107年輻射災害情資模組
電子地圖建置勞務採購案
成果報告書

執行單位：國家災害防救科技中心

中華民國　一〇七年十二月十日

目 錄

目 錄 I

圖目錄 II

表目錄 IV

第一章 緣起目的 1

第二章 計畫期程 3

第三章 執行成果 4

第一節 輻射災害情資模組規劃 4

第二節 輻射災害情資網頁籤架構規劃 5

第四章 結論與建議..13

附錄一、資安檢測項目..15

A.網站弱點掃描..15

B.滲透測試報告..27

C.系統壓力測試..30

D.程式碼檢測..33

E.ISO27001..35

附錄二、教育訓練..37

附錄三、簽訂合作備忘錄會議..53

圖目錄

圖 1 災害情資服務平台與其子系統 1
圖 2 輻射災害情資平台架構 1
圖 3 輻射災害情資網資訊整合架構圖 2
圖 4 輻射災害情資模組系統規劃 4
圖 5 使用者權限規劃說明 5
圖 6 輻射災害情資模組功能規劃 5
圖 7 核電廠即時運轉狀態 6
圖 8 核電廠輻射偵測 6
圖 9 電力資訊(一般時期) 6
圖 10 電力資訊(梅姬颱風案例) 6
圖 11 供水即時資訊 6
圖 12 道路資訊 6
圖 13 火山監測 7
圖 14 環境輻射偵測 7
圖 15 劑量評估系統分析 7
圖 16 境外輻射系統分析 8
圖 17 動態大氣觀測 8
圖 18 風速觀測 8
圖 19 核電廠基礎設施分析-村里人口 8
圖 20 核電廠基礎設施分析-醫院 8
圖 21 核一廠民眾預警涵蓋率 9
圖 22 核二廠民眾預警涵蓋率 9
圖 23 核三廠民眾預警涵蓋率 9
圖 24 核一廠疏散分區 9
圖 25 核二廠疏散分區 9
圖 26 核三廠疏散分區 9
圖 27 核一廠 3 公里區域劃分 9
圖 28 核二廠 3 公里區域劃分 9
圖 29 核三廠 3 公里區域劃分 10
圖 30 輻傷醫院(級別) 10
圖 31 家庭訪問訪查資訊 10
圖 32 民眾告警資訊 10
圖 33 現地即時觀測 11

圖 34 現地訊息回報 11
圖 35 災害情勢 11
圖 36 示警燈號 11
圖 37 綜合研判指標 11
圖 38 一周內地震分布 11
圖 39 地震 CCTV 監看 12
弱點掃描檢測結果.. 15
模擬 30 人同時上線回應時間 1.2 秒 31
模擬 300 人同時上線回應時間 10 秒 31
模擬 600 人同時上線回應時間 22 秒 31
模擬 600 人同時上線回應時間 22 秒 32
模擬 1,000 人同時上線回應時間 30 秒 32
雙方長官簽署備忘錄合影.. 54
雙方大合照.. 54

表目錄

表 1計畫期程進度表 3

第一章　緣起目的

「災害情資服務平台」(以下簡稱：情資網)是防救災資訊的發布流通站，平台設計主軸係以串聯起中央部會、縣市政府及全台民眾共同參與防救災為導向，協助中央部會對地方縣市的縱向資訊傳遞，並串聯地方縣市之間的橫向聯絡，執行多面向的資訊傳遞(圖 1)。

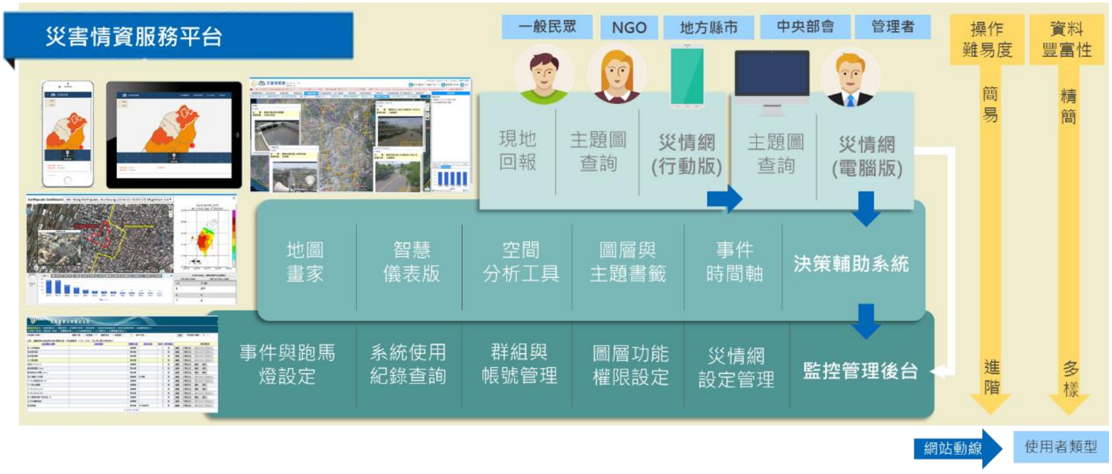

災害情資服務平台
一般民眾
NGO
地方縣市
中央部會
管理者
操作難易度
資料豐富性
現地回報
主題圖查詢
災情網(行動版)
主題圖查詢
災情網(電腦版)
簡易
精簡
地圖畫家
智慧儀表版
空間分析工具
圖層與主題書籤
事件時間軸
決策輔助系統
事件與跑馬燈設定
系統使用紀錄查詢
群組與帳號管理
圖層功能權限設定
災情網設定管理
監控管理後台
進階
多樣
網站動線
使用者類型

圖 1 災害情資服務平台與其子系統

今年度建置針對輻射災害的輻射情資模組，本平台營運涵蓋 3 個子系統－災情網輻射情資模組、輔助系統及監控管理後台（圖 2）：

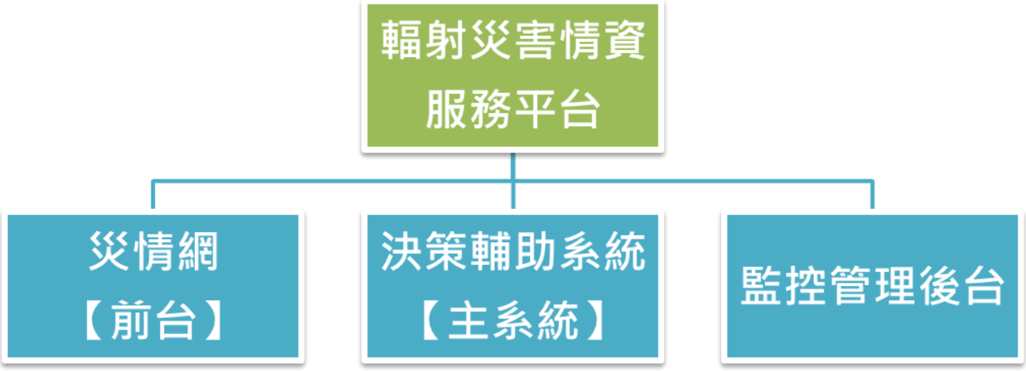

輻射災害情資服務平台
災情網【前台】
決策輔助系統【主系統】
監控管理後台

圖 2 輻射災害情資平台架構

輻射災害可能因不同災害發生，伴隨而來，因此本平台除情資網既有水文、氣象、火山、地震等監測資訊外，更整合基礎點位資料、輻射監測、輻射劑量評估、輻射預警涵蓋、境外輻射災害模擬及家戶訪問調查等資訊等(如圖 3)。透過資訊的整合，縮短決策者決策判定時間，降低災害之影響。

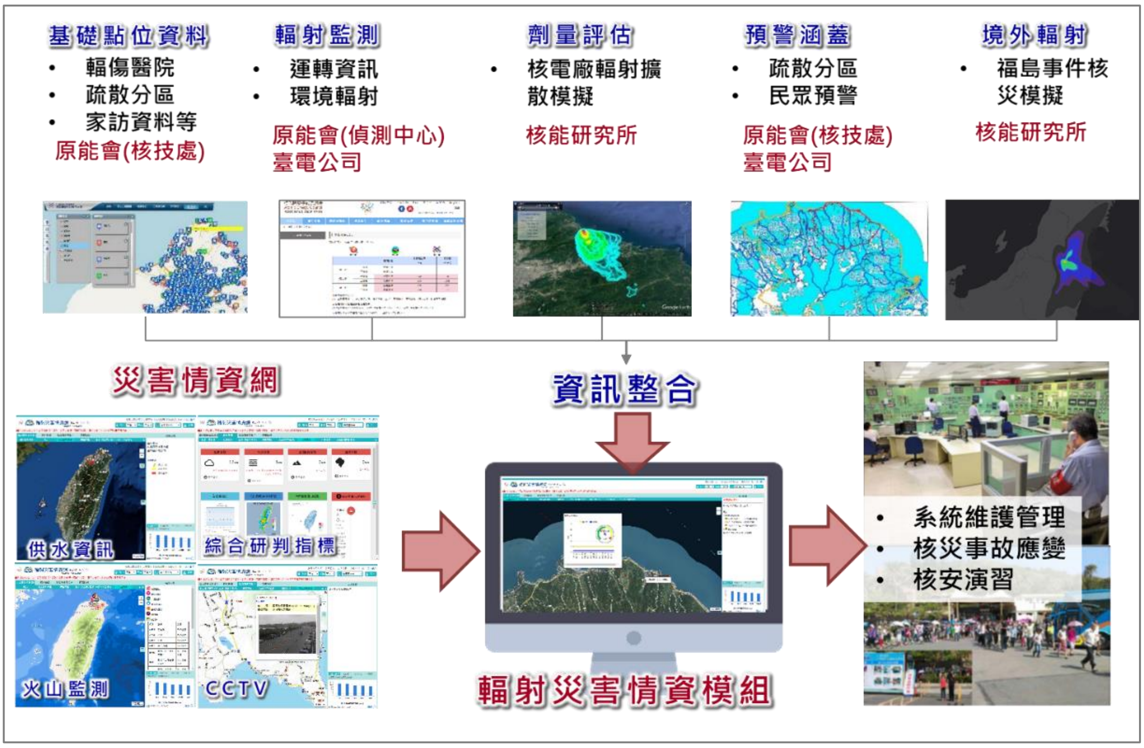

基礎點位資料
輻傷醫院
疏散分區
家訪資料等
原能會(核技處)
輻射監測
運轉資訊
環境輻射
原能會(偵測中心)
臺電公司
劑量評估
核電廠輻射擴散模擬
核能研究所
預警涵蓋
疏散分區
民眾預警
原能會(核技處)
臺電公司
境外輻射
福島事件核災模擬
核能研究所
災害情資網
供水資訊
綜合研判指標
火山監測
CCTV
資訊整合
輻射災害情資模組
系統維護管理
核災事故應變
核安演習

圖 3輻射災害情資網資訊整合架構圖

第二章　計畫期程

本計畫期程進度詳如表 1說明。

表 1計畫期程進度表

工作項目	計畫執行進度													
	5			6		7		8		9		10		11
日期	5/14	5/21	5/31	6/15	6/30	7/25							10/31	11/23
1.提交執行進度規劃表	🟩													
2.資料庫處理 電子地圖資彙整與分析	🟩	🟩												
3.開發模組應用介面 模組介面規劃與設計		🟩	🟩											
4.空間資訊操作功能設計 a. 主題圖圖層展示操作之功能 b. 系統底圖採圖磚方式設計 c. 地圖操作之功能			🟩	🟩										
5.資料屬性查詢功能規劃與設計 a. 頁面功能雛型 b. EPZ3 公里內圖資建置 c. 核電廠半徑 30 公里內，人口及重要點位建置 d. 核電廠村里疏散分區及分區人口數資訊建置				🟩	🟩									
6.資料屬性查詢功能規劃與設計 a. 頁面功能開發與展示 b. 劑量評估與境外核輻射擴散模擬介接與展示 c. 家庭訪問調查結果查詢與展示 d. 核電廠機組運轉情形及環境輻射監測之即時數據展示 e. 道路災況圖資套疊功能 f. 民眾預警涵蓋率圖層套疊					🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
7.教育訓練 ◎教育訓練與頁面雛型測試 (配合核安演習時程初步規劃)														
工作進度百分比（累積數）	5%	15%	25%	35%	40%	50%	55%	60%	65%	70%	75%	80%	90%	100%
簽訂 MOU													🟩◎	

第三章　執行成果

第一節　輻射災害情資模組規劃

本計畫考量輻射災害應變時期及平時使用情境，進行輻射災害情資模組規劃，分為輻射災害情資網(前台)，決策輔助系統(主系統)及後台管理系統(後台)，以供各執掌人員使用，圖 4。

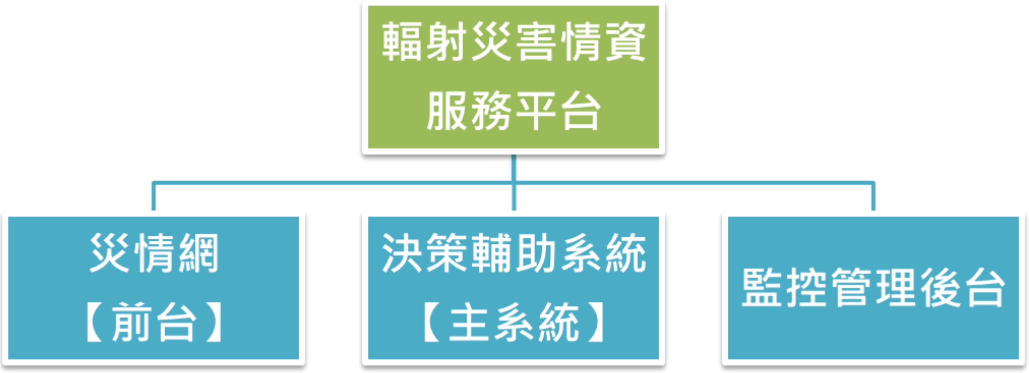

輻射災害情資服務平台
災情網【前台】
決策輔助系統【主系統】
監控管理後台

圖 4 輻射災害情資模組系統規劃

在權責規劃上，後台權限管理者與系統操作使用者為規劃區別，皆具有使用輻射災害情資網(前台)與主系統(決策輔助系統)，前者主要為情境式主題頁籤，後者則為應變時突發狀況之所需，需彈性使用主系統做其他的資訊分析。而後台權限管理者則具有頁籤新增與公告設定等功能(圖 5)。

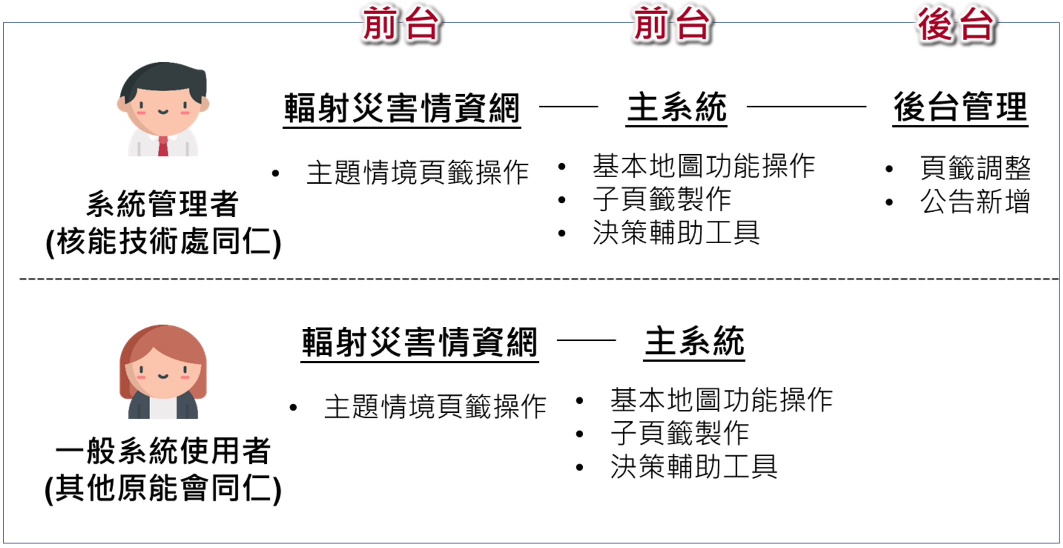

前台
前台
後台
輻射災害情資網
主系統
後台管理
系統管理者
(核能技術處同仁)
• 主題情境頁籤操作
• 基本地圖功能操作
• 子頁籤製作
• 決策輔助工具
• 頁籤調整
• 公告新增
輻射災害情資網
主系統
一般系統使用者
(其他原能會同仁)
• 主題情境頁籤操作
• 基本地圖功能操作
• 子頁籤製作
• 決策輔助工具

圖 5 使用者權限規劃說明

第二節　輻射災害情資網頁籤架構規劃

本研究依據輻射災害應變之所需，規劃出五大主題頁籤設定，分別如下(圖 6)：

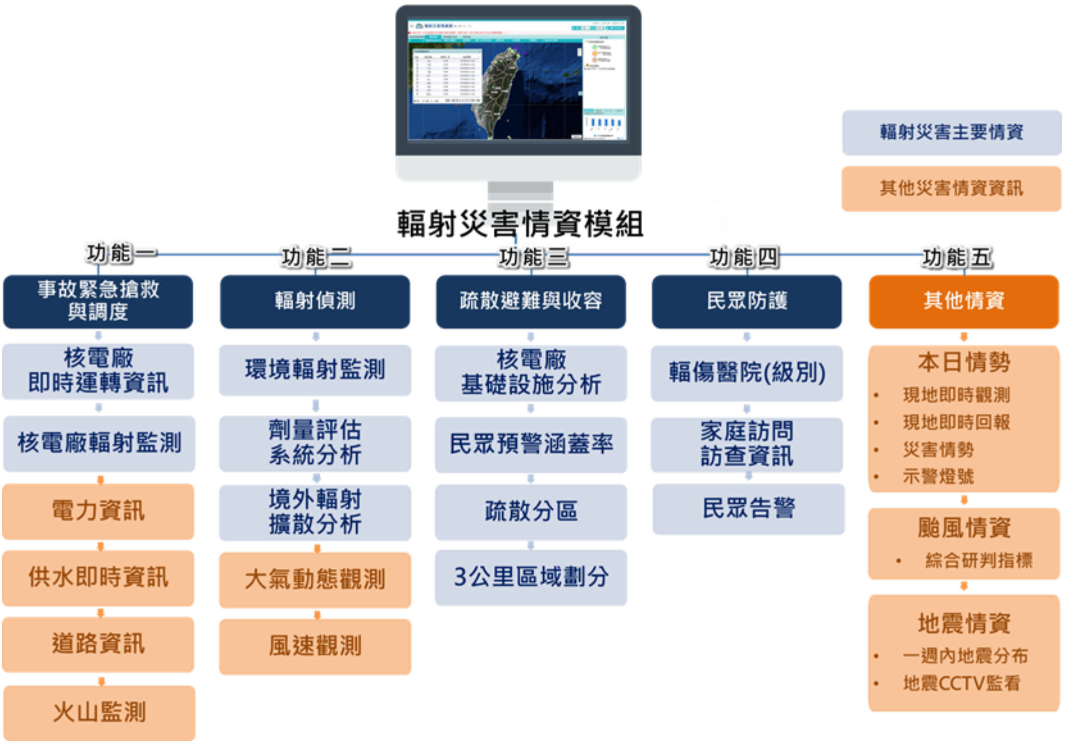

輻射災害主要情資
其他災害情資資訊
輻射災害情資模組
功能一
事故緊急搶救與調度
核電廠即時運轉資訊
核電廠輻射監測
電力資訊
供水即時資訊
道路資訊
火山監測
功能二
輻射偵測
環境輻射監測
劑量評估系統分析
境外輻射擴散分析
大氣動態觀測
風速觀測
功能三
疏散避難與收容
核電廠基礎設施分析
民眾預警涵蓋率
疏散分區
3公里區域劃分
功能四
民眾防護
輻傷醫院(級別)
家庭訪問訪查資訊
民眾告警
功能五
其他情資
本日情勢
• 現地即時觀測
• 現地即時回報
• 災害情勢
• 示警燈號
颱風情資
• 綜合研判指標
地震情資
• 一週內地震分布
• 地震CCTV監看

圖 6 輻射災害情資模組功能規劃

一、 事故緊急搶救與調度

以核能發電廠內核事故情況為主，隨時了解各核電廠運作狀況、環境輻射偵測值，並於災時可得知電力、供水即時狀態及道路狀況等資訊，如圖 7 至圖 12 圖示。

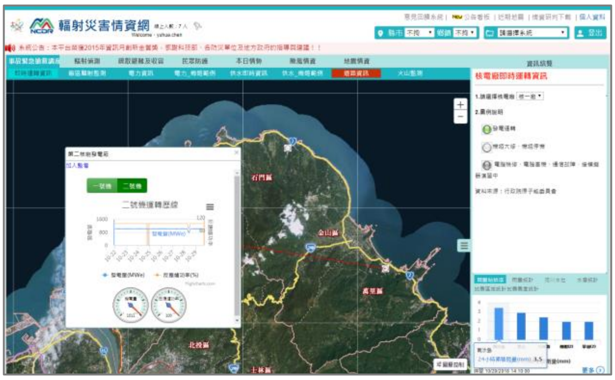
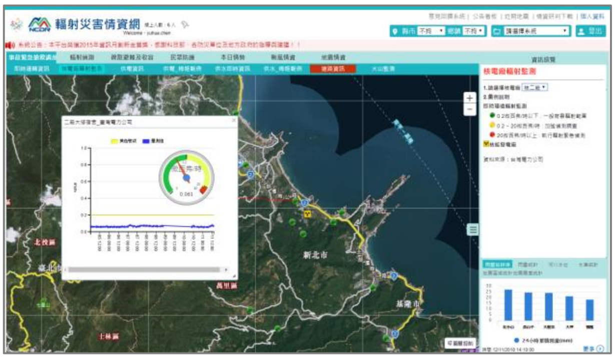
	

圖 7 核電廠即時運轉狀態	圖 8 核電廠輻射偵測

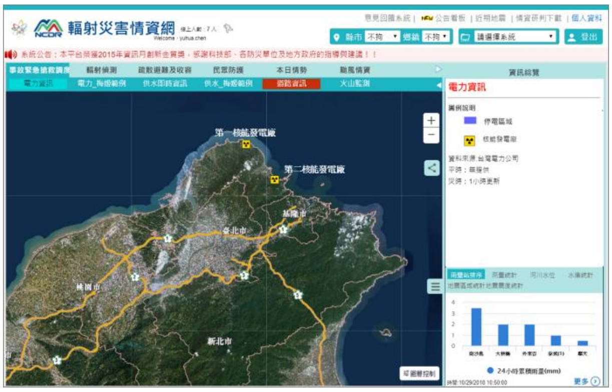
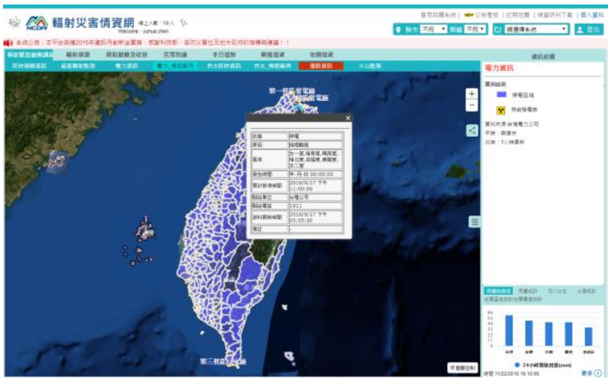

	

圖 9 電力資訊(一般時期)	圖 10 電力資訊(梅姬颱風案例)

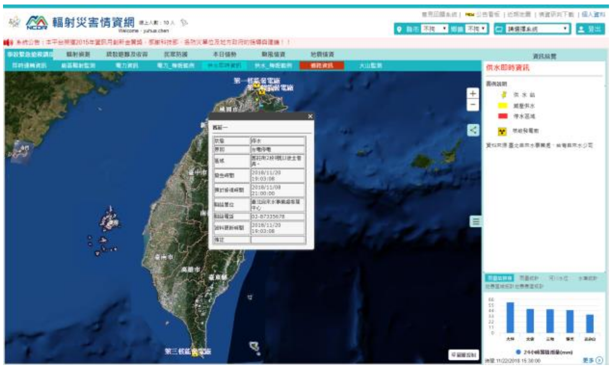
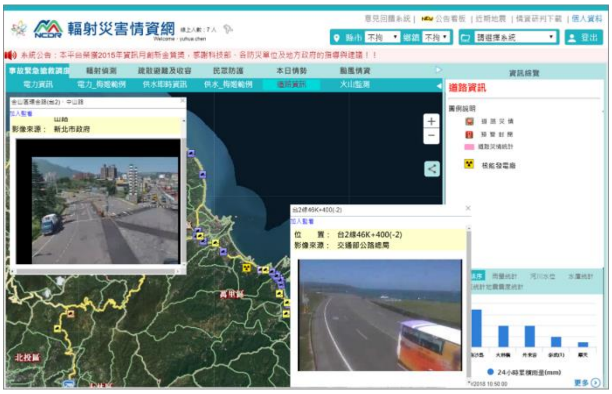
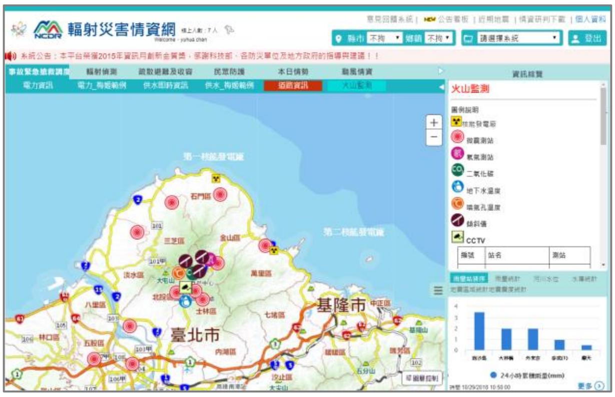
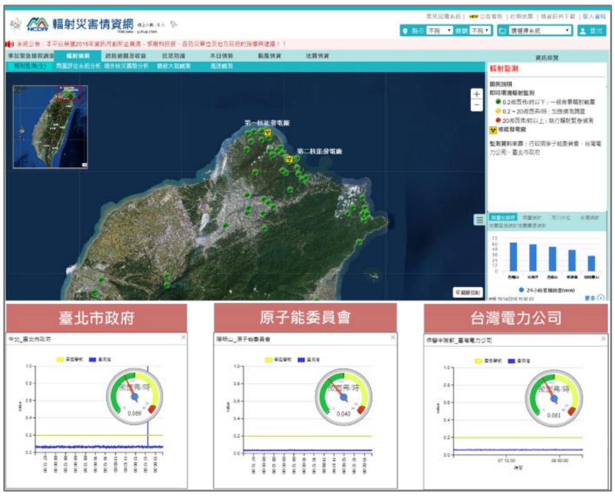
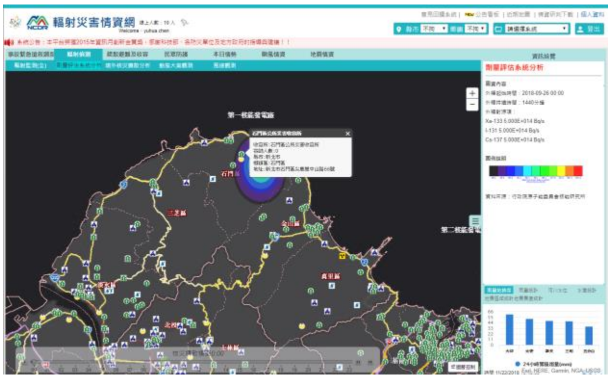

	

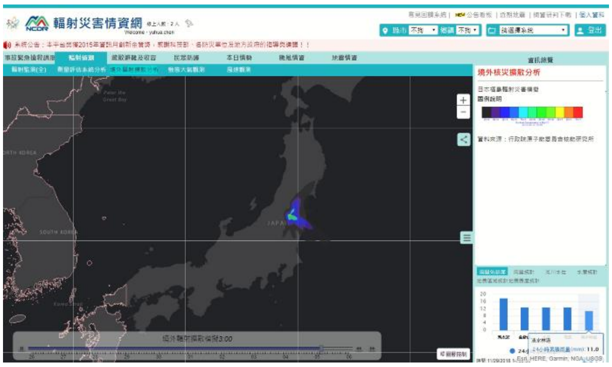
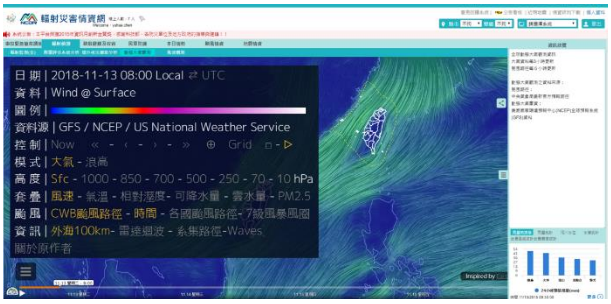
圖 11 供水即時資訊	圖 12 道路資訊

 輻射災害情資網 火山監測 臺北市 基隆市
圖 13 火山監測

二、 輻射偵測

提供全台環境輻射偵測資訊、劑量評估系統分析與境外輻射系統分析等資訊，並搭配大氣動態風向等，推測受災位置與情況等如圖 14 至圖 18 圖示說明。

 輻射災害情資網 臺北市政府 原子能委員會 台灣電力公司	 輻射災害情資網 劑量評估系統分析
圖 14 環境輻射偵測	圖 15 劑量評估系統分析

	 日 期 | 2018-11-13 08:00 Local ⇄ UTC 資 料 | Wind @ Surface 資料源 | GFS / NCEP / US National Weather Service 控 制 | Now « - ‹ - › - » ⊕ Grid □ - ▷ 模 式 | 大氣 - 浪高 高 度 | Sfc - 1000 - 850 - 700 - 500 - 250 - 70 - 10 hPa 套 疊 | 風速 - 氣溫 - 相對溼度- 可降水量 - 雲水量 - PM2.5 颱 風 | CWB颱風路徑 - 時間 - 各國颱風路徑- 7級風暴風圈 資 訊 | 外海100km- 雷達迴波 - 系集路徑-Waves 關於原作者
圖 16 境外輻射系統分析	圖 17 動態大氣觀測

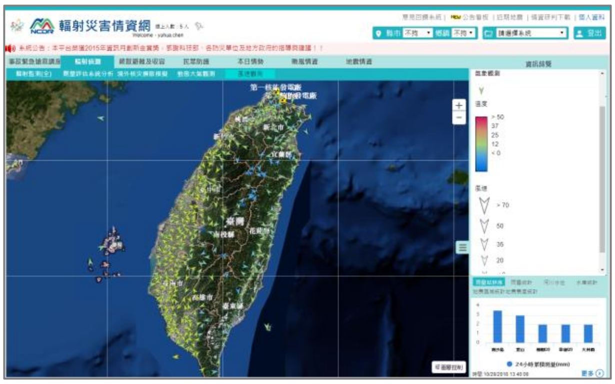
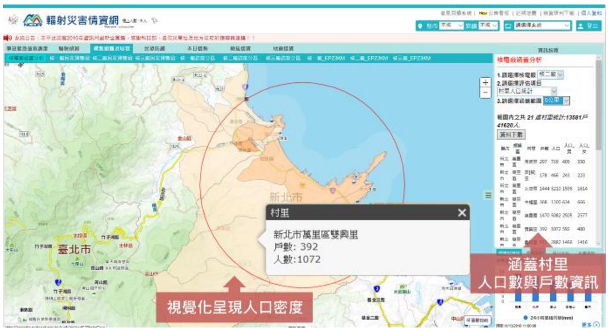
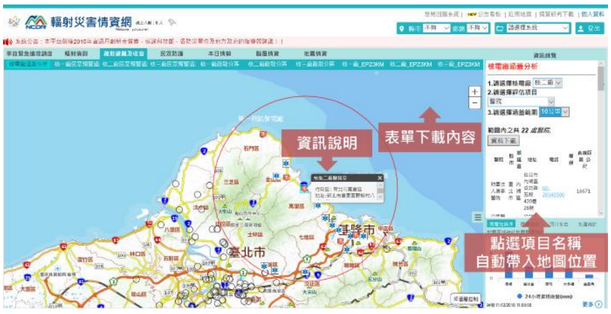



圖 18 風速觀測	

三、 疏散避難與收容

當輻射災害影像範圍擴及電廠周邊，將啟動疏散避難與收容機制，藉由此頁籤類別內容能了解各別電廠周邊維生基礎設施、疏散區域與人口分布在空間上相互關係，如圖 19 至圖 29 圖示說明。

 村里 新北市萬里區雙興里 戶數: 392 人數:1072 視覺化呈現人口密度 涵蓋村里 人口數與戶數資訊	 資訊說明 表單下載內容 點選項目名稱 自動帶入地圖位置
圖 19 核電廠基礎設施分析-村里人口	圖 20 核電廠基礎設施分析-醫院

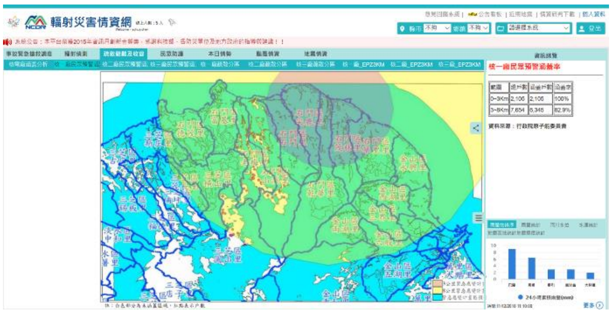


圖 21 核一廠民眾預警涵蓋率

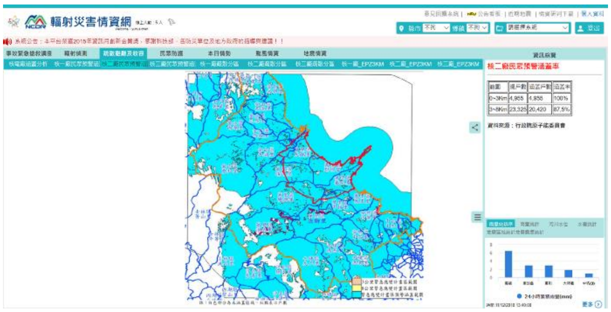


圖 22 核二廠民眾預警涵蓋率

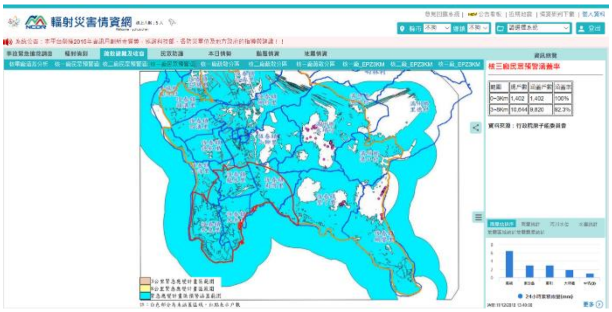


圖 23 核三廠民眾預警涵蓋率

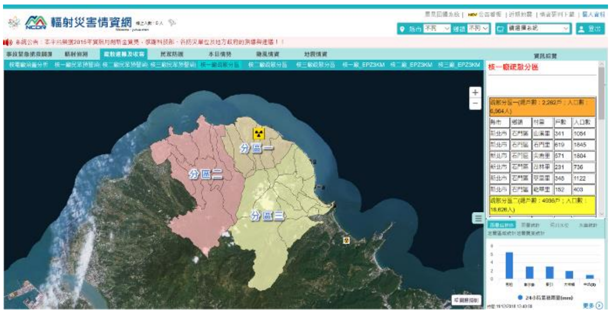

輻射災害情資網
分區一
分區二
分區三

圖 24 核一廠疏散分區

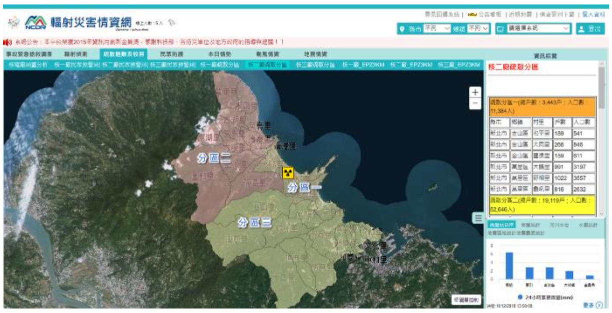

輻射災害情資網
分區二
分區一
分區三

圖 25 核二廠疏散分區

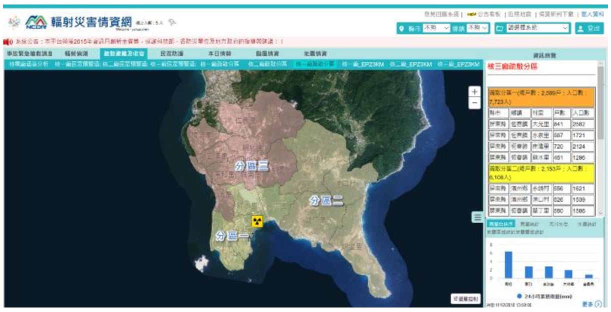

輻射災害情資網
分區三
分區二
分區一

圖 26 核三廠疏散分區

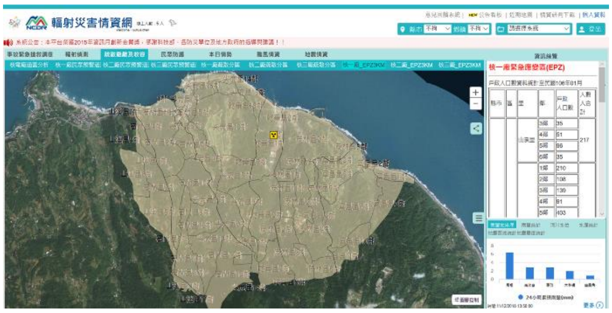


圖 27 核一廠 3 公里區域劃分

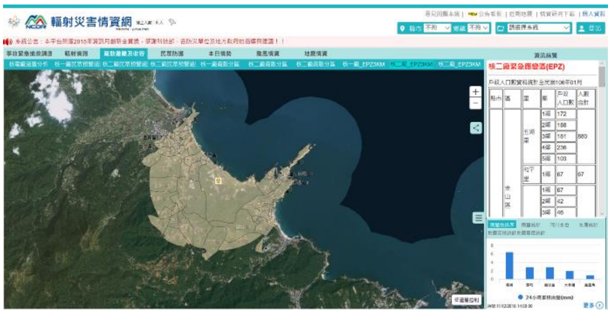


圖 28 核二廠 3 公里區域劃分

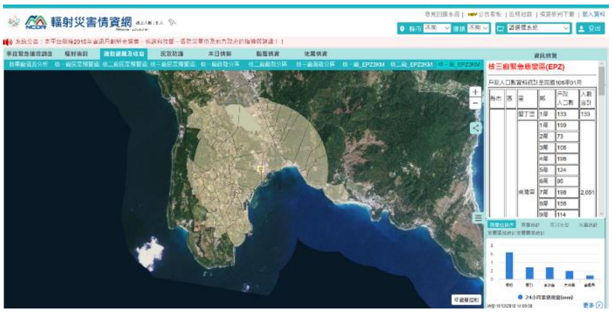
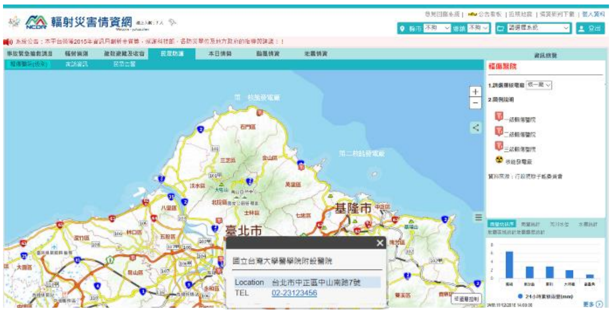

輻射災害情資網
核三廠緊急應變區(EPZ)

圖 29 核三廠 3 公里區域劃分

四、 民眾防護

針對原能會提供輻射災害急救醫院及以民國103年家庭訪問訪查之資訊進行規劃設計，以快速提供資訊，如圖 30 至圖 32 圖示說明。


輻射災害情資網
輻傷醫院
臺北市
基隆市

國立台灣大學醫學院附設醫院
Location 台北市中正區中山南路7號
TEL 02-23123456

圖 30 輻傷醫院(級別)

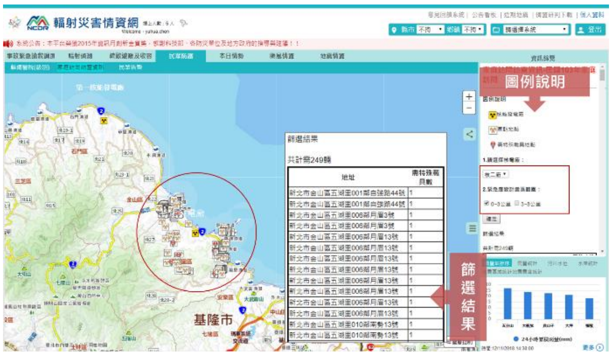
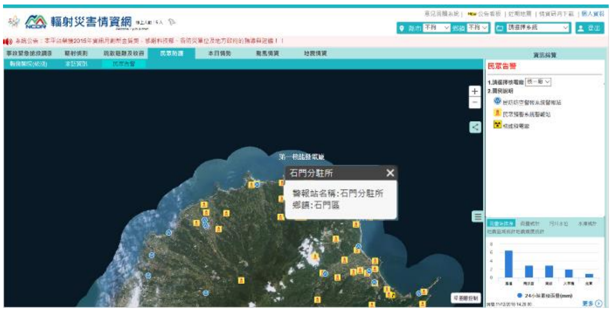

輻射災害情資網
圖例說明
篩選結果
共計有249筆
篩選結果
基隆市

圖 31 家庭訪問訪查資訊


輻射災害情資網
民眾告警

石門分駐所
警報站名稱:石門分駐所
鄉鎮:石門區

圖 32 民眾告警資訊

五、 其他情資

包含本日情勢、颱風情資與地震情資等即時訊息，可藉由此迅速得知，如圖 33 至圖 39 圖示說明。

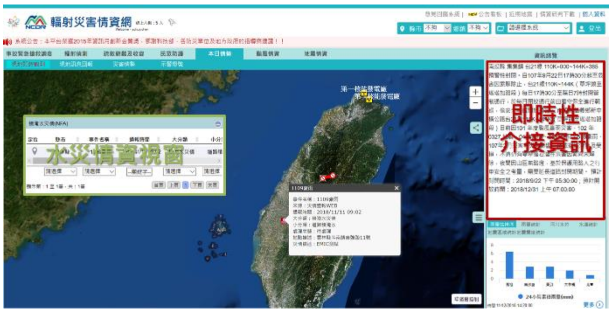

輻射災害情資網
即時性
介接資訊
水災情資視窗

圖 33 現地即時觀測

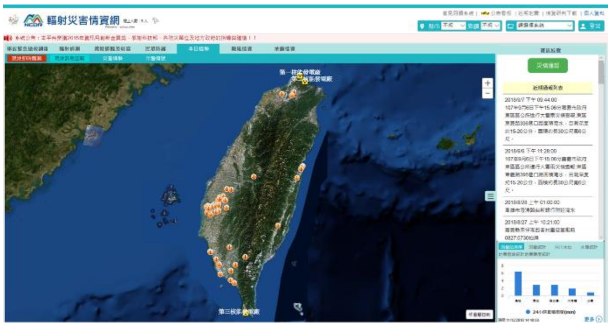


圖 34 現地訊息回報

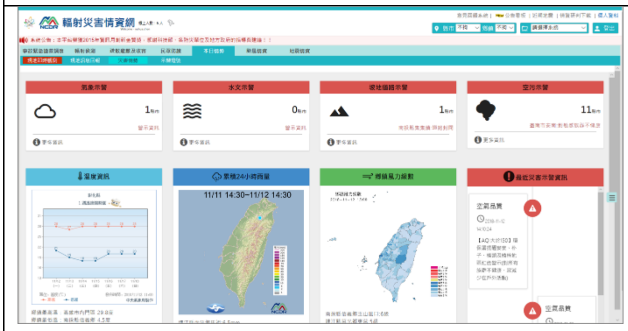


圖 35 災害情勢

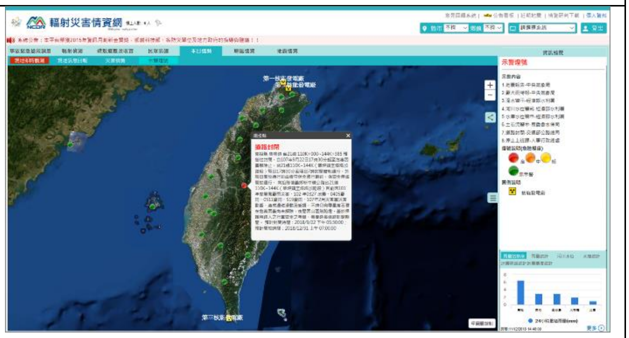


圖 36 示警燈號

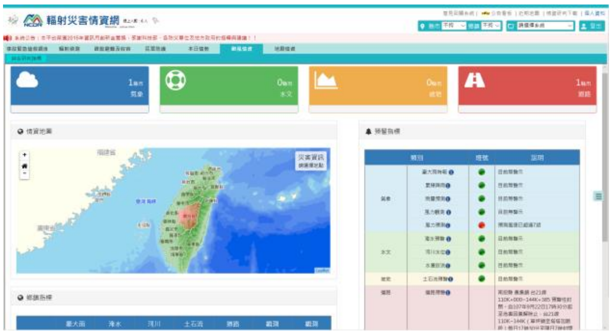


圖 37 綜合研判指標

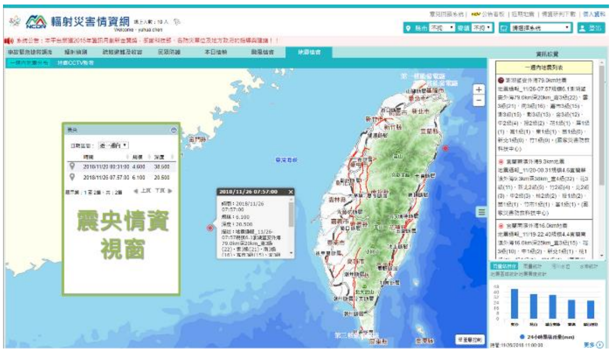

輻射災害情資網
震央情資
視窗

圖 38 一周內地震分布

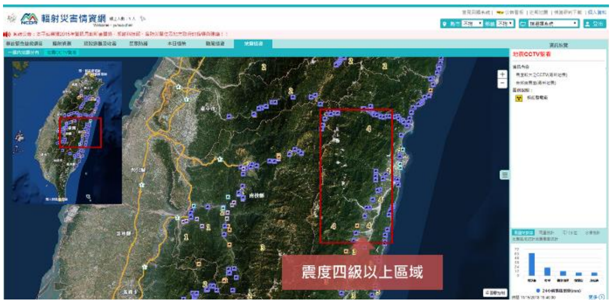

輻射災害情資網
地震CCTV監看
臺中市
南投縣
雲林縣
震度四級以上區域

圖 39 地震 CCTV 監看

第四章　**結論與建議**

一、　結論

考量複合式災害情況下，輻射災害可能伴隨其他天然災害而發生，而當核電廠發生輻射外洩，將會造成周邊地區受嚴重之影響，是故災時緊急應變非常重要。而本中心目前所開發的災害情資服務平台，綜整國內各天然災害即時監測與災害情資，並運用於中央災害應變中心開設時期情資研判重要科技技術。

本研究將輻射災害相關資訊，包含核電廠即時運轉資訊、環境輻射監測、境外與境內輻射災害評估分析，及核電廠周邊涵蓋民生基礎設施等資訊，並結合災害情資服務平台之其他即時災害情資，以核電廠發生事故作為背景設定，規劃出五大功能項目，事故緊急搶救與調度、輻射偵測、疏散避難與收容、民眾防護及其他情資，進行開發輻射災害情資模組，以提供輻射災害應變時期之用，縮短決策之時間。

二、 建議

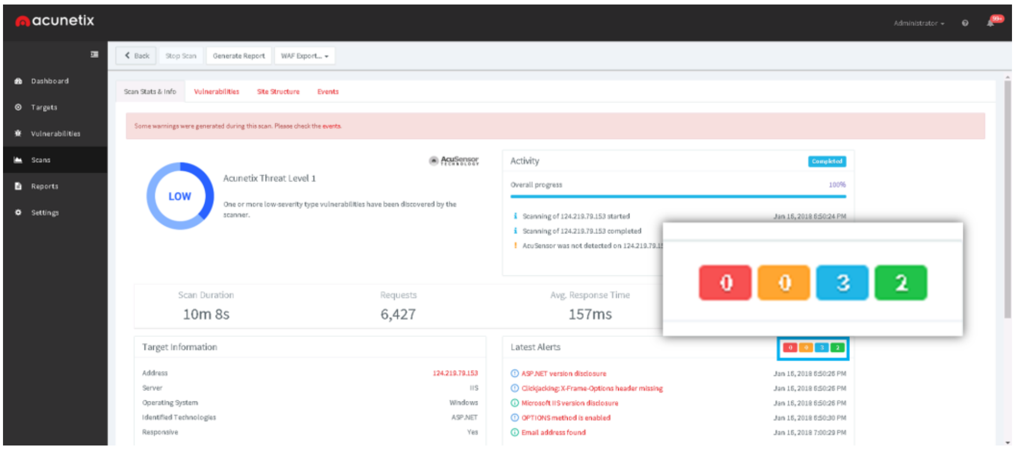
本研究嘗試開發災害情資服務平台-輻射災害情資模組，目前屬初步雛形階段，然災害屬即時性，能縮短應變決策時間，即降低災害所帶來影響，下列提出建議事項：

- 境內劑量評估系統分析與境外輻射擴散分析，目前屬人工更新資料方式，未來可規劃即時性介接服務，透過即時介接方式，快速更新資料。
- 現階段環境輻射偵測資訊為固定點位形式，然在災時會具有臨時環境輻射偵測儀器為非固定點位，未來可將臨時點位納入規劃項目。

附錄一、資安檢測項目

A.網站弱點掃描

本次掃描係採用 Acunetix 軟體（Acunetix Vulnerability Scanner）進行網站弱點掃描，按照契約規定，依「政府機關（構）資通安全等級分級作業規定」，採資訊系統「高」等級執行相關防護基準，且符合 2017 年 OWASP 所發佈的最新十大 Web 弱點程式碼檢測。**今年度經檢測結果無任何高風險或中風險，3 項低風險，2 項普通（對用戶無影響）**（弱點掃描檢測結果）。


acunetix
Administrator
Dashboard
Targets
Vulnerabilities
Scans
Reports
Settings
Back
Stop Scan
Generate Report
WAF Export...
Scan Stats & Info
Vulnerabilities
Site Structure
Events
LOW
AcuSensor
Completed
0
0
3
2

Some warnings were generated during this scan. Please check the events.

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Activity

Overall progress 100%

Scanning of 124.219.79.153 started — Jan 16, 2018 6:50:24 PM

Scanning of 124.219.79.153 completed

AcuSensor was not detected on 124.219.79.1

Scan Duration	Requests	Avg. Response Time
10m 8s	6,427	157ms

Target Information

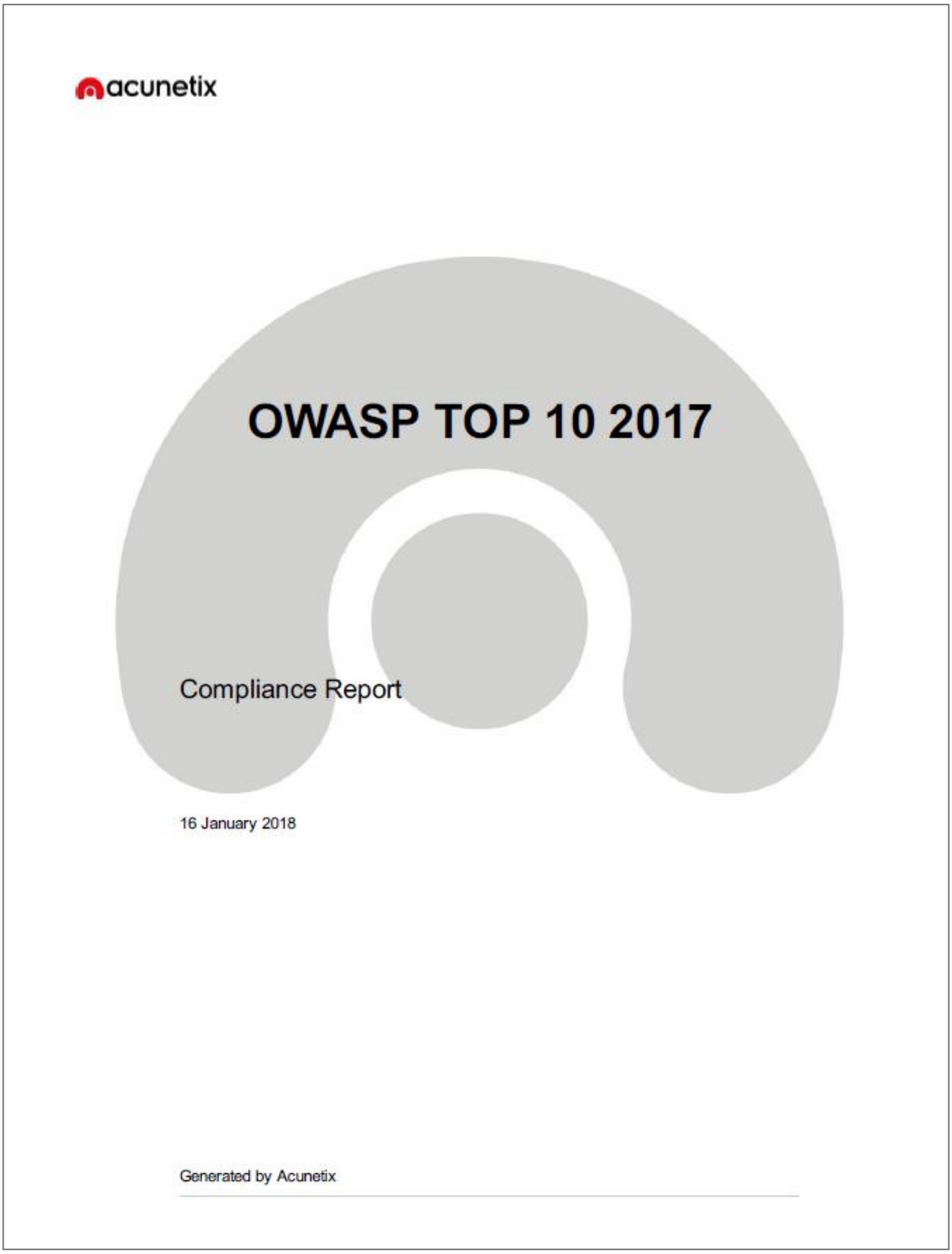
Address	124.219.79.153
Server	IIS
Operating System	Windows
Identified Technologies	ASP.NET
Responsive	Yes

Latest Alerts

ASP.NET version disclosure	Jan 16, 2018 6:50:26 PM
Clickjacking: X-Frame-Options header missing	Jan 16, 2018 6:50:26 PM
Microsoft IIS version disclosure	Jan 16, 2018 6:50:26 PM
OPTIONS method is enabled	Jan 16, 2018 6:50:30 PM
Email address found	Jan 16, 2018 7:00:29 PM

弱點掃描檢測結果

➢ 成果報告



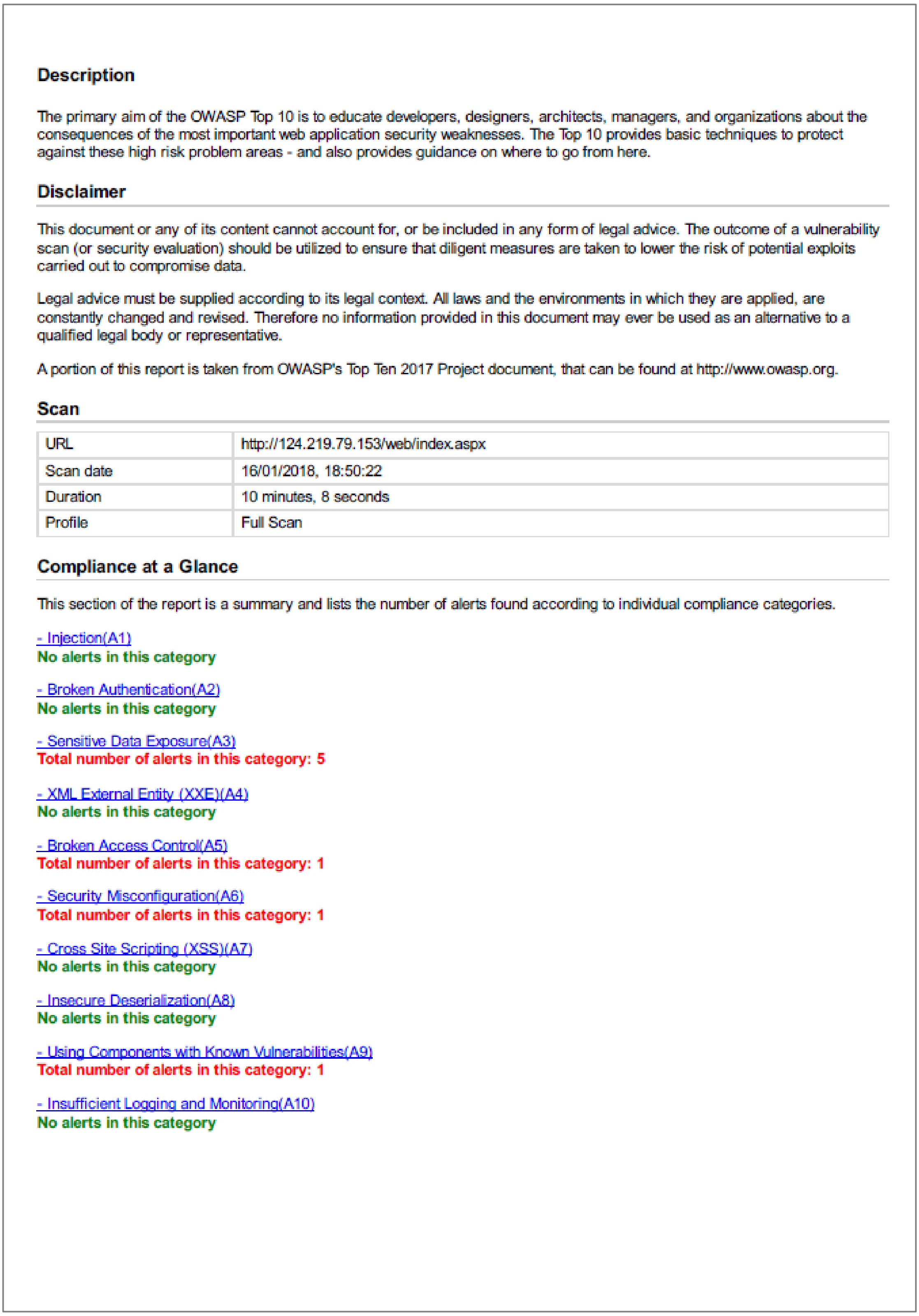
acunetix

OWASP TOP 10 2017

Compliance Report

16 January 2018

Generated by Acunetix



Description

The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risk problem areas - and also provides guidance on where to go from here.

Disclaimer

This document or any of its content cannot account for, or be included in any form of legal advice. The outcome of a vulnerability scan (or security evaluation) should be utilized to ensure that diligent measures are taken to lower the risk of potential exploits carried out to compromise data.

Legal advice must be supplied according to its legal context. All laws and the environments in which they are applied, are constantly changed and revised. Therefore no information provided in this document may ever be used as an alternative to a qualified legal body or representative.

A portion of this report is taken from OWASP's Top Ten 2017 Project document, that can be found at http://www.owasp.org.

Scan

URL	http://124.219.79.153/web/index.aspx
Scan date	16/01/2018, 18:50:22
Duration	10 minutes, 8 seconds
Profile	Full Scan

Compliance at a Glance

This section of the report is a summary and lists the number of alerts found according to individual compliance categories.

- Injection(A1)
No alerts in this category

- Broken Authentication(A2)
No alerts in this category

- Sensitive Data Exposure(A3)
Total number of alerts in this category: 5

- XML External Entity (XXE)(A4)
No alerts in this category

- Broken Access Control(A5)
Total number of alerts in this category: 1

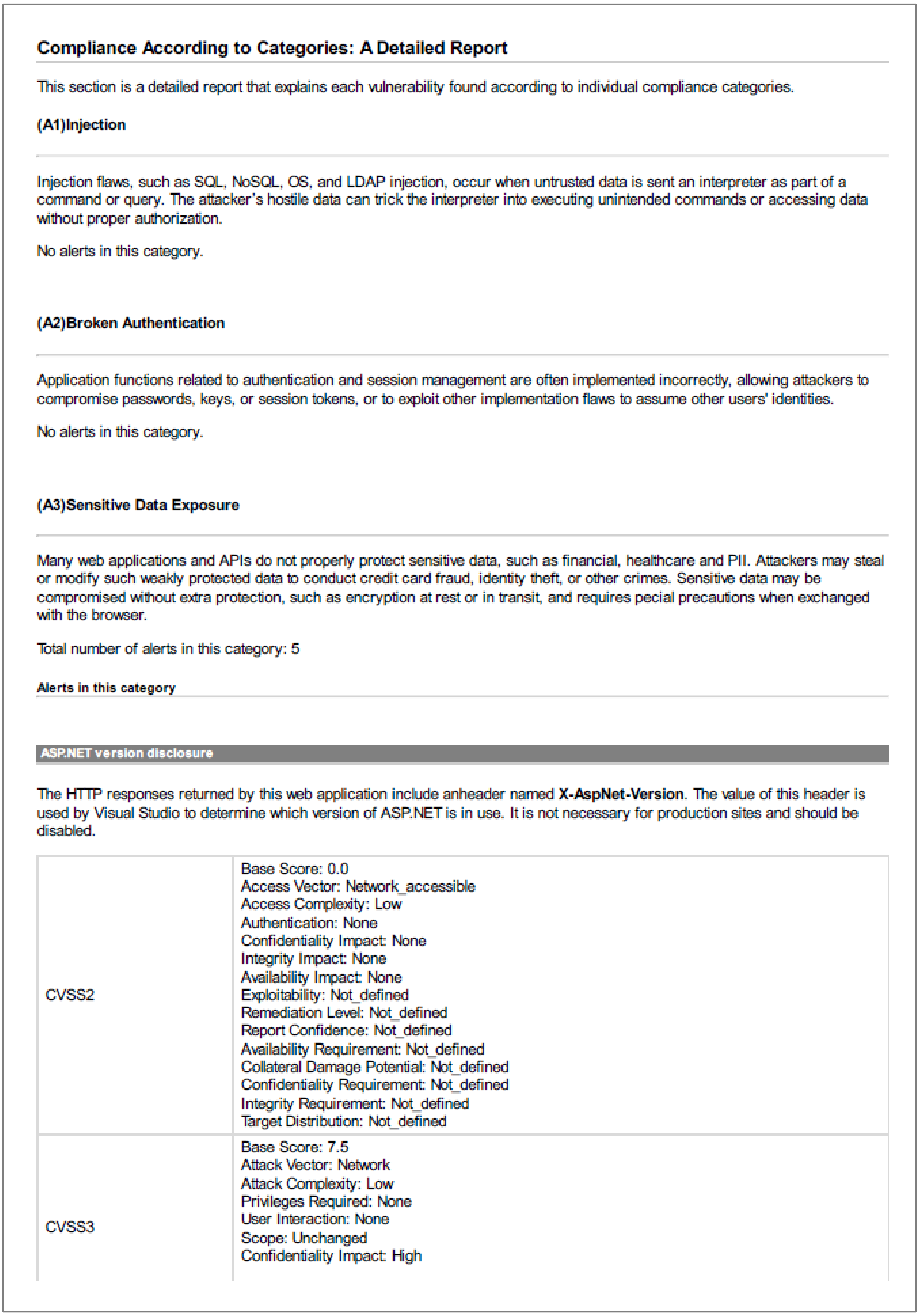
- Security Misconfiguration(A6)
Total number of alerts in this category: 1

- Cross Site Scripting (XSS)(A7)
No alerts in this category

- Insecure Deserialization(A8)
No alerts in this category

- Using Components with Known Vulnerabilities(A9)
Total number of alerts in this category: 1

- Insufficient Logging and Monitoring(A10)
No alerts in this category



Compliance According to Categories: A Detailed Report

This section is a detailed report that explains each vulnerability found according to individual compliance categories.

(A1)Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

No alerts in this category.

(A2)Broken Authentication

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

No alerts in this category.

(A3)Sensitive Data Exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires pecial precautions when exchanged with the browser.

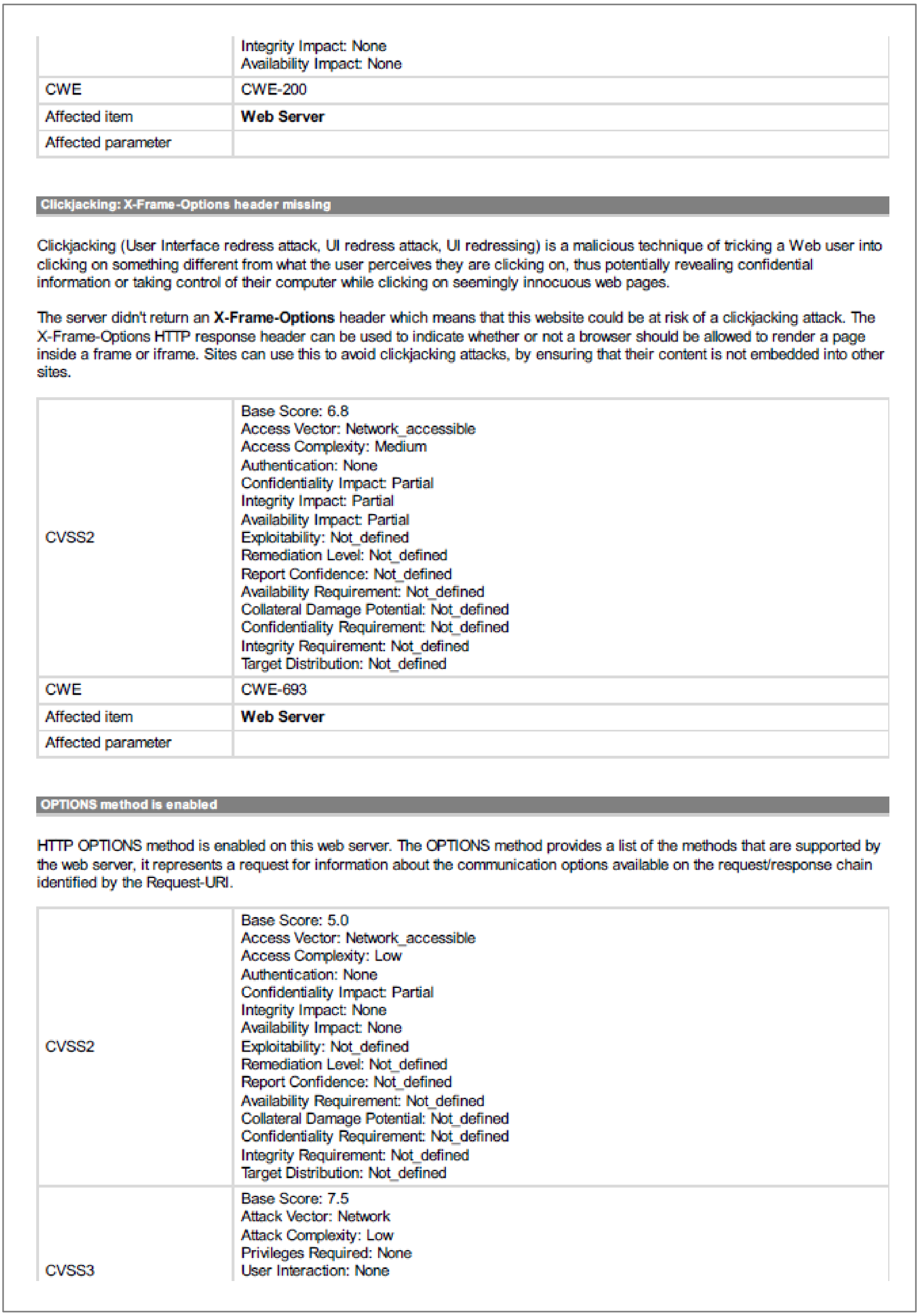
Total number of alerts in this category: 5

Alerts in this category

ASP.NET version disclosure

The HTTP responses returned by this web application include anheader named **X-AspNet-Version**. The value of this header is used by Visual Studio to determine which version of ASP.NET is in use. It is not necessary for production sites and should be disabled.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High



	Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	**Web Server**
Affected parameter	

Clickjacking: X-Frame-Options header missing

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

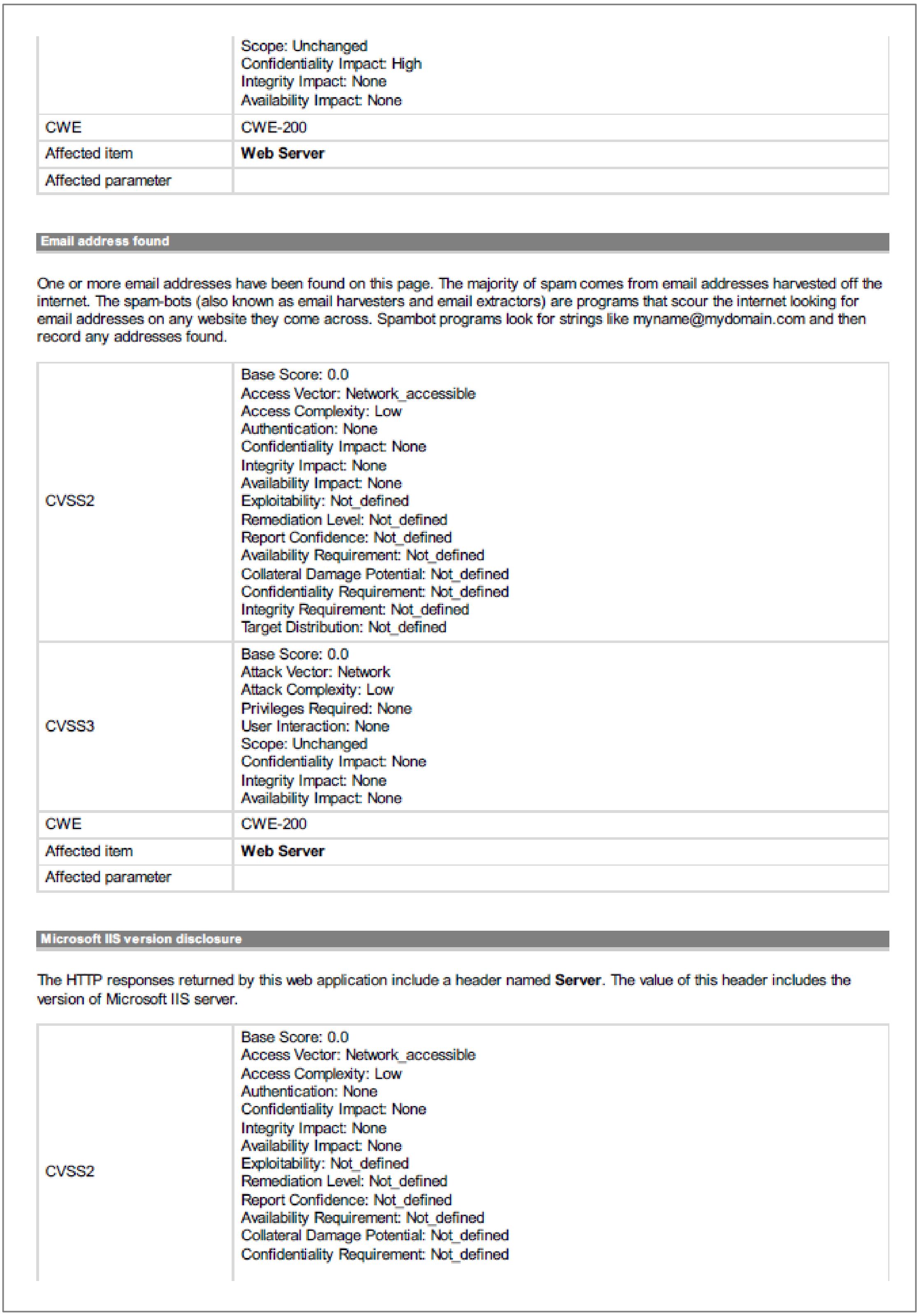
The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-693
Affected item	**Web Server**
Affected parameter	

OPTIONS method is enabled

HTTP OPTIONS method is enabled on this web server. The OPTIONS method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None



	Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	**Web Server**
Affected parameter	

Email address found

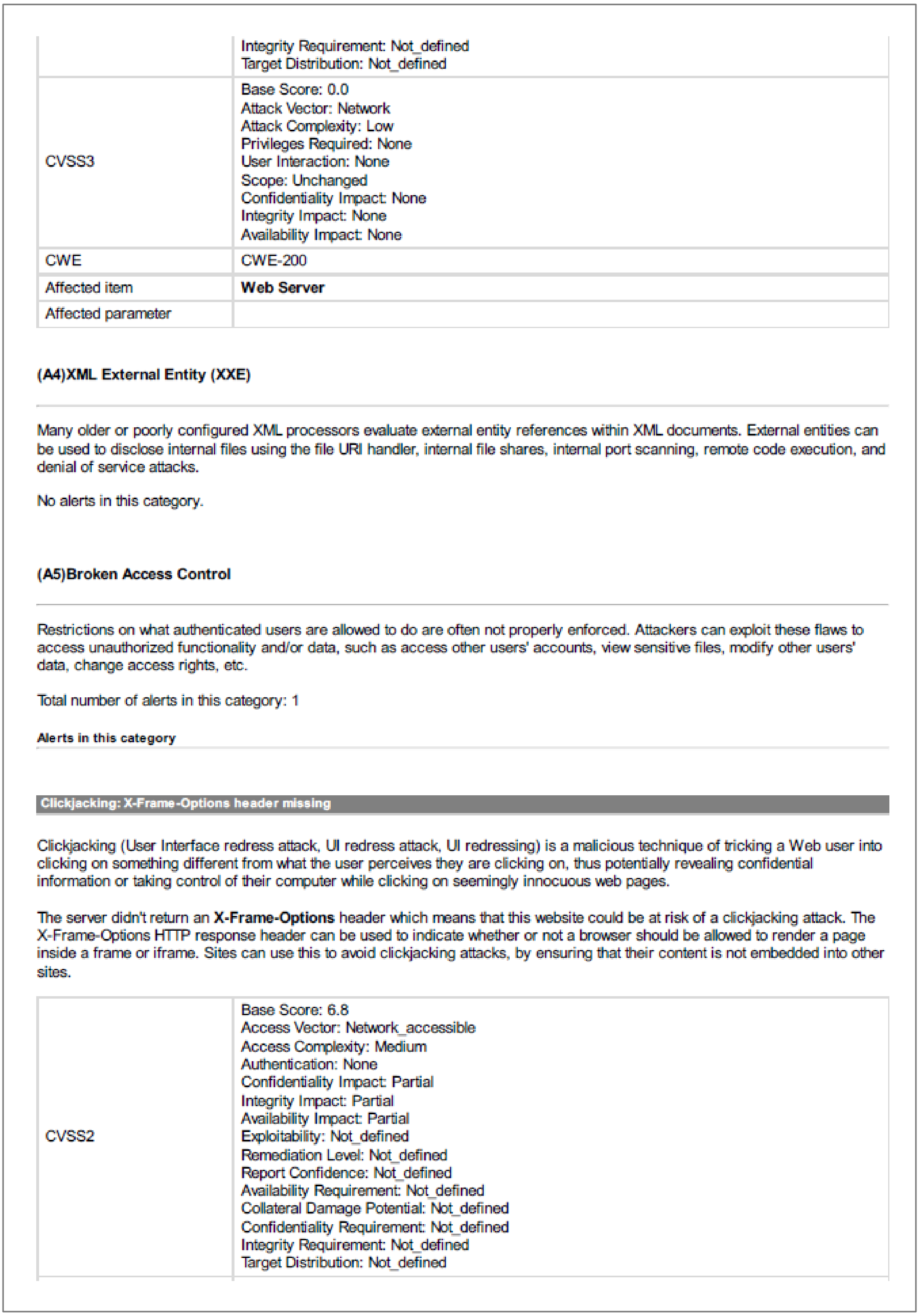
One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	**Web Server**
Affected parameter	

Microsoft IIS version disclosure

The HTTP responses returned by this web application include a header named **Server**. The value of this header includes the version of Microsoft IIS server.

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined



	Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	**Web Server**
Affected parameter	

(A4)XML External Entity (XXE)

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

No alerts in this category.

(A5)Broken Access Control

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

Total number of alerts in this category: 1

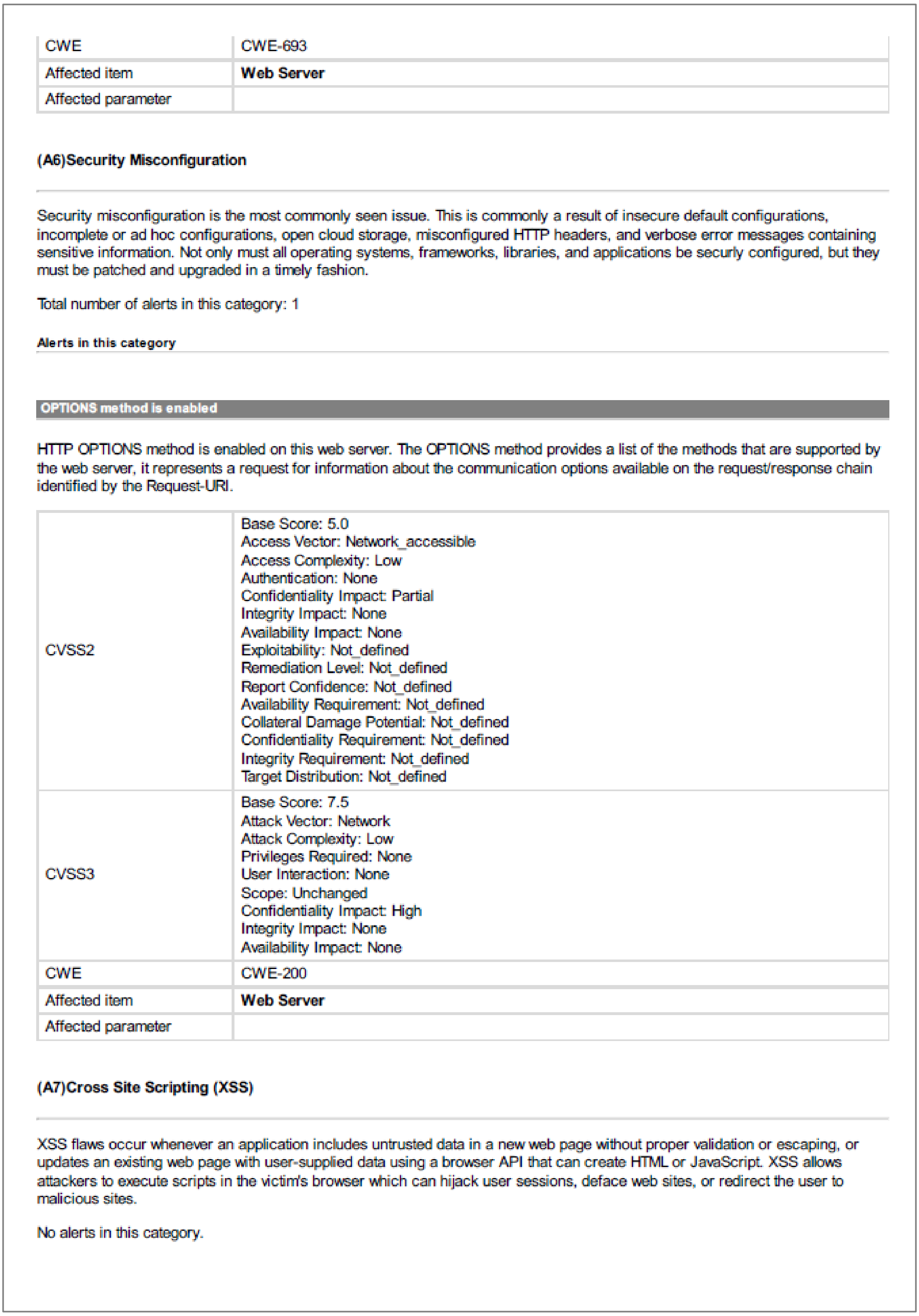
Alerts in this category

Clickjacking: X-Frame-Options header missing

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined



CWE	CWE-693
Affected item	**Web Server**
Affected parameter	

(A6)Security Misconfiguration

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securly configured, but they must be patched and upgraded in a timely fashion.

Total number of alerts in this category: 1

Alerts in this category

OPTIONS method is enabled

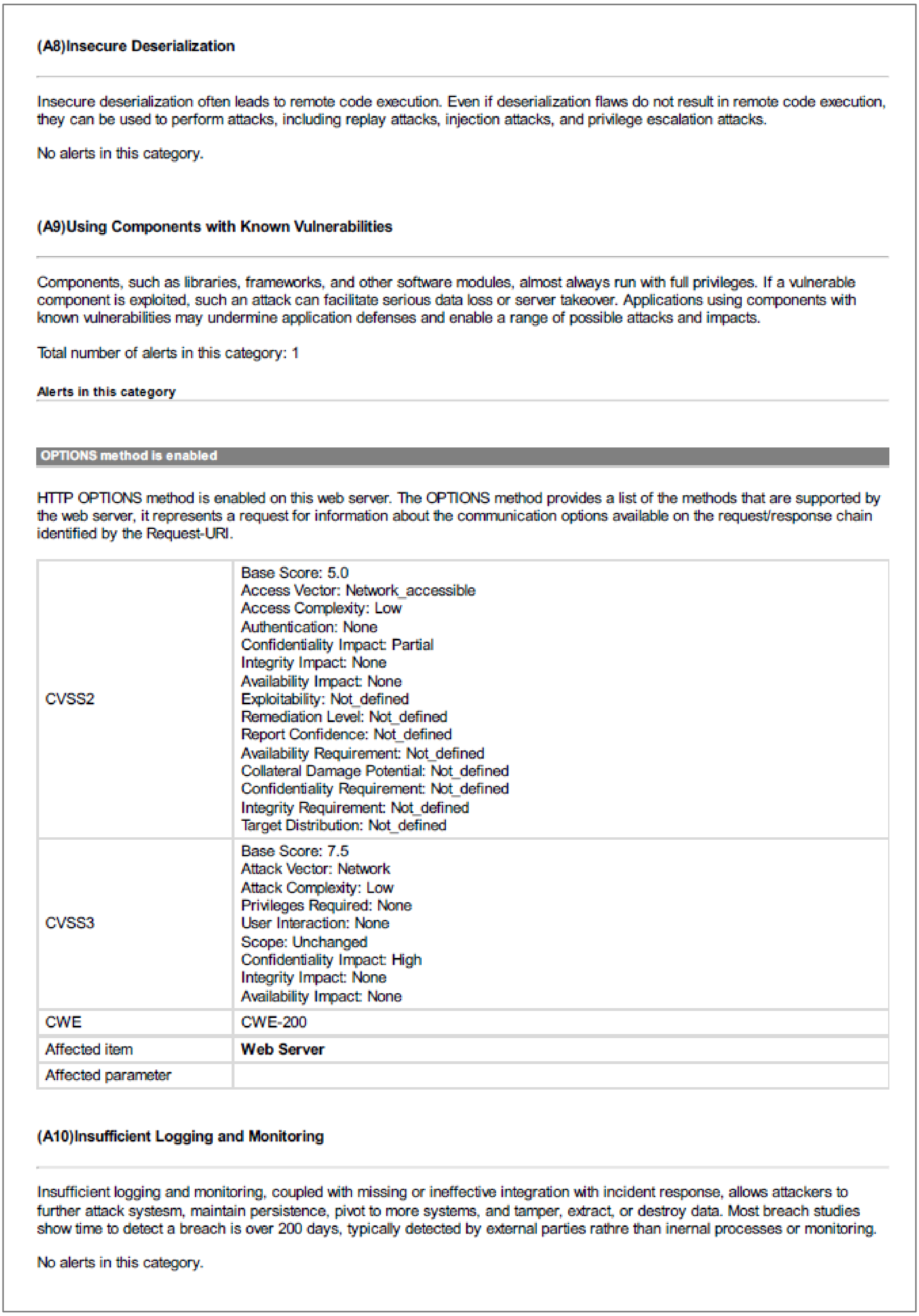
HTTP OPTIONS method is enabled on this web server. The OPTIONS method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	**Web Server**
Affected parameter	

(A7)Cross Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

No alerts in this category.



(A8)Insecure Deserialization

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

No alerts in this category.

(A9)Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

Total number of alerts in this category: 1

Alerts in this category

OPTIONS method is enabled

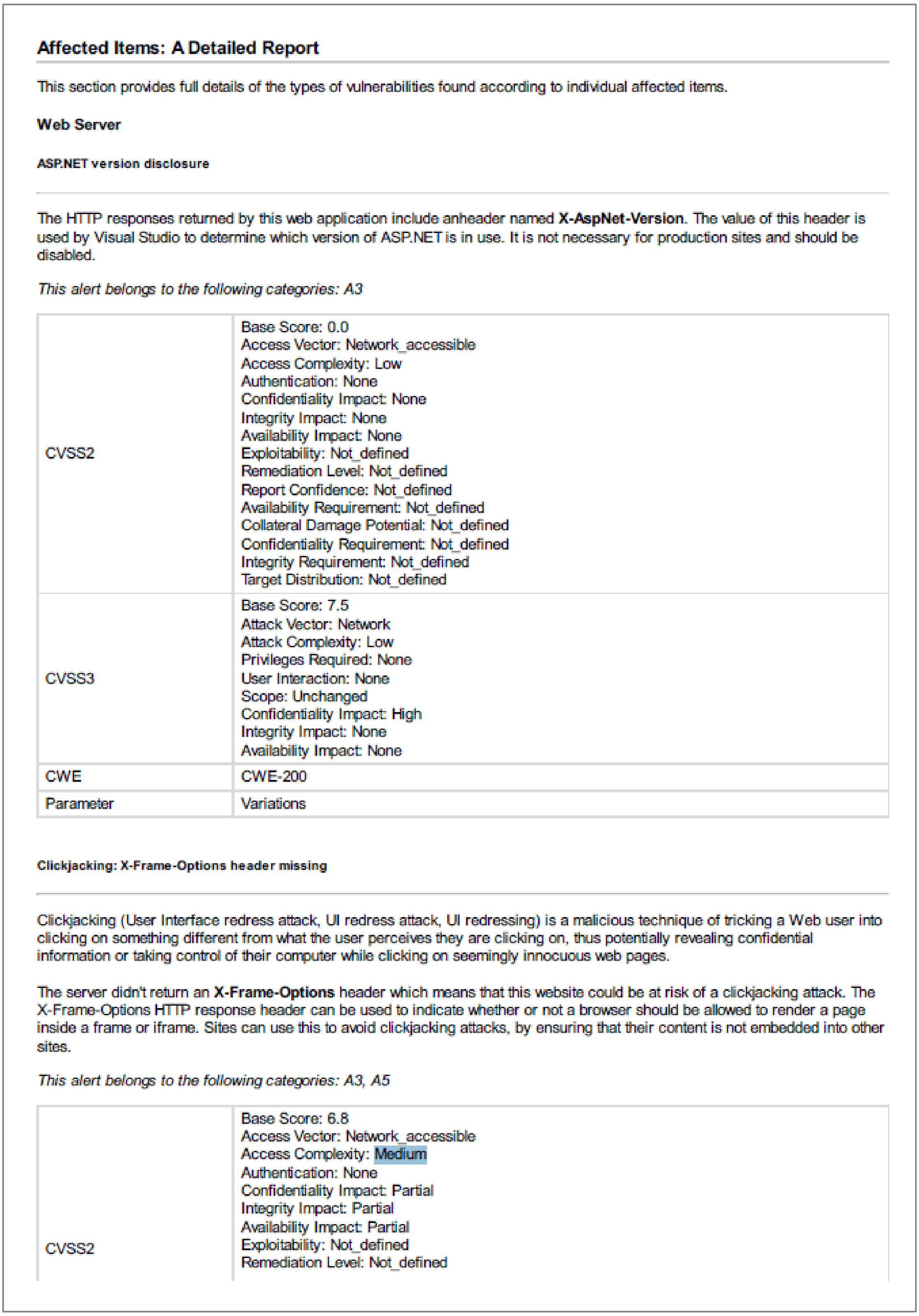
HTTP OPTIONS method is enabled on this web server. The OPTIONS method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI.

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Affected item	**Web Server**
Affected parameter	

(A10)Insufficient Logging and Monitoring

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systesm, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rathre than inernal processes or monitoring.

No alerts in this category.



Affected Items: A Detailed Report

This section provides full details of the types of vulnerabilities found according to individual affected items.

Web Server

ASP.NET version disclosure

The HTTP responses returned by this web application include anheader named **X-AspNet-Version**. The value of this header is used by Visual Studio to determine which version of ASP.NET is in use. It is not necessary for production sites and should be disabled.

This alert belongs to the following categories: A3

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

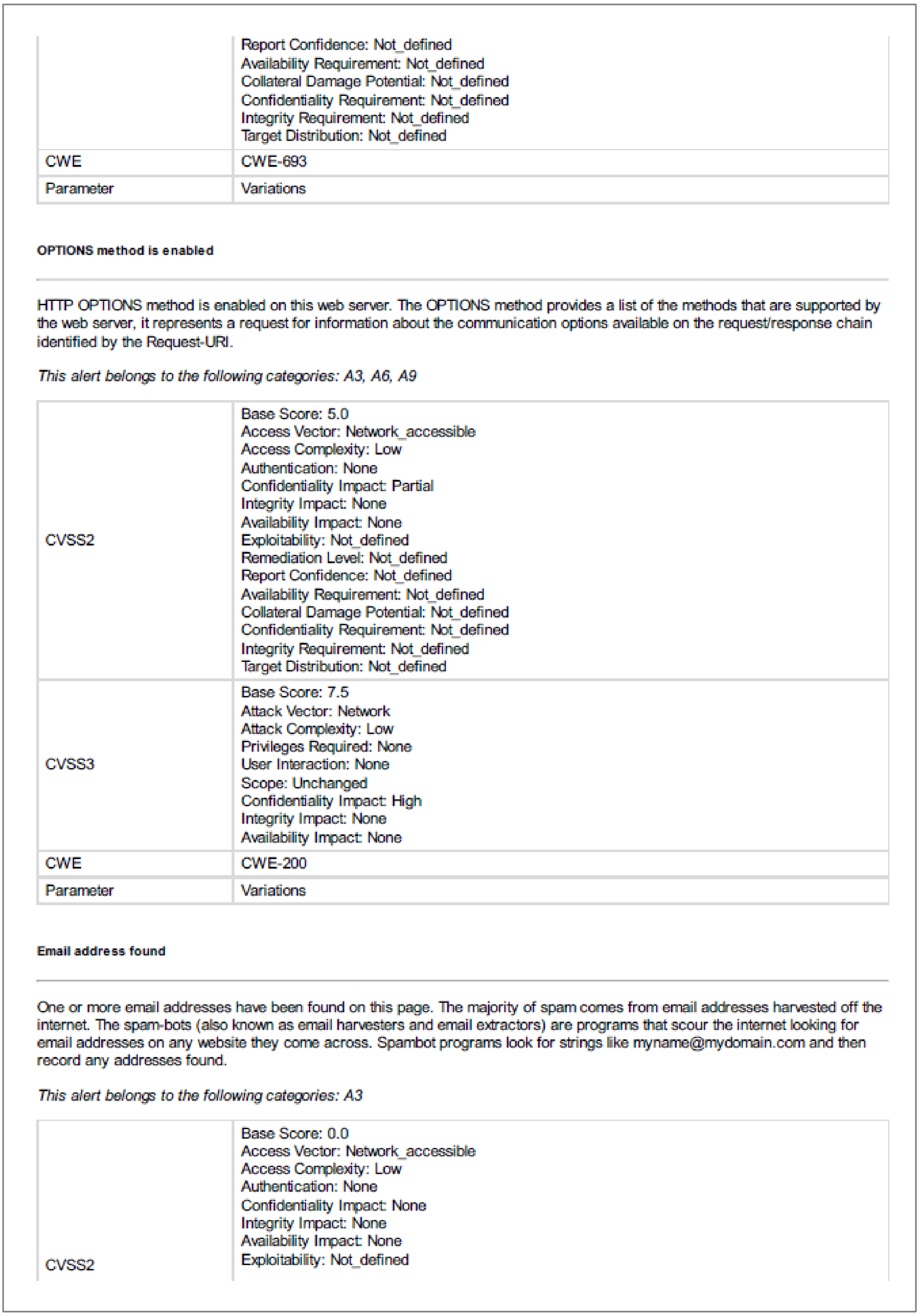
Clickjacking: X-Frame-Options header missing

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

This alert belongs to the following categories: A3, A5

CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined



	Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-693
Parameter	Variations

OPTIONS method is enabled

HTTP OPTIONS method is enabled on this web server. The OPTIONS method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI.

This alert belongs to the following categories: A3, A6, A9

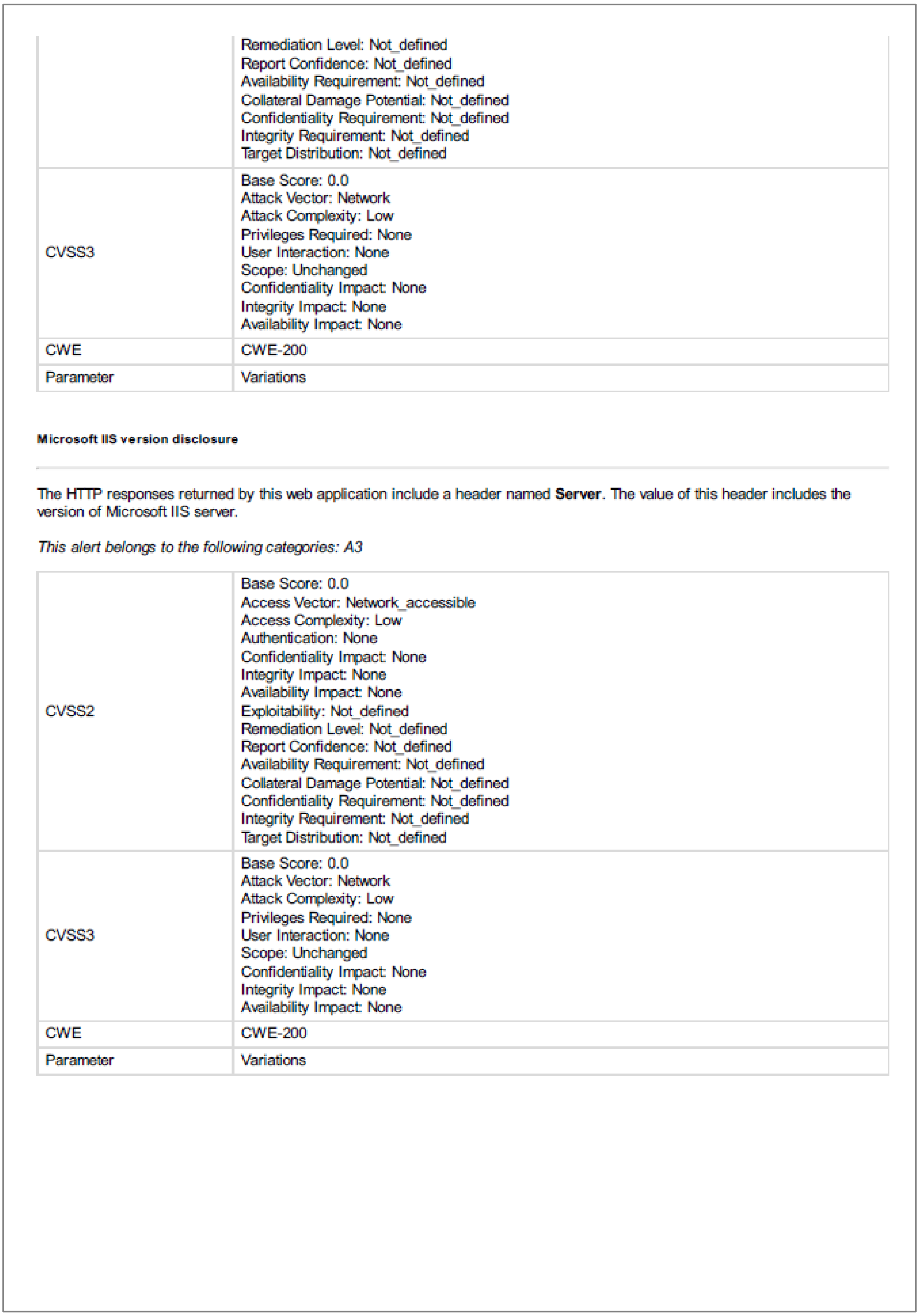
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Email address found

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

This alert belongs to the following categories: A3

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined



	Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

Microsoft IIS version disclosure

The HTTP responses returned by this web application include a header named **Server**. The value of this header includes the version of Microsoft IIS server.

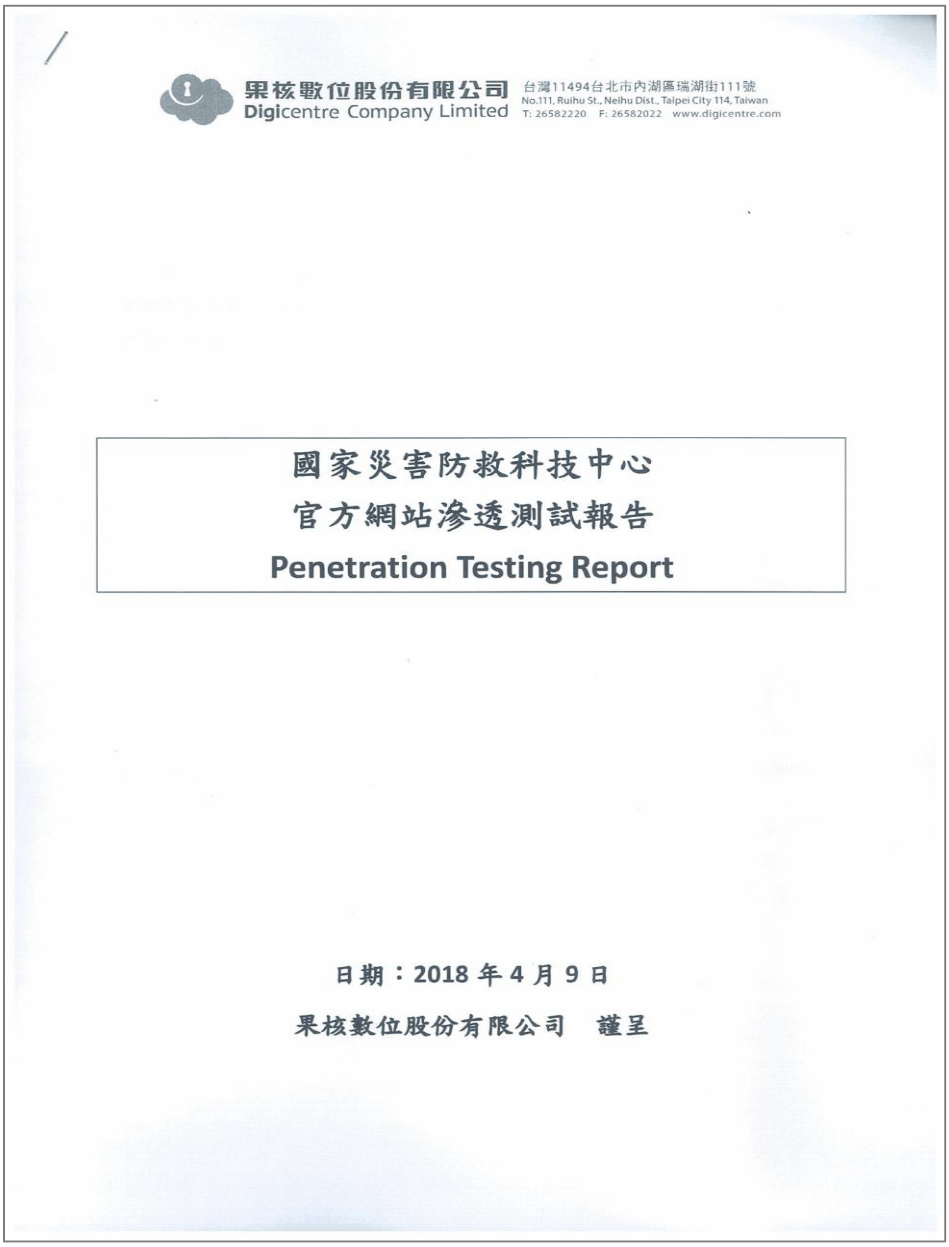
This alert belongs to the following categories: A3

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200
Parameter	Variations

B.滲透測試報告

災害情資服務平台【http://ceocdss.ncdr.nat.gov.tw/】，今年度**經測試結果並無高、中等級風險。**

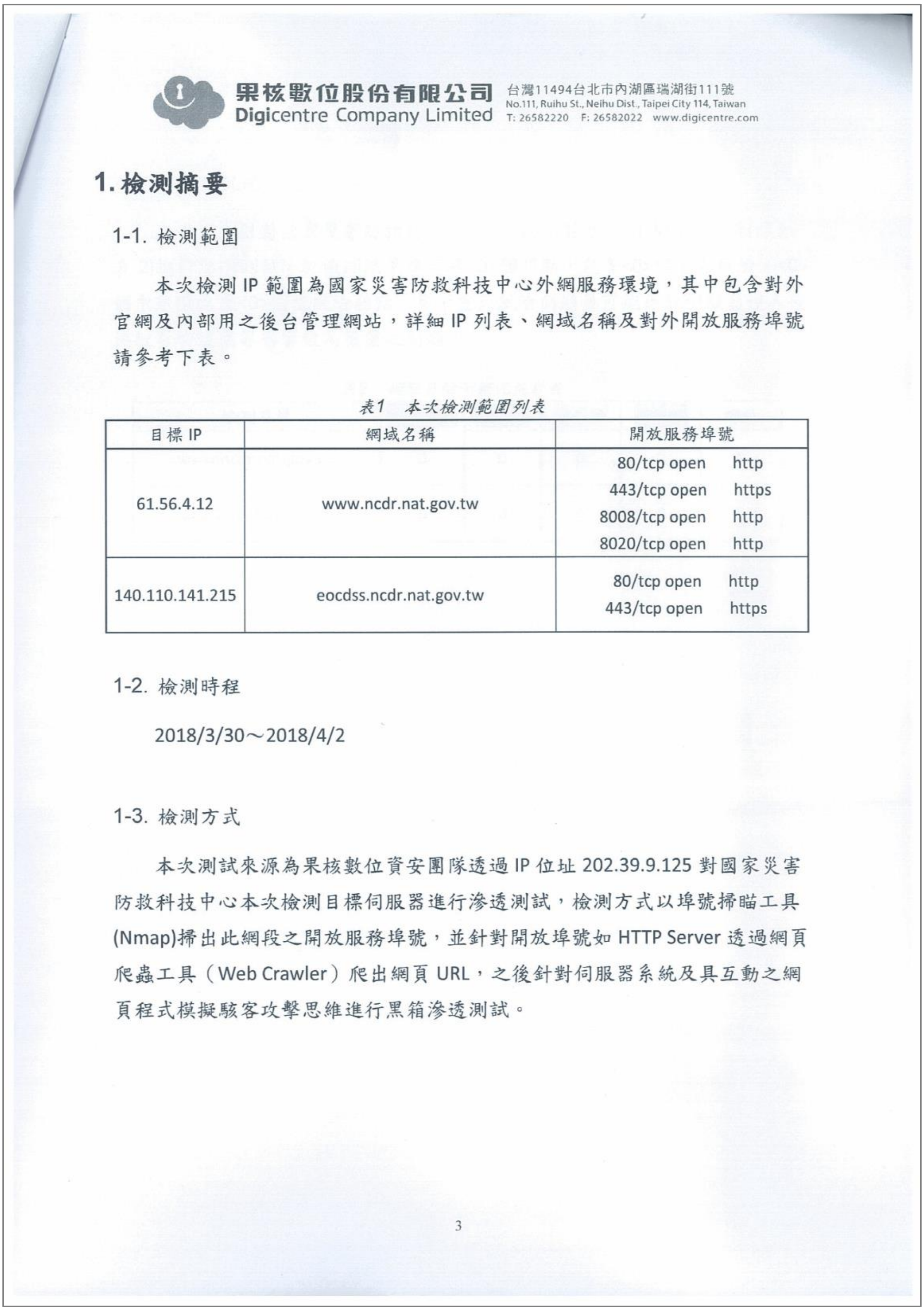
- 成果報告



果核數位股份有限公司
Digicentre Company Limited
台灣11494台北市內湖區瑞湖街111號
No.111, Ruihu St., Neihu Dist., Taipei City 114, Taiwan
T: 26582220 F: 26582022 www.digicentre.com

國家災害防救科技中心
官方網站滲透測試報告
Penetration Testing Report

日期：2018 年 4 月 9 日
果核數位股份有限公司 謹呈



果核數位股份有限公司
Digicentre Company Limited
台灣11494台北市內湖區瑞湖街111號
No.111, Ruihu St., Neihu Dist., Taipei City 114, Taiwan
T: 26582220 F: 26582022 www.digicentre.com

1. 檢測摘要

1-1. 檢測範圍

本次檢測 IP 範圍為國家災害防救科技中心外網服務環境，其中包含對外官網及內部用之後台管理網站，詳細 IP 列表、網域名稱及對外開放服務埠號請參考下表。

表1 本次檢測範圍列表

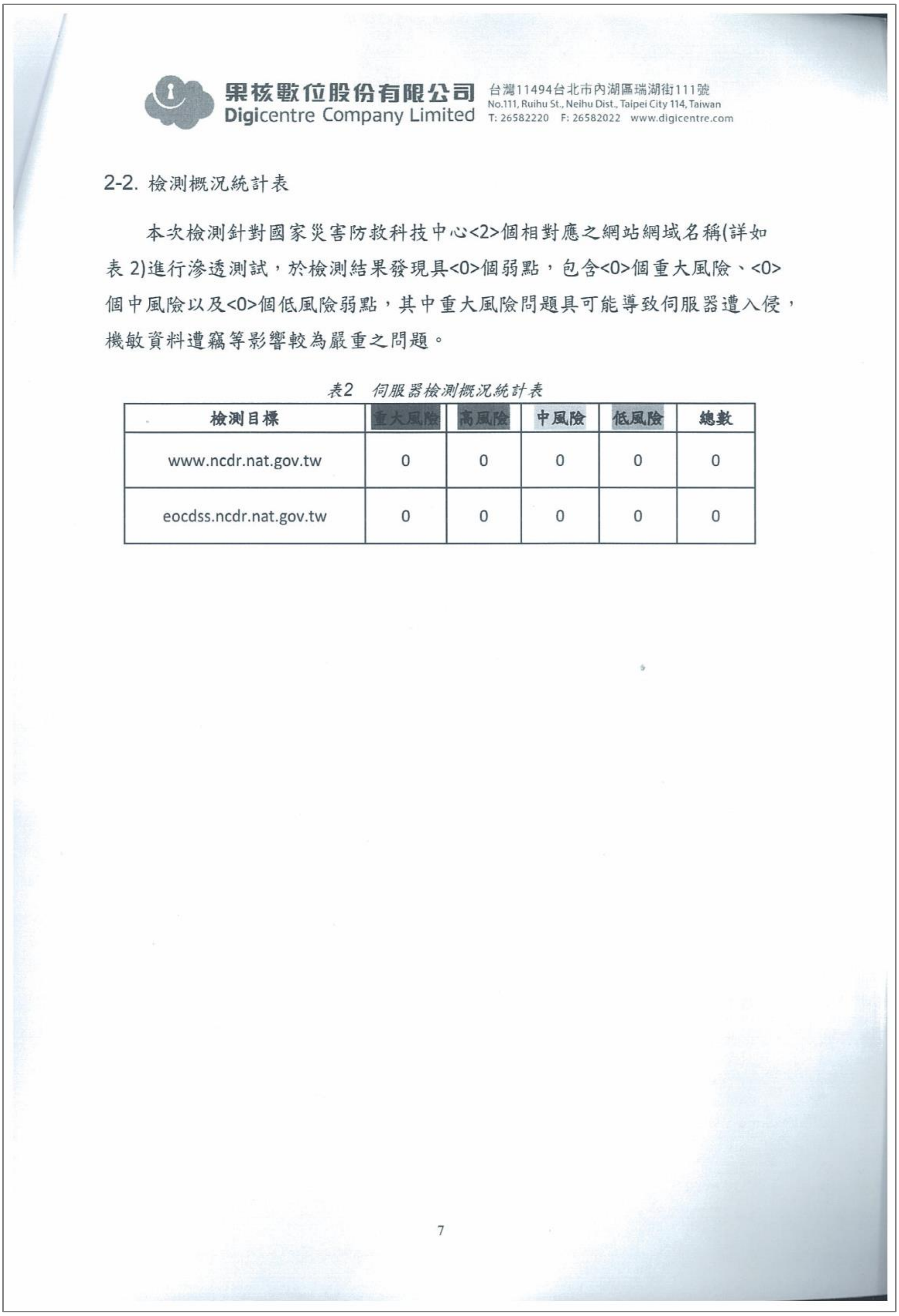
目標 IP	網域名稱	開放服務埠號
61.56.4.12	www.ncdr.nat.gov.tw	80/tcp open http 443/tcp open https 8008/tcp open http 8020/tcp open http
140.110.141.215	eocdss.ncdr.nat.gov.tw	80/tcp open http 443/tcp open https

1-2. 檢測時程

2018/3/30～2018/4/2

1-3. 檢測方式

本次測試來源為果核數位資安團隊透過 IP 位址 202.39.9.125 對國家災害防救科技中心本次檢測目標伺服器進行滲透測試，檢測方式以埠號掃瞄工具(Nmap)掃出此網段之開放服務埠號，並針對開放埠號如 HTTP Server 透過網頁爬蟲工具（Web Crawler）爬出網頁 URL，之後針對伺服器系統及具互動之網頁程式模擬駭客攻擊思維進行黑箱滲透測試。



2-2. 檢測概況統計表

本次檢測針對國家災害防救科技中心<2>個相對應之網站網域名稱(詳如表 2)進行滲透測試，於檢測結果發現具<0>個弱點，包含<0>個重大風險、<0>個中風險以及<0>個低風險弱點，其中重大風險問題具可能導致伺服器遭入侵，機敏資料遭竊等影響較為嚴重之問題。

表2 伺服器檢測概況統計表

檢測目標	重大風險	高風險	中風險	低風險	總數
www.ncdr.nat.gov.tw	0	0	0	0	0
eocdss.ncdr.nat.gov.tw	0	0	0	0	0

C.系統壓力測試

壓力測試（Stress Test）是用以驗證本中心災害情資服務平台在大量負載下的穩定程度，系統的功能是否還能正常運作。此外，隨著系統使用者人數的增加，可能會造成系統回應時間越來越慢，甚至無法正常進行作業，透過壓力測試了解系統的負載上限，確保在多少人數下操作系統，每位使用者所發出的請求（Request）都能正常被處理，同時可以很快的將資訊回應（Response）給使用者。

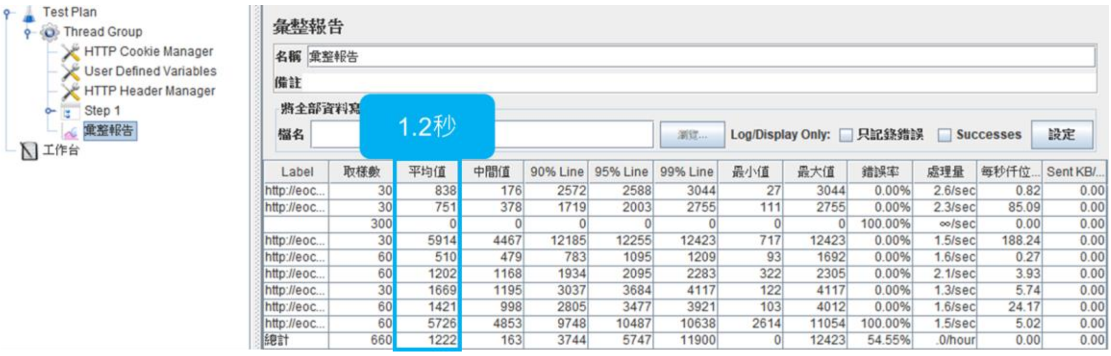
依現行本平台的使用者環境訂定壓力測試計畫，此測試係以**Simon Sadedin 所開發之軟體**進行腳本錄製，模擬多人同時連線至【http://ceocdss.ncdr.nat.gov.tw/】站台。

操作情境與腳本說明如下：

- 模擬多人同時連線至災防科技中心環境主機。
- 待連線至災情網後，點擊災害發生時最常查看之頁籤，模擬操作後資料回應時間。

將上述情境之腳本匯入 JMeter 軟體進行壓力檢測，**檢測結果符合規範，詳細說明與統計結果數據展示如下：**

- 30 人同時上線連線至本中心機房之回應時間：1.2 秒。
- 回應時間超過 10 秒的同時上線人數：300 人。
- 回應時間超過 20 秒的同時上線人數：600 人。
- 回應時間超過 30 秒的同時上線人數：1,000 人。


Test Plan
Thread Group
HTTP Cookie Manager
User Defined Variables
HTTP Header Manager
Step 1
彙整報告
工作台
瀏覽...
設定
1.2秒

彙整報告

名稱 彙整報告

備註

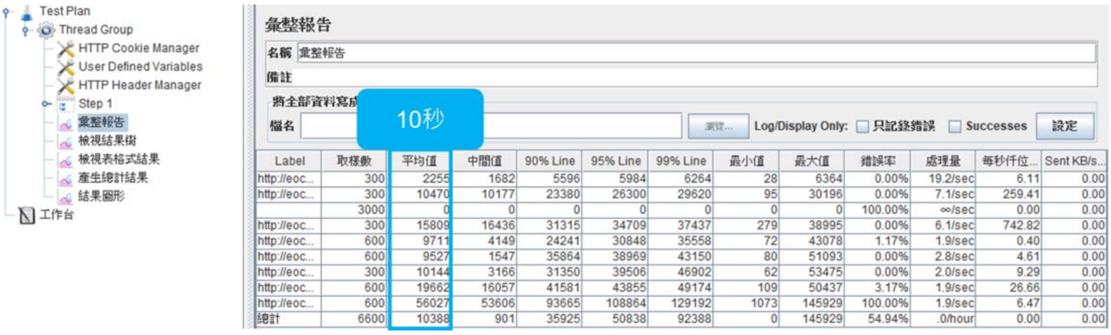
將全部資料寫

檔名

Log/Display Only: ☐ 只記錄錯誤 ☐ Successes

Label	取樣數	平均值	中間值	90% Line	95% Line	99% Line	最小值	最大值	錯誤率	處理量	每秒仟位...	Sent KB/...
http://eoc...	30	838	176	2572	2588	3044	27	3044	0.00%	2.6/sec	0.82	0.00
http://eoc...	30	751	378	1719	2003	2755	111	2755	0.00%	2.3/sec	85.09	0.00
	300	0	0	0	0	0	0	0	100.00%	∞/sec	0.00	0.00
http://eoc...	30	5914	4467	12185	12255	12423	717	12423	0.00%	1.5/sec	188.24	0.00
http://eoc...	60	510	479	783	1095	1209	93	1692	0.00%	1.6/sec	0.27	0.00
http://eoc...	60	1202	1168	1934	2095	2283	322	2305	0.00%	2.1/sec	3.93	0.00
http://eoc...	30	1669	1195	3037	3684	4117	122	4117	0.00%	1.3/sec	5.74	0.00
http://eoc...	60	1421	998	2805	3477	3921	103	4012	0.00%	1.6/sec	24.17	0.00
http://eoc...	60	5726	4853	9748	10487	10638	2614	11054	100.00%	1.5/sec	5.02	0.00
總計	660	1222	163	3744	5747	11900	0	12423	54.55%	.0/hour	0.00	0.00

模擬 30 人同時上線回應時間 1.2 秒


Test Plan
Thread Group
HTTP Cookie Manager
User Defined Variables
HTTP Header Manager
Step 1
彙整報告
檢視結果樹
檢視表格式結果
產生總計結果
結果圖形
工作台
瀏覽...
設定
10秒

彙整報告

名稱 彙整報告

備註

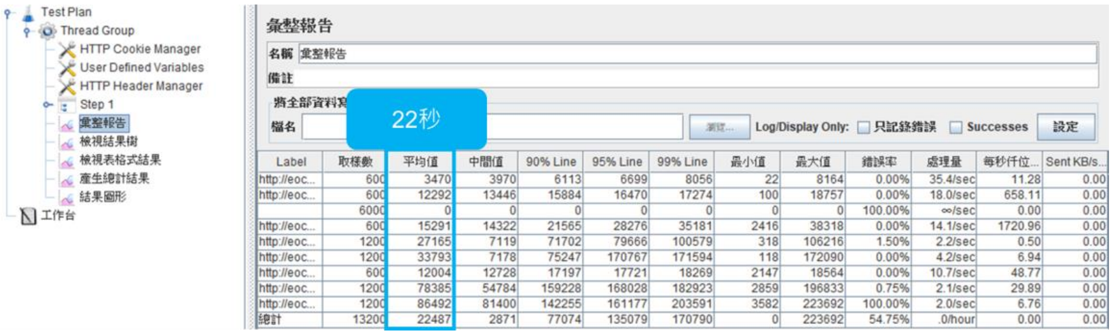
將全部資料寫成

檔名

Log/Display Only: ☐ 只記錄錯誤 ☐ Successes

Label	取樣數	平均值	中間值	90% Line	95% Line	99% Line	最小值	最大值	錯誤率	處理量	每秒仟位...	Sent KB/s...
http://eoc...	300	2255	1682	5596	5984	6264	28	6364	0.00%	19.2/sec	6.11	0.00
http://eoc...	300	10470	10177	23380	26300	29620	95	30196	0.00%	7.1/sec	259.41	0.00
	3000	0	0	0	0	0	0	0	100.00%	∞/sec	0.00	0.00
http://eoc...	300	15809	16436	31315	34709	37437	279	38995	0.00%	6.1/sec	742.82	0.00
http://eoc...	600	9711	4149	24241	30848	35558	72	43078	1.17%	1.9/sec	0.40	0.00
http://eoc...	600	9527	1547	35864	38969	43150	80	51093	0.00%	2.8/sec	4.61	0.00
http://eoc...	300	10144	3166	31350	39506	46902	62	53475	0.00%	2.0/sec	9.29	0.00
http://eoc...	600	19662	16057	41581	43855	49174	109	50437	3.17%	1.9/sec	26.66	0.00
http://eoc...	600	56027	53606	93665	108864	129192	1073	145929	100.00%	1.9/sec	6.47	0.00
總計	6600	10388	901	35925	50838	92388	0	145929	54.94%	.0/hour	0.00	0.00

模擬 300 人同時上線回應時間 10 秒


Test Plan
Thread Group
HTTP Cookie Manager
User Defined Variables
HTTP Header Manager
Step 1
彙整報告
檢視結果樹
檢視表格式結果
產生總計結果
結果圖形
工作台
瀏覽...
設定
22秒

彙整報告

名稱 彙整報告

備註

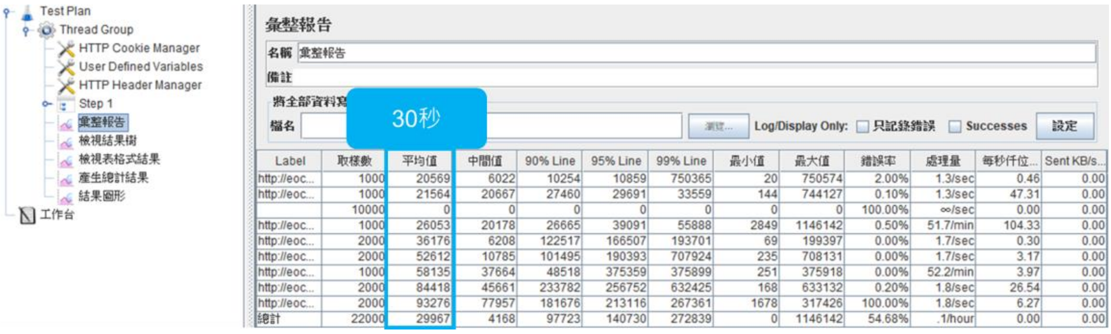
將全部資料寫

檔名

Log/Display Only: ☐ 只記錄錯誤 ☐ Successes

Label	取樣數	平均值	中間值	90% Line	95% Line	99% Line	最小值	最大值	錯誤率	處理量	每秒仟位...	Sent KB/s...
http://eoc...	600	3470	3970	6113	6699	8056	22	8164	0.00%	35.4/sec	11.28	0.00
http://eoc...	600	12292	13446	15884	16470	17274	100	18757	0.00%	18.0/sec	658.11	0.00
	6000	0	0	0	0	0	0	0	100.00%	∞/sec	0.00	0.00
http://eoc...	600	15291	14322	21565	28276	35181	2416	38318	0.00%	14.1/sec	1720.96	0.00
http://eoc...	1200	27165	7119	71702	79666	100579	318	106216	1.50%	2.2/sec	0.50	0.00
http://eoc...	1200	33793	7178	75247	170767	171594	118	172090	0.00%	4.2/sec	6.94	0.00
http://eoc...	600	12004	12728	17197	17721	18269	2147	18564	0.00%	10.7/sec	48.77	0.00
http://eoc...	1200	78385	54784	159228	168028	182923	2859	196833	0.75%	2.1/sec	29.89	0.00
http://eoc...	1200	86492	81400	142255	161177	203591	3582	223692	100.00%	2.0/sec	6.76	0.00
總計	13200	22487	2871	77074	135079	170790	0	223692	54.75%	.0/hour	0.00	0.00

模擬 600 人同時上線回應時間 22 秒


Test Plan
Thread Group
HTTP Cookie Manager
User Defined Variables
HTTP Header Manager
Step 1
彙整報告
檢視結果樹
檢視表格式結果
產生總計結果
結果圖形
工作台
彙整報告
將全部資料寫
瀏覽...
Log/Display Only:
設定
30秒

名稱 彙整報告

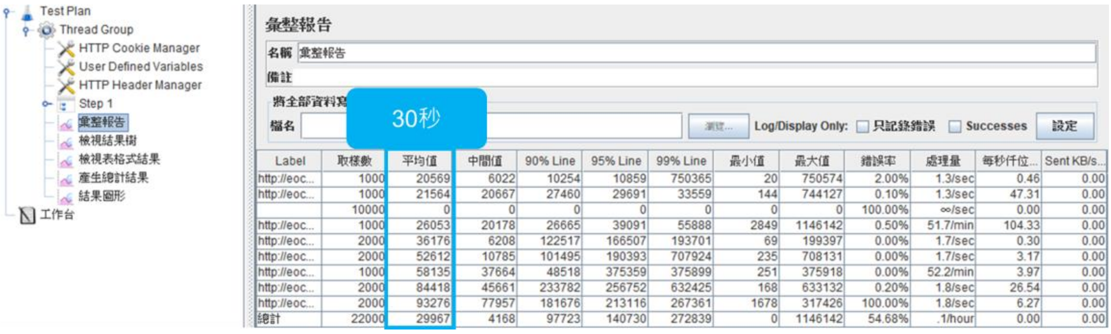
備註

檔名

☐ 只記錄錯誤 ☐ Successes

Label	取樣數	平均值	中間值	90% Line	95% Line	99% Line	最小值	最大值	錯誤率	處理量	每秒仟位...	Sent KB/s...
http://eoc...	1000	20569	6022	10254	10859	750365	20	750574	2.00%	1.3/sec	0.46	0.00
http://eoc...	1000	21564	20667	27460	29691	33559	144	744127	0.10%	1.3/sec	47.31	0.00
	10000	0	0	0	0	0	0	0	100.00%	∞/sec	0.00	0.00
http://eoc...	1000	26053	20178	26665	39091	55888	2849	1146142	0.50%	51.7/min	104.33	0.00
http://eoc...	2000	36176	6208	122517	166507	193701	69	199397	0.00%	1.7/sec	0.30	0.00
http://eoc...	2000	52612	10785	101495	190393	707924	235	708131	0.00%	1.7/sec	3.17	0.00
http://eoc...	1000	58135	37664	48518	375359	375899	251	375918	0.00%	52.2/min	3.97	0.00
http://eoc...	2000	84418	45661	233782	256752	632425	168	633132	0.20%	1.8/sec	26.54	0.00
http://eoc...	2000	93276	77957	181676	213116	267361	1678	317426	100.00%	1.8/sec	6.27	0.00
總計	22000	29967	4168	97723	140730	272839	0	1146142	54.68%	.1/hour	0.00	0.00

模擬 600 人同時上線回應時間 22 秒


Test Plan
Thread Group
HTTP Cookie Manager
User Defined Variables
HTTP Header Manager
Step 1
彙整報告
檢視結果樹
檢視表格式結果
產生總計結果
結果圖形
工作台
彙整報告
將全部資料寫
瀏覽...
Log/Display Only:
設定
30秒

名稱 彙整報告

備註

檔名

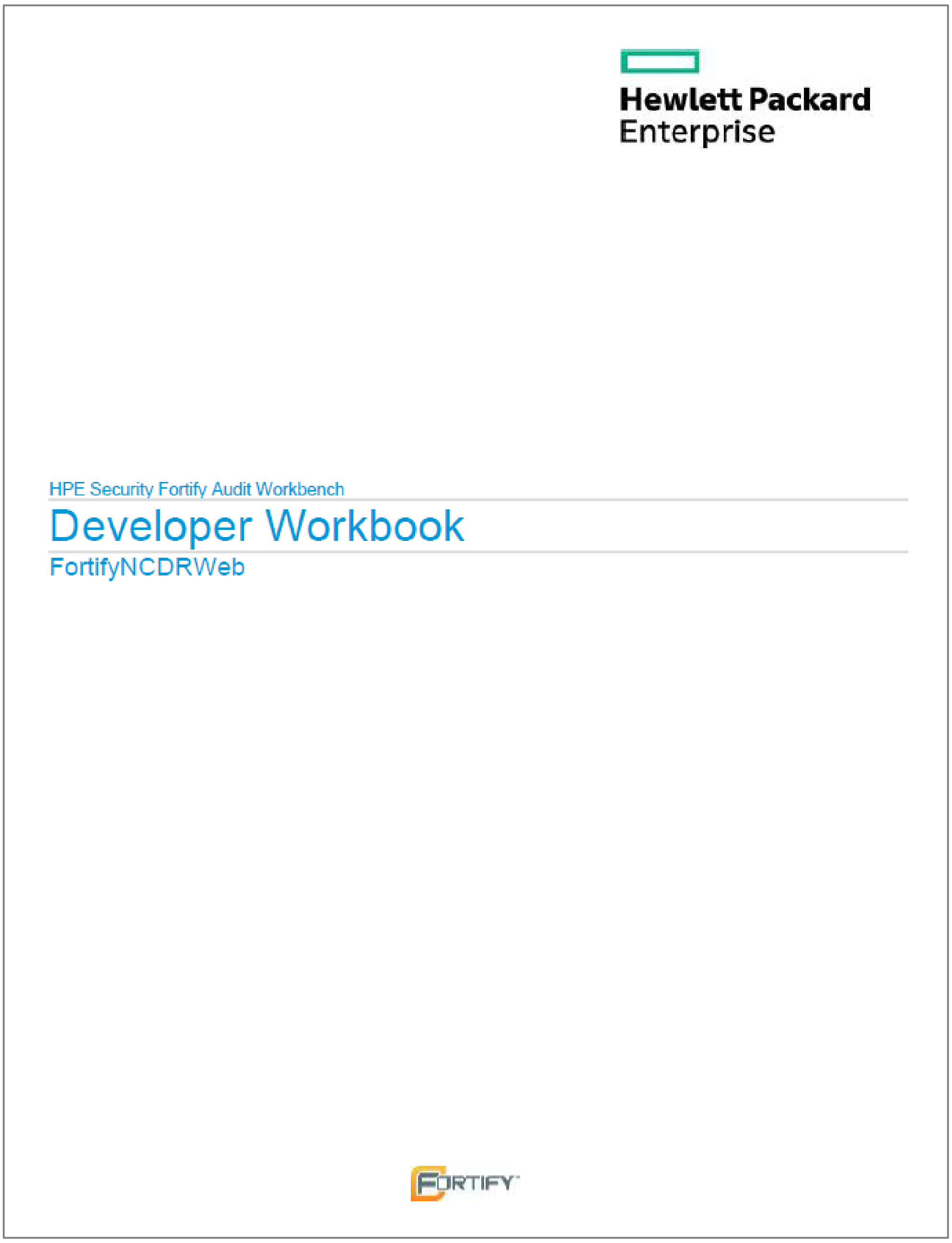
☐ 只記錄錯誤 ☐ Successes

Label	取樣數	平均值	中間值	90% Line	95% Line	99% Line	最小值	最大值	錯誤率	處理量	每秒仟位...	Sent KB/s...
http://eoc...	1000	20569	6022	10254	10859	750365	20	750574	2.00%	1.3/sec	0.46	0.00
http://eoc...	1000	21564	20667	27460	29691	33559	144	744127	0.10%	1.3/sec	47.31	0.00
	10000	0	0	0	0	0	0	0	100.00%	∞/sec	0.00	0.00
http://eoc...	1000	26053	20178	26665	39091	55888	2849	1146142	0.50%	51.7/min	104.33	0.00
http://eoc...	2000	36176	6208	122517	166507	193701	69	199397	0.00%	1.7/sec	0.30	0.00
http://eoc...	2000	52612	10785	101495	190393	707924	235	708131	0.00%	1.7/sec	3.17	0.00
http://eoc...	1000	58135	37664	48518	375359	375899	251	375918	0.00%	52.2/min	3.97	0.00
http://eoc...	2000	84418	45661	233782	256752	632425	168	633132	0.20%	1.8/sec	26.54	0.00
http://eoc...	2000	93276	77957	181676	213116	267361	1678	317426	100.00%	1.8/sec	6.27	0.00
總計	22000	29967	4168	97723	140730	272839	0	1146142	54.68%	.1/hour	0.00	0.00

模擬 1,000 人同時上線回應時間 30 秒

D.程式碼檢測

本次掃描使用 **HPE Security Fortify 軟體**，於 107 年 10 月 5 日完成檢測，輻射災害情資模組無中、高以上風險。惟此項文件，本中心列為機密等級，完整報告不對外公開。



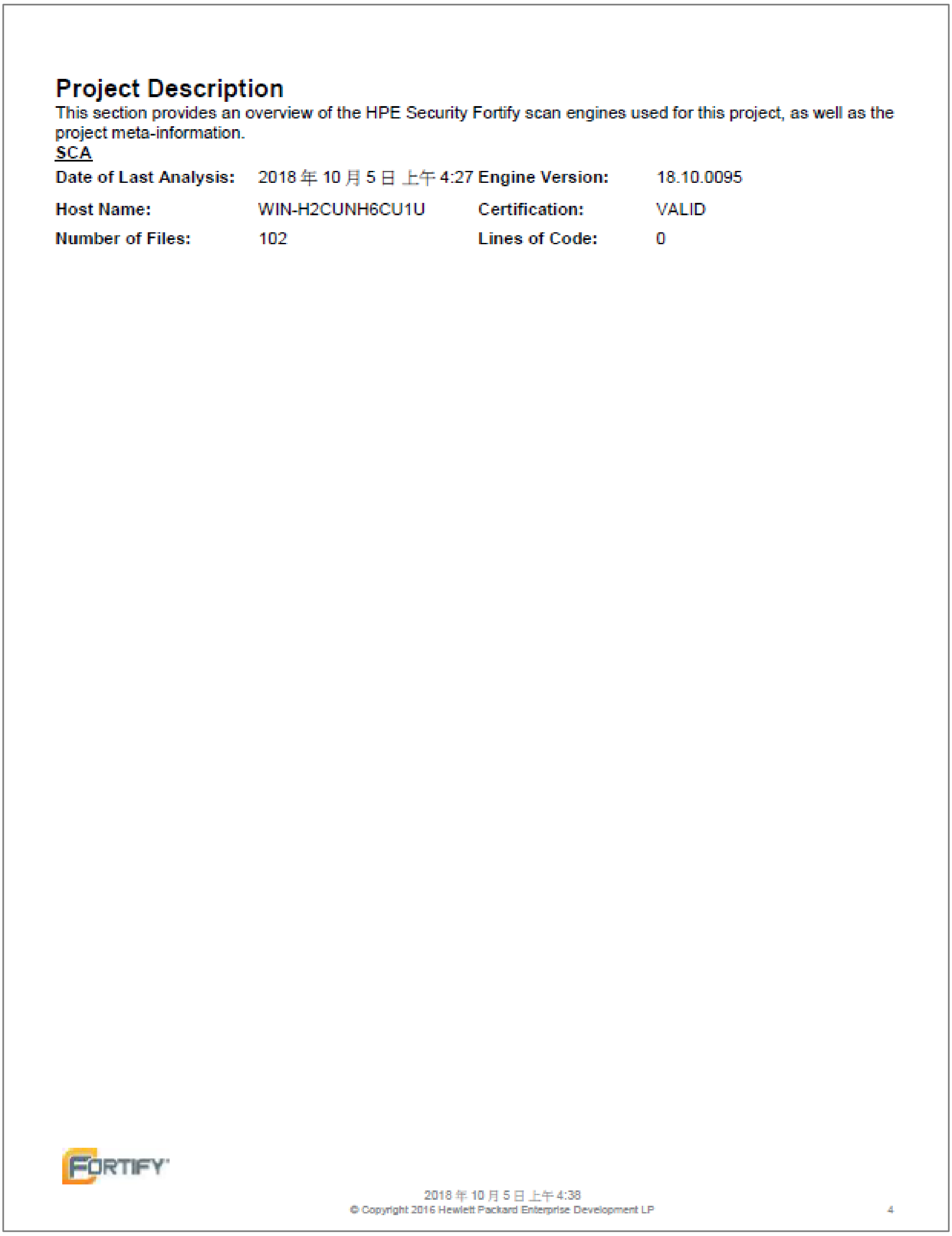
Hewlett Packard
Enterprise

HPE Security Fortify Audit Workbench

Developer Workbook

FortifyNCDRWeb

FORTIFY



Project Description

This section provides an overview of the HPE Security Fortify scan engines used for this project, as well as the project meta-information.

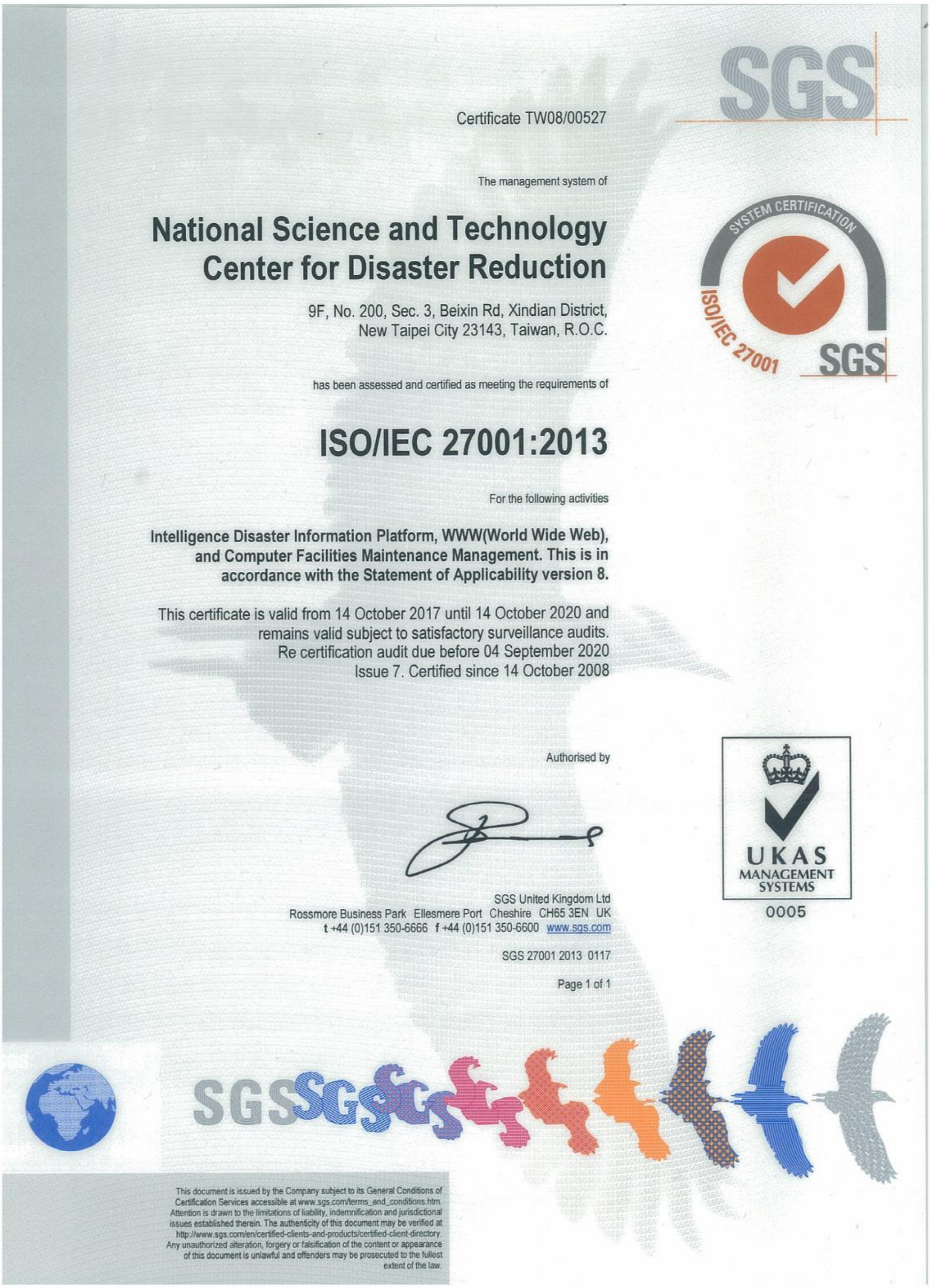
SCA

Date of Last Analysis:	2018年10月5日 上午4:27	**Engine Version:**	18.10.0095
Host Name:	WIN-H2CUNH6CU1U	**Certification:**	VALID
Number of Files:	102	**Lines of Code:**	0

2018年10月5日 上午4:38

© Copyright 2016 Hewlett Packard Enterprise Development LP

E.ISO27001



Certificate TW08/00527

The management system of

National Science and Technology Center for Disaster Reduction

9F, No. 200, Sec. 3, Beixin Rd, Xindian District,
New Taipei City 23143, Taiwan, R.O.C.

has been assessed and certified as meeting the requirements of

ISO/IEC 27001:2013

For the following activities

Intelligence Disaster Information Platform, WWW(World Wide Web), and Computer Facilities Maintenance Management. This is in accordance with the Statement of Applicability version 8.

This certificate is valid from 14 October 2017 until 14 October 2020 and remains valid subject to satisfactory surveillance audits.
Re certification audit due before 04 September 2020
Issue 7. Certified since 14 October 2008

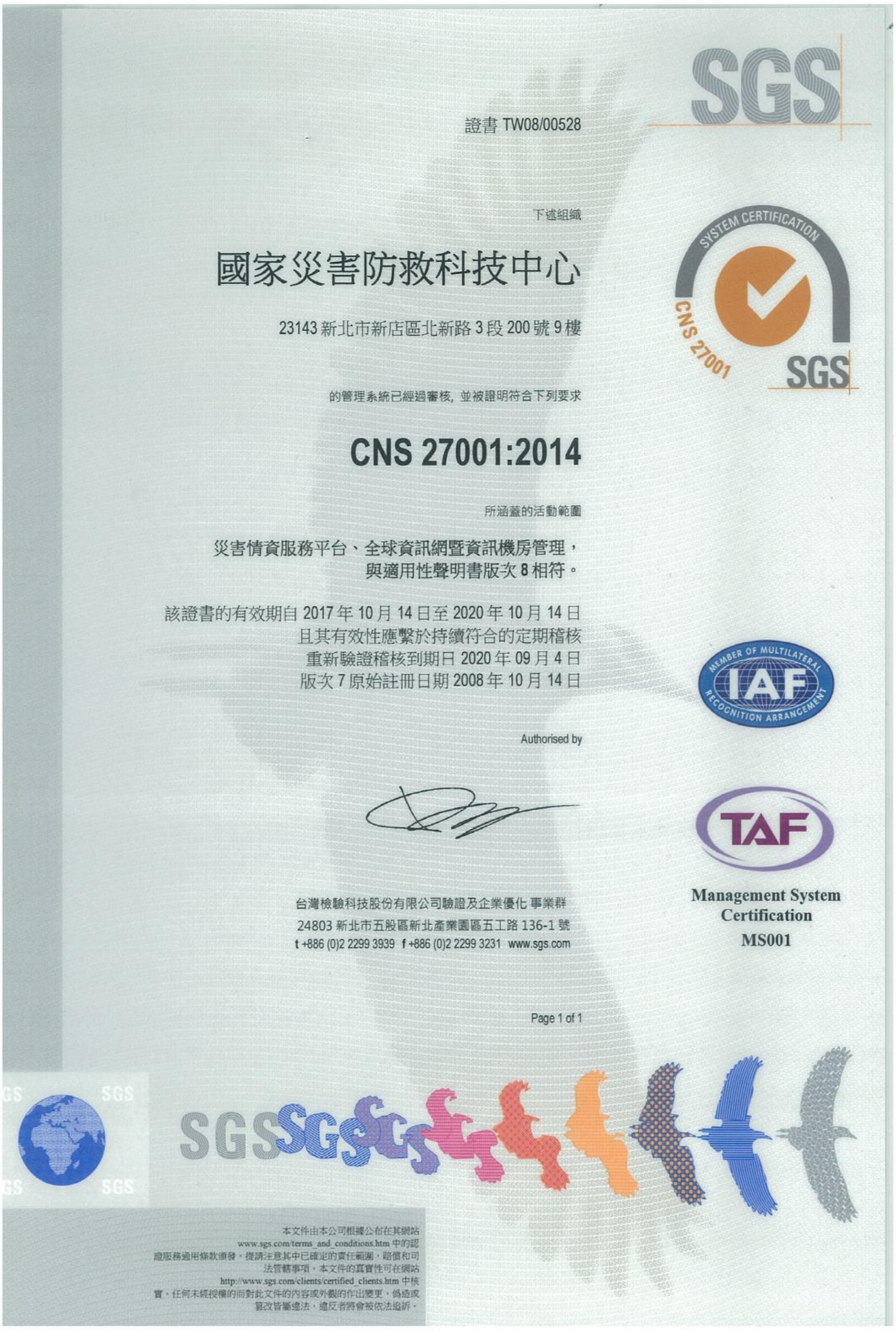
Authorised by

SGS United Kingdom Ltd
Rossmore Business Park Ellesmere Port Cheshire CH65 3EN UK
t +44 (0)151 350-6666 f +44 (0)151 350-6600 www.sgs.com

SGS 27001 2013 0117

Page 1 of 1

This document is issued by the Company subject to its General Conditions of Certification Services accessible at www.sgs.com/terms_and_conditions.htm. Attention is drawn to the limitations of liability, indemnification and jurisdictional issues established therein. The authenticity of this document may be verified at http://www.sgs.com/en/certified-clients-and-products/certified-client-directory. Any unauthorized alteration, forgery or falsification of the content or appearance of this document is unlawful and offenders may be prosecuted to the fullest extent of the law.



SGS

證書 TW08/00528

下述組織

國家災害防救科技中心

23143 新北市新店區北新路 3 段 200 號 9 樓

的管理系統已經過審核，並被證明符合下列要求

CNS 27001:2014

所涵蓋的活動範圍

**災害情資服務平台、全球資訊網暨資訊機房管理，
與適用性聲明書版次 8 相符。**

該證書的有效期自 2017 年 10 月 14 日至 2020 年 10 月 14 日
且其有效性應繫於持續符合的定期稽核
重新驗證稽核到期日 2020 年 09 月 4 日
版次 7 原始註冊日期 2008 年 10 月 14 日

Authorised by

台灣檢驗科技股份有限公司驗證及企業優化 事業群
24803 新北市五股區新北產業園區五工路 136-1 號
t +886 (0)2 2299 3939 f +886 (0)2 2299 3231 www.sgs.com

Page 1 of 1

SYSTEM CERTIFICATION
CNS 27001
SGS

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT
IAF

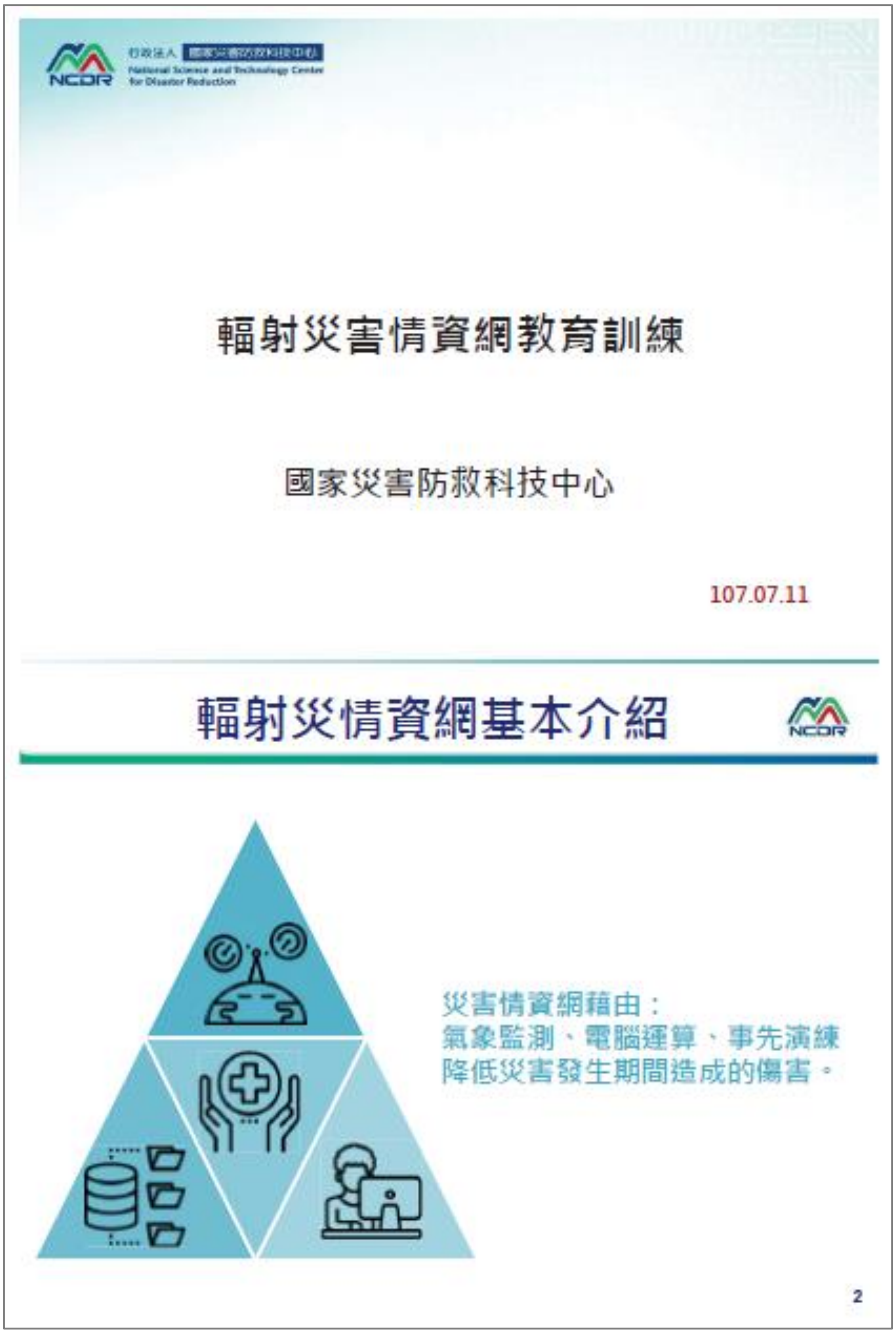
TAF
Management System
Certification
MS001

本文件由本公司根據公佈在其網站 www.sgs.com/terms_and_conditions.htm 中的認證服務適用條款頒發，提請注意其中已確定的責任範圍，賠償和司法管轄事項。本文件的真實性可在網站 http://www.sgs.com/clients/certified_clients.htm 中核實。任何未經授權的而對此文件的內容或外觀的作出變更、偽造或篡改皆屬違法，違反者將會被依法追訴。

附錄二、教育訓練

三、　時間：107年7月11日 14:00-17:00

四、　地點：行政院原子能委員會(新北市永和區成功路一段80號)



行政法人 國家災害防救科技中心
National Science and Technology Center for Disaster Reduction

輻射災害情資網教育訓練

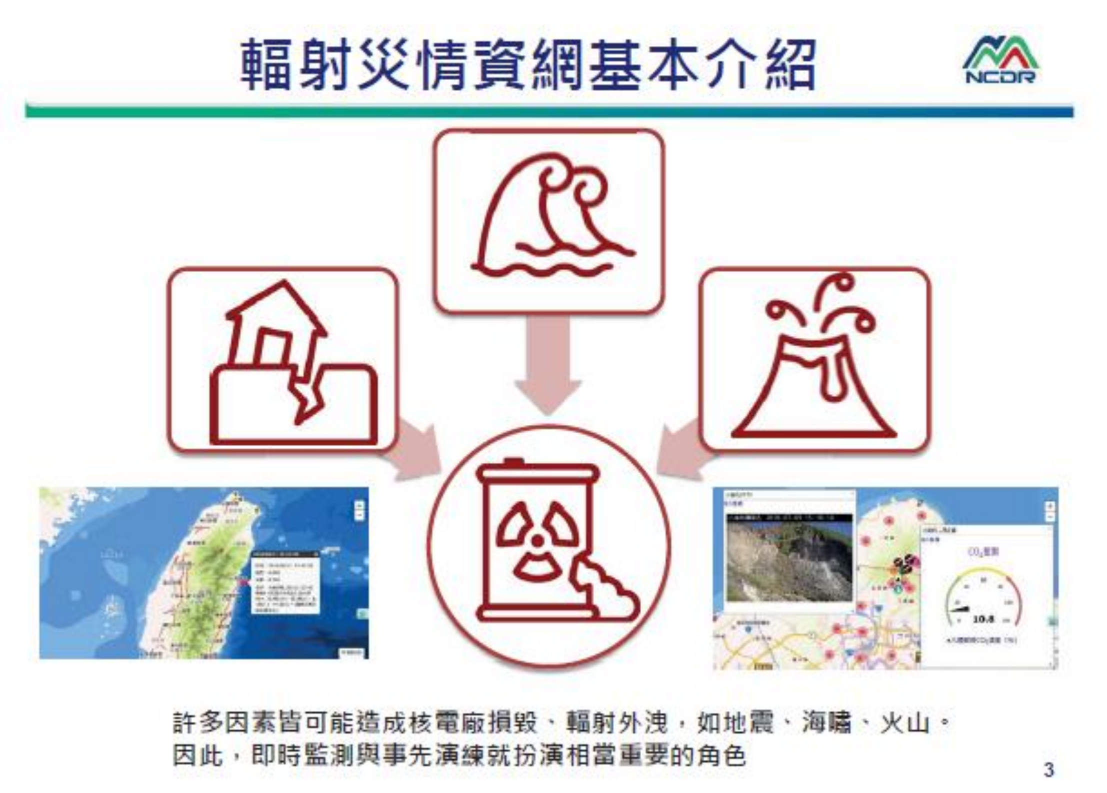
國家災害防救科技中心

107.07.11

輻射災情資網基本介紹

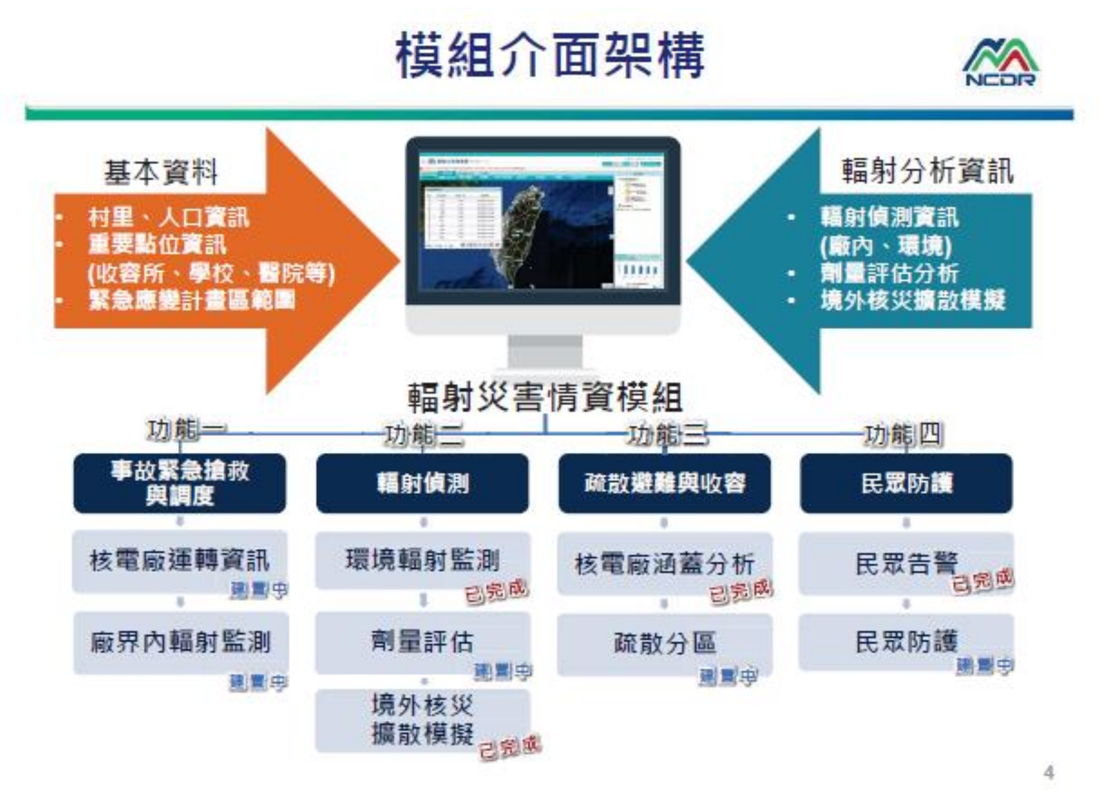
災害情資網藉由：
氣象監測、電腦運算、事先演練
降低災害發生期間造成的傷害。

2



輻射災情資網基本介紹

許多因素皆可能造成核電廠損毀、輻射外洩，如地震、海嘯、火山。
因此，即時監測與事先演練就扮演相當重要的角色



模組介面架構

基本資料

- 村里、人口資訊
- 重要點位資訊
(收容所、學校、醫院等)
- 緊急應變計畫區範圍

輻射分析資訊

- 輻射偵測資訊
(廠內、環境)
- 劑量評估分析
- 境外核災擴散模擬

輻射災害情資模組

功能一

事故緊急搶救與調度

- 核電廠運轉資訊 規劃中
- 廠界內輻射監測 規劃中

功能二

輻射偵測

- 環境輻射監測 已完成
- 劑量評估 規劃中
- 境外核災擴散模擬 已完成

功能三

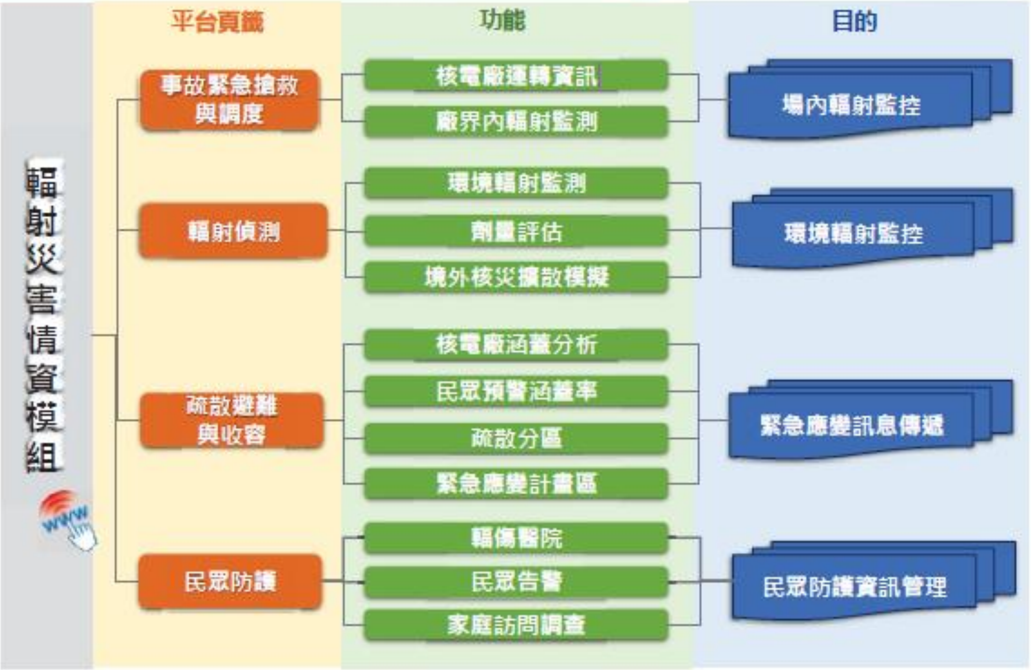
疏散避難與收容

- 核電廠涵蓋分析 已完成
- 疏散分區 規劃中

功能四

民眾防護

- 民眾告警 已完成
- 民眾防護 規劃中



平台貢獻 | 功能 | 目的

輻射災害情資模組

- 事故緊急搶救與調度
  - 核電廠運轉資訊
  - 廠界內輻射監測
  - → 場內輻射監控
- 輻射偵測
  - 環境輻射監測
  - 劑量評估
  - 境外核災擴散模擬
  - → 環境輻射監控
- 疏散避難與收容
  - 核電廠涵蓋分析
  - 民眾預警涵蓋率
  - 疏散分區
  - 緊急應變計畫區
  - → 緊急應變訊息傳遞
- 民眾防護
  - 輻傷醫院
  - 民眾告警
  - 家庭訪問調查
  - → 民眾防護資訊管理

功能一：事故緊急搶救與調度

功能

- 核電廠災害狀況研判
- 提供應變計劃決策情資

資訊綜覽

- 核電廠即時資訊：運轉資訊、廠界內輻射監測
- 災害資訊(民生資訊:電力、供水、道路資訊；颱風情資:綜合研判指標；地震情資；本日情勢(即時):火山監測、火山監測綜合指標)

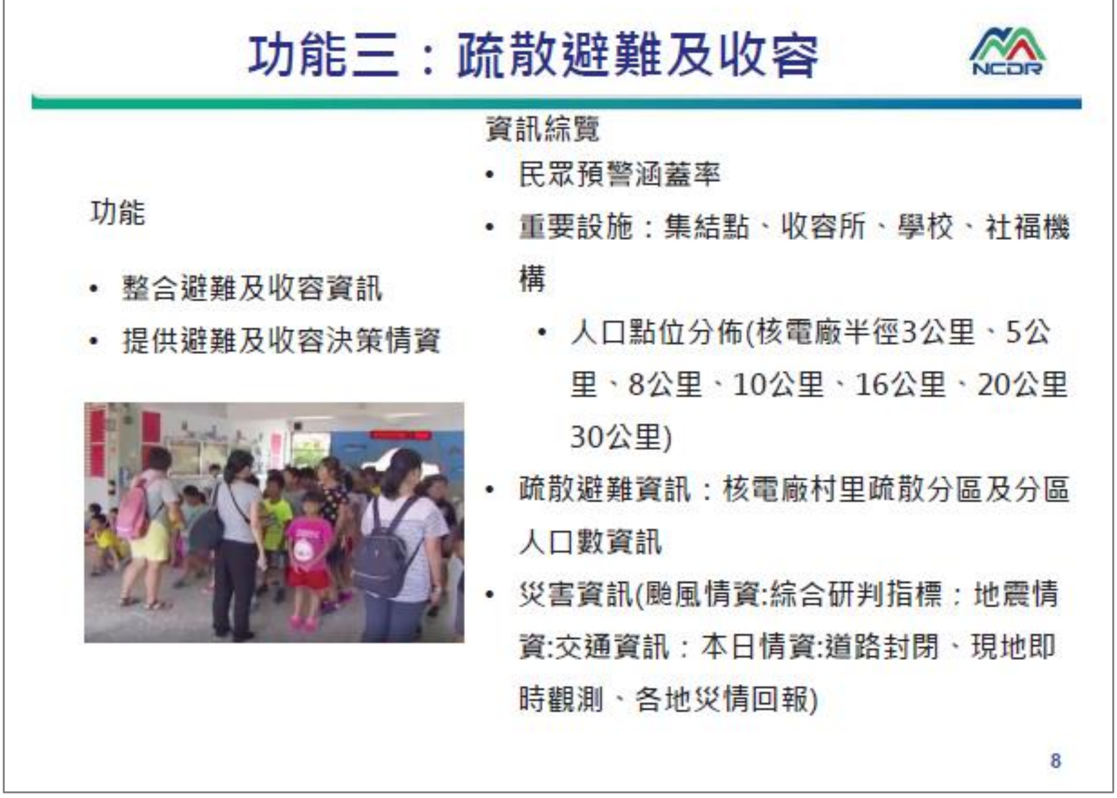
功能二：輻射偵測

功能

- 整合環境輻射監測資訊
- 放射性物質擴散範圍推估

資訊綜覽

- 環境輻射監測
- 劑量評估系統分析
  - 重要基礎設施：油(加油站)、氣(天然氣儲存槽)、水(自來水廠、淨水場、水庫)、電(變電站)消防局圖資
- 境外核災擴散模擬
- 災害資訊(颱風情資:動態大氣觀測資訊、風速觀測、綜合研判指標：地震情資：本日情勢(即時):災害情勢、示警燈號、火山監測綜合指標)



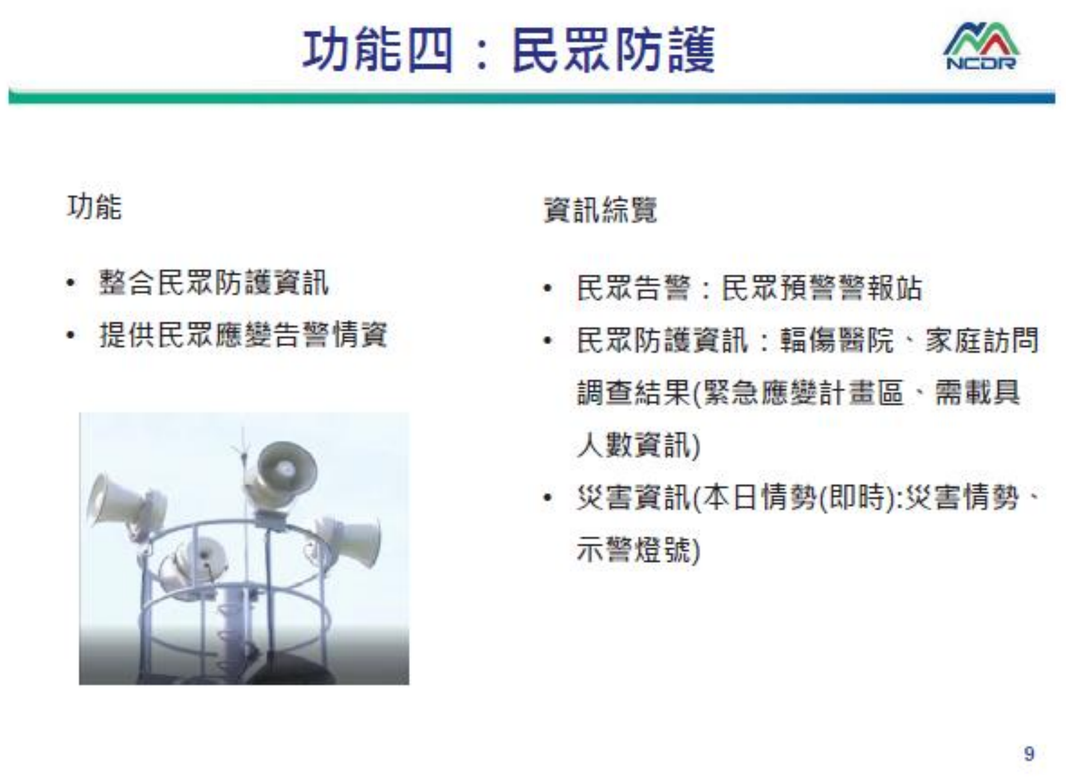
功能三：疏散避難及收容

功能

- 整合避難及收容資訊
- 提供避難及收容決策情資

資訊綜覽

- 民眾預警涵蓋率
- 重要設施：集結點、收容所、學校、社福機構
  - 人口點位分佈(核電廠半徑3公里、5公里、8公里、10公里、16公里、20公里30公里)
- 疏散避難資訊：核電廠村里疏散分區及分區人口數資訊
- 災害資訊(颱風情資:綜合研判指標：地震情資:交通資訊：本日情資:道路封閉、現地即時觀測、各地災情回報)



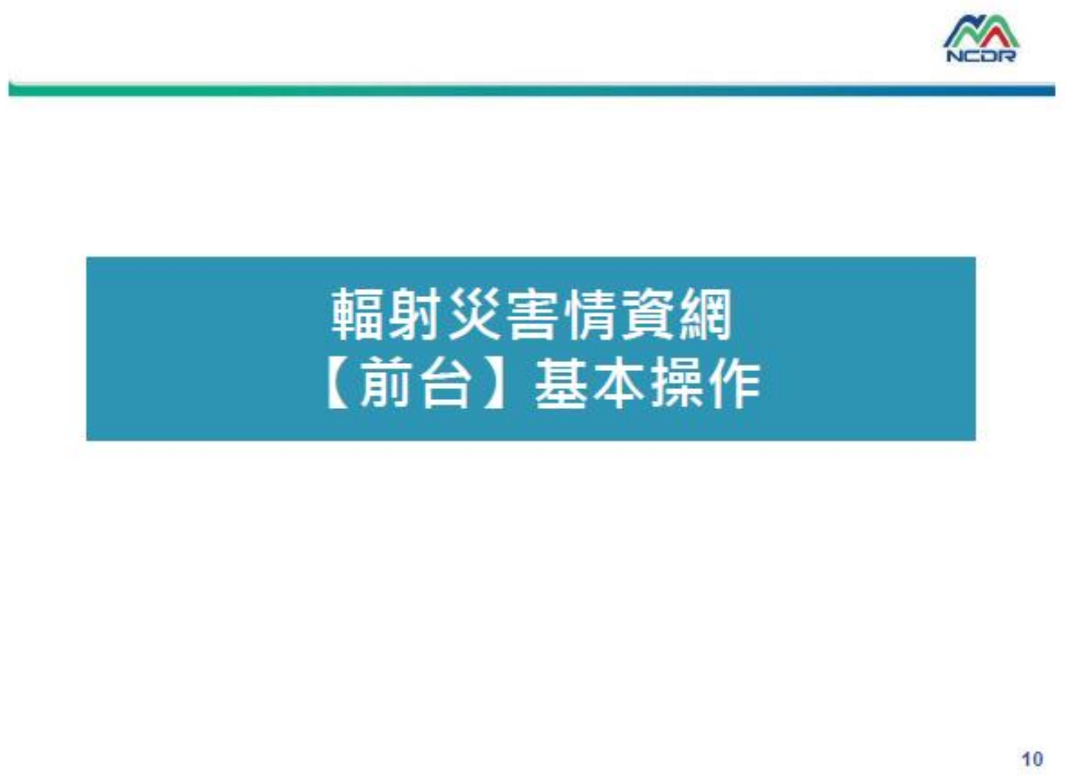
功能四：民眾防護

功能

- 整合民眾防護資訊
- 提供民眾應變告警情資

資訊綜覽

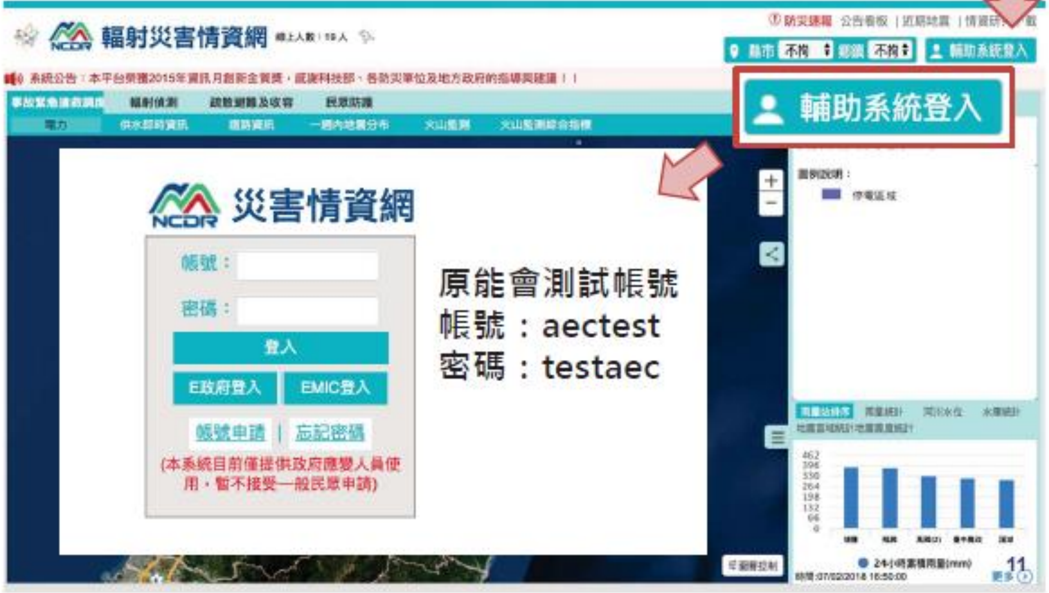
- 民眾告警：民眾預警警報站
- 民眾防護資訊：輻傷醫院、家庭訪問調查結果(緊急應變計畫區、需載具人數資訊)
- 災害資訊(本日情勢(即時):災害情勢、示警燈號)



輻射災害情資網
【前台】基本操作

【前台】輻射災情資網基本操作

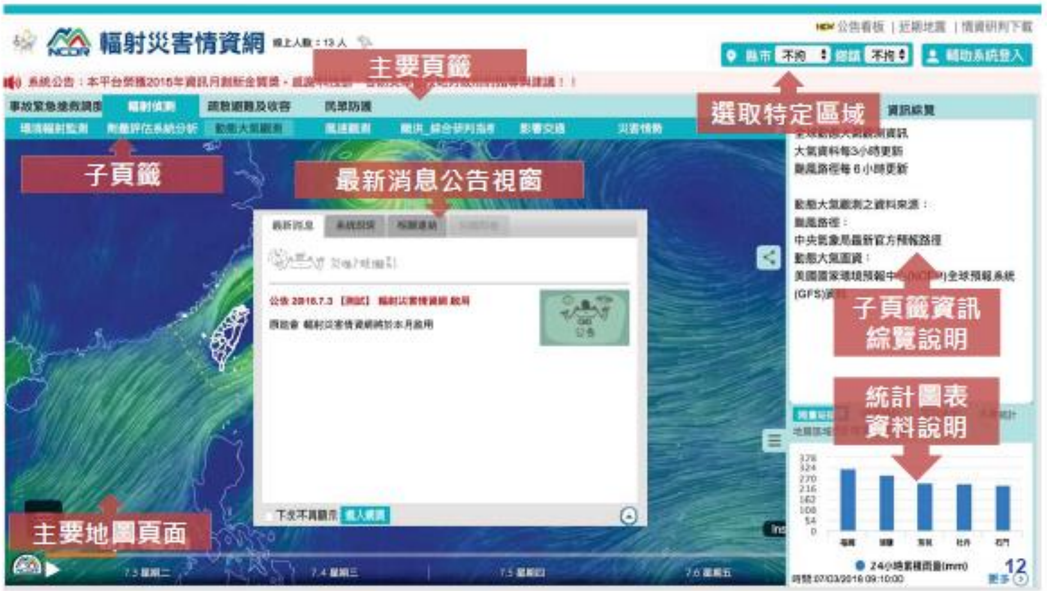
- 系統登入操作 http://eocdss.ncdr.nat.gov.tw/web/ot/AEC


輻射災害情資網
防災講堂 公告看板 | 近期地震 | 情資研判下載
縣市 不拘 鄉鎮 不拘
輔助系統登入
系統公告：本平台榮獲2015年資訊月創新金質獎，感謝科技部、各防災單位及地方政府的指導與建議！！
事故緊急應變調度
輻射偵測
疏散避難及收容
民眾防護
電力
供水即時資訊
道路資訊
一週內地震分布
火山監測
火山監測綜合指標
輔助系統登入
災害情資網
帳號：
密碼：
登入
E政府登入
EMIC登入
帳號申請 | 忘記密碼
(本系統目前僅提供政府應變人員使用，暫不接受一般民眾申請)
圖例說明：
停電區域
24小時累積雨量(mm)
11
更多

原能會測試帳號
帳號：aectest
密碼：testaec

【前台】輻射災情資網基本操作

- 網頁頁面基本說明


輻射災害情資網
公告看板 | 近期地震 | 情資研判下載
縣市 不拘 鄉鎮 不拘
輔助系統登入
系統公告：本平台榮獲2015年資訊月創新金質獎
事故緊急應變調度
輻射偵測
疏散避難及收容
民眾防護
環境輻射監測
劑量評估系統分析
動態大氣觀測
風速觀測
颱洪_綜合研判指標
影響交通
災害情勢
資訊綜覽
大氣資料每3小時更新
颱風路徑每6小時更新
動態大氣觀測之資料來源：
颱風路徑：
中央氣象局最新官方預報路徑
最新消息
系統說明
相關連結
下次不再顯示
24小時累積雨量(mm)
12
更多

主要頁籤

選取特定區域

子頁籤

最新消息公告視窗

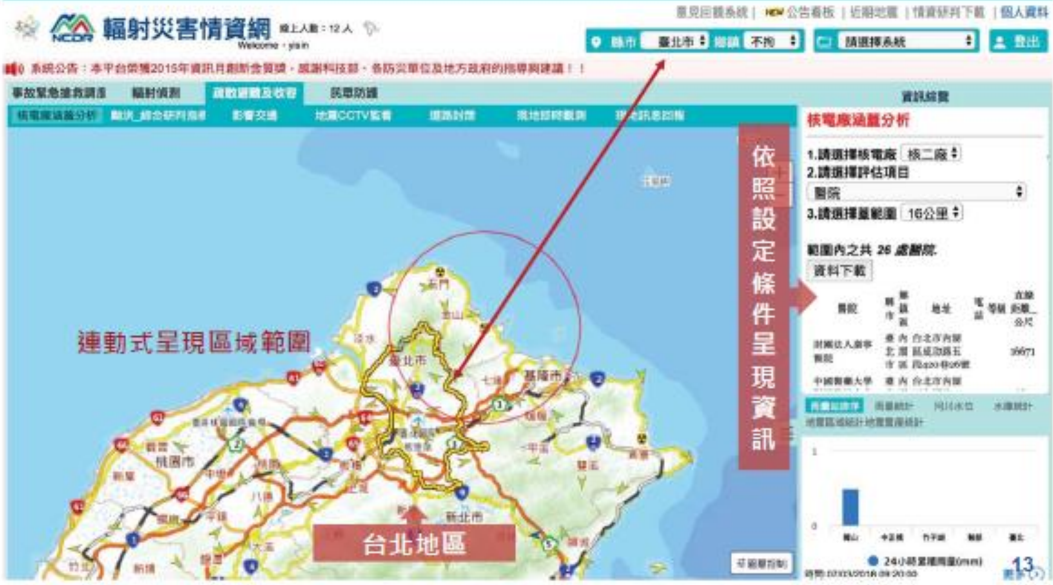
子頁籤資訊綜覽說明

統計圖表資料說明

主要地圖頁面

【前台】輻射災情資網基本操作

- 網頁頁面基本說明

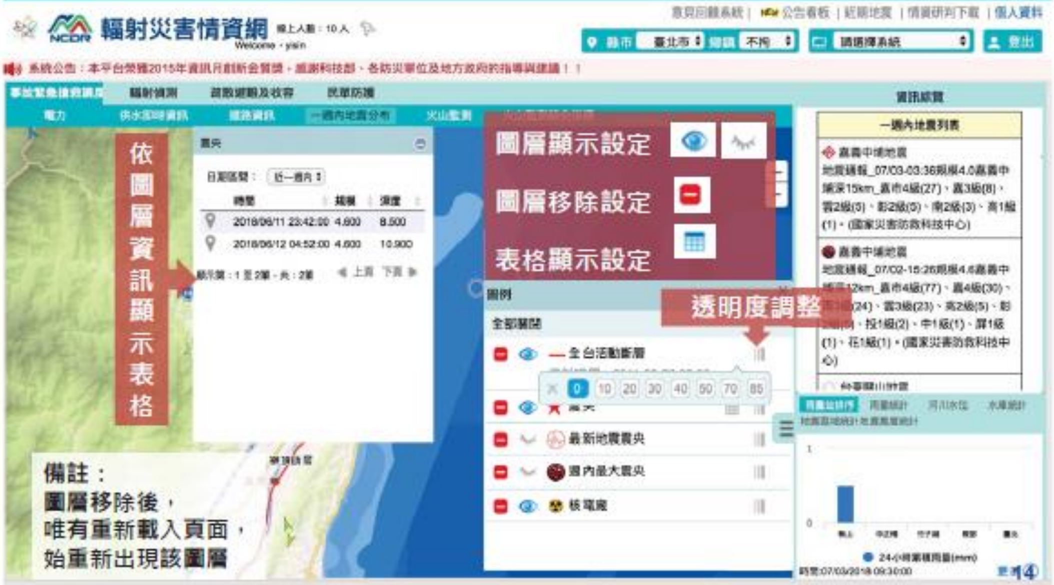

輻射災害情資網
意見回饋系統 | 公告看板 | 近期地震 | 情資研判下載 | 個人資料
縣市 臺北市 鄉鎮 不拘
請選擇系統
登出
資訊綜覽
核電廠涵蓋分析
1.請選擇核電廠 核二廠
2.請選擇評估項目
醫院
3.請選擇量範圍 16公里
範圍內之共 26 處醫院
資料下載
臺北市
基隆市
桃園市
新北市
24小時累積雨量(mm)

依照設定條件呈現資訊

連動式呈現區域範圍

台北地區

【前台】輻射災情資網基本操作


輻射災害情資網
意見回饋系統 | 公告看板 | 近期地震 | 情資研判下載 | 個人資料
縣市 臺北市 鄉鎮 不拘
請選擇系統
登出
資訊綜覽
一週內地震列表
嘉義中埔地震
圖例
全部圖層
全台活動斷層
最新地震震央
週內最大震央
核電廠
0 10 20 30 40 50 70 85
24小時累積雨量(mm)

依圖層資訊顯示表格

圖層顯示設定

圖層移除設定

表格顯示設定

透明度調整

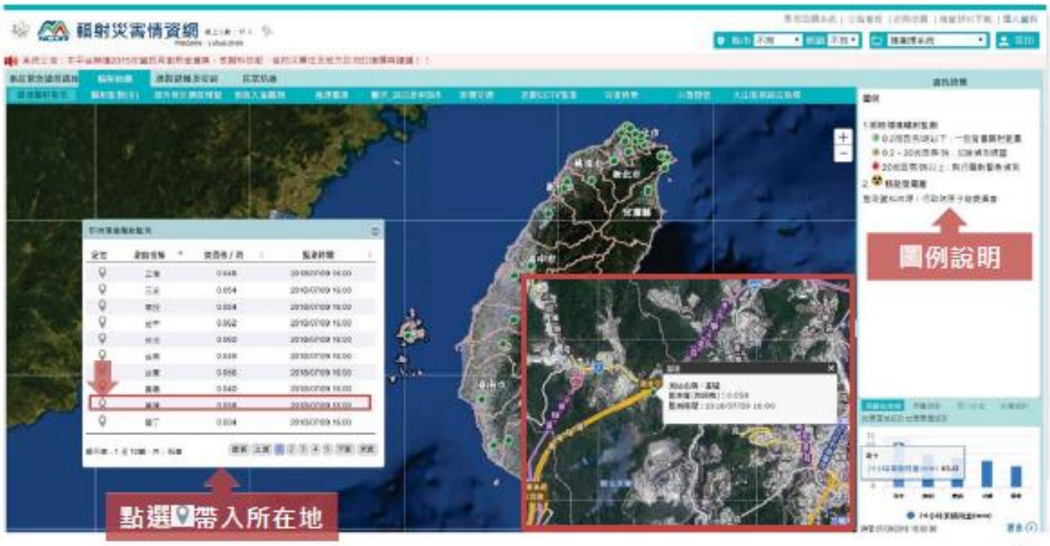
備註：
圖層移除後，
唯有重新載入頁面，
始重新出現該圖層

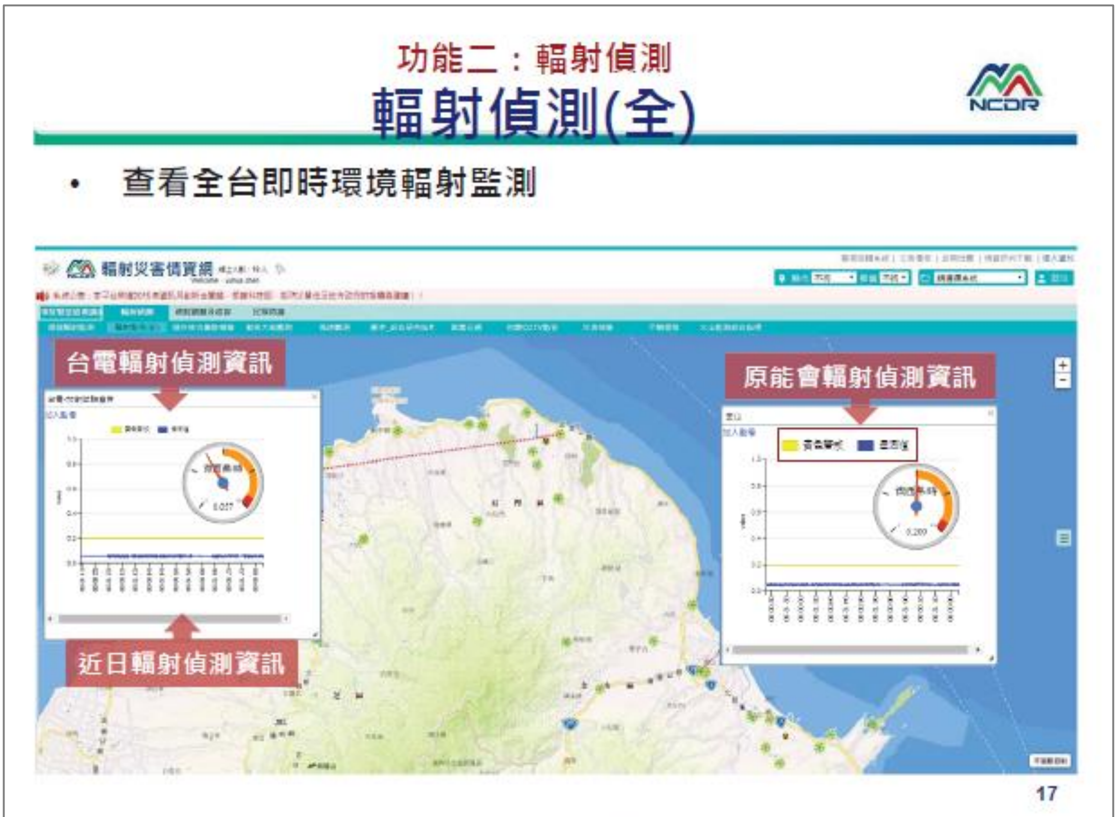
輻射災害情資網
【前台】基本介紹

功能二：輻射偵測

輻射偵測

- 查看全台即時環境輻射監測

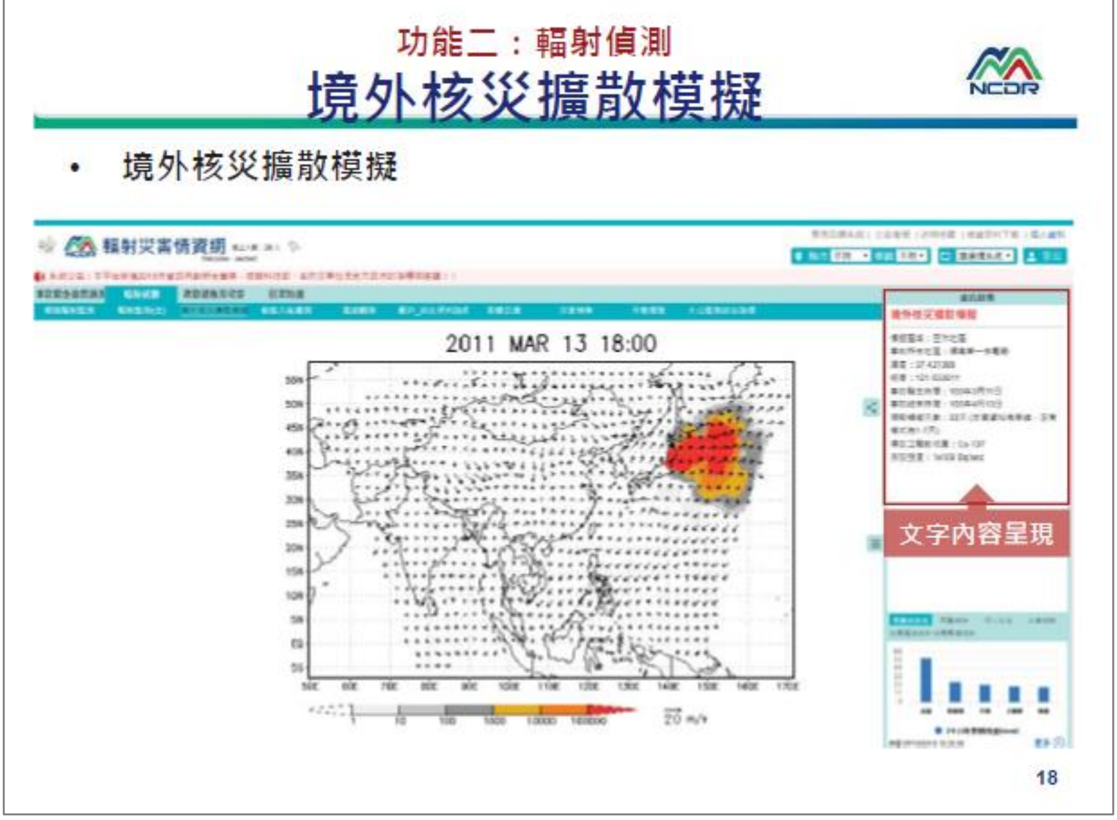

輻射災害情資網
圖例說明
點選📍帶入所在地



功能二：輻射偵測
輻射偵測(全)

- 查看全台即時環境輻射監測

NCDR
輻射災害情資網
台電輻射偵測資訊
原能會輻射偵測資訊
近日輻射偵測資訊



功能二：輻射偵測
境外核災擴散模擬

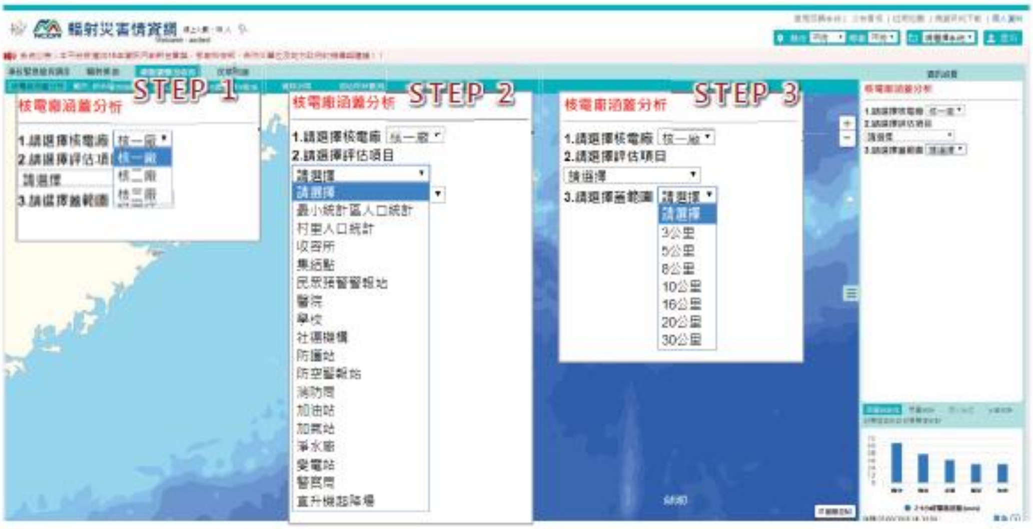
- 境外核災擴散模擬

NCDR
輻射災害情資網
2011 MAR 13 18:00
20 m/s
文字內容呈現

功能三：疏散避難及收容

核電廠涵蓋分析

- 評估項目選取



輻射災害情資網

STEP 1

核電廠涵蓋分析

1.請選擇核電廠 核一廠

2.請選擇評估項目

請選擇

3.請選擇蓋範圍

核一廠
核二廠
核三廠

STEP 2

核電廠涵蓋分析

1.請選擇核電廠 核一廠

2.請選擇評估項目

請選擇

請選擇
最小統計區人口統計
村里人口統計
收容所
集結點
民眾預警警報站
醫院
學校
社福機構
防護站
防空警報站
消防局
加油站
加氣站
淨水廠
變電站
警察局
直升機起降場

STEP 3

核電廠涵蓋分析

1.請選擇核電廠 核一廠

2.請選擇評估項目

請選擇

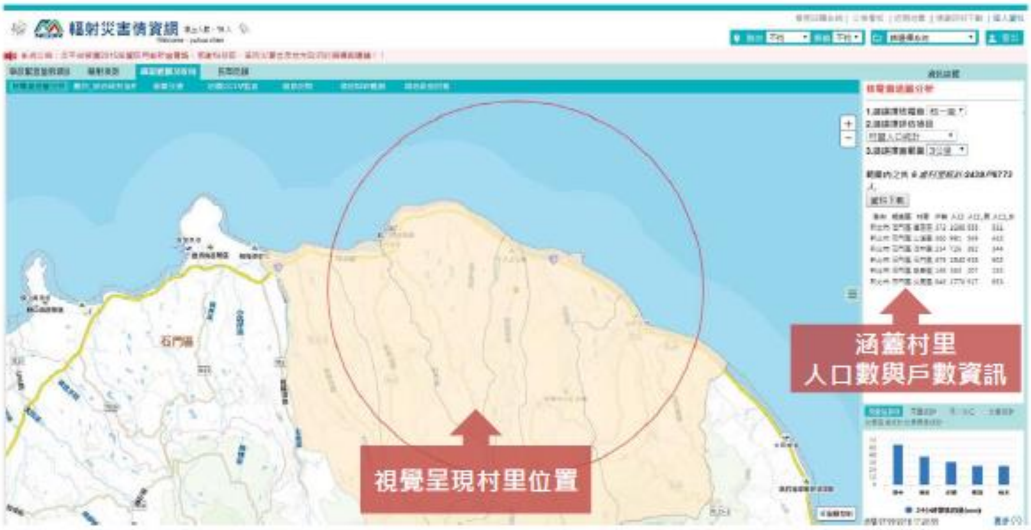
3.請選擇蓋範圍 請選擇

請選擇
3公里
5公里
8公里
10公里
16公里
20公里
30公里

功能三：疏散避難及收容

核電廠涵蓋分析

- 村里人口資訊分析



輻射災害情資網

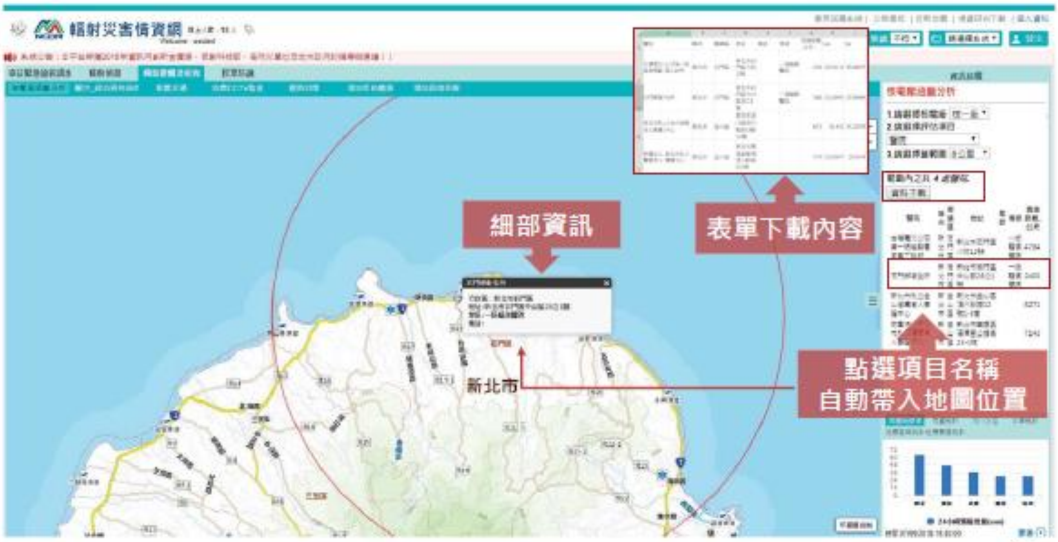
涵蓋村里
人口數與戶數資訊

視覺呈現村里位置

功能三：疏散避難及收容

核電廠涵蓋分析

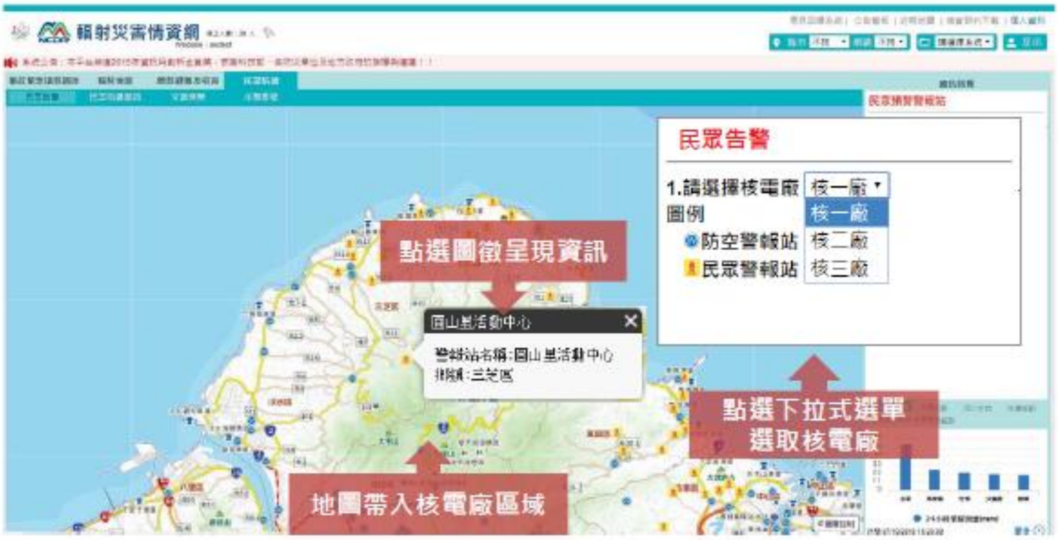
- 醫院資訊分析


輻射災害情資網
細部資訊
表單下載內容
新北市
點選項目名稱
自動帶入地圖位置

功能四：民眾防護

民眾告警

- 民眾告警資訊


輻射災害情資網
民眾告警
圖例
防空警報站
民眾警報站
核一廠
核二廠
核三廠
點選圖徵呈現資訊
點選下拉式選單
選取核電廠
地圖帶入核電廠區域

1.請選擇核電廠 核一廠

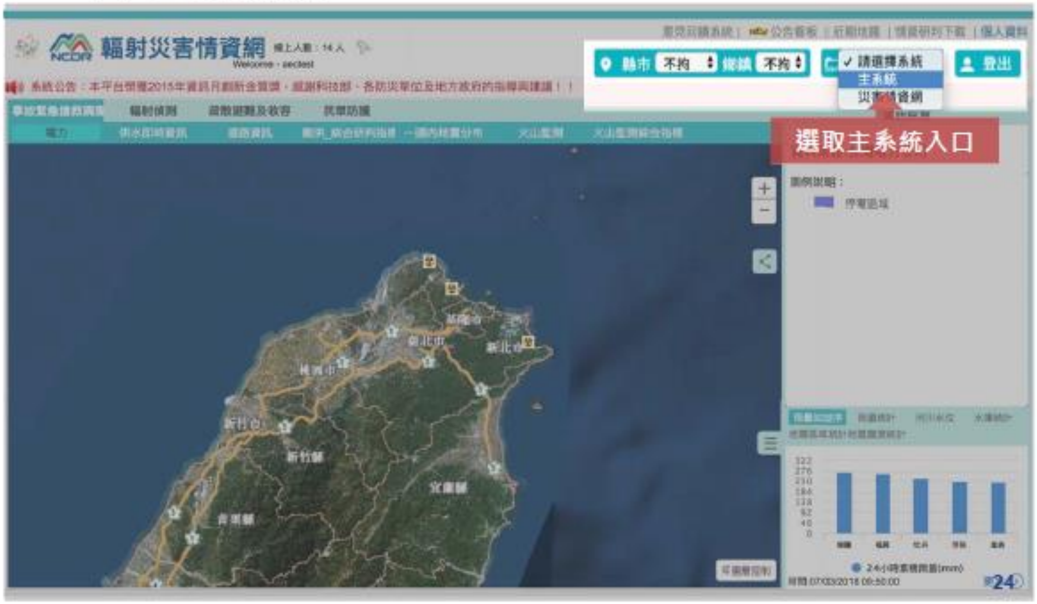
圓山里活動中心

警報站名稱:圓山里活動中心
鄉鎮:三芝區

輻射災害情資網
【主系統】基本介紹

【主系統】輻射災情資網操作

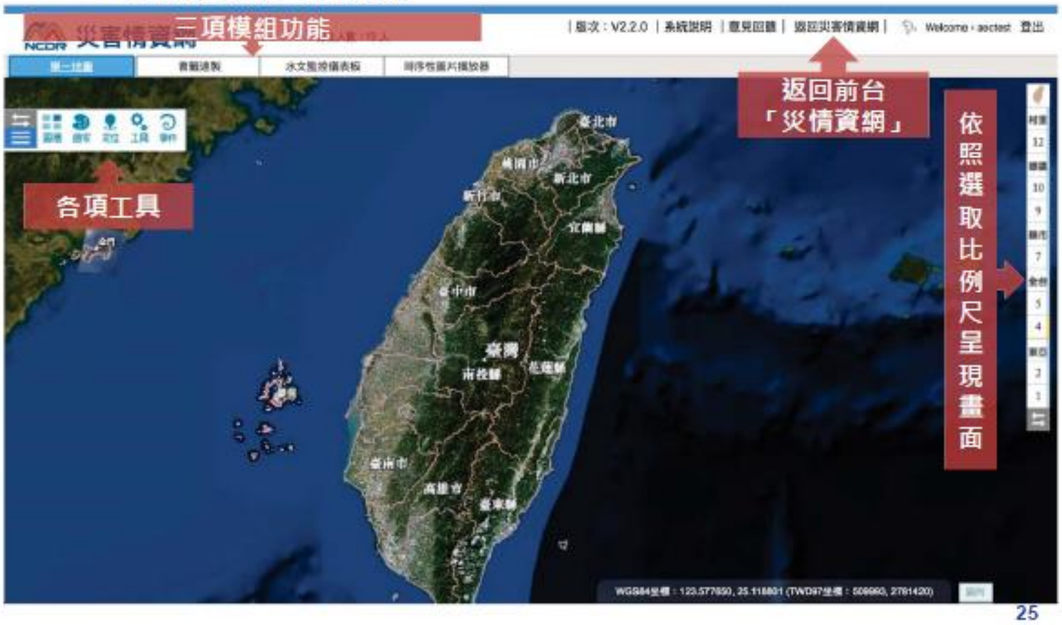
- 進入主系統說明


輻射災害情資網
Welcome
縣市
不拘
鄉鎮
不拘
✓ 請選擇系統
主系統
災害情資網
登出
+
−

選取主系統入口

【主系統】輻射災情資網操作

- 主系統頁面基本說明


災害情資網
| 版次：V2.2.0 | 系統說明 | 意見回饋 | 返回災害情資網 |
Welcome，aectest 登出
單一地圖
水文監測儀表板
時序性圖片播放器
圖層
定位
工具
事件
臺北市
桃園市
新北市
新竹市
宜蘭縣
臺中市
臺灣
南投縣
花蓮縣
臺南市
高雄市
臺東縣
WGS84坐標：123.577650, 25.118801 (TWD97坐標：509990, 2781420)

三項模組功能

返回前台
「災情資網」

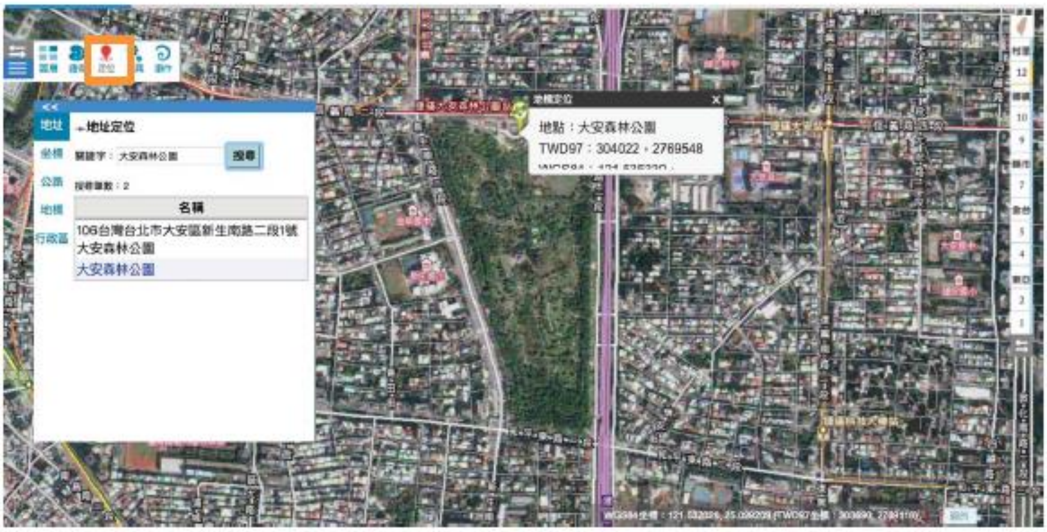
各項工具

依照選取比例尺呈現畫面

輻射災害情資網
主系統【工具列】
操作介紹

【主系統】輻射災情資網操作

- 主系統工具列「定位」操作說明


定位
<<
地址
坐標
公路
地標
行政區
地標定位
×

地址定位

關鍵字：大安森林公園 搜尋

搜尋筆數：2

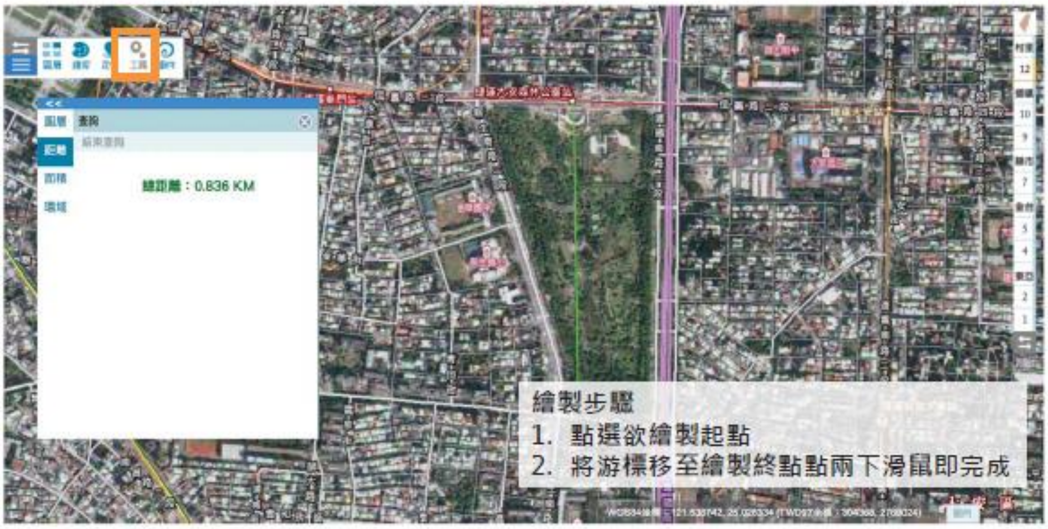
名稱
106台灣台北市大安區新生南路二段1號 大安森林公園
大安森林公園

地點：大安森林公園

TWD97：304022，2769548

【主系統】輻射災情資網操作

- 主系統工具列「工具：距離、面積」操作說明


工具
<<
圖層
距離
面積
環域

查詢

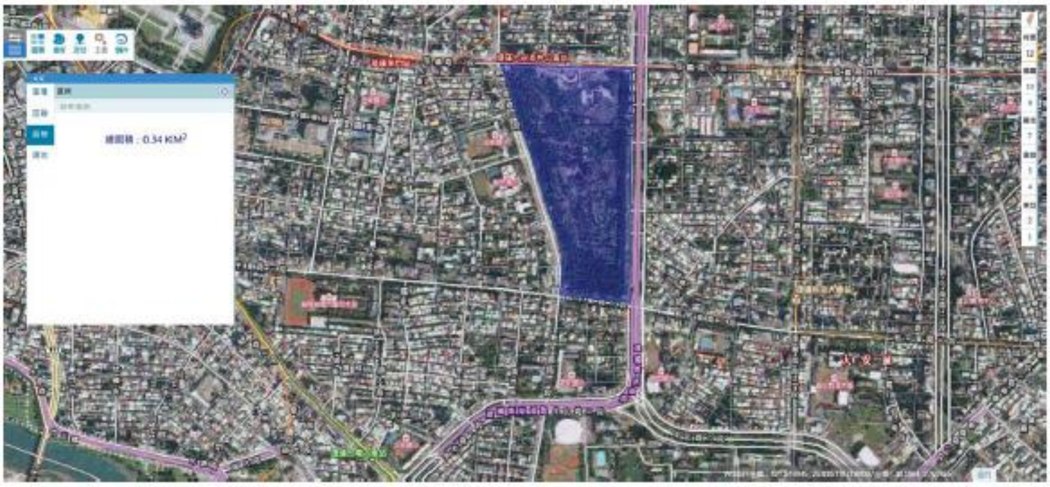
結束查詢

總距離：0.836 KM

繪製步驟
1. 點選欲繪製起點
2. 將游標移至繪製終點點兩下滑鼠即完成

【主系統】輻射災情資網操作

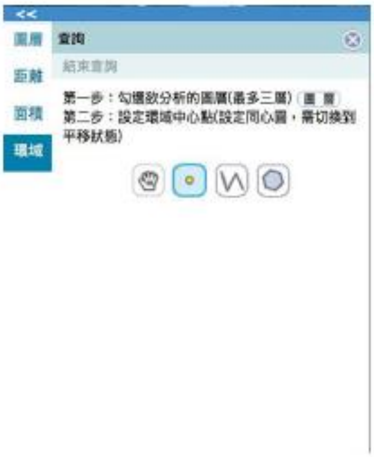
- 主系統工具列「工具：距離、面積」操作說明



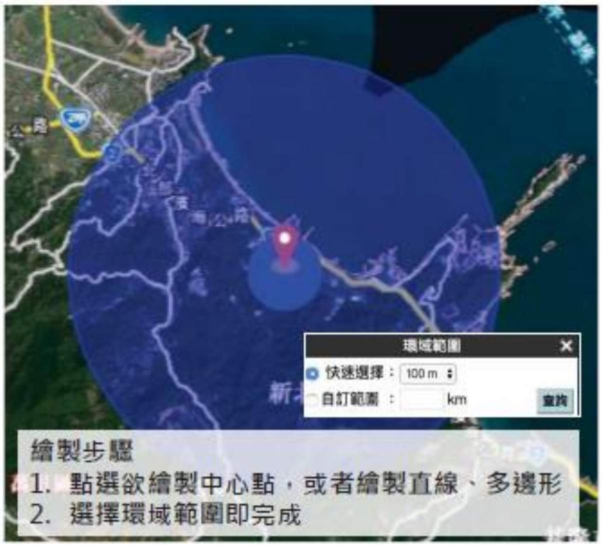
總面積：0.34 KM²

【主系統】輻射災情資網操作

- 主系統工具列「工具：環域」操作說明


<<
圖層
距離
面積
環域
查詢
結束查詢

第一步：勾選欲分析的圖層(最多三層)（重 置）
第二步：設定環域中心點(設定同心圓，需切換到平移狀態)



● 快速選擇：100 m
○ 自訂範圍：km

繪製步驟
1. 點選欲繪製中心點，或者繪製直線、多邊形
2. 選擇環域範圍即完成

NCDR
行政法人 國家災害防救科技中心
National Science and Technology Center
for Disaster Reduction

簡報結束

敬請指教

附錄三、簽訂合作備忘錄會議

本會與國家災害防救科技中心
輻射災害防救科技研發與應用合作備忘錄簽署儀式

一、時間：2018年10月31日（三）10:00-10:45

二、地點：本會 4樓會議室

三、流程：

時間	流程	備註
09:50-10:00	處長辦公室相見歡(陳主任)	其餘貴賓於會議室
10:00-10:05	本會 廖處長家群 致詞	
10:05-10:10	國家災害防救科技中心 陳主任宏宇 致詞	
10:10-10:11	雙方簽署備忘錄	
10:11-10:12	互贈紀念禮品	
10:12-10:15	大合照(於本處大門)	
10:15-10:45	參觀核安監管中心	

雙方長官簽署備忘錄合影

雙方大合照