衛生福利部
114年度資訊安全服務案
資安事件調查報告-
EEC_PD_WebShell

Jane Chang
2025/11/03

1

盡責聲明

- 本報告所使用之分析、檢測與調查之方法與技術，為當前資訊安全產業所通用之技術與工具，所有方法與技術均有其極限，也將隨科技進步而更新，本公司謹盡合理可能之最大努力，就所見所聞如實提出本報告，容或有不足之處，仍請考量當前科技所能達成之極限，予以諒解

2

2

事件起源

- 2025/10/30 安碁資訊鑑識調查部門收到衛生福利部的來信通知，說明電子病歷交換中心主機 EEC_PD 有收到防毒偵測到 WebShell 的紀錄

建案時間	2025/10/29 下午 04:18:36
問題說明	MxDR 監控觀察到主機 EEC_PD (203.65.108.116) 有觸發『[Heuristic Attribute] Backdoor File Detection」警報。 事件說明：主機偵測到一個惡意 ASP Web Shell (Backdoor.ASP.WEBSHELL.AJ)，位於 D:\EECOnline\EUSERVICE-Blank\trunk\assests\style\ 路徑下檔案名為 assest.aspx，即時掃描已將其隔離。 該主機的網頁應用程式可能已遭入侵，攻擊者試圖建立持久性後門 貴單位先行檢視事件紀錄，確認觸發主機所在網段與角色功能，並 認是否為已知行為以釐清風險。

Managed XDR Service Center

回應時間：2025/10/30 下午 05:21:25

Hi,Sir

經檢查相關路徑，這兩個檔案也有問題。

D:\EECOnline\EUSERVICE-Blank\trunk\assests\js\bootstrap.aspx

D:\EECOnline\EUSERVICE-Blank\trunk\assests\js\bootstrap.min.aspx

3

通報資訊-INC101761670538

資通安全威脅偵測管理（SOC）服務

資安警訊通報

專案名稱	衛生福利部-114 年度資訊安全服務案		
通報單號	INC101761670538	通報發布時間	114/10/29 15:50:43 GMT+8
通報類別	疑似惡意惡意程式	資安院通報類別	情資分析單（惡意程式）
通報主旨	Workbench 事件偵測(Vision One)		
風險等級	中度 Medium	偵測來源	/EDR
防毒主機	mohw_workbench	病毒名稱	0
攻擊主機		目標主機	ANCHOR1N（203.65.104.21）
現象描述	於 WorkBench mohw_workbench 設備查得偵點設備：[[203.65.104.21,10.10.10.32,203.65.108.116,203.65.108.41,10.10.10.33,10. ANCHOR1N]，事件[[Heuristic Attribute] Backdoor File Detection]，Work [https://portal.sg.xdr.trendmicro.com/index.html#/workbench/alerts/WB 202S1029-00001?ref=0c12e642ca5b7ed4436e5f23f568ae10066608d3] 的紀錄。		

assest.aspx 已於 2025/10/29 15:41 遭防毒軟體隔離

2025-10-29 15:41:45 | View event

EEC_PD

(fileHash) e489a472efcb666b40765ee73af211b5d7d3e8ac

(fullPath) D:\EECOnline\EUSERVICE-Blank\trunk\assests\style\assest.aspx

(fileName) assest.aspx

(endpointIp) 203.65.108.116

(scanType) Real-time Scan

(actResult) File quarantined

4

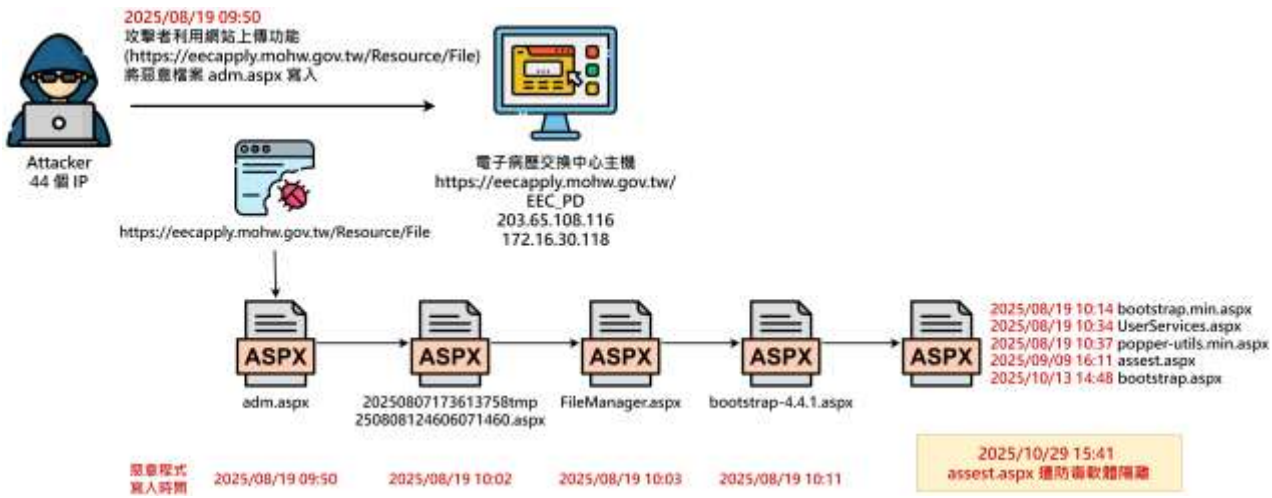
執行調查細節

- 調查時程
  - 2025/10/31 – 2025/11/03
- 分析項目
  - Windows 的 Event Log、Registry、MFT
  - XDR 紀錄、ThreatSonar APT 掃描結果分析
- 調查範圍
  - 主機 1 台，EEC_PD（203.65.108.116）
- 調查人員
  - Jane Chang
- 使用工具
  - MFTEcmd v1.3.0、Registry Explorer v1.6.0.0、NotePad++ v8.8.7、ThreatSonar 2410p3、Excel O365

5

5

攻擊示意圖



6

6

調查結果說明

- **事件根因分析**
  - **網站 https://eecapply.mohw.gov.tw/Resource/File 應有上傳檔案功能的漏洞，使攻擊者可上傳後門程式**
- **入侵攻擊手法**
  - **攻擊者利用上傳檔案功能，將後門程式寫入，又再透過自行上傳的後門程式寫入其他惡意程式**
- **攻擊時間**
  - **2025/08/19 – 2025/10/29**

7

建議

#	問題	建議
1	網站上傳功能漏洞	• 盡速修復網站漏洞，並執行滲透測試等檢測，以釐清是否有其他漏洞可遭攻擊者利用 • 針對網站上傳功能限制的修改，詳細可參考附件[防止檔案上傳攻擊]
2	主機遭寫入多個檔案至不同目錄	• 網站重新建置，以乾淨的原始碼重建網站

8

事件調查威脅指標彙總_攻擊來源

#	IP	#	IP	#	IP	#	IP
1	1.164.229.158	12	114.37.139.79	23	140.124.144.8 國立臺北科技大學	34	59.124.67.138
2	1.164.253.101	13	118.160.207.102	24	202.39.60.193	35	60.251.161.67
3	1.164.253.152	14	118.165.66.147	25	203.204.26.180	36	61.216.67.163
4	1.171.161.217	15	118.166.17.46	26	211.72.118.118	37	61.220.29.183
5	1.171.162.178	16	118.232.114.229	27	211.75.236.206	38	61.220.37.61
6	103.137.247.67	17	123.192.192.63	28	220.132.72.80	39	61.222.207.106
7	103.137.247.69	18	123.193.198.3	29	220.134.96.94	40	61.222.32.181
8	106.104.134.62	19	123.194.160.98	30	220.135.68.8	41	61.228.101.81
9	111.185.1.81	20	123.194.172.228	31	36.226.10.39	42	61.30.172.143
10	111.71.212.80	21	125.228.119.181	32	49.218.231.89	43	89.117.42.12
11	114.34.185.252	22	140.118.122.146 國立臺灣科技大學	33	59.120.10.22		**皆為 TW IP**

9

9

事件調查威脅指標彙總_惡意檔案

#	檔案位置	HASH 值	Memo
1	D:\EECOnline\EUSERVICE-Blank\trunk\assests\style\assest.aspx	MD5：2bba450a883946e4369c0f896df0b171	已遭防毒隔離
		SHA1：e489a472efcb666b40765ee73af211b5d7d3e8ac	
		SHA256：10475835e5c5cbdc607706ca26fb1f4e69218393c20b91119dca01306db25a36	
2	• D:\EECOnline\EUSERVICE-Blank\trunk\assests\js\assests\js\bootstrap.min.aspx • D:\EECOnline\EUSERVICE-Blank\trunk\Scripts\popper-utils.min.aspx	MD5：6f093b9d0add4e962c097105593b8818	具有檔案管理功能
		SHA1：81d0879c9a2bd50e50a7045e6a6a23e0872feab3	
		SHA256：d92348f20260e2d8e96e13e4a93e3d78bda606bebe4e0151d796856063ec3dca	
3	D:\EECOnline\EUSERVICE-Blank\trunk\assests\js\assests\js\bootstrap.aspx	MD5：b7a3315f7453f2b53ff7809fed58426d	可列出主機與環境相關資訊
		SHA1：de189c02eb68657b03527b292d75ed07745d2f50	
		SHA256：27951df9069389a4a3a340eff43e165f5fdd9b5b54cc5b45cbafdae0636ae30e	
4	D:\EECOnline\EUSERVICE-Blank\trunk\assests\js\bootstrap-4.4.1.aspx	調查時檔案已不存在	
5	D:\EECOnline\EUSERVICE-Blank\trunk\Uploads\WordTemplate\FileManager.aspx	調查時檔案已不存在	

10

10

事件調查威脅指標彙總_惡意檔案

#	檔案位置	HASH 值	Memo
6	D:\EEOnline\EUSERVICE-Blank\trunk\Uploads\WordTemplate\20250807173613758tmp250808124606071460.aspx	MD5：3595a7853a6f15d3b2ebf68550deea99	有上傳檔案的功能
		SHA1：562bef0647be749048cf69c02c7ac9d589232551	
		SHA256：5f3fd535c723131de4edb31c5db75190ee5949a9a743c95b557822621a1f210d	
7	D:\EEOnline\EUSERVICE-Blank\trunk\Uploads\WordTemplate\adm.aspx	MD5：bc58175cf38ae15e33e1fb436d9cb984	可直接寫入任意檔案
		SHA1：2335e2ea272f3b3afc9c7a3feff8a6122d197887	
		SHA256：110795eff9c328628e15976da90ab6b16244b7c0ec4b54e15aeacd48d4b9952e	
8	D:\EEOnline\EUSERVICE-Blank\trunk\Services\UserServices.aspx	MD5：8019314bcec9b894ffa9c1c2ec36d110	具有檔案管理功能，與bootstrap.aspx相同
		SHA1：2e881e0be6b858205aaeb394af327e19e63e2ed6	
		SHA256：eedf65cf786fb9da01d7264c9380a5d4ca5ca2afb699b84a23b1805f69add6aa	

11

11

詳細調查過程

12

12

調查主機資訊

- 主機用途　電子病歷交換中心主機
- 主機名稱　EEC_PD
- 作業系統名稱　Microsoft Windows Server 2016 Datacenter
- 作業系統版本　10.0.14393 N/A 組建 14393
- 作業系統設定　獨立伺服器
- 原始安裝日期　2021/11/08, 下午 02:48:54
- 系統開機時間　2025/03/11, 下午 12:43:21
- 時區　(UTC+08:00) 台北
- 網路設定資訊
  - IP 位址　203.65.108.116、172.16.30.118
  - 預設閘道　203.65.108.254
  - 子網路遮罩　255.255.255.0

13

通報現象確認

- 比對檔案目錄，確認 assest.aspx 於 2025/10/29 15:41 遭防毒軟體隔離

ParentPath	FileName	FileSize	Created(UTC+0)
.\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\6	jp41wimv.tmp	0	2025/10/29 07:42:39
.\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\6	App_Web_bootstrap.min.aspx.f6ef47	1217	2025/10/29 07:42:39
.\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\6	App_Web_bootstrap.min.aspx.f6ef47	34138	2025/10/29 07:42:39
.\Program Files (x86)\Trend Micro\OfficeScan Client\Suspect\Backup	assest.aspx.1761723703.qtn	43812	2025/10/29 07:41:44
.\Windows\Logs\WindowsUpdate	WindowsUpdate.20251029.152415.5	8192	2025/10/29 07:24:16
.\Program Files (x86)\Trend Micro\OfficeScan Client\Misc	NCIE.log	0	2025/10/29 07:14:52
.\Program Files (x86)\Trend Micro\OfficeScan Client\Misc	CCCACln.log	0	2025/10/29 07:14:52

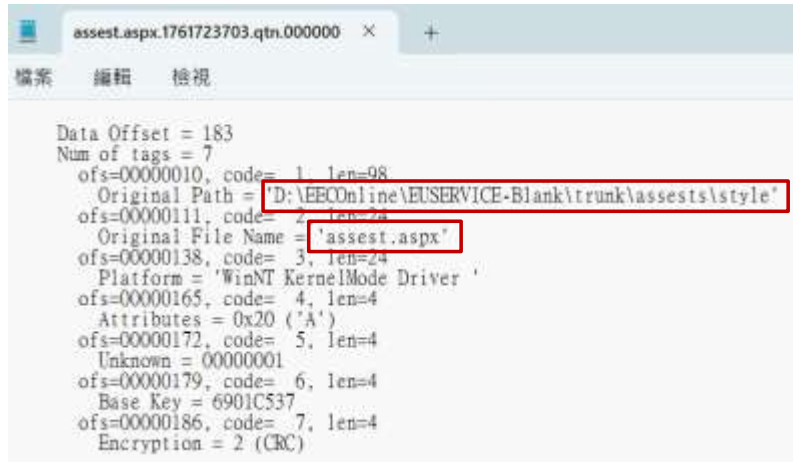
- bootstrap.aspx 及 bootstrap.min.aspx 分別建立於 2025/10/13 14:48 及 2025/08/19 10:14

ParentPath	FileName	FileSize	Created0x10	Created(UTC+0)
.\EECOnline\EUSERVICE-Blank\trunk\bin	EECModules.dll	5632	2023/10/23 06:02:02	2025/10/13 07:03:09
.\EECOnline\EUSERVICE-Blank\trunk\assests\js	bootstrap.aspx	97204	2024/03/27 07:10:38	2025/10/13 06:48:50
.\EECOnline\EUSERVICE-Blank\trunk\Scripts	popper-utils.min.aspx	17150	2024/03/27 07:11:00	2025/08/19 02:37:20
.\EECOnline\EUSERVICE-Blank\trunk\Services	UserServices.aspx	67983	2025/08/19 02:34:00	2025/08/19 02:34:58
.\EECOnline\EUSERVICE-Blank\trunk\assests\js	bootstrap.min.aspx	17150	2024/03/27 07:10:00	2025/08/19 02:14:09

14

assest.aspx 原始路徑

- assest.aspx 還原檔案，確認其原始路徑為 D:\EECOnline\EUSERVICE-Blank\trunk\assests\style



15

15

assest.aspx 檔案內容

- 經編碼混淆的惡意程式
- 功能為：可以透過 HTTP 建立 Tunnel 的連線，進一步與攻擊者主機溝通，例如傳輸任意資料、執行指令或文件上傳

16

16

惡意程式寫入紀錄_1

- 於 2025/09/09 16:11，由攻擊者IP 61.30.172.143 (TW)，利用 /assests/js/bootstrap-4.4.1.aspx 寫入 assest.aspx

Date	Time(UTC+0)	Server IP	Method	URL		Status	Port		Client IP
2025/9/9	08:10:35	203.65.108.116	GET	/Login/C101M	-	200	443	-	211.79.205.35
2025/9/9	08:11:14	203.65.108.116	POST	/assests/js/bootstrap-4.4.1.aspx	-	200	443	-	61.30.172.143
2025/9/9	08:11:15	203.65.108.116	GET	/assests/js/bootstrap-4.4.1.aspx	path=RDpcRUVDT25saW5lXE\	200	443	-	61.30.172.143
2025/9/9	08:11:23	203.65.108.116	GET	/assests/	-	403	443	-	61.30.172.143
2025/9/9	08:11:43	203.65.108.116	GET	/assests/style/assest.aspx	-	200	443	-	61.30.172.143
2025/9/9	08:12:50	203.65.108.116	GET	/Home/Login	-	200	443	-	218.173.154.21
2025/9/9	08:12:50	203.65.108.116	GET	/Home/GetValidateCode2	-	200	443	-	218.173.154.21

- 於 2025/10/13 14:48，由攻擊者IP 89.117.42.12 (TW)，利用 /assests/js/bootstrap-4.4.1.aspx 寫入 bootstrap.aspx

Date	Time(UTC+0)	Server IP	Method	URL		Status	Port		Client IP
2025/10/13	06:48:45	203.65.108.116	POST	/Home/SearchLoginForm3	-	302	443	-	118.165.89.148
2025/10/13	06:48:49	203.65.108.116	POST	/assests/js/bootstrap-4.4.1.aspx	-	200	443	-	89.117.42.12
2025/10/13	06:48:49	203.65.108.116	GET	/	result=€	200	443	-	118.165.89.148
2025/10/13	06:48:51	203.65.108.116	GET	/assests/js/bootstrap-4.4.1.aspx	-	200	443	-	89.117.42.12
2025/10/13	06:49:06	203.65.108.116	GET	/assests/js/	-	403	443	-	89.117.42.12
2025/10/13	06:49:34	203.65.108.116	GET	/assests/js/bootstrap.aspx	-	200	443	-	89.117.42.12
2025/10/13	06:49:36	203.65.108.116	POST	/Home/SearchGridDetail	-	200	443	-	118.165.89.148
2025/10/13	06:49:56	203.65.108.116	GET	/Login/C101M	-	200	443	-	211.79.205.35

17

惡意程式寫入紀錄_2

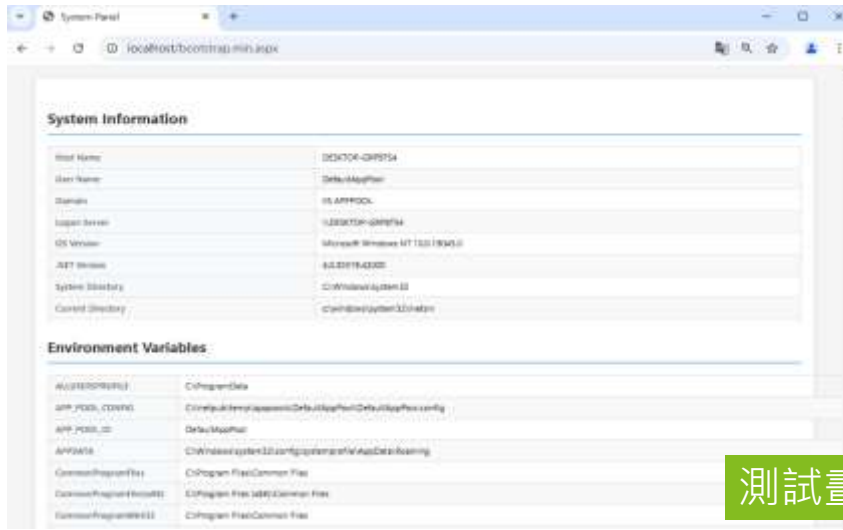
- 於 2025/08/19 10:14，由攻擊者IP 118.160.207.102 (TW)，利用 /assests/js/bootstrap-4.4.1.aspx 寫入 bootstrap.min.aspx

Date	Time(UTC+0)	Server IP	Method	URL		Status	Port		Client IP
2025/8/19	02:14:03	203.65.108.116	GET	/assests/js/bootstrap-4.4.1.aspx	path=RD	200	443	-	106.104.134.62
2025/8/19	02:14:09	203.65.108.116	GET	/assests/js/bootstrap-4.4.1.aspx	action=v	200	443	-	106.104.134.62
2025/8/19	02:14:09	203.65.108.116	POST	/assests/js/bootstrap-4.4.1.aspx	-	200	443	-	118.160.207.102
2025/8/19	02:14:10	203.65.108.116	GET	/assests/js/bootstrap-4.4.1.aspx	-	200	443	-	118.160.207.102
2025/8/19	02:27:25	203.65.108.116	GET	/Login/C101M	-	200	443	-	211.79.205.35
2025/8/19	02:27:41	203.65.108.116	GET	/assests/js/bootstrap.min.aspx	-	200	443	-	103.137.247.67
2025/8/19	02:28:17	203.65.108.116	GET	/assests/js/bootstrap-4.4.1.aspx	action=n	200	443	-	118.160.207.102

18

bootstrap.aspx

- 可列出主機資訊，如系統資訊、環境變數、網域資訊、網卡資訊、網路連線等



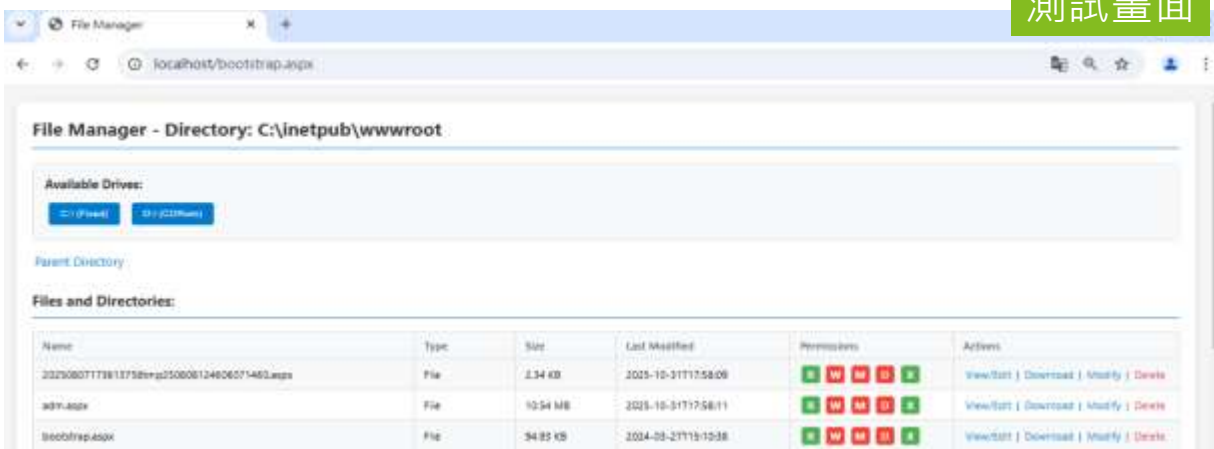
測試畫面

19

bootstrap.min.aspx

- 具有檔案管理功能，如查看檔案目錄、上傳檔案等

測試畫面



20

bootstrap-4.4.1.aspx

- bootstrap-4.4.1.aspx 調查時已不存在
- 比對網站存取紀錄，研判該檔案於 2025/08/19 10:11 由攻擊者IP 118.160.207.102 (TW) 透過 /Uploads/WordTemplate/FileManager.aspx 寫入

Date	Time(UTC+0)	Server IP	Method	URL		Status	Port		Client IP
2025/8/19	02:10:41	203.65.108.116	GET	/Uploads/WordTemplate/FileManager.aspx	path=RD	200	443	-	118.160.207.102
2025/8/19	02:10:51	203.65.108.116	GET	/Uploads/WordTemplate/FileManager.aspx	action=n	200	443	-	118.160.207.102
2025/8/19	02:11:58	203.65.108.116	POST	/Uploads/WordTemplate/FileManager.aspx	-	200	443	-	118.160.207.102
2025/8/19	02:12:00	203.65.108.116	GET	/Uploads/WordTemplate/FileManager.aspx	path=RD	200	443	-	118.160.207.102
2025/8/19	02:12:25	203.65.108.116	GET	/Login/C101M	-	200	443	-	211.79.205.35
2025/8/19	02:12:59	203.65.108.116	GET	/assests/js/bootstrap-4.4.1.aspx	-	200	443	-	118.160.207.102
2025/8/19	02:13:23	203.65.108.116	GET	/assests/js/bootstrap-4.4.1.aspx	-	200	443	-	106.104.134.62

21

FileManager.aspx

- FileManager.aspx 調查時已不存在
- 比對網站存取紀錄，研判該檔案於 2025/08/19 10:03 由攻擊者IP 118.160.207.102 (TW) 透過 /Uploads/WordTemplate/20250807173613758tmp250808124606071460.aspx 寫入

Date	Time(UTC+0)	Server IP	Method	URL		Status	Port		Client IP
2025/8/19	02:03:04	203.65.108.116	GET	/Uploads/WordTemplate/20250807173613758tmp250808124606071460.aspx	-	200	443	-	118.160.207.102
2025/8/19	02:03:04	203.65.108.116	GET	/favicon.ico	-	200	443	-	118.160.207.102
2025/8/19	02:03:18	203.65.108.116	POST	/Uploads/WordTemplate/20250807173613758tmp250808124606071460.aspx	-	200	443	-	118.160.207.102
2025/8/19	02:03:24	203.65.108.116	GET	/Login/C101M	-	200	443	-	211.79.205.35
2025/8/19	02:03:37	203.65.108.116	GET	/assests/style/hover.css	-	200	443	-	1.173.202.204
2025/8/19	02:03:37	203.65.108.116	GET	/webfonts/fa-solid-900.woff2	-	200	443	-	1.173.202.204
2025/8/19	02:03:37	203.65.108.116	GET	/assests/images/apple-touch-icon.png	-	200	443	-	1.173.202.204
2025/8/19	02:03:37	203.65.108.116	GET	/assests/images/favicon.png	-	200	443	-	1.173.202.204
2025/8/19	02:04:06	203.65.108.116	GET	/Uploads/WordTemplate/FileManager.aspx	-	200	443	-	118.160.207.102
2025/8/19	02:04:28	203.65.108.116	GET	/Uploads/WordTemplate/FileManager.aspx	-	200	443	-	118.160.207.102

22

20250807173613758tmp250808124606071460.aspx

- 比對檔案目錄，該檔案建立於 2025/08/19 10:02

ParentPath	FileName	FileSize	Created(UTC+0)
.\EECOnline\EUSERVICE-Blank\trunk\Services	UserServices.aspx	67983	2025/08/19 02:34:00
.\EECOnline\EUSERVICE-Blank\trunk\Uploads\WordTemplate	20250807173613758tmp250808124606071460.aspx	2397	2025/08/19 02:02:03
.\EECOnline\EUSERVICE-Blank\trunk\logs	trace.log20250819-10	3077042	2025/08/19 02:00:03

- 比對網站存取紀錄，該檔案為攻擊者IP 106.104.134.62 (TW) 透過 /Uploads/WordTemplate/adm.aspx 寫入

Date	Time(UTC+0)	Server IP	Method	URL		Status	Port		Client IP
2025/8/19	02:01:48	203.65.108.116	GET	/assests/webfonts/fa-regular-400.svg	-	404	443	-	39.15.22.77
2025/8/19	02:02:03	203.65.108.116	POST	/Uploads/WordTemplate/adm.aspx	-	200	443	-	106.104.134.62
2025/8/19	02:02:28	203.65.108.116	GET	/	-	200	443	-	106.104.134.62
2025/8/19	02:02:46	203.65.108.116	GET	/Uploads/WordTemplate/20250807173613758tmp250808124606071460.aspx	-	200	443	-	106.104.134.62
2025/8/19	02:03:04	203.65.108.116	GET	/Uploads/WordTemplate/20250807173613758tmp250808124606071460.aspx	-	200	443	-	118.160.207.102

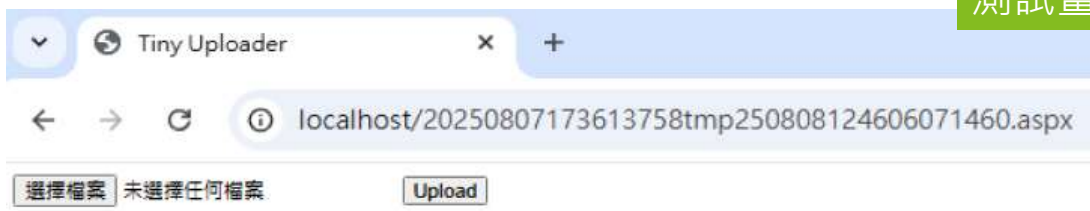
23

23

20250807173613758tmp250808124606071460.aspx 檔案功能

- 其功能為上傳檔案

測試畫面



24

24

adm.aspx

- 比對檔案目錄，該檔案建立於 2025/08/19 09:50

ParentPath	FileName	FileSize	Created(UTC+0)
.\EECOnline\EUSERVICE-Blank\trunk\logs	trace.log20250819-10	3077042	2025/08/19 02:00:03
.\EECOnline\EUSERVICE-Blank\trunk\Uploads\WordTemplate	adm.aspx	11053982	2025/08/19 01:50:56
.\EECOnline\EUSERVICE-Blank\trunk\logs	trace.log20250819-09	3141903	2025/08/19 01:00:01

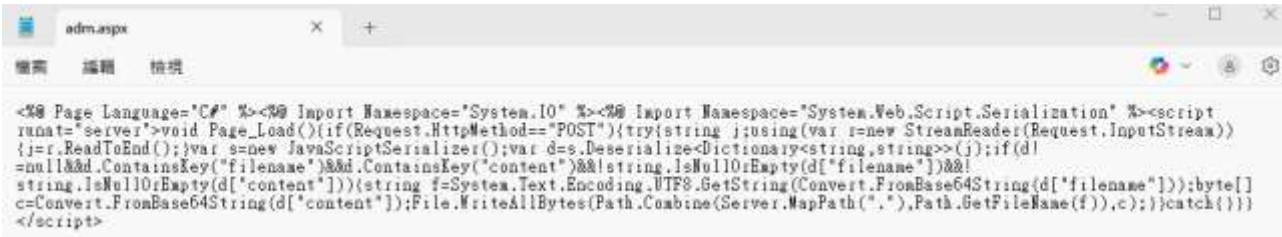
- 比對網站存取紀錄，該檔案為攻擊者IP 106.104.134.62 (TW) 透過網站功能 /Resource/File 寫入

Date	Time(UTC+0)	Server IP	Method	URL		Status	Port		Client IP
2025/8/19	01:49:49	203.65.108.116	GET	/style/base.css	-	404	443	-	106.104.134.62
2025/8/19	01:49:49	203.65.108.116	GET	/style/bootstrap.css	-	404	443	-	106.104.134.62
2025/8/19	01:50:56	203.65.108.116	POST	/Resource/File	-	200	443	-	106.104.134.62
2025/8/19	01:51:24	203.65.108.116	GET	/Login/C101M	-	200	443	-	211.79.205.35
2025/8/19	01:51:29	203.65.108.116	GET	/Uploads/WordTemplate	-	301	443	-	106.104.134.62
2025/8/19	01:51:29	203.65.108.116	GET	/Uploads/WordTemplate/	-	403	443	-	106.104.134.62
2025/8/19	01:51:41	203.65.108.116	GET	/Uploads/WordTemplate/adm.aspx	-	200	443	-	106.104.134.62
2025/8/19	01:52:13	203.65.108.116	GET	/Home/GetValidateCode3	-	200	443	-	114.136.109.239

25

adm.aspx 檔案內容

- 功能為：攻擊者能以此直接寫入任意檔案



26

其他惡意檔案

- 其他寫入時間同為 2025/08/19 10時的惡意檔案
  - 兩者皆未發現有遭存取過
  - popper-utils.min.aspx 可列出主機資訊，如系統資訊、環境變數、網域資訊、網卡資訊、網路連線等（與 bootstrap.min.aspx 相同）
  - UserServices.aspx 具有檔案管理功能，如查看檔案目錄、上傳檔案等（與 bootstrap.aspx 相同）

ParentPath	FileName	FileSize	Created(UTC+0)	Created(UTC+0)
.\EECOnline\EUSERVICE-Blank\trunk\Scripts	popper-utils.min.aspx	17150	2024/03/27 07:11:00	2025/08/19 02:37:20
.\EECOnline\EUSERVICE-Blank\trunk\Services	UserServices.aspx	67983	2025/08/19 02:34:00	2025/08/19 02:34:58

27

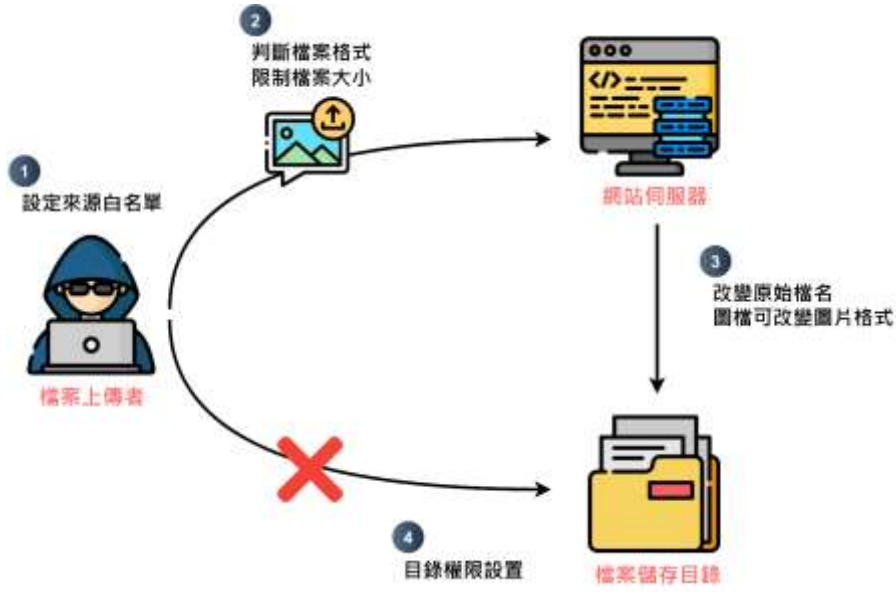
27

THE BEST IS YET TO COME

28

28

如何防止檔案上傳攻擊

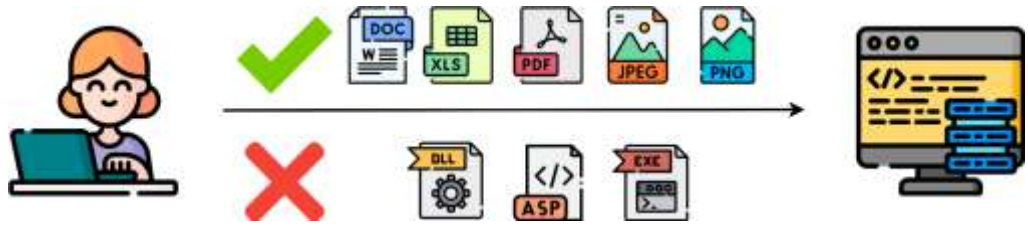


29

限縮可存取上傳功能來源

30

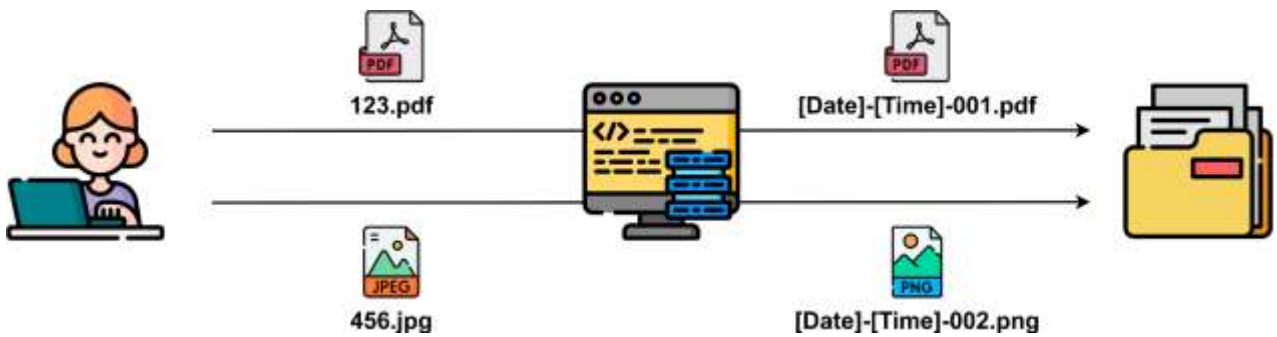
判斷檔案格式合法性



31

31

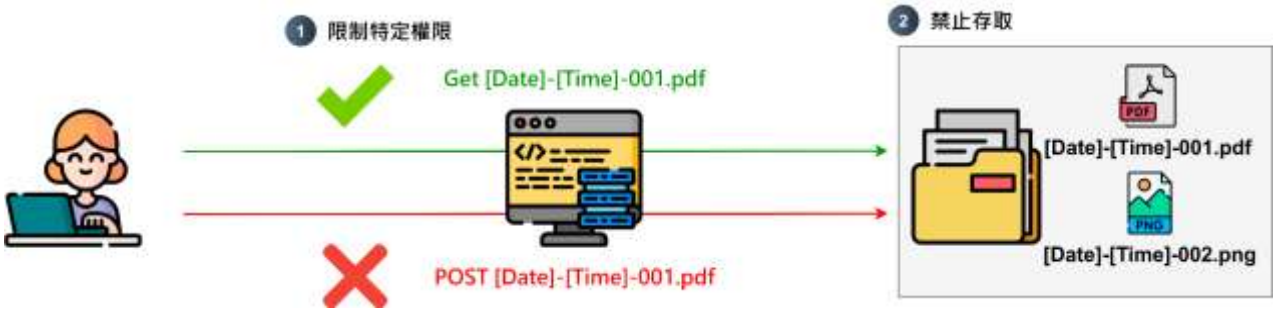
改變隨機檔名和圖片格式



32

32

目錄權限設置


1 限制特定權限
Get [Date]-[Time]-001.pdf
POST [Date]-[Time]-001.pdf
2 禁止存取
[Date]-[Time]-001.pdf
[Date]-[Time]-002.png

33

33