6780 Pittsford-Palmyra Rd.,
Fairport, NY 14450
585.425.2260
jthon@xdefenders.com
www.xdefenders.com

*App*Defender …*protecting your DMZ and web applications from attacks*

Business Problem:

Companies that deploy web-based applications and accept client information over the Internet are vulnerable to many exploits. Client-based (browser) software can't be trusted. Anyone can change data that is received from the web application and send back a command that could cause the application to misbehave or worse, open up the machine on system to more devious attacks.

The very nature of web applications – their ability to collate, process, and disseminate information over the Internet, exposes them in at least two ways. First, **they have total exposure by nature of being Internet accessible**. This makes security through obscurity impossible and heightens the requirement for hardened code. Second, and most critically from a penetration testing perspective, they process data elements from within HTTP requests – a protocol that can employ a myriad of encoding and encapsulation techniques – or **Vulnerabilites!**

Most web application environments including ASP and PHP, expose data elements to the developer in a manner that fails to identify how they were captured and hence what kind of validation and sanity checking should apply to them. Because the web "environment" is so diverse, and contains so many forms of programmatic content, input validation and sanity checking is the key to web applications security. This involves both identifying and enforcing the valid domain of every user-definable data element, as well as a sufficient understanding of the source of all data elements to determine what is potentially user definable.

Application security is a constant struggle to maintain balance between functional requirements and business drivers, deadlines, and limited resources. Smart security measures should not disrupt the development or performance of your applications – they should streamline them.

xDefenders offers (2) solutions; a **Security Appliance** and a **Professional Testing Service** to address the issue of web application security.

***App*Defender Appliance:**

As a hardened Linux WebFirewall appliance, ***App*Defender** provides network isolation, address translation (NAT) and HTTPS to HTTP conversion. This **Reverse Proxy** provides a *physical layer of security* in front of vulnerable, typically Microsoft-based, Web Applications. This Proxy can inspect and stop invalid or malicious web traffic. Additionally, the AppDefender can provide load balancing among multiple web servers, being a single point of access-control. There are overall performance advantages of this solution because the appliance does caching, handles SSL and compresses outbound traffic, and frees up web server resources. Our **IDS** (*Net*Defender) can co-exist with *App*Defender, to provide real-time alert notification and forensics database of activity on the DMZ.

Hardware Platforms:

Choices include*: Small*, *Medium* and *Large*-size Appliances from HP. They range from 1-2 CPU, up to 4 GB memory, very large disk storage, multiple NIC's and CD. They are rack-mountable appliances.

Professional Testing Service:

xDefenders, with its extensive experience in software application development, utilizing secure software principles, provides a web application testing service, too. This service will help a company determine if its Internet-facing applications are safe from the many exploits that are being deployed by unscrupulous persons from the privacy of their homes or offices. This service can help a company that is contemplating a new application. We can help your in-house *Software Quality Assurance (SQA)* group with extensive security testing.

"Discovery" Phase, includes:

a) Evaluation of the design and architecture of your applications.

b) We will analyze the existing web application environment, such as application servers, web servers, and databases.

c) We will run tools that will fingerprint TCP/ICMP and services available on the web server. We will also *"crawl"* the website

"Penetration" Phase includes the following 'Black and White Box' techniques:

a) Exploitation of Server and Client software

b) Buffer overflow attacks, Root-kit installation attacks

c) Use of automated tools to uncover popular exploits such as Cross-Site Scripting, Cookie Poisoning, any many other

a) Use of source code analyzers

"Report" Phase - findings, recommendations and remediation is delivered.

For more information call (585) 425-2260 or email jthon@xdefenders.com