

【限閱】

測試報告因涉及敏感資訊僅摘錄部分內容

114年度
法鼓文理學院
儲存雲
滲透測試服務報告
(初測)

執行單位：聯準科技股份有限公司

中華民國 114 年 12 月 15 日

目錄

1. 執行結果摘要說明.....	1
1.1. 受測目標風險等級與數量列表	1
1.2. 受測目標風險漏洞名稱列表	1
1.3. 風險漏洞分佈列表.....	3
2. 執行計畫	4
2.1. 執行期間.....	4
2.2. 執行範圍.....	4
2.3. 執行項目	4
2.4. 專案成員	13
3. 滲透測試執行結果.....	15
3.1. 檢測目標.....	15
3.2. 風險等級說明.....	15
3.3. 執行結果說明.....	16
4. 結果建議.....	21
5. 結論.....	22
6. 附錄.....	23

6.1. HTTP SERVER OWASP 檢測結果.....	23
---	-----------

圖目錄

圖 1 專案組織與成員架構.....	13
圖 2 儲存雲-Nmap 掃描結果	20

表目錄

表 1	儲存雲滲透測試弱點種類統計	1
表 2	滲透測試規範項目與執行結果摘要說明	1
表 3	儲存雲滲透測試弱點分佈列表	3
表 4	測試標的物資訊.....	4
表 5	OWASP Testing Guide v4.2 滲透測試規範項目	4
表 6	滲透測試服務專案成員與職掌	13
表 7	發現弱點類別風險清單表.....	22
表 8	HTTP Server OWASP 檢測結果.....	23

1. 執行結果摘要說明

1.1. 受測目標風險等級與數量列表

本次滲透測試針對儲存雲進行滲透測試服務之測試標的，依風險等級與數量摘要說明如下表：

表1 儲存雲滲透測試弱點種類統計

受測目標	風險等級					合計
	嚴重	高	中	低	參考資訊	
儲存雲 https://drive2.dila.edu.tw:5001	0	0	0	3	0	3
合計	0	0	0	3	0	3

1.2. 受測目標風險漏洞名稱列表

本次滲透測試針對儲存雲進行滲透測試服務之測試標的，依規範項目摘要說明如下表：

表2 滲透測試規範項目與執行結果摘要說明

測試 類型	測試 類別	測試項目	儲存雲
	使用者授權	至少包含目錄跨越測試、網站授權機制測試及權限控管機制測試等項目	
	邏輯漏洞	至少包含網站功能測試、網站功能設計缺失測試及附件上傳測試等項目	無
	輸入驗證 (1)	至少包含 XSS 漏洞測試、SQL Injection 測試、LDAP Injection 測試、XML Injection 測試、SSL Injection 測試、XPath Injection 測試及 Code Injection 測試等項目	無
	輸入驗證 (2)	至少包含 XSS 漏洞測試、SQL Injection 測試、OS Commanding 測試及偽造 HTTP 協定測試等項目	無
	Web Service	至少包含 WSDL 測試、XML 架構測試、XML 內容測試及 XML 參數傳遞測試等項目	無
	Ajax	至少包含 Ajax 弱點測試等項目，如輸入驗證缺失、權限控管及套件弱點等測試項目	無
應用程式	網路服務 套件	包含 SMTP、POP3 及 IMAP 等常見對外郵件服務之弱點測試，如設定缺失、權限控管及套件弱點等項目	無
	網站服務 套件	包含常見 WEB 伺服器弱點測試，如設定缺失、權限控管及套件弱點等測試項目	無
	檔案傳輸 服務套件	包含 FTP、NETBIOS 及 NFS 等常見檔案傳輸服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目	無
	遠端連線 服務套件	包含 SSH、TELNET、VNC 及 RDP 等常見遠端連線服務之弱點測試，如	無

測試 類型	測試 類別	測試項目	儲存雲
		設定缺失、權限控管及套件弱點等測試項目	
	網路服務 套件	包含 DNS、PROXY 及 SNMP 等常見網路服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目	無
	其它	包含 Firewall、IDS/IPS、Database、LDAP 及 SMB 等常見應用程式或網路套件之弱點測試項目	無
密碼 破解	密碼強度 測試	包含 WEB、FTP、SSH、TELNET、SMTP、POP3、IMAP、SNMP、NetBIOS、RDP、VNC 及 Database 等常見對外服務之密碼字典檔測試	無

註：風險等級：(嚴)為嚴重風險；(高)為高風險；(中)為中風險；(低)為低風險；(參)為參考資訊。

2. 執行計畫

2.1. 執行期間

初測：114 年 12 月 9 日。

2.2. 執行範圍

本次測試來源及目的標的物資訊如下表：

表4 測試標的物資訊

項目	單位	IP/Domain
滲透來源端	聯準科技股份有限公司	61.230.192.47
受測目標端	儲存雲	https://drive2.dila.edu.tw:5001

2.3. 執行項目

測試團隊執行滲透測試服務，主要參考並符合 OWASP（Open Web Application Security Project）組織所規範（OWASP Testing Guide v4.2）之定義以及本案採購規範所定義之項目，測試項目如下表。

表5 OWASP Testing Guide v4.2 滲透測試規範項目

OWASP 編碼	測試項目	檢測項目說明
資訊蒐集(Information Gathering)		
WSTG-INFO-01	Conduct Search Engine Discovery and Reconnaissance for Information Leakage	利用搜尋引擎查看是否有資訊洩漏。
WSTG-INFO-02	Fingerprint Web Server	蒐集 Webserver 伺服器版本與類型。
WSTG-INFO-03	Review Webserver Metafiles for Information Leakage	蒐集 Webserver 的 metafiles 看是否有敏感資訊洩漏。
WSTG-INFO-04	Enumerate Applications on Webserver	蒐集 Webserver 上的應用程式資訊。

OWASP 編碼	測試項目	檢測項目說明
WSTG-INFO-05	Review Webpage Comments and Metadata for Information Leakage	檢視並蒐集 Webpage 的註解與 metadata。
WSTG-INFO-06	Identify application entry points	檢測網頁程式中，存在的滲透切入點。
WSTG-INFO-07	Map execution paths through application	蒐集目標程式的流程的資訊。
WSTG-INFO-08	Fingerprint Web Application Framework	測試 Fingerprint 框架是否存在漏洞。
WSTG-INFO-09	Fingerprint Web Application	蒐集 web 應用程式和版本，看是否存在已知漏洞。
WSTG-INFO-10	Map Application Architecture	蒐集互相連接的應用程式架構的相關資訊。
配置與佈署管理測試(Configuration and Deploy Management Testing)		
WSTG-CONF-01	Test Network/Infrastructure Configuration	測試網路組態設定是否存在漏洞。
WSTG-CONF-02	Test Application Platform Configuration	測試應用程式平台的組態設定是否存在漏洞。
WSTG-CONF-03	Test File Extensions Handling for Sensitive Information	測試文件擴展是否有洩漏敏感資訊。
WSTG-CONF-04	Backup and Unreferenced Files for Sensitive Information	測試備份或引用文件是否有洩漏敏感資訊。
WSTG-CONF-05	Enumerate Infrastructure and Application Admin Interfaces	測試管理員介面是否存在漏洞。
WSTG-CONF-06	Test HTTP Methods	測試 HTTP 的方法是否有洩漏安全的風險存在。

OWASP 編碼	測試項目	檢測項目說明
WSTG-CONF-07	Test HTTP Strict Transport Security	測試 HSTS 的相關加密是否存在漏洞。
WSTG-CONF-08	Test RIA cross domain policy	測試 RIA 的跨 domain 策略是否有洩漏敏感資訊的漏洞。
WSTG-CONF-09	Test File Permission	測試檔案及目錄是否符合權限設置。
WSTG-CONF-10	Test for Subdomain Takeover	測試 DNS 子網域是否存在漏洞
WSTG-CONF-11	Test Cloud Storage	測試雲端服務是否有洩漏敏感資訊的漏洞
身分管理測試(Identity Management Testing)		
WSTG-IDNT-01	Test Role Definitions	測試系統定義不同使用者的功能與權限是否存在漏洞。
WSTG-IDNT-02	Test User Registration Process	測試使用者註冊過程。
WSTG-IDNT-03	Test Account Provisioning Process	測試帳戶設置過程。
WSTG-IDNT-04	Testing for Account Enumeration and Guessable User Account	測試帳號是否有被暴力破解的可能。
WSTG-IDNT-05	Testing for Weak or unenforced username policy	測試帳號錯誤時返回的訊息，是否有被利用的可能。
認證測試(Authentication Testing)		
WSTG-ATHN-01	Testing for Credentials Transported over an Encrypted Channel	測試帳號密碼傳輸是否走加密通道。
WSTG-ATHN-02	Testing for default credentials	測試預設或常見的帳號密碼。
WSTG-ATHN-03	Testing for Weak lock out mechanism	測試防止暴力破解機制。

OWASP 編碼	測試項目	檢測項目說明
WSTG-ATHN-04	Testing for bypassing authentication schema	測試規避認證機制。
WSTG-ATHN-05	Test remember password functionality	測試記憶密碼功能。
WSTG-ATHN-06	Testing for Browser cache weakness	測試 Browser 快取是否有漏洞。
OTG-AUTHN-007	Testing for Weak password policy	測試密碼是否為弱密碼。
WSTG-ATHN-08	Testing for Weak security question/answer	測試密碼相關問題時，確認其答案有足夠的安全性。
WSTG-ATHN-09	Testing for weak password change or reset functionalities	測試變更或重置密碼時，是否有漏洞存在。
WSTG-ATHN-10	Testing for Weaker authentication in alternative channel	測試認證機制是否有其他替代性通道的漏洞。
權限管理測試(Authorization Testing)		
WSTG -AUTHZ-001	Testing Directory traversal/file include	測試目錄走訪或是檔案引入漏洞。
WSTG -AUTHZ-002	Testing for bypassing authorization schema	測試繞過驗證授權機制。
WSTG -AUTHZ-003	Testing for Privilege Escalation	測試用戶權限是否有非法提升的漏洞。
WSTG -AUTHZ-004	Testing for Insecure Direct Object References	測試資料輸入部分是否有直接存取系統資料的漏洞。
Session 管理測試(Session Management Testing)		
WSTG-SESS-01	Testing for Bypassing Session Management Schema	測試 Session 管理是否有規避的漏洞。
WSTG-SESS-02	Testing for Cookies attributes	測試是否存在 Cookies attributes 漏

OWASP 編碼	測試項目	檢測項目說明
		洞。
WSTG-SESS-03	Testing for Session Fixation	測試 是否 存在 Session Fixation 漏洞。
WSTG-SESS-04	Testing for Exposed Session Variables	測試 Session 變數 是否有暴露的漏洞。
WSTG-SESS-05	Testing for Cross Site Request Forgery	測試 是否有 CSRF 攻擊的漏洞。
WSTG-SESS-06	Testing for logout functionality	測試 Session Termination 的安全性。
WSTG-SESS-07	Testing for Session Timeout	測試 已經過時效的 Session 是否有被重用的漏洞。
WSTG-SESS-08	Testing for Session puzzling	測試 是否 存在 Session 變數過載漏洞。
WSTG-SESS-09	Testing for Session Hijacking	測試 Session Cookie 是否 Hijacking 的漏洞
輸入認證測試(Input Validation Testing)		
WSTG-INPV-01	Testing for Reflected Cross Site Scripting	檢測 是否 存在 Reflected XSS 漏洞。
WSTG-INPV-02	Testing for Stored Cross Site Scripting	檢測 是否 存在 Stored XSS 漏洞。
WSTG-INPV-03	Testing for HTTP Verb Tampering	測試 HTTP 傳輸中自定義的傳輸動詞。
WSTG-INPV-04	Testing for HTTP Parameter pollution	測試重複的 HTTP 參數 是否 存在攻擊者繞過驗證的可能。

OWASP 編碼	測試項目	檢測項目說明
WSTG-INPV-05	Testing for SQL Injection	檢測是否存在 SQL Injection 漏洞。
WSTG-INPV-06	Testing for LDAP Injection	檢測是否存在 LDAP Injection 漏洞。
WSTG-INPV-07	Testing for XML Injection	檢測是否存在 XML Injection 漏洞。
WSTG-INPV-08	Testing for SSI Injection	檢測是否存在 SSI Injection 漏洞。
WSTG-INPV-09	Testing for XPath Injection	檢測是否存在 XPath Injection 漏洞。
WSTG-INPV-10	IMAP/SMTP Injection	檢 測 是 否 存 在 IMAP/SMTP Injection 漏洞。
WSTG-INPV-11	Testing for Code Injection	檢測是否存在 Code Injection 漏洞。
WSTG-INPV-12	Testing for Command Injection	檢 測 是 否 存 在 Command Inclusion 漏洞。
WSTG-INPV-13	Testing for Format String Injection	檢測是否存在 Format String 漏洞。
WSTG-INPV-14	Testing for Incubated Vulnerability	檢 測 是 否 存 在 Incubated Vulnerability 漏洞。
WSTG-INPV-15	Testing for HTTP Splitting/Smuggling	檢測是否存在 HTTP Splitting, Smuggling 漏洞。
WSTG-INPV-16	Testing for HTTP Incoming Requests	檢測是否存在 HTTP Incoming Requests 漏洞。
WSTG-INPV-17	Testing for Host Header Injection	檢測是否存在 Host Header Injection 漏洞。

OWASP 編碼	測試項目	檢測項目說明
WSTG-INPV-18	Testing for Server-side Template Injection	檢測是否存在 Server-side Template Injection 漏洞。
WSTG-INPV-19	Testing for Server-Side Request Forgery	檢測是否存在 Server-Side Request Forgery Requests 漏洞。
錯誤處理(Error Handling)		
WSTG-ERRH-01	Testing for Improper Error Handling	分析錯誤頁面中的系統訊息。
WSTG-ERRH-02	Testing for Stack Traces	分析堆疊資訊，研判是否有攻擊者留下的痕跡。
密碼 (Cryptography)		
WSTG-CRYP-01	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection	測試不同類型資訊的傳輸，是否有通過 HTTP 的可能。
WSTG-CRYP-02	Testing for Padding Oracle	測試padding oracle 是否有敏感資訊洩漏的問題。
WSTG-CRYP-03	Testing for Sensitive information sent via unencrypted channels	測試敏感資訊的傳送是否有不受加密的通道。
WSTG-CRYP-04	Testing for Weak Encryption	測試加密通道安全級別。
商業邏輯測試(Business Logic Testing)		
WSTG-BUSL-01	Test Business Logic Data Validation	測試商業邏輯資料的驗證。
WSTG-BUSL-02	Test Ability to Forge Requests	測試外部是否有發送 Forge 請求的漏洞。
WSTG-BUSL-03	Test Integrity Checks	測試程序邏輯上的完整性是否有漏洞。