Google釋出兩項CSP安全工具以防範 XSS 攻擊

為協助開發人員制定有效的CSP內容安全政策，防範XSS跨站指令碼攻擊，Google 釋出 CSP Evaluator 及 CSP Mitigator 兩項工具，其中 CSP Evaluator 可協助偵測內容政策的成效，而 CSP Mitigator 並檢驗應用程式與 CSP 的相容性。

兩項 CSP 安全工具之一的 CSP Mitigator 為 Chrome 擴充程式。

Google 於本周釋出了 CSP Evaluator 及 CSP Mitigator 兩項工具以協助網站管理人員防禦跨站指令碼（Cross-site Scripting, XSS）攻擊。

跨站指令碼一直是這十幾年來最主要的網頁安全漏洞之一，駭客可利用相關漏洞在合法網站或服務上注入惡意程式，並帶來惡意廣告、水坑攻擊或偷渡式下載攻擊等，光是這兩年 Google 就付出超過 120 萬美元給找出 Google 各種應用程式中 XSS 安全漏洞的研究人員。

而最常用來防範 XSS 攻擊的則是內容安全政策（Content Security Policy，CSP），它允許開發人員彈性設定各種政策，限制可執行的程式，例如即使駭客在網頁上注入了惡意的 HTML，也無法載入惡意程式，現階段市場上主要的瀏覽器都支援 CSP。

然而，Google 指出，CSP 的彈性造成了更大的問題，因為開發人員所制定的安全政策也許表面上看來是可行的，但實際上並無真正的安全效益。Google 近日分析了逾 10 億個網域，發現部署 CSP 的網域中，有 95%的政策是無效的，根本無法抵擋 XSS 攻擊，其中一個原因是在 15 個開發人員最常用的白名單網域名，有 14 個允許駭客繞過 CSP 保護。

因此，Google 釋出了 CSP Evaluator 與 CSP Mitigator 來強化 CSP。其中，CSP Evaluator 可視覺化政策設定的成效，並偵測是否有細微的配置錯誤，而 CSP Mitigator 則為一 Chrome 擴充程式，可協助開發人員來檢驗應用程式與以隨機亂數為基礎（nonce-based）的 CSP 相容性。

此外，Google 也在本周將 CSP 納入修補程式獎勵計畫（Patch Reward Program）中，只要主動協助受歡迎的開放源碼網頁框架相容於基於隨機亂數的 CSP 就有機會贏得獎勵，此一計畫的獎勵金額自 500 美元到 1 萬美元不等。

資料來源：iThome