出國報告（出國類別：開會）

2023年 SECCON 大會

出國報告書

服務機關：數位發展部資通安全署

姓名職稱：鄭欣明副署長

周士楨主任秘書

林鉦烜科長

劉囿維分析師

派赴國家：日本

出國期間：112年12月21日至113年12月24日

報告日期：113年3月

摘　要

在全球數位轉型浪潮推波助瀾下，資安風險隨之提升，面對多樣化的資安威脅，多數國家均擴大培育資安人才，以厚植資安防護能量，而透過舉辦資安競賽活動，可促進相關人員提升對於資安攻防技能的興趣，從而引導其學習方向及目標。

SECCON 是國際性的資安競賽活動，於2012年首次辦理，由日本非營利組織日本網路安全協會（JNSA）所舉辦，其成立目的係為發現及培養資安人才，並透過競賽活動提供相關人員應用資安技能之實戰場所，包含以搶旗攻防賽（CTF）形式辦理的駭客競賽。

2023年 SECCON CTF 分為初賽及決賽兩階段，其中決賽併同 SECCON 大會召開，於12月23日至12月24日以實體方式在日本東京都舉行。透過參訪日本 SECCON 大會，觀摩其資安競賽及相關活動之辦理方式，期汲取經驗作為我方後續推動作業參考。

目　錄

壹、　基本資料.....5
貳、　目的.....5
參、　活動說明.....5
肆、　活動議程.....6
伍、　過程紀要.....7
一、　SECCON 大會.....7
二、　SECCON CTF 決賽.....9
三、　Capsule CTF 競賽.....11
陸、　心得與建議事項.....15
柒、參考資料.....16

壹、基本資料

一、活動名稱：2023年 SECCON 大會（SECCON 2023 電脳会議）

二、活動時間：112年12月23日至12月24日，上午10時至下午6時（東京）

三、活動地點：HULIC HALL＆CONFERENCE（浅草橋ヒューリックホール＆ヒューリック カンファレンス）

四、參訪時間：112年12月23日（第1天）

五、參訪人員：數位發展部（以下稱本部）資通安全署鄭欣明副署長、周士楨主任秘書、林鉦烜科長、劉囿維分析師等4人（以下稱我參訪團隊）

註：本報告書揭露範圍，係本次出國行程所參與之國際交流合作相關會議與活動未涉及機敏部分。

貳、目的

在全球數位轉型浪潮推波助瀾下，資通安全（以下簡稱資安）風險隨之大幅提升，面對多樣化的資安威脅，多數國家均投入資源擴大培育資安人才，以厚植資安防護能量，而透過舉辦資安競賽活動，可促進相關人員提升對於資安攻防技能的興趣，從而引導其學習方向及目標。

我國即有透過政府機關及民間社群舉辦之資安競賽活動，如資安技能金盾獎、HITCON CTF 等。本次參訪前往日本 SECCON 大會，觀摩其資安競賽及相關活動之辦理方式，期汲取經驗作為我方後續推動作業參考。

參、活動說明

SECCON（SECurity CONtest）是國際性的資安競賽活動，於2012年首次辦理，由日本非營利組織日本網路安全協會（JNSA）所舉辦，其成立目的係為發現及培養資安人才，並透過競賽活動提供相關人員應用資安技能之實戰場所，其活動範圍包含以搶旗攻防賽（Capture the flag, CTF）形式辦理的駭客競賽，以及其他講座與社群相關活動。

2023年 SECCON 搶旗攻防賽（以下稱 CTF）駭客競賽，分為初賽（Quals）及決賽（Finals）兩階段，初賽於2023年9月16日至9月17日以線上方式舉

行，競賽採用解謎式（Jeopardy）模式，並依初賽結果產出10個國際隊伍及10個日本國家隊伍參加決賽；決賽則併同 SECCON 大會召開，於2023年12月23日至12月24日以實體方式在日本東京都舉行。

肆、活動議程

活動首日（112年12月23日）之議程詳如圖1。

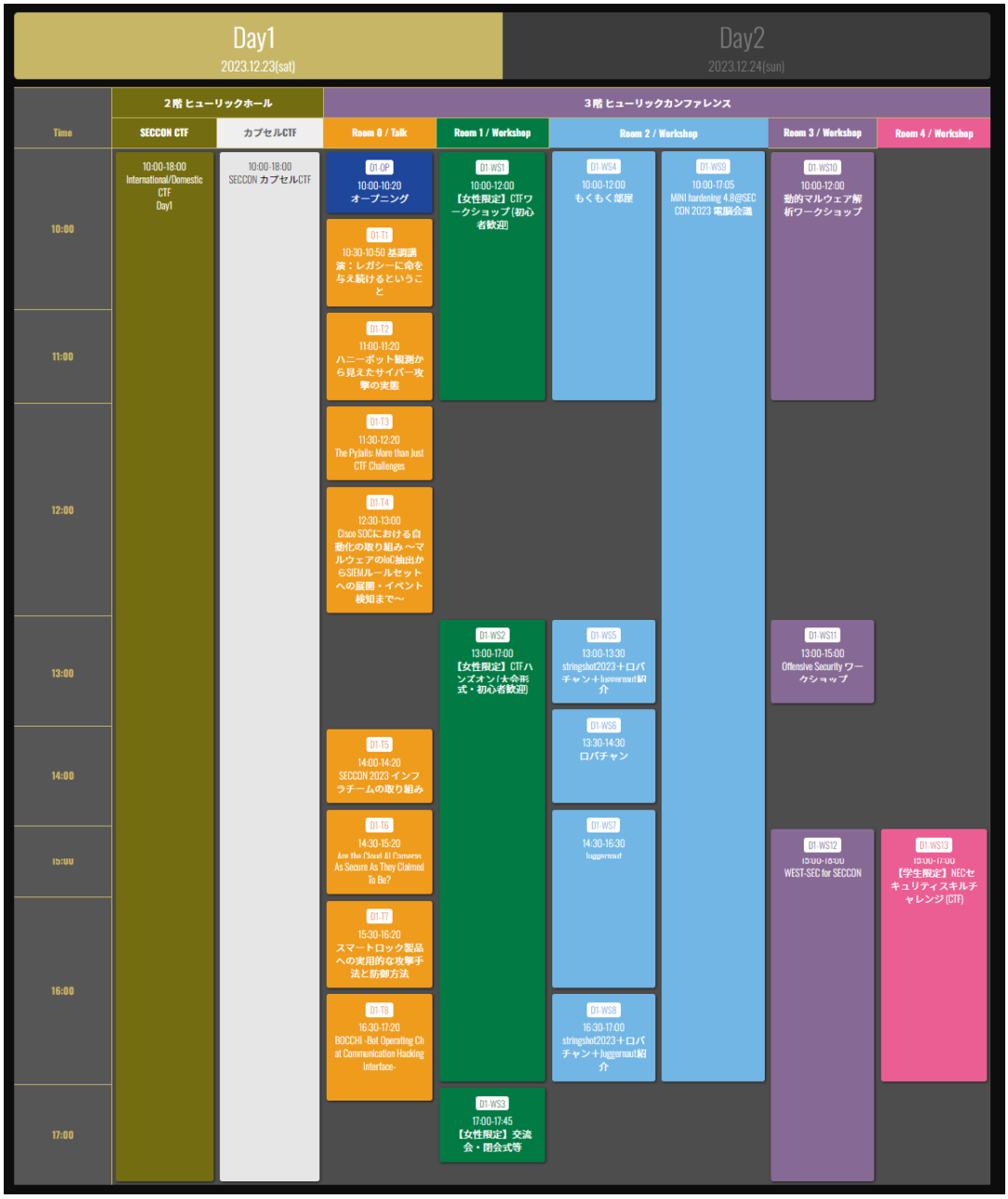

圖1、SECCON 大會第1天議程

（資料來源：SECCON 官網，https://www.seccon.jp/2023/ep231223.html）

伍、過程紀要

一、SECCON 大會

我參訪團隊於112年12月23日抵達位於日本東京都 HULIC HALL & CONFERENCE 之 SECCON 大會（SECCON 2023 電脳会議）現場（如圖2），除實地瞭解 SECCON CTF 決賽之辦理情形，並參觀大會相關整體規劃，如 Capsule CTF 競賽及主題講座等相關活動。

圖2、SECCON 大會會場入口

SECCON 大會無收取門票費用，參加人員透過 SECCON 活動網站進行免費註冊帳號及完成報名後，取得一組通行 QR 碼，並於會場入口提供通行 QR 碼予活動工作人員，以換取 SECCON 大會實體通行證。SECCON 大會實體通行證之設計，係以電腦主機板做為創意發想來源（如圖3），將通行證卡片本體結合日常資訊科技元素，整體設計呈現具質感且切合活動性質，提升其記憶點及紀念性質。我參訪團隊配戴實體通行證之合影如圖4。

開幕式活動於會場 Room 0舉行，採線上會議、線下實體方式同步

進行，並啟用電腦輔助即時翻譯，以利與不同國家參加人員溝通。隨後並由大阪大學猪俣敦夫教授進行首場主題演講「讓遺產永存（レガシーに命を与え続けるということ）」，說明近期 IT 科技發展與其針對舊時代計算機遺產保存所做的努力（如圖5）。

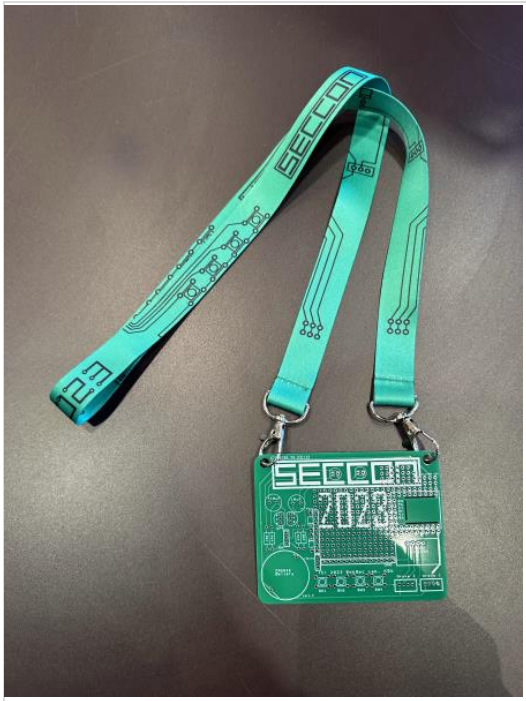

圖3、SECCON 大會實體通行證

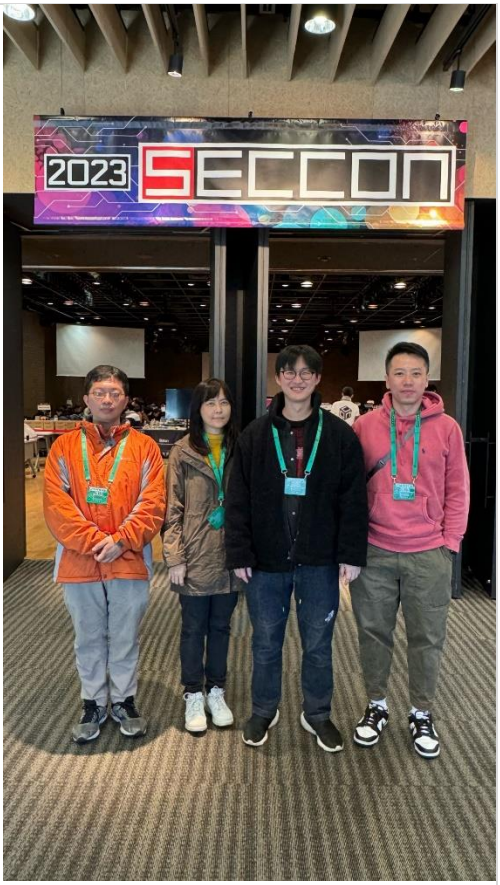

圖4、我參訪團隊合影

圖5、SECCON 大會首場主題演講「讓遺產永存」

二、SECCON CTF 決賽

SECCON CTF 決賽場地位於會場大禮堂（如圖6），依組別進行分桌入座，主辦單位並提供參賽隊伍簡易飲食。參賽隊伍1組至多4人，且不允許以遠端方式參與，競賽則同樣採用解謎式（Jeopardy）模式。

現場設有3個大型螢幕記分板，實時呈現各參賽隊伍之資安攻防態勢及得分情形（如圖7），惟可能配合系統調校，實際於決賽開始後數小時才正式於記分板顯示相關成績。

圖6、SECCON CTF 決賽會場

圖7、SECCON CTF 決賽記分板

本屆 SECCON CTF 國際組決賽第1名至第3名均設有獎金，分別為40萬日圓、20萬日圓及10萬日圓。國際組決賽第1名為「Maple Mallard Magistrates」隊（由傳統強隊美國卡內基美隆大學的 PPP 成員以及韓國的 The Duck 組成），亦同為2023世界駭客大賽之第1名得獎隊伍。

我國參賽隊伍包含「${cystick}」及「BALSN」等2隊，並於最後分別取得國際組決賽第3名、第4名之優異成績（如圖8、圖9）。

CTFTIME CTFs Upcoming Archive Calendar Teams FAQ Contact us About

Scoreboard

Place	Team	CTF points	Rating points
1	Maple Mallard Magistrates	3286.000	50.000
2	Azure Assassin Alliance	3026.000	35.522
3	${cystick}	2837.000	29.917
4	Balsn	2516.000	25.392
5	Super Guesser	2206.000	21.783
6	kalmarunionen	2040.000	19.687
7	r3kapig	1990.000	18.711
8	blue-lotus	1835.000	17.086
9	More Smoked Leet Chicken	1829.000	16.693
10	ierae	1650.000	15.053

圖8、SECCON CTF 決賽結果

資料來源：CTFtime.org，https://ctftime.org/event/2159/

圖9、我國隊伍${cystick}榮獲決賽第3名

三、Capsule CTF 競賽

圖10、Capsule CTF 競賽官方宣傳圖樣

本屆 SECCON 大會除 CTF 決賽等正規競賽活動，於會場大禮堂場外，另舉辦 Capsule CTF 競賽活動（如圖10），只要是有報名本屆大會的參加人員，都可以現場跟活動工作人員索取一個實體代幣，將代幣投入扭蛋機後隨機轉出扭蛋（如圖11、圖12），扭蛋內容物可能為 Capsule CTF 競賽題目之解鎖密碼或紀念小禮；透過互動活動，擴大人員活動參與感及整體趣味性。

圖11、Capsule CTF 競賽扭蛋機

圖12、Capsule CTF 競賽扭蛋

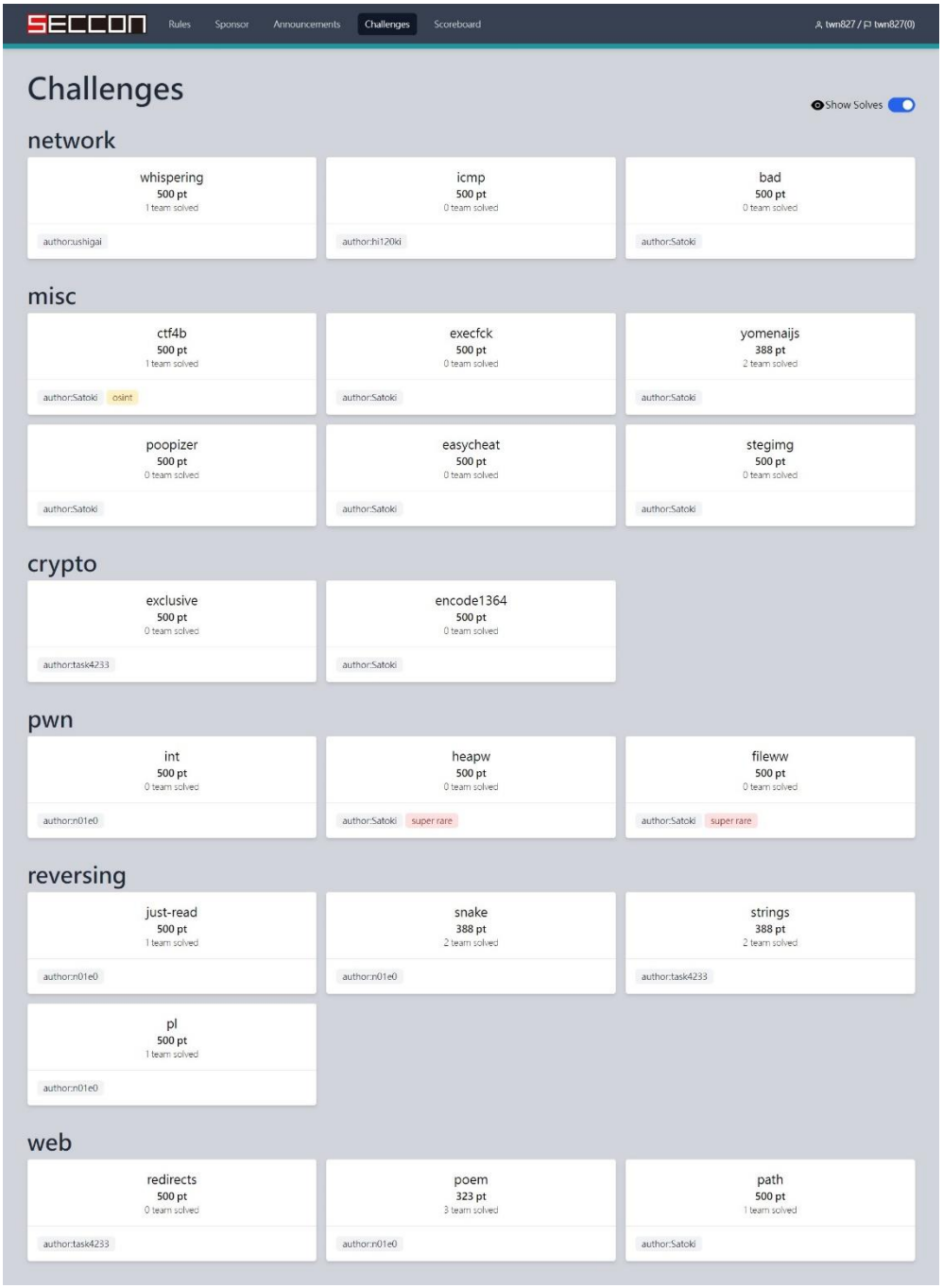

圖13、Capsule CTF 競賽網站及題目

主辦單位於內網架設 Capsule CTF 競賽網站（如圖13），參賽人員必須透過主辦單位提供之會場官方無線網路連入；各競賽題目之主檔亦有加密，須透過前述扭蛋內藏之密碼進行解鎖。因個人能轉出之扭蛋次數有限，參賽人員需透過彼此互動交流以取得更多解鎖密碼。

競賽題型屬一般 CTF 競賽常見之 network（網路）、misc（其他綜

合）、crypto（加解密演算法）、pwn（具漏洞的服務）、reversing（逆向工程）及 web（網站相關）等類型項目。為瞭解活動出題規劃設計，我參訪團隊亦實際派員參與 Capsule CTF 競賽解題，以下就所取得之兩題競賽題目進行說明。

(一)題目 yomenaijs（其他綜合題型）

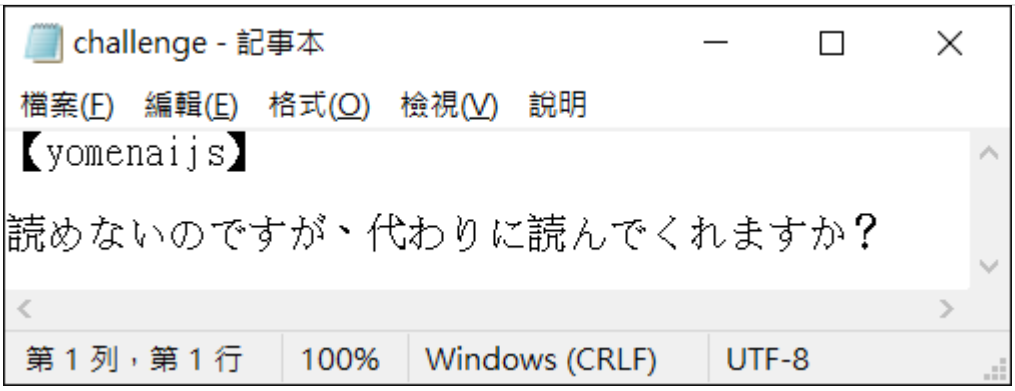

圖14之1：題目敘述檔

- Step1：透過網站取得題目敘述檔（challenge.txt）及題目主檔（yomenaijs.js），查題目敘述內容為「（中譯）我看不懂，你能幫我讀嗎？」。

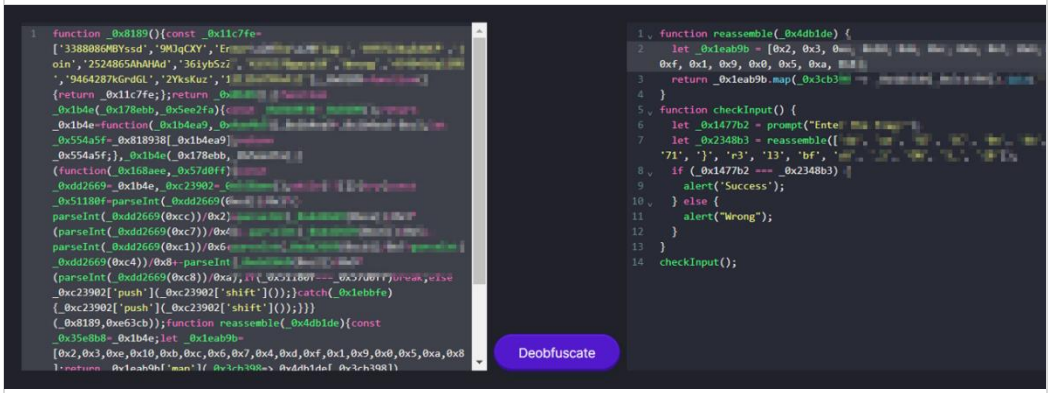

圖14之2：JavaScript 程式碼轉換

- Step2：依上述提示，復經判讀題目主檔內容，推測應為經加密混淆（obfuscate）之 JavaScript 程式碼，故使用線上工具進行反混淆（deobfuscate）處理，取得原始 JavaScript 程式碼內容。再依處理後之 JavaScript 程式碼內容提示，針對字串陣列內容進行重組，取得解題 flag。

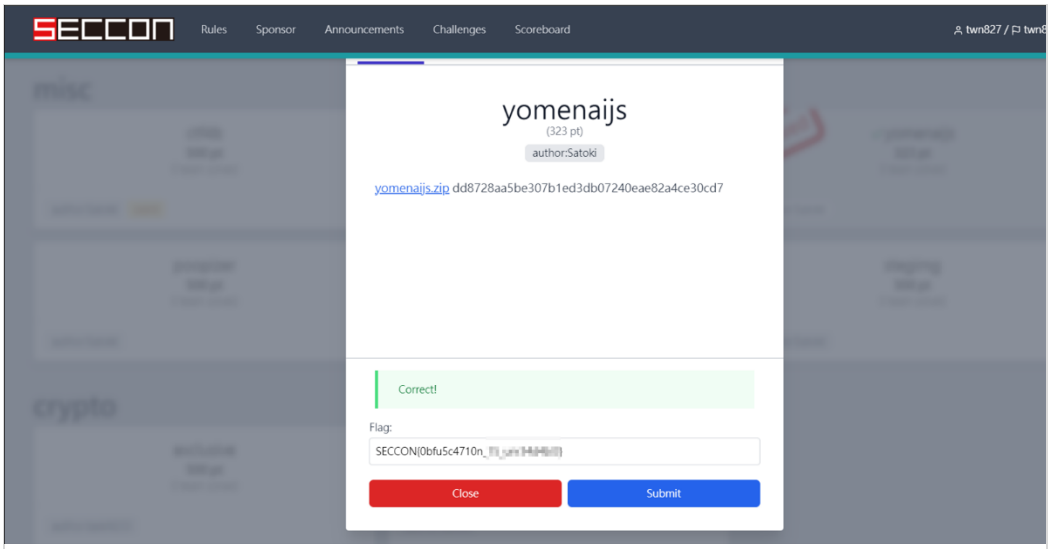

圖14之3：取得積分

- Step3：依解題 flag 成功取得本題積分。

(二)題目 int（具漏洞的服務題型）

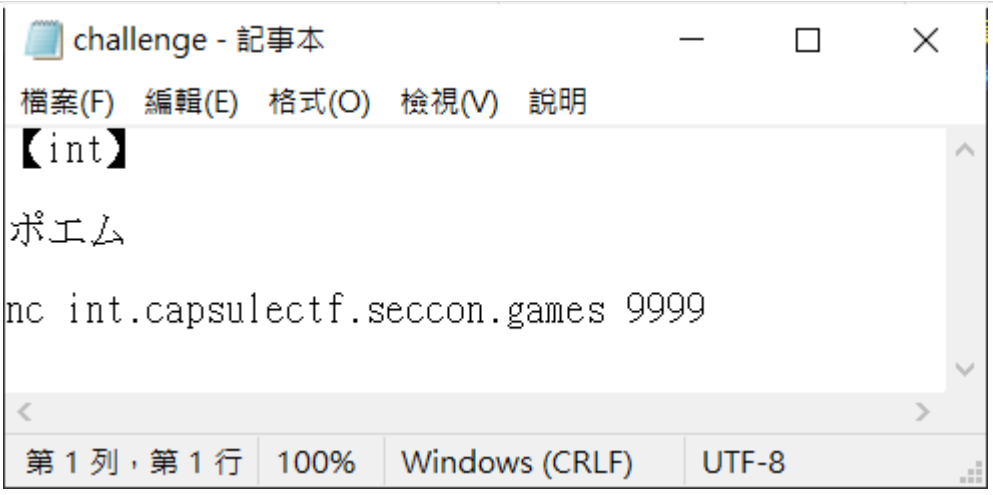

圖15之1：題目敘述檔

- Step1：透過網站取得題目敘述檔（challenge.txt）及題目主檔（ysrc.c 等），查題目敘述內容為「（中譯）詩」及一串指令。

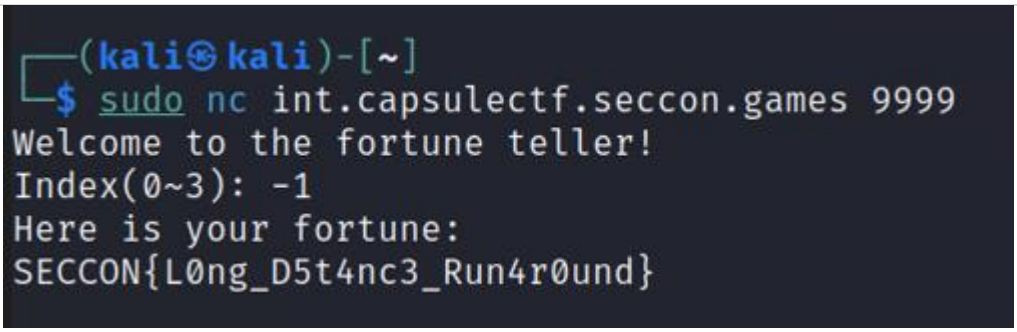

圖15之2：執行 nc 指令

- Step2：經判讀題目主檔（ysrc.c）原始碼內容，推測應可利用陣列邊界檢查不當所造成之緩衝區溢位。復依指示透過 Kali Linux 內建之 nc 工具連結至網站應用程式，嘗試輸入 outbound index（-1），取得解題 flag。

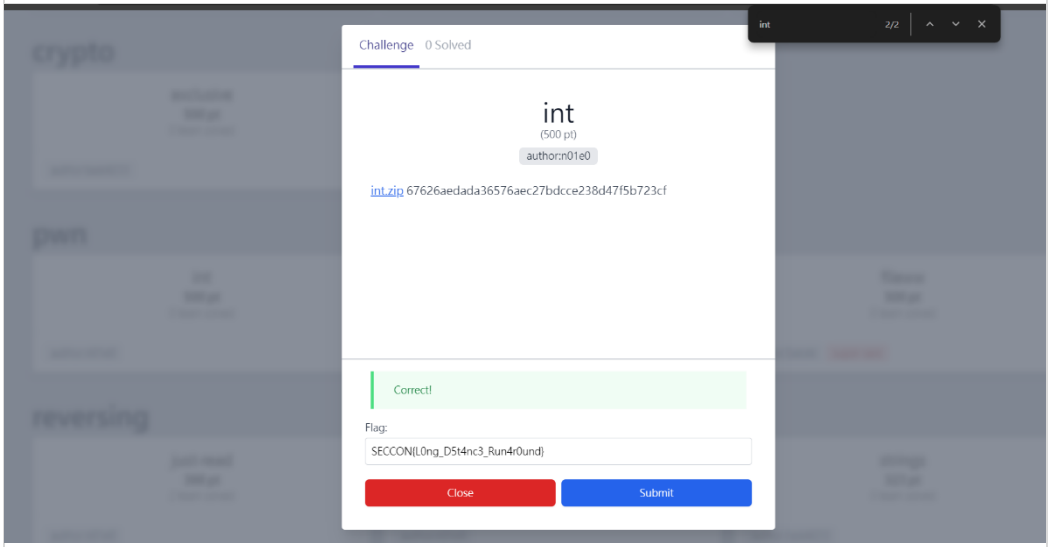

圖15之3：取得積分

- Step3：依解題 flag 成功取得本題積分。

陸、心得與建議事項

本次參訪2023年 SECCON 大會，透過觀摩其資安競賽及相關活動之辦理，瞭解日方為擴大培育其資安人才之推動方式。以下摘要本屆 SECCON 大會值得借鑒之辦理作法：

一、活動文創小物設計：SECCON 大會本次實體通行證之設計結合了日常資訊科技元素，整體設計呈現具質感且切合活動性質，提升其記憶點及紀念性質，亦有助於宣導推廣作業。

二、CTF 競賽系統建置：SECCON CTF 決賽現場設有3個大型螢幕記分板，實時呈現各參賽隊伍之資安攻防態勢及得分情形，透過視覺化方式，除可提升競賽現場緊張感及熱絡氣氛，亦可讓本屆大會參加人員、媒體容易瞭解競賽辦況。

三、針對非主要競賽人員規劃活動：SECCON 大會本次另舉辦 Capsule CTF 競賽活動，開放本屆大會的報名人員均可參加，透過遊戲化（代幣、扭蛋機等）及互動方式做引導，擴大人員活動參與感及整體趣味性；另競賽題目難易度適合 CTF 入門新手，可吸引其參加後續相關資安活動，擴大資安競賽基本客群。

本部將參考上開辦理作法據以精進本部後續自辦（如資安技能金盾獎）或合作／協同辦理相關競賽活動之相關作業，希望透過持續為資安人才培育注入心力，進而提升臺灣整體在國際上的資安實戰力及競爭力。

柒、參考資料

- 2023年 SECCON 大會活動網站：
  https://www.seccon.jp/2023/ep231223.html