

114 年度台水資安抓漏競賽活動_企劃

一、活動訊息公告

1. 本公司「台水資安抓漏競賽活動」即日起開跑，歡迎各方好手熱情參與！
2. 參賽資格：持有本國國民身分證者即可參加本次活動
3. 開始/截止日期：2025/04/28 ~2025/05/31
4. 如遇緊急狀況，本公司得單方面終止活動，並公告於活動網頁，恕不另行通知。
5. 將於活動結束後刊登獲獎名單至本公司官網 <https://www.water.gov.tw/>。
6. 有關本次活動內容及規則，本公司保有最終解釋權利。

二、活動檢測範圍

類型	目標
本公司全球資訊網	https://www.water.gov.tw/
本公司工程施工即時影像	https://w3.water.gov.tw/CRIMS/
本公司專訓中心系統	https://web.water.gov.tw/ptc/
本公司即時水質系統	https://web.water.gov.tw/wq/
本公司人事差勤	https://w3.water.gov.tw/hrweb/
本公司圖資系統	https://w3.water.gov.tw/gis/
本公司 1910 客服網	https://web.water.gov.tw/1910/
本公司水表 e 管家	https://web.water.gov.tw/cmmssc/
本公司供水監測平台系統	https://w3.water.gov.tw/info01app/ https://w3.water.gov.tw/info02app/ https://w3.water.gov.tw/info03app/ https://w3.water.gov.tw/info04app/ https://w3.water.gov.tw/info05app/ https://w3.water.gov.tw/info06app/ https://w3.water.gov.tw/info07app/ https://w3.water.gov.tw/info08app/ https://w3.water.gov.tw/info09app/ https://w3.water.gov.tw/info10app/ https://w3.water.gov.tw/info11app/ https://w3.water.gov.tw/info12app/ https://w3.water.gov.tw/info13app/

三、通報流程

1. 請您發現漏洞後依據規範書寫並寄至 wica@mail.water.gov.tw
2. 本公司將於 7 個工作天內回覆您並根據漏洞嚴重性盡速修正問題(一般性漏洞約 2 個月內會修正完成)
3. 漏洞修正完成後將通知您協助複測

四、通報規範

通報請包含以下內容：(倘若檔案壓縮後超過 15MB, 請切割檔案批次寄出)

1. 姓名、連絡電話、聯絡郵件
2. IP 位址(請提供所有刺探當下使用的 IP Address)
3. 探測網址(Target)
4. 概念性驗證(PoC)說明
5. 修補建議

五、漏洞的揭露政策

1. 請務必於提交之通報中提供執行攻擊當下之 IP 位址。
2. 請提供完整詳細的漏洞說明(例如:網址連結或參數), 以及對網站系統影響提出佐證(例如: 於發動攻擊前、後之對照畫面), 回報之通報經確認為可驗證、重現且符合獎勵資格的漏洞並包含可重現漏洞的步驟, 請務必於通報中完整說明, 事後再提出佐證則不予以採納, 請提供充足資訊以重現您所回報的問題。
3. 於活動期間所執行之系統資安抓漏行為, 在不影響公司信譽及服務正常運行下, 本公司不會對您採取任何的行為。
4. 於活動期間所有通報之漏洞不得公開揭露, 取得的系統資料或是個人資料, 均不得洩漏, 如有違反「營業秘密法」、「公平交易法」、「國家機密保護法」等相關之法規內容, 除依其情形負刑事責任外, 對於本公司因而所致之一切損失, 均應依實際損失情形負起全部之損害賠償責任。
5. 下列攻擊手法不在本次活動範圍。
 - (1). 實體存取使用者設備 (Physical access to a user's device)
 - (2). 社交工程 (Social engineering)
 - (3). 中間人攻擊 (MITM attacks)
 - (4). DDoS / Fuzzing / High-Bandwidth 攻擊

六、獎金相關說明

1. 需具有本國國民身分證者之中華民國國民，並且領取獎金前需提供身分證資料。
2. 須遵守本活動的所有規定。
3. 需透過本公司唯一管道 E-mail(wica@mail.water.gov.tw)提交漏洞通報才可獲得獎金。
4. 總獎金新台幣 20 萬元為上限，獎金發放順序依漏洞嚴重程度由嚴重至低排序發放，其次依通報時間順序發放，若有二人以上發現相同漏洞，則僅發放通報時間最早者，通報時間依本公司電子郵件系統收件紀錄為準，若通報時間仍相同者則依抽籤決定，若獎金發放完畢則改以頒發感謝狀。
5. 依所得稅法規定，得獎金額 1,001 元(含)以上者須列入個人綜合所得申報，得獎獎金在 NT\$20,001(含)以上者，依法扣繳 10% 所得稅。
6. 獎金領取方式：於本公司總管理處(地址：台中市雙十路二段 2-1 號)頒發獎金。
7. 回報之通報經確認為可驗證、重現且符合獎勵資格的漏洞，請提供充足資訊以重現您所回報的問題。
8. 漏洞嚴重程度分類、獎金額度及說明參考：

嚴重程度	獎金額度(NTD)	漏洞影響說明	範例
【嚴重】	10,000 元 頒發感謝狀	任何由本公司 10 項對外資訊系統，進入本公司內部系統或企業內網（對外服務網段外之 10.X.X.X 網段）且能造成實質影響之攻擊行為。 *請務必提出侵入本公司內部系統或企業內網網段之佐證	取得 Super user 權限
			取得機密檔案、資料
			新增資料影響系統運作
			取得內網主機完整權限
			其他嚴重風險攻擊
【高】	5,000 元 頒發感謝狀	於本次活動範圍內，對本公司 10 項對外資訊系統，造成嚴重影響之任何攻擊行為。	遠端程式碼執行
			新增一筆可對外顯示之檔案、資料
			取得重要檔案、資料
			其他高風險攻擊
【中】	2,000 元 頒發感謝狀	於本次活動範圍內，對本公司 10 項對外資訊系統，造成實質影響之任何攻擊行為。	進入後端管理系統
			新增檔案、資料
			其他中風險攻擊

【低】	頒發感謝狀	於本次活動範圍內，對本公司 10 項對外資訊系統，發現任何符合 OWASP Top 10 (2017、2021)、OWASP Mobile Top 10 (2014、2016、2024)之漏洞且並未對服務系統造成任何實質影響。	安全設定缺陷
			使用已知漏洞元件
			邏輯漏洞
			其他漏洞

七、與我們聯繫

本公司資安抓漏活動聯絡及**通報唯一信箱**：wica@mail.water.gov.tw