WAF 網頁應用程式防火牆

5G手機逐漸進入實測並成為主流，智慧型手機與平板電腦的高持有率，讓人們加速資訊的流通，可隨時隨地快速上網瀏覽網站、購物、查詢資料，已逐漸取代電腦成為上網的主要工具。而現今電子商務網站內容呈現更多樣性，實現在家購物的需求，讓我們享受網路帶來的便利性，但這樣的改變卻也隱藏巨大的風險。

架設好網站後，需要注意什麼嗎？

多數網站會跟後端的資料庫進行存取，以儲存會員資料、購買商品等資訊。
以舊架構來說，為了提供對網站伺服器的保護，通常會在前端設置防火牆。
但為何舊架構已不足以保護後端的網站呢?

1. 大部分網站架設於Windows的IIS或Linux的Apache伺服器上。當出現漏洞時，會釋出更新包修正，以確保系統的安全性。但此時更新網站系統需要執行網站關機，且更新完可能造成網頁無法正常瀏覽等問題，而使企業單位產生損失。
2. 除了服務本身的風險漏洞，網頁本身不夠嚴謹的語法也可能造成可入侵的風險，舉例如在帳密欄位輸入程式語言就可以竊取會員資料，導致個資外洩機率大增。
3. 一般傳統防火牆的辨識範圍最多只到網路架構第四層-傳輸層 (OSI 4 layer)，管控如IP、通訊埠號等，無法有效針對 HTTP 與網站應用程序加以過濾辨識。

台中總公司 04-2705-0888
台中市西屯區西屯路二段256巷6號3F-6

台北分公司 02-2501-1185
台北市中山區松江路129號6F-2

高雄分公司 07-229-8788
高雄市新興區民權一路251號8F-6

免付費專線 0800-666-188

官方網站 | www.sharetech.com.tw
銷售諮詢 | sales@sharetech.com.tw
技術支援 | help@sharetech.com.tw

WAF網頁應用程式防火牆(Web Application Firewall) 與防禦方式

為解決上述問題，眾至推出「WAF網頁應用程式防火牆」，當擋在網站前的一道防火牆，在 HTTP/HTTPS 訪問與請求進入網站前對所有流量進行分析與過濾，針對Layer 7層級的封包內容進行過濾判斷，有效排除掉惡意、可疑的連線。如SQL Injection資料庫注射攻擊、Cross Site Scripting (XSS) 跨站攻擊或其他OWASP定義等漏洞等。只允許合法的連線即進入網站檢索網頁內容，以確保網站資訊安全與服務正常運作。如下圖一所示：

圖示一: WAF防禦方式

眾至的WAF提供多達19項資料庫的比對內容，如下圖二所示：

分類
⊞ Numeric IP Address (1)
⊞ IP Reputation (6)
⊞ Scanner Detection (5)
⊞ Protocol Violations (38)
⊞ Protocol Anomalies (7)
⊞ Local File Inclusion Attack (4)
⊞ Remote File Inclusion Attack (4)
⊞ Remote Command Execution (14)
⊞ PHP Injection Attack (16)
⊞ Application Attack Nodejs (1)
⊞ Cross-site Scripting (XSS) Attack (30)
⊞ SQL Injection Attack (49)
⊞ Session Fixation Attack (3)
⊞ Application Attack Java (9)
⊞ Information Leakage (3)
⊞ SQL Data Leakage (16)
⊞ Java Data Leakage (2)
⊞ PHP Data Leakage (3)
⊞ IIS Data Leakages (4)

圖示二: 眾至WAF資料庫對比內容

WAF 網頁應用程式防火牆

當偵測到可疑的連線時（如幾分鐘內觸發多少次）就會直接封鎖其IP，使其無法再繼續針對網站進行滲透攻擊。管理員也可藉由19項的資料庫內容進行調整通行規則，哪些要記錄、哪些要阻擋等，來加強篩選機制。
當觸發時，設定畫面就會顯示阻擋紀錄。如下圖三所示：

紀錄列表　7 / 7　跳至 7 頁數 每頁 16 筆　匯出

日期	動作	來源 IP	Url	目的主機	分類	事件	連線次數
2020-07-21 02:07:55	阻擋	102.43.41.74	http://127.0.0.1:80/shell?cd+/tmp;rm+-rf+...	192.168.195.110:80	Numeric IP Address	[902350]: Host header is a numeric IP...	1
2020-07-21 01:47:19	阻擋	196.52.43.117	https://125.227.221.217:443	192.168.195.170:443	Numeric IP Address	[902350]: Host header is a numeric IP...	1
2020-07-21 01:42:50	阻擋	192.35.168.203	https://125.227.221.217	192.168.195.170:443	Numeric IP Address	[902350]: Host header is a numeric IP...	1
2020-07-21 01:42:49	阻擋	192.35.168.203	https://125.227.221.217:443	192.168.195.170:443	Numeric IP Address	[902350]: Host header is a numeric IP...	1
2020-07-21 01:00:12	阻擋	49.156.252.148	http://kav.sharetech.com.tw/KavQuery.php	192.168.195.110:80	SQL Injection Attack	[942450]: SQL Hex Encoding Identified	1
2020-07-21 00:51:55	阻擋	183.136.225.56	http://60.249.6.184	192.168.195.110:80	Numeric IP Address	[902350]: Host header is a numeric IP...	1
2020-07-21 00:00:57	阻擋	185.39.11.105	http://60.249.6.184:80/config/getuser?ind...	192.168.195.110:80	Numeric IP Address	[902350]: Host header is a numeric IP...	1
2020-07-21 00:00:36	阻擋	110.4.190.232	http://kav.sharetech.com.tw/KavQuery.php	192.168.195.110:80	SQL Injection Attack	[942450]: SQL Hex Encoding Identified	1
2020-07-21 00:00:27	阻擋	153.212.200.178	http://kav.sharetech.com.tw/KavQuery.php	192.168.195.110:80	SQL Injection Attack	[942340]: Detects basic SQL authentication	1

圖示三：WAF 防護紀錄

WAF白名單

此外，在網站使用正常情況下，但因為網站本身語法不夠嚴謹而造成阻擋，也可以先將其加入WAF白名單，讓網站服務能夠在優化安全機制前，暫時能夠正常瀏覽。如下圖三所示：

新增 WAF 白名單

名稱　Web

白名單 URL　http(s):// www.sharetech.com.tw

白名單項目

分類	☐
⊞ Numeric IP Address (1)	☑
⊞ IP Reputation (6)	☑
⊞ Scanner Detection (5)	☐
⊞ Protocol Violations (38)	☐
⊞ Protocol Anomalies (7)	☐

圖示四：WAF白名單

可設定的網站數與連線數上限

避免WAF資源被使用過量，眾至對於不同型號規格有進行分類，避免影響整體功能使用。
舉例 NU系列UTM 如下

NU 系列	型號	限制網站數	單網站同時最大為100條連線
初階系列	NU-840 NU-840H	20個	共計 100 x 20 = 2,000 條
中階系列	NU-860H NU-860T NU-860C	50個	共計 100 x 50 = 5,000 條
高階系列	NU-8700C NU-8700F NU-8700T	100個	共計 100 x 100 = 10,000 條
	NU-8800T	200個	共計 100 x 200 = 20,000 條