證 loginForm 之 userName 欄位的範例：

```
<form-validation> <global> ... <validator name="required" classname="org.apache.struts.validator.FieldChecks" method="validateRequired"
msg="errors.required"> </validator> <validator name="mask" classname="org.apache.struts.validator.FieldChecks" method="validateMask"
msg="errors.invalid"> </validator> ... </global> <formset> <form name="loginForm"> <!-- userName is required and is alpha-numeric case
insensitive --> <field property="userName" depends="required,mask"> <!-- message resource key to display if validation fails --> <msg
name="mask" key="login.userName.maskmsg"/> <arg0 key="login.userName.displayName"/> <var> <var-name>mask</var-name> <var-
value>^[a-zA-Z0-9]*$</var-value> </var> </field> ... </form> ... </formset> </form-validation>
```

[2] JavaServer Faces 技術

「JavaServer Faces 技術」是一組代表使用者介面元件、管理元件狀態、處理事件及輸入驗證的 Java API (JSR 127)。JavaServer Faces API 實作下列基本驗證器，但可以定義自訂驗證器：

validate_doublerrange：登錄元件的 `DoubleRangeValidator`

validate_length：登錄元件的 `LengthValidator`

validate_longrange：登錄元件的 `LongRangeValidator`

validate_required：登錄元件的 `RequiredValidator`

validate_stringrange：登錄元件的 `StringRangeValidator`

validator：登錄元件的自訂 `Validator`

JavaServer Faces API 定義下列 UIInput 和 UIOutput 展現器（標籤）：

input_date：接受以 `java.text.Date` 實例格式化的 `java.util.Date`

output_date：顯示以 `java.text.Date` 實例格式化的 `java.util.Date`

input_datetime：接受以 `java.text.Time` 實例格式化的 `java.util.Date`

output_datetime：顯示以 `java.text.Time` 實例格式化的 `java.util.Date`

input_number：顯示以 `java.text.NumberFormat` 格式化的數值資料類型（`java.lang.Number` 或基本資料類型）

output_number：顯示以 `java.text.NumberFormat` 格式化的數值資料類型（`java.lang.Number` 或基本資料類型）

input_text：接受單行字串。

output_text：顯示單行字串。

input_time：接受以 `java.text.DateFormat` 時間實例格式化的 `java.util.Date`

output_time：顯示以 `java.text.DateFormat` 時間實例格式化的 `java.util.Date`

input_hidden：可讓頁面作者將隱藏變數併入頁面

input_secret：接受不含空格的單行文字，輸入之時，將它顯示成一組星號

input_textarea：接受多行文字

output_errors：顯示整個頁面的錯誤訊息，或指定之用戶端 ID 的相關錯誤訊息

output_label：將巢狀元件顯示為指定輸入欄位的標籤

output_message：顯示本地化訊息

利用 JavaServer Faces 驗證 loginForm 之 userName 欄位的範例：

```
<%@ taglib uri="https://docs.oracle.com/javaee/6/tutorial/doc/glxce.html" prefix="h" %> <%@ taglib uri="http://mrbool.com/how-to-create-a-
login-validation-with-jsf-java-server-faces/27046" prefix="f" %> ... <jsp:useBean id="UserBean" class="myApplication.UserBean"
scope="session" /> <f:use_faces> <h:form formName="loginForm"> <h:input_text id="userName" size="20"
modelReference="UserBean.userName"> <f:validate_required/> <f:validate_length minimum="8" maximum="20"/> </h:input_text> <!-- display
```

```
errors if present --> <h:output_errors id="loginErrors" clientId="userName"/> <h:command_button id="submit" label="Submit"
commandName="submit" /><p> </h:form> </f:use_faces>
```

參照

Java API 1.3 -

<https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html>

Java API 1.4 -

<https://www.oracle.com/java/technologies/java-archive-14docs-downloads.html>

Java Servlet API 2.3 -

<https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api>

Java 正規表示式套件 -

<http://jakarta.apache.org/regexp/>

Jakarta 驗證器 -

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技術 -

<http://www.javaserverfaces.org/>

** 錯誤處理：

許多 J2EE Web 應用程式架構都遵循「模型視圖控制器 (MVC)」型樣。在這個型樣中，Servlet 扮演控制器的角色。Servlet 將應用程式處理程序委派給 JavaBean，例如，EJB Session Bean（模型）。之後，Servlet 再將要求轉遞給 JSP（視圖）來呈現處理結果。Servlet 應該檢查所有輸入、輸出、回覆碼、錯誤碼及已知的異常狀況，以確保會實際進行預期的處理程序。資料驗證可以保護應用程式免於遭受惡意的資料竄改，有效的錯誤處理策略則是防止應用程式意外揭露內部錯誤訊息（例如：異常狀況堆疊追蹤）所不可或缺。好的錯誤處理策略會處理下列項目：

[1] 定義錯誤

[2] 報告錯誤

[3] 呈現錯誤

[4] 錯誤對映

[1] 定義錯誤

應該避免將錯誤訊息寫在應用程式層（例如：Servlet）。相反地，應用程式應該使用對映至已知之應用程式失敗的錯誤索引鍵。在實務中，好的做法是定義錯誤索引鍵來對映至 HTML 表單欄位或其他 Bean 內容的驗證規則。比方說，如果需要 "user_name" 欄位，它必須是英數字元，且在資料庫中必須是唯一，便應該定義下列錯誤索引鍵：

(a) ERROR_USERNAME_REQUIRED：這個錯誤索引鍵用來顯示一則訊息，通知使用者需要 "user_name" 欄位；

(b) ERROR_USERNAME_ALPHANUMERIC：這個錯誤索引鍵用來顯示一則訊息，通知使用者 "user_name" 欄位應該是英數字元；

(c) ERROR_USERNAME_DUPLICATE：這個錯誤索引鍵用來顯示一則訊息，通知使用者 "user_name" 值在資料庫中重複；

(d) ERROR_USERNAME_INVALID：這個錯誤索引鍵用來顯示一則一般訊息，通知使用者 "user_name" 值無效；

在實務中，好的做法是定義下列架構 Java 類別來儲存及報告應用程式錯誤：

- ErrorKeys：定義所有錯誤索引鍵

```
// Example: ErrorKeys defining the following error keys: // - ERROR_USERNAME_REQUIRED // - ERROR_USERNAME_ALPHANUMERIC // -
ERROR_USERNAME_DUPLICATE // - ERROR_USERNAME_INVALID // ... public Class ErrorKeys { public static final String
ERROR_USERNAME_REQUIRED = "error.username.required"; public static final String ERROR_USERNAME_ALPHANUMERIC =
"error.username.alphanumeric"; public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate"; public static final
String ERROR_USERNAME_INVALID = "error.username.invalid"; ... }
```

- Error：封裝個別錯誤

```
// Example: Error encapsulates an error key. // Error is serializable to support code executing in multiple JVMs. public Class Error implements
Serializable { // Constructor given a specified error key public Error(String key) { this(key, null); } // Constructor given a specified error key and
array of placeholder objects public Error(String key, Object[] values) { this.key = key; this.values = values; } // Returns the error key public String
getKey() { return this.key; } // Returns the placeholder values public Object[] getValues() { return this.values; } private String key = null; private
Object[] values = null; }
```

- Errors：封裝錯誤的集合

```
// Example: Errors encapsulates the Error objects being reported to the presentation layer. // Errors are stored in a HashMap where the key is
the bean property name and value is an // ArrayList of Error objects. public Class Errors implements Serializable { // Adds an Error object to the
Collection of errors for the specified bean property. public void addError(String property, Error error) { ArrayList propertyErrors =
(ArrayList)errors.get(property); if (propertyErrors == null) { propertyErrors = new ArrayList(); errors.put(property, propertyErrors); }
propertyErrors.put(error); } // Returns true if there are any errors public boolean hasErrors() { return (errors.size > 0); } // Returns the Errors for
the specified property public ArrayList getErrors(String property) { return (ArrayList)errors.get(property); } private HashMap errors = new
HashMap(); }
```

以下是利用上述架構類別來處理 "user_name" 欄位驗證錯誤的範例：

```
// Example to process validation errors of the "user_name" field. Errors errors = new Errors(); String userName =
request.getParameter("user_name"); // (a) Required validation rule if (!Validator.validateRequired(userName)) { errors.addError("user_name",
new Error(ErrorKeys.ERROR_USERNAME_REQUIRED)); } // (b) Alpha-numeric validation rule else if (!Validator.matchPattern(userName, "[a-
zA-Z0-9]*$")) { errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC)); } else { // (c) Duplicate check
validation rule // We assume that there is an existing UserValidationEJB session bean that implements // a checkIfDuplicate() method to verify if
the user already exists in the database. try { ... if (UserValidationEJB.checkIfDuplicate(userName)) { errors.addError("user_name", new
Error(ErrorKeys.ERROR_USERNAME_DUPLICATE)); } } catch (RemoteException e) { // log the error logger.error("Could not validate user for
specified userName: " + userName); errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE)); } } // set the
errors object in a request attribute called "errors" request.setAttribute("errors", errors); ...
```

[2] 報告錯誤

報告 Web 層應用程式錯誤的方式有兩種：

(a) Servlet 錯誤機制

(b) JSP 錯誤機制

[2-a] Servlet 錯誤機制

Servlet 報告錯誤的可能方式如下：

- 轉遞至輸入 JSP（已將錯誤儲存在要求屬性中），或
- 利用 HTTP 錯誤碼引數來呼叫 `response.sendError`，或
- 擲出異常狀況

在實務中，好的做法是處理所有已知的應用程式錯誤（依照 [1] 區段所說明），將它們儲存在要求屬性中，再轉遞給輸入 JSP。輸入 JSP 應該顯示錯誤訊息，並提示使用者重新輸入資料。下列範例說明如何轉遞到輸入 JSP (`userInput.jsp`)：

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd =
getServletContext().getRequestDispatcher("/user/userInput.jsp"); if (rd != null) { rd.forward(request, response); }
```

如果 Servlet 無法轉遞到已知的 JSP 頁面，第二個選項是利用 `response.sendError` 方法，設定

`HttpServletResponse.SC_INTERNAL_SERVER_ERROR` 引數（狀態碼 500）來報告錯誤。

請參閱 `javax.servlet.http.HttpServletResponse` javadoc，以取得各種 HTTP 狀態碼的詳細資訊。

傳回 HTTP 錯誤的範例：

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp"); if (rd == null) {
// messages is a resource bundle with all message keys and values
response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID)); }
```

作為最後的手段，Servlet 可以擲出異常狀況，它必須是下列類別之一的子類別：

- `RuntimeException`
- `ServletException`
- `IOException`

[2-b] JSP 錯誤機制 JSP 頁面依照下列範例所示來定義 `errorPage` 指引，從而提供了執行時期異常狀況的處理機制：

```
<%@ page errorPage="/errors/userValidation.jsp" %>
```

未捕捉的 JSP 異常狀況是轉遞到指定的 `errorPage`，而原始異常狀況則設在稱為 `javax.servlet.jsp.jspException` 的要求參數中。錯誤頁面必須包含 `isErrorPage` 指引，如下所示：

```
<%@ page isErrorPage="true" %>
```

`isErrorPage` 指引會使 "exception" 變數起始設定為所擲出的異常狀況物件。

[3] 呈現錯誤

J2SE Internationalization API 提供用來提出應用程式資源以及將訊息格式化的公用程式類別，其中包括：

(a) 資源組

(b) 訊息格式化

[3-a] 資源組

資源組會將本地化的資料與使用它的原始碼分開，從而支援國際化。每個資源組都會儲存特定語言環境之鍵值配對的對映。

通常是利用或延伸 `java.util.PropertyResourceBundle`，它會將內容儲存在外部內容檔中，如下列範例所示：

```
##### # ErrorMessages.properties
##### # required user name error message
error.username.required=User name field is
required # invalid user name format
error.username.alphanumeric=User name must be alphanumeric # duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one ...
```

定義多重資源可以支援不同的語言環境（因此稱為資源組）。例如，定義 `ErrorMessages_fr.properties` 可以支援資源組系列的法國成員。如果要求之語言環境的資源成員不存在，便會使用預設成員。

在上述範例中，預設資源是 `ErrorMessages.properties`。

在上述範例中，預設資源是 `ErrorMessages.properties`。依使用者的語言環境而定，應用程式（JSP 或 Servlet）會從適當的資源擷取內容。

[3-b] 訊息格式化

J2SE 標準類別 `java.util.MessageFormat` 提供以取代位置保留元來建立訊息的一般方式。`MessageFormat` 物件包含內嵌了格式指定元的型樣字串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

以下是利用 `ResourceBundle` 和 `MessageFormat` 來呈現錯誤訊息的更綜合性的範例：

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public Class ErrorMessageResource { // Returns the error message for the specified error key in the environment locale
public String getErrorMessage(String errorKey) { return getErrorMessage(errorKey, defaultLocale); } // Returns the error message for the specified error key in the specified locale
public String getErrorMessage(String errorKey, Locale locale) { return getErrorMessage(errorKey, null, locale); } // Returns a formatted error message for the specified error key in the specified locale
public String getErrorMessage(String errorKey, Object[] args, Locale locale) { // Get localized ErrorMessageResource
ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale); // Get localized error message
String errorMessage = errorMessageResource.getString(errorKey); if (args != null) { // Format the message using the specified placeholders
args return MessageFormat.format(errorMessage, args); } else { return errorMessage; } } // default environment locale
private Locale defaultLocale = Locale.getDefaultLocale(); } ... // Get the user's locale
Locale userLocale = request.getLocale(); // Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors"); if (errors != null && errors.hasErrors()) { // iterate through errors and output error messages corresponding to the "user_name" property
ArrayList userNameErrors = errors.getErrors("user_name"); ListIterator iterator = userNameErrors.iterator(); while (iterator.hasNext()) { // Get the next error object
Error error = (Error)iterator.next(); String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale); output.write(errorMessage + "\r\n"); } }
```

建議您定義自訂 JSP 標籤（如 `displayErrors`）來疊代處理及呈現錯誤訊息，如上述範例所示。

[4] 錯誤對映

一般而言，「Servlet 儲存器」會傳回對應於回應狀態碼或異常狀況的預設錯誤頁面。您可以利用自訂錯誤頁面來指定狀態碼或異常狀況與 Web 資源之間的對映。

在實務中，好的做法是開發不揭露內部錯誤狀態的靜態錯誤頁面（依預設，大部分 Servlet 儲存器都會報告內部錯誤訊息）。這項對映是依照下列範例所指定，配置在「Web 部署描述子 (web.xml)」中：

```
<!-- Mapping of HTTP error codes and application exceptions to error pages --> <error-page> <exception-
type>UserValidationException</exception-type> <location>/errors/validationError.html</error-page> </error-page> <error-page> <error-
code>500</error-code> <location>/errors/internalError.html</error-page> </error-page> ... </error-page> ...
```

建議的 Java 工具

適用於伺服器端驗證的兩個主要的 Java 架構如下：

[1] Jakarta 一般驗證器（整合 Struts 1.1）

「Jakarta 一般驗證器」是依照上述說明來定義錯誤處理機制的 Java 架構。驗證規則配置在 XML 檔中，檔案定義了表單欄位的輸入驗證規則以及對應的驗證錯誤索引鍵。Struts 提供國際化支援，供您利用資源組和訊息格式化來建置本地化應用程式。

利用「Struts 驗證器」驗證 loginForm 之 userName 欄位的範例：

```
<form-validation> <global> ... <validator name="required" classname="org.apache.struts.validator.FieldChecks" method="validateRequired"
msg="errors.required"> </validator> <validator name="mask" classname="org.apache.struts.validator.FieldChecks" method="validateMask"
msg="errors.invalid"> </validator> ... </global> <formset> <form name="loginForm"> <!-- userName is required and is alpha-numeric case
insensitive --> <field property="userName" depends="required,mask"> <!-- message resource key to display if validation fails --> <msg
name="mask" key="login.userName.maskmsg"/> <arg0 key="login.userName.displayName"/> <var> <var-name>mask</var-name> <var-
value>^[a-zA-Z0-9]*$</var-value> </var> </field> ... </formset> </form-validation>
```

Struts JSP 標籤庫定義了有條件地顯示一組累計錯誤訊息的 "errors" 標籤，如下列範例所示：

```
<%@ page language="java" %> <%@ taglib uri="/WEB-INF/struts-bean.tld"
prefix="bean" %> <html:html> <head> <body> <html:form action="/login.do"> <table border="0" width="100%"> <tr> <th align="right">
<html:errors property="username"/> <bean:message key="prompt.username"/> </th> <td align="left"> <html:text property="username"
size="16"/> </td> </tr> <tr> <td align="right"> <html:submit><bean:message key="button.submit"/></html:submit> </td> <td align="right">
<html:reset><bean:message key="button.reset"/></html:reset> </td> </tr> </table> </html:form> </body> </html:html>
```

[2] JavaServer Faces 技術

「JavaServer Faces 技術」是一組代表使用者介面元件、管理元件狀態、處理事件、驗證輸入，以及支援國際化的 Java API (JSR 127)。

JavaServer Faces API 定義了 "output_errors" UIOutput 展現器，以顯示整個頁面的錯誤訊息，或指定之用戶端 ID 的相關錯誤訊息。

利用 JavaServer Faces 驗證 loginForm 之 userName 欄位的範例：

```
<%@ taglib uri="https://docs.oracle.com/javaee/6/tutorial/doc/glxce.html" prefix="h" %> <%@ taglib uri="http://mrbool.com/how-to-create-a-
login-validation-with-jsf-java-server-faces/27046" prefix="f" %> ... <jsp:useBean id="UserBean" class="myApplication.UserBean"
scope="session" /> <f:use_faces> <h:form formName="loginForm"> <h:input_text id="userName" size="20"
modelReference="UserBean.userName"> <f:validate_required/> <f:validate_length minimum="8" maximum="20"/> </h:input_text> <!-- display
errors if present --> <h:output_errors id="loginErrors" clientId="userName"/> <h:command_button id="submit" label="Submit"
commandName="submit" /><p> </h:form> </f:use_faces>
```

參照

Java API 1.3 -

<https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html>

Java API 1.4 -

<https://www.oracle.com/java/technologies/java-archive-14docs-downloads.html>

Java Servlet API 2.3 -

<https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api>

Java 正規表示式套件 -

<http://jakarta.apache.org/regexp/>

Jakarta 驗證器 -

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技術 -

<http://www.javaserverfaces.org/>

** 驗證輸入資料：

雖然為了使用者的方便，可以在用戶端層提供資料驗證，但一律必須在伺服器層執行資料驗證。用戶端驗證原本就不安全，因為它們可以輕易略過，例如：停用 JavaScript。

好的設計通常需要 Web 應用程式架構提供伺服器端公用程式常式來驗證下列項目：

[1] 必要欄位

[2] 欄位資料類型（依預設，所有 HTTP 要求參數都是 String）

[3] 欄位長度

[4] 欄位範圍

[5] 欄位選項

[6] 欄位型態

[7] Cookie 值

[8] HTTP 回應

在實務中，好的做法是實作一或多個驗證各個應用程式參數的函數。下列各節說明一些檢查範例。

[1] 必要欄位

一律檢查確認欄位不是空值，欄位長度大於零，且不含在前端及尾端的空格。

如何驗證必要欄位的範例：

```
// PHP example to validate required fields function validateRequired($input) { ... $pass = false; if (strlen(trim($input))>0){ $pass = true; } return
$pass; ... } ... if (validateRequired($fieldName)) { // fieldName is valid, continue processing request ... }
```

[2] 欄位資料類型

在 Web 應用程式中，所輸入的輸入參數設定不良。例如，所有 HTTP 要求參數或 Cookie 值都是 String 類型。開發人員負責確認輸入的資料類型正確。

[3] 欄位長度

一律確定輸入參數（HTTP 要求參數或 Cookie 值）在長度下限及/或長度上限的範圍內。

[4] 欄位範圍

一律確定輸入參數在函數需求定義的範圍內。

[5] 欄位選項

Web 應用程式通常會向使用者呈現一組可供選擇的選項（例如：使用 SELECT HTML 標籤），但無法執行伺服器端驗證來確保所選的值是容許的選項之一。請記住，惡意的使用者可以輕易修改任何選項值。一律檢查使用者輸入是否符合功能需求所定義的型樣。

[6] 欄位型樣 一律檢查使用者輸入是否符合功能需求所定義的型樣。比方說，如果 userName 欄位只應接受英數字元，且不區分大小寫，請使用下列正規表示式：

```
^[a-zA-Z0-9]+$
```

[7] Cookie 值

依應用程式需求而定，相同的驗證規則（說明如上）也適用於 Cookie 值，例如：驗證必要的值、驗證長度，等等。

[8-1] 過濾使用者輸入

如果要保護應用程式免於遭受跨網站 Scripting，開發人員應該將機密字元轉換成對應的字元實體來消毒 HTML。以下是 HTML 區分字元：

```
<>"'%;)( & +
```

PHP 包括一些 htmlentities() 之類的自動化消毒公用程式函數：

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

此外，為了避免「跨網站 Scripting」的 UTF-7 變式，您應該明確定義回應的 Content-Type 標頭，例如：

```
<?php header('Content-Type: text/html; charset=UTF-8'); ?>
```

[8-2] 維護 Cookie 安全

當機密資料儲存在 Cookie 中，且透過 SSL 來傳輸它時，請務必先在 HTTP 回應中設定 Cookie 的安全旗標。這會指示瀏覽器只透過 SSL 連線來使用這個 Cookie。

您可以利用下列程式碼範例來維護 Cookie 安全：

```
<$php $value = "some_value"; $time = time()+3600; $path = "/application/"; $domain = ".example.com"; $secure = 1; setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE); ?>
```

此外，我們建議您使用 HttpOnly 旗標。當 HttpOnly 旗標設為 TRUE 時，只能透過 HTTP 通訊協定來存取 Cookie。這表示無法用 JavaScript 之類的 Scripting 語言存取 Cookie。這個設定有助於實際減少透過 XSS 攻擊來盜用身分的情況（不過，並非所有瀏覽器都支援）。PHP 5.2.0 新增 HttpOnly 旗標。

參照

[1] 利用「HTTP 專用 Cookie」緩和「跨網站 Scripting」：

<http://msdn2.microsoft.com/en-us/library/ms533046.aspx>

[2] PHP 安全聯盟：

<http://phpsec.org/>

[3] PHP & Web 應用程式安全部落格 (Chris Shiflett)：

<http://shiflett.org/>

低 檢閱將 SameSite Cookie 屬性配置為建議值的可能解決方案

目錄

此作業所修正的問題類型

- SameSite 屬性不安全、不適當或遺漏的 Cookie

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。

諮詢

SQL 注入

目錄

測試類型：

Application

威脅分類：

SQL 注入

原因：

未正確地消毒使用者所輸入的危險字元

安全風險：

有可能檢視、修改或刪除資料庫項目和表格

CWE：

89

參照：

OWASP - SQL 注入預防速查表

技術說明：

未正確地消毒使用者輸入上的危險字元。

動態產生包括未驗證使用者輸入的查詢，可能會導致 SQL 注入攻擊。攻擊者可以在可能導致以不安全方式執行查詢的使用者輸入中插入 SQL 指令或修飾元。

如果未對使用者可控制輸入進行充分驗證和封裝，則所產生的 SQL 查詢可能會導致將這些輸入解譯為 SQL，而非一般使用者資料。這可能用來變更查詢邏輯以略過安全檢查，或插入其他可修改後端資料庫的陳述式，可能會包括執行系統指令。

SQL 有效負載可以透過任何不受信任的資料進入系統，包括使用者輸入、先前儲存在資料庫中的資料、檔案、第三方 API 等。

可能的結果包括遺失：

機密性 - 因為 SQL 資料庫一般會保留機密資料，所以減損機密性是常見的 SQL 注入漏洞問題。

鑑別 - 如果使用不佳的 SQL 指令檢查使用者名稱和密碼，則可能會以另一個先前不知道密碼的使用者身分來連接至系統。

授權 - 如果授權資訊保留在 SQL 資料庫中，則可能可以透過成功惡意探索 SQL 注入漏洞來變更此資訊。

完整性 - 如同可能可以讀取機密性資訊一樣，也可能進行變更，甚至使用 SQL 注入攻擊來刪除此資訊。

未加密的登入要求

目錄

測試類型：

Application

威脅分類：

傳輸層保護不足

原因：

機密性輸入欄位（如：使用者名稱、密碼和信用卡號碼）傳遞時未加密

安全風險：

有可能竊取以未加密方式傳送的使用者登入資訊，如：使用者名稱和密碼

CWE：

0

技術說明：

SSL (Secure Socket Layer) 可為 HTTP 提供資料機密性和整合性。透過加密 HTTP 訊息，SSL 可保護訊息不受攻擊者竊聽或更改訊息內容。登入頁面應一律運用 SSL，在使用者名稱和密碼從用戶端轉移至伺服器時加以保護。若未使用 SSL，會導致使用者認證在傳輸至伺服器期間以純文字形式暴露，並使得認證容易遭到竊聽。

查詢中的 Password 參數

[目錄](#)

測試類型：

Application

威脅分類：

資訊洩漏

原因：

查詢字串中傳遞了機密性輸入欄位（如：使用者名稱、密碼和信用卡號碼）

安全風險：

有可能竊取查詢字串中傳送的機密資料，如：使用者名稱和密碼

CWE：

0

技術說明：

SSL (Secure Socket Layer) 可為 HTTP 提供資料機密性和整合性。透過加密 HTTP 訊息，SSL 可保護訊息不受攻擊者竊聽或更改訊息內容。登入頁面應一律運用 SSL，在使用者名稱和密碼從用戶端轉移至伺服器時加以保護。若未使用 SSL，會導致使用者認證在傳輸至伺服器期間以純文字形式暴露，並使得認證容易遭到竊聽。

不適當地封鎖帳戶

測試類型：

Application

威脅分類：

強制入侵

原因：

不安全的 Web 應用程式設計或配置

安全風險：

有可能透過 Web 應用程式升級使用者專用權及取得管理許可權

受影響的產品：

CWE：

307

參照：

"Blocking Brute-Force Attacks"，作者：Mark Burnett

技術說明：

不安全的 Web 應用程式設計或配置

有可能透過 Web 應用程式升級使用者專用權及取得管理許可權

AppScan 偵測到應用程式未限制錯誤登入嘗試次數。

其用不正確的密碼傳送了 10 次要求，接著使用正確的認證順利登入。

未限制錯誤登入嘗試次數，會使應用程式易受到強制入侵攻擊。

強制入侵攻擊是指惡意使用者嘗試傳送大量可能的密碼及/或使用者名稱，以便存取應用程式。

由於這個技術包含大量登入嘗試，未限制錯誤登入要求次數的應用程式很容易遭到這類攻擊。

因此，強烈建議您限制容許帳戶錯誤登入的嘗試次數，超過這個次數，便鎖定帳戶。不當運用範例如下：

下列要求說明密碼猜測要求：

`http://site/login.asp?username=EXISTING_USERNAME&password=GUESSED_PASSWORD`

如果在嘗試錯誤若干次之後，網站不鎖定帳戶，攻擊者最終可能會探索出帳戶密碼，並利用它來假冒帳戶的合法使用者。

未更新階段作業 ID

測試類型：

Application

威脅分類：

階段作業固定

原因：

不安全的 Web 應用程式設計或配置

安全風險：

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

受影響的產品：

CWE：

304

參照：

"Session Fixation Vulnerability in Web-based Applications"，作者：Mitja Kolsek - Acros Security
PHP Manual, Session Handling Functions, Sessions and security

技術說明：

不安全的 Web 應用程式設計或配置

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

鑑別使用者，或是建立新的使用者階段作業，而不使任何現有的階段作業 ID 失效，會讓攻擊者有機會竊取已鑑別的階段作業。

在下列情況中，經常會觀察到這類實務：

[1] Web 應用程式鑑別使用者時未先使現有的階段作業失效，因而繼續使用已經與該使用者相關聯的階段作業

[2] 攻擊者能夠對某位使用者強制使用已知的階段作業 ID，當該使用者鑑別之後，攻擊者即有權存取已鑑別的階段作業

[3] 應用程式或儲存器使用了可預測的階段作業 ID。

在階段作業固定漏洞的一般運用中，攻擊者會對 Web 應用程式建立新的階段作業，並記錄相關聯的階段作業 ID。接著攻擊者會使受害者利用該階段作業 ID 來對伺服器產生關聯（可能還會進行鑑別），讓攻擊者透過作用中的階段作業有權存取該使用者的帳號。

AppScan 發現登入程序前後的該階段作業 ID 未更新，表示假冒使用者是有可能的。初步得知階段作業 ID 之後，遠端攻擊者就有可能冒充已登入的合法使用者。

攻擊的流程：

a) 攻擊者會使用受害者的瀏覽器來開啟有漏洞網站的登入表單。

b) 開啟表單之後，攻擊者會記下階段作業 ID 值並等待。

c) 當受害者登入有漏洞的網站時，其階段作業 ID 並未更新。

d) 接著攻擊者就可以使用該階段作業 ID 值來假冒受害使用者，並代替他來進行操作。

利用「跨網站 Scripting」漏洞可以取得階段作業 ID 值，導致受害者的瀏覽器在聯絡有漏洞的網站時，使用預定的階段作業 ID；啟動「階段作業固定」攻擊也可以取得階段作業 ID 值，導致網站在受害者的瀏覽器中呈現預定的階段作業 ID。

偽造跨網站要求

目錄

測試類型：

Application

威脅分類：

偽造跨網站要求

原因：

應用程式所使用的鑑別方法不足

安全風險：

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

CWE：

352

參照：

[OWASP CSRF 速查表](#)

[OWASP CSRFGuard](#)

技術說明：

當應用程式在未驗證要求是否為故意傳送的情況下即容許使用者執行某個機密動作時，就會產生漏洞。

攻擊者可以讓受害者的瀏覽器對應用程式中的任意 URL 發出 HTTP 要求。從已鑑別受害者的瀏覽器傳送此要求時，其中將會包括受害者的階段作業 **Cookie** 或鑑別標頭。應用程式會將此要求接受為來自已鑑別使用者的有效要求。

如果設計 Web 伺服器接收來自用戶端的要求，但沒有任何機制驗證是否故意傳送該要求，則攻擊者可能可以誘騙用戶端從不同的網站提出非故意要求，而應用程式會將這個非故意要求視為真實要求。此作業的作法是提交表單、載入影像、以 JavaScript 傳送 XMLHttpRequest 等。

例如，此 IMG 標籤可以內嵌於攻擊者的網頁，而受害者的瀏覽器將會提交擷取該影像的要求。應用程式將會處理此有效要求，而瀏覽器不會顯示損毀影像。``。因此，系統會使用受害者的階段作業，將金錢從受害者的帳戶轉移給攻擊者。

攻擊者可以惡意探索此漏洞，以利用另一個使用者的帳戶或使用其專用權來執行機密動作。

攻擊者可能會濫用客戶的階段作業有效地假冒合法使用者。這容許攻擊者變更使用者記錄，以及以該使用者的身分來執行交易。

如果使用者目前登入受害者網站，則要求將會自動使用使用者的認證，例如階段作業 **Cookie**、IP 位址及其他瀏覽器鑑別方法。使用此方法時，攻擊者會偽造受害者的身分並代表他們提交動作。

此漏洞的嚴重性取決於應用程式環境定義中受影響的功能。例如，與轉帳或設定檔更新頁面上的 **CSRF** 攻擊相較之下，搜尋頁面上的 **CSRF** 攻擊較不嚴重。

登入錯誤訊息認證列舉

目錄

測試類型：

Application

威脅分類：

強制入侵

原因：

已向使用者顯示可能含有機密性除錯資訊的異常狀況和錯誤訊息

安全風險：

有可能透過 Web 應用程式升級使用者專用權及取得管理許可權

受影響的產品：

CWE：

204

參照：

"Blocking Brute-Force Attacks"，作者：Mark Burnett

技術說明：

已向使用者顯示可能含有機密性除錯資訊的異常狀況和錯誤訊息

有可能透過 Web 應用程式升級使用者專用權及取得管理許可權

當試圖利用不正確的認證來登入，在使用者分別輸入無效的使用者名稱及無效的密碼時，應用程式會分別產生不同的錯誤訊息。攻擊者可以利用這個行為，透過試誤法實驗（強制入侵技術）以建立應用程式的有效使用者名稱，再繼續嘗試探索相關的密碼。結果會列舉有效的使用者名稱和密碼，可供攻擊者用來存取帳戶。

不當運用範例如下：

如果下列要求收到不同的錯誤訊息，就有可能對網站發出強制入侵攻擊，並列舉使用者名稱和密碼：

[1] GET /login.asp?username=BAD_USERNAME&password=correct_password

[2] GET /login.asp?username=correct_username&password=BAD_PASSWORD

SameSite 屬性不安全、不適當或遺漏的 Cookie

目錄

測試類型：

Application

威脅分類：

伺服器配置錯誤

原因：

SameSite 屬性不適當、不安全或遺漏的機密 Cookie

安全風險：

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。

受影響的產品：

CWE：

1275

參照：

WASC 威脅分類：資訊洩漏

SameSite Cookie

技術說明：

SameSite 屬性不適當、不安全或遺漏的機密 Cookie

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**

未停用密碼欄位的自動完成 **HTML** 屬性

目錄

測試類型：

Application

威脅分類：

資訊洩漏

原因：

不安全的 **Web** 應用程式設計或配置

安全風險：

有可能略過 **Web** 應用程式的鑑別機制

受影響的產品：

CWE：

522

技術說明：

不安全的 **Web** 應用程式設計或配置

有可能略過 **Web** 應用程式的鑑別機制

在 **HTML5** 標準中，"**autocomplete**" 屬性已經標準化。W3C 的網站陳述該屬性有兩種狀態，"**on**" 和 "**off**"，如果完全省略，等同於設定為 "**on**"。此頁面是有漏洞的，因為對於 "**input**" 元素中的 "**password**" 欄位，並不會將 "**autocomplete**" 屬性設為 "**off**"。這樣可能會讓未獲授權的使用者（擁有進入授權用戶端的本端存取權）趁機自動填入使用者名稱和密碼欄位，從而登入網站。

在階段作業 **Cookie** 中遺漏 **HttpOnly** 屬性

目錄

測試類型：

Application

威脅分類：

資訊洩漏

原因：

Web 應用程式設定的階段作業 Cookie 不含 HttpOnly 屬性

安全風險：

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

受影響的產品：

CWE：

653

技術說明：

Web 應用程式設定的階段作業 Cookie 不含 HttpOnly 屬性

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

在應用程式測試期間，偵測到所測試的 Web 應用程式設定了不含 "HttpOnly" 屬性的階段作業 Cookie。由於這個階段作業 Cookie 不含 "HttpOnly" 屬性，因此其可由注入網站的惡意 Script 來存取，值也可能被竊取。儲存在階段作業記號中的任何資訊都可能被竊取，之後再用來盜用身分或模擬使用者。

找到資料庫錯誤型樣

[目錄](#)

測試類型：

Application

威脅分類：

SQL 注入

原因：

未正確地消毒使用者所輸入的危險字元

安全風險：

有可能檢視、修改或刪除資料庫項目和表格

受影響的產品：

參照：

"Web Application Disassembly with ODBC Error Messages"（作者：David Litchfield）

技術說明：

未正確地消毒使用者所輸入的危險字元

有可能檢視、修改或刪除資料庫項目和表格

AppScan 在測試回應中探索到「SQL 注入」以外的攻擊所觸發的「資料庫錯誤」。

雖然不確定，但這個錯誤可能表示應用程式有「SQL 注入」漏洞。

若是如此，請仔細閱讀下列「SQL 注入」諮詢。

軟體會使用受外部影響的輸入來建構所有或部分 SQL 指令，但是在傳送至資料庫時，其會誤使可修改預期 SQL 指令的特殊元素失效。

如果未針對可由使用者控制的輸入進行充分移除或加引號，其所產生的 SQL 查詢可能會造成這些輸入被解譯為 SQL 而非一般使用者資料。這可能會被用來改變查詢邏輯以略過安全檢查，或插入其他陳述式以修改後端資料庫，且可能包括執行系統指令。

例如，假設有一個 HTML 頁面含有登入表單，最終會使用使用者輸入對資料庫執行下列 SQL 查詢：

```
SELECT * FROM accounts WHERE username='$user' AND password='$pass'
```

\$user 和 \$pass 這兩個變數包含使用者在登入表單中所輸入的使用者認證。

因此，如果使用者輸入 "jsmith" 作為使用者名稱，且輸入 "Demo1234" 作為密碼，則 SQL 查詢會看起來如下：

```
SELECT * FROM accounts WHERE username='jsmith' AND password='Demo1234'
```

但是，如果使用者輸入 ""（一個單引號）作為使用者名稱，且輸入 ""（一個單引號）作為密碼，則 SQL 查詢會看起來如下：

```
SELECT * FROM accounts WHERE username="" AND password=""
```

這當然是形態異常的 SQL 查詢，且會呼叫可能在 HTTP 回應中傳回的錯誤訊息。

這類錯誤會通知攻擊者 SQL 注入已成功，而會引導攻擊者嘗試進一步攻擊手法。

不當運用範例如下：

下列 C# 程式碼會以動態方式建構並執行 SQL 查詢，來搜尋與指定名稱相符的項目。查詢會將顯示的項目限定為其擁有者與目前已鑑別之使用者的使用者名稱相符的項目。

```
... string userName = ctx.getAuthenticatedUserName(); string query = "SELECT * FROM items WHERE owner = "" + userName + "" AND itemname = "" + ItemName.Text + """; sda = new SqlDataAdapter(query, conn); DataTable dt = new DataTable(); sda.Fill(dt); ...
```

這個程式碼打算執行的查詢如下：

```
SELECT * FROM items WHERE owner = AND itemname = ;
```

然而，由於查詢是以動態方式連結（藉由將常數基本查詢字串連結到使用者輸入字串），只有當 itemName 未包含單引號字元時，查詢才可以正常運作。如果使用者名為 wiley 的攻擊者輸入字串 "name' OR 'a'='a" 來作為 itemName，則查詢會變成下列項目：

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name' OR 'a'='a';
```

額外的 OR 'a'='a' 條件會導致 where 子句一律評估為 true，所以查詢在邏輯上相當於更簡易的查詢：

```
SELECT * FROM items;
```

偵測到隱藏目錄

目錄

測試類型：

Infrastructure

威脅分類：

資訊洩漏

原因：

使用不安全的方式配置 Web 伺服器或應用程式伺服器

安全風險：

有可能擷取網站檔案系統結構的相關資訊，其可能會幫助攻擊者對映網站

受影響的產品：

CWE：

200

技術說明：

已使用不安全的方式配置 **Web** 伺服器或應用程式伺服器

有可能擷取網站檔案系統結構的相關資訊，其可能會幫助攻擊者對映網站 **Web** 應用程式顯現了網站中的目錄。

雖然目錄並沒有列出它的內容，但這個資訊可以協助攻擊者對網站展開進一步的攻擊。

例如，知道目錄名稱之後，攻擊者便可以猜測它的內容類型，也許還能猜出其中的檔名或其下的子目錄，並嘗試存取它們。內容的機密性愈高，這個問題也愈嚴重。

遺漏「Content-Security-Policy」標頭

目錄

測試類型：

Application

威脅分類：

資訊洩漏

原因：

不安全的 **Web** 應用程式設計或配置

安全風險：

- 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

受影響的產品：

CWE：

1032

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

技術說明：

不安全的 **Web** 應用程式設計或配置

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」標頭的目的是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。為了抵禦跨網站 Scripting、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。

如需詳細資訊，請參考以下鏈結。

遺漏或不安全的 "X-Content-Type-Options" 標頭

目錄

測試類型：

Application

威脅分類：

資訊洩漏

原因：

不安全的 Web 應用程式設計或配置

安全風險：

- 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

受影響的產品：

CWE：

200

參照：

有用的 HTTP 標頭清單

減少 MIME 類型的安全風險

技術說明：

不安全的 Web 應用程式設計或配置

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

具有 "nosniff" 值的 "X-Content-Type-Options" 標頭可防止 IE 和 Chrome 忽視回應的內容類型。

此動作可防止使用者的瀏覽器（例如在惡意命名後）執行未受信任的內容（例如使用者上傳的內容）。

遺漏或不安全的 "X-XSS-Protection" 標頭

目錄

測試類型：

Application

威脅分類：

資訊洩漏

原因：

不安全的 Web 應用程式設計或配置

安全風險：

- 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

受影響的產品：

CWE：

200

參照：

有用的 HTTP 標頭清單
IE XSS 過濾器

技術說明：

不安全的 Web 應用程式設計或配置

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

即使使用者已停用跨網站 Scripting 過濾器，值為 1 的 X-XSS-Protection 標頭仍會將過濾器強制變更為「啟用」模式。

這個過濾器內建於最新的 Web 瀏覽器 (IE 8+、Chrome 4+)，且通常依預設為啟用。雖然這個過濾器並非設計為跨網站 Scripting 的首要及唯一防禦手段，但可做為額外的保護層。

遺漏或不安全的跨頁框 Scripting 防禦

目錄

測試類型：

Application

威脅分類：

資訊洩漏

原因：

不安全的 Web 應用程式設計或配置

安全風險：

- 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

受影響的產品：

CWE：

693

參照：

跨框架 Scripting
點擊劫持

技術說明：

不安全的 Web 應用程式設計或配置

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
跨框架 Scripting 是一種攻擊技術，攻擊者會在其惡意網站的 iFrame 中載入有漏洞的應用程式。
接著，攻擊者可以發動「點擊劫持」攻擊，可能會造成網路釣魚、偽造跨網站要求、機密資訊洩漏等等。
為獲得最佳保護，建議將標頭值設為 DENY 或 SAMEORIGIN。
惡意探索範例：
惡意網站可能會內嵌有漏洞的頁面：
<frame src="http://vulnerable.com/login.html">

應用程式中找到不必要的 HTTP 回應標頭

目錄

測試類型：

Application

威脅分類：

資訊洩漏

原因：

不安全的 Web 應用程式設計或配置

安全風險：

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

受影響的產品：

CWE：

200

參照：

產生指紋
避免資訊洩漏

技術說明：

不安全的 Web 應用程式設計或配置

可以收集關於 Web 伺服器類型、版本、作業系統等機密資訊。

AppScan 偵測到不必要的 Http 回應標頭。

基於安全和隱私原因，諸如 "Server"、"X-Powered-By"、"X-AspNetMvc-Version" 和 "X-AspNet-Version" 等 HTTP 回應標頭不應出現在網頁中。

"Server" 標頭是每當回應由伺服器傳送給用戶端時，通常依預設新增的標頭。

"X-Powered-By" 標頭是每當回應由伺服器傳送給用戶端時，可能依預設新增的標頭。

新增的標頭可能會顯示有關內部伺服器軟體版本與類型的機密資訊，讓攻擊者產生指紋並進行攻擊，以進行特定的不當運用。此外，當新型的不當運用方式公開時，伺服器非常可能遭受到攻擊。

檢查是否有 SRI（子資源完整性）支援

目錄

測試類型：

Application

威脅分類：

併入遠端檔案

原因：

不支援 SRI（子資源完整性）

安全風險：

假設第三方伺服器已受損，網站的內容/行為會變更

受影響的產品：

CWE：

829

參照：

FrontPage 伺服器延伸：安全考量
說明

技術說明：

不支援子資源完整性。

使用者代理程式無法驗證來自協力廠商服務的 Script。萬一協力廠商服務受到侵害，使用者將不受保護。

原始碼來自另一個網域的 Script 和鏈結標籤不支援完整性檢查。

如果含有這個 Script 的服務受到侵害，則這會遭到不當運用。

不支援 SRI 的範例 Script 元素：

```
<script src="https://example.com/example-framework.js" crossorigin="anonymous"></script>
```

支援 SRI 的範例 Script 元素：

```
<script src="https://example.com/example-framework.js" integrity="sha384-
```

```
Li9vy3DqF8tnTXuiaAJuML3ky+er10rcgNR/VqsVpcw+ThHmYcwiB1pbOxEbzJr7" crossorigin="anonymous"></script>
```

找到可能的伺服器路徑揭露型樣

目錄

測試類型：

Application

威脅分類：

資訊洩漏

原因：

未安裝協力廠商產品最新的修補程式或緊急修復程式

安全風險：

有可能擷取 Web 伺服器安裝架構的絕對路徑，其可能會幫助攻擊者展開進一步攻擊，以及取得 Web 應用程式之檔案系統結構的相關資訊

受影響的產品：

CWE：

200

技術說明：

未安裝協力廠商產品最新的修補程式或緊急修復程式

攻擊者有可能擷取 Web 伺服器安裝架構的絕對路徑，並可能進一步展開攻擊，以及取得 Web 應用程式檔案系統結構的相關資訊
AppScan 偵測到含有檔案絕對路徑的回應。（例如 Windows 中的 c:\dir\file, 或 Unix 中的 /dir/file）
攻擊者可能會利用這項資訊在伺服器的目錄結構中取得機密資訊，並進一步利用機密資訊攻擊網站。

遺漏「查閱者原則」安全標頭

目錄

測試類型：

Application

威脅分類：

資訊洩漏

原因：

不安全的 Web 應用程式設計或配置

安全風險：

- 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

受影響的產品：

CWE：

200

參照：

[MDN web 文件 - 查閱者原則](#)

技術說明：

不安全的 **Web** 應用程式程式設計或設定

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。

應用程式錯誤

[目錄](#)

測試類型：

Application

威脅分類：

資訊洩漏

原因：

- 未對送入的參數值執行適當的範圍檢查
- 未執行驗證，以確定使用者輸入符合預期的資料類型

安全風險：

有可能收集機密性除錯資訊

受影響的產品：

CWE：

550

參照：

如需利用單引號來入侵網站的範例，請參閱 "How I hacked PacketStorm"（作者：Rain Forest Puppy），RFP 的網站

"Web Application Disassembly with ODBC Error Messages"（作者：David Litchfield）

CERT Advisory (CA-1997-25)：消毒 CGI Script 中的使用者提供資料

技術說明：

未對送入的參數值執行適當的範圍檢查

未執行驗證，以確定使用者輸入符合預期的資料類型

有可能收集機密性除錯資訊

如果攻擊者偽造含有非應用程式所預期的參數或參數值（範例如下）來探測應用程式，應用程式可能會陷入容易遭到攻擊的未定義狀態。

攻擊者可以從應用程式對這項要求的回應中，取得有用的資訊；這項資訊可能會遭到不當運用，從而找出應用程式的弱點。

比方說，如果參數欄位應該是單引號括住的字串（例如：在 **ASP Script** 或 **SQL** 查詢中），

注入的單引號會提早終止字串串流，從而變更 **Script** 的正常流程/語法。

錯誤訊息顯露重要資訊的另一個原因，是 **Scripting** 引擎、**Web** 伺服器或資料庫配置錯誤。以下是一些不同的變式：

[1] 移除參數

[2] 移除參數值

[3] 將參數值設為空值

[4] 將參數值設為數值溢位 (+/- 99999999)

[5] 將參數值設為 '"\''); 之類的危險字元

[6] 將某字串附加到數值參數值

[7] 將 "."（句號）或 "()"（角括弧）附加至參數名稱