NG-UTM WAF網頁應用防火牆

在網路普及和5G時代的來臨之下，人手一支智慧型手機，便可隨時隨地快速上網瀏覽。網站也不再如同以往，單單只是公告訊息的地方，更多的是畫面呈現的豐富性以及網站內容的多樣性，比如電子商務網站，讓我們不須出門，在家就可以直接購物，享受網路帶來的便利性。

架好網站，就好了嗎？

在這當中卻也隱藏著巨大風險。多數網站都會跟後端的資料庫做存取，用來儲存會員資料、購買商品等資訊。就以往的架構來說，通常會在前端設置防火牆，以提供對網站伺服器的保護，但現在看來卻遠不足以保護後端的網站，怎麼說呢？

1.網站大多架設於windows的IIS或Linux的Apache伺服器上。當出現漏洞時，就會釋出更新包來修正，以確保系統的安全性。但更新網站系統首先就要面臨網站需要關機，且更新完可能造成網頁無法正常瀏覽等問題，因而使企業單位產生損失...

2.除了服務本身的風險漏洞，有時也會因撰寫網頁時，語法上不夠嚴謹，造成可入侵的風險，比方說：在帳號密碼的欄位輸入程式語言就可竊取會員資料，導致個資外洩機率大增。

3.以上兩點都是防火牆無法防護的，且一般防火牆只能控管傳輸層，如IP、通訊埠號等，無法有效針對網頁應用面上傳輸的內容加以過濾辨識。

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

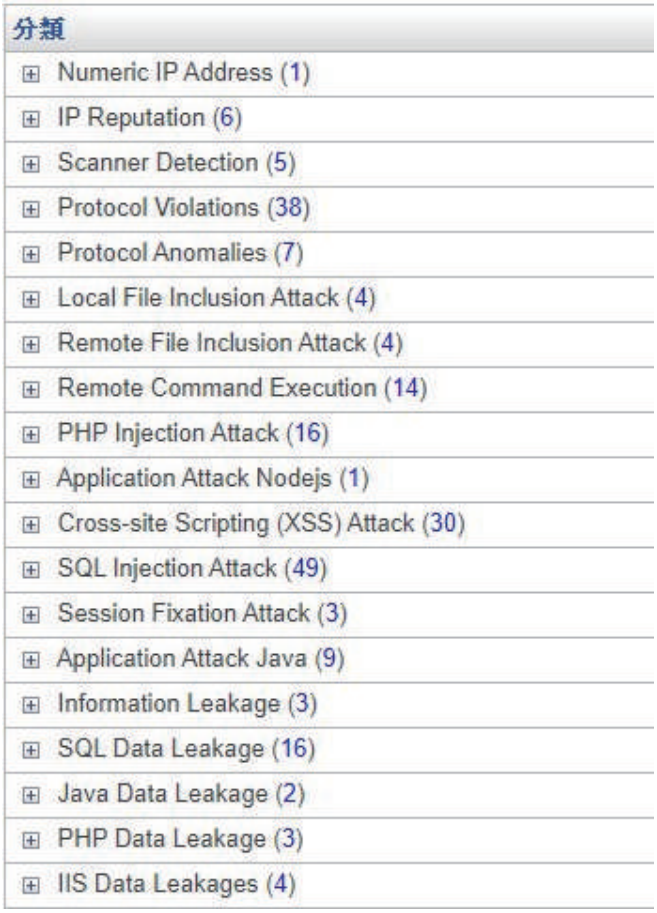
高雄分公司 07-229-8788
高雄市新興區民權一路251號8F-6

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網頁應用程序防火牆(Web Application Firewall)

因應此問題，眾至推出了「WAF網頁應用程序防火牆」，用來加強原本防火牆對網站防護的不足之處；WAF是針對Layer 7層級的封包內容進行過濾判斷，若為合法的連線即允許連入，可疑的連線就會在此被拒絕。因此如常見的SQL Injection資料庫注射攻擊、Cross Site Scripting (XSS) 跨站攻擊或是系統本身的漏洞等，都可透過WAF來偵測及阻擋。

眾至的WAF提供多達19項資料庫的比對內容，如下圖一所示：



圖示一：WAF資料庫

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項的資料庫內容去做設定，哪些要記錄哪些要阻擋等，彈性調整以符合企業需求。當觸發時，設定畫面就會顯示阻擋紀錄。如下圖二所示：

紀錄列表

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

圖示二：WAF 防護紀錄

WAF白名單

此外，若是因網站本身語法上不夠嚴謹而造成阻擋，但其使用是正常的狀況下，也可以先加入WAF白名單，讓網站服務先正常瀏覽。不過當然還是建議盡早完善網站本身的安全機制囉！如下圖三所示：

圖示三：WAF白名單