CodeSecure™ 源碼檢測安全性評估報告

此報告提供: Production 專案採用源碼檢測技術所獲得之安全性評估. 報告的內容屬於機敏資料, 報告的擁有者於檢視與散佈時應妥善進行適當的安控措施. 不適當或未經授權的揭露此報告內容可能會導致嚴重的損失. 此報告的任何副本均需要妥善保管.

規範說明

此報告的安全性評估乃基於Open Web Application Security Project (OWASP)規範與遵循其源碼檢測相關之參考指引.

OWASP(開放Web軟體安全計畫 - Open Web Application Security Project)是一個開放社群、非營利性組織，目前全球有82個分會近萬名會員，其主要目標是研議協助解決Web軟體安全之標準、工具與技術文件，長期致力於協助政府或企業瞭解並改善網頁應用程式與網頁服務的安全性。由於應用範圍日廣，網頁應用安全已經逐漸的受到重視，並漸漸成為在安全領域的一個熱門話題，在此同時，駭客們也悄悄的將焦點轉移到網頁應用程式開發時所會產生的弱點來進行攻擊與破壞。 美國聯邦貿易委員會(FTC)強烈建議所有企業需遵循OWASP所發佈的十大Web弱點防護守則、美國國防部亦列為最佳實務，國際信用卡資料安全技術PCI標準更將其列為必要元件。目前OWASP有30多個進行中的計畫，包括最知名的OWASP Top 10(十大Web弱點)、WebGoat(代罪羔羊)練習平台、安全PHP/Java/ASP.Net等計畫，針對不同的軟體安全問題在進行討論與研究。

更多的資訊可參考: http://www.owasp.org/index.php/Taiwan

目錄

重點精華

檢測摘要

Application	docSI
專案	Production
Scan Trigger	kduser
Scan ID	3105
排程時間	2024/12/5 AM 09:54:56 CST
開始時間	2024/12/5 PM 03:48:21 CST
結束時間	2024/12/5 PM 03:48:27 CST
歷時	5秒,803毫秒
檢測檔案數	7
檢測行數	1,409
進入點	2
弱點進入點	0
弱點總數	0
弱點敘述句	0
脆弱檔案數	0

檢測設定

檢測類型	immediate
規則名稱	Default Policy
不可信任的來源類型	Web Request, Network Input, Web Service, Database, Window Form, None
弱點模組	Reflection Injection, Cross-Site Scripting, HTTP Response Splitting, XPath Injection, Resource Injection, SQL Injection, Command Injection, LDAP Injection, Open Redirect, Tag Injection, CRLF Injection, Risky Cryptographic Algorithm, Log Forging, Session Variable Poisoning
Web Root	docSI.zip/docSI/
專案根目錄	docSI.zip/
追蹤設定	最嚴重的一條弱點追蹤
不明的合併	否
未處理的函式傳遞	否
掃描模式	建議

報表設定

產生報表起始時間	2024/12/5 PM 03:52:21 CST
報表包含誤報數	否
報表過濾器	完整。所有弱點都加入。

源碼位置

源碼位置類型	編碼	檔案路徑	存取狀態
ZIP Directory	UTF-8	docSI.zip/	是

附錄 A | 全部的進入點

目錄	檔案	弱點數	警示
/docSI/	Default.aspx	0	0
/docSI/	doc.aspx	0	0

版本 : CodeSecure-4.5.3
製作來源 : codesecure