

DragonSoft Web Protector (For IIS)



DragonSoft Web Protector

採取入侵行為辨識技術，提供使用者簡易的操作介面，阻斷各種意圖攻擊行為以強化Web Server的安全性。

在整體Security Wheel內，負責「保護」與「過濾」Web Server 的一環。過濾已知與未知的弱點攻擊，在層出不窮的攻擊中，保護 Web Server 並將異常的執行過濾掉。

保護功能：

- SQL Injection
- Buffer Overflow
- Shell Command
- HTTP Method
- Encoding Attack
- Directory Traversal

系統支援：

- Windows NT/2000/XP/2003
- IIS Web Service 4.x
- IIS Web Service 5.x
- IIS Web Service 6.x

保護與過濾功能：

緩衝區溢位：

一些程式中輸入過長的字串到系統的緩衝區,超出了系統所設定的記憶區大小而發生的錯誤我們稱為緩衝區溢位，管理者利用 Web Protector 來控制 Web Server 收受的請求的長度，過濾掉 Web Server 本身已存在的弱點攻擊或者是未發現的弱點攻擊。

HTTP 指令：

過濾當遠端攻擊者對 Web Server 傳送出含 HTTP 攻擊性的指令, 像是 Delete 指令。

目錄允許：

在相關的目錄是不允許任意讀取或更改，管理者可以將所要保護的目錄設定在保護項目中，當有惡意使用者意圖存取未開放目錄時,DragonSoft Web Protector 就會阻絕惡意的存取動作，防止重要資料外洩。

關鍵字串過濾：

設定 Web Server 在接收到像是 C:\WINNT\system32\cmd.exe 中的 cmd.exe 會造成傷害的程式時，只要接收到的請求中含有這類的指令時，DragonSoft Web Protector 便會將它過濾掉。

ShellCode 保護：

設定在多種語言 Web Server 環境中，Web Server 接收到屬於高位元(High-Bit)和編譯程式請求會造成傷害，在 DragonSoft Web Protector 設定將含有高位元(High-Bit)和編譯程式的資料過濾掉。

開拓保護：

這是設定當接收到多種的連線測試 Web Server 弱點，去進行過濾，避免因 Web Server 所存在的已知弱點和未知弱點遭到攻擊。

SQL Injection 過濾：

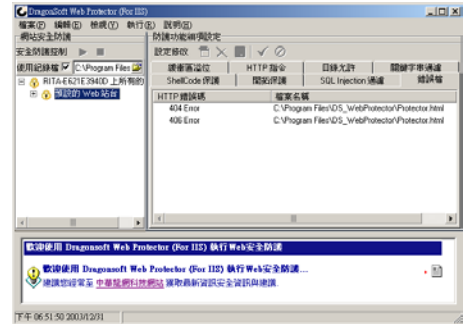
當 Web Server 接收到含有對資料庫進行攻擊的指令,而導致資料庫資料的外洩與其它可能的損害，在 DragonSoft Web Protector 設定將含有各種 SQL 指令請求過濾。

錯誤訊息：

管理者可自行設定當 Web Server 接受到攻擊訊息時，在攻擊者的瀏覽器所顯示的警示訊息。

Web Protector 簡易設定功能：

採取了列表勾選的方式，一分設定十分的保障。

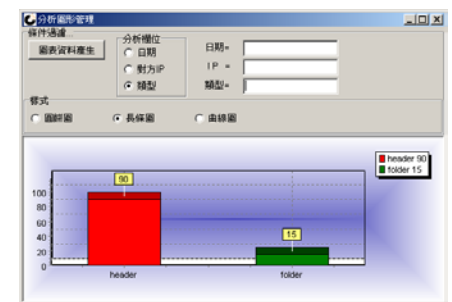


Web Protector 紀錄與分析功能：

Web Protector 將所阻擋的攻擊逐一寫入紀錄檔，管理者可依照『日期』、『IP』、『攻擊類型』等方式進行統計及分析。

Web Protector 多元化圖形比對分析：

具備長條圖、圓餅圖、曲線圖等圖形化之統計分析，有效的了解 Web Server 防護狀況。



Web Protector 多元報表輸出分析：

Web Protector 採取多元方式選取報表資料，再依個人需求方式輸出呈現，清楚的了解與分析 Web Server 狀態。