

Web**S**niper



Stand out in a crowd
Our innovations are your best solutions

Web Application Firewalls (WAF) represents a new breed of information security technology that is designed to protect web sites (web applications) from attacks. WAF solutions are capable of preventing attacks that network firewalls and intrusion detection systems can't. They also do not require modification of the application source code.

As part of the IOP package of BugSec, WebSniper is a Web Application Firewall which prevents the possibility of exposure on web servers – such as SQL Injections, Buffer Overflows, Path Traversal, Cross Site Scripting, etc.

WebSniper identifies and monitors the requests sent by the user via the Internet, and distinguishes between the legitimate requests that are approved, and the illegitimate requests that are interpreted as attempted attacks, and which will be blocked before they arrive at the organization's Web server.

The product's innovative features enable:

- Monitoring mode
- Blocking mode
- Monitoring & Blocking mode
- Remove the attack instead of blocking it
- Modifying the responses returned from the web server to prevent information leakage
- Client side protection by un-saving cache and cookies of login details such as sessions on clients PC's



Web**S**niper

By implementing appropriate identification and blocking mechanisms. The identification is performed via signatures of known attacks and "behavioral patterns" of unknown attacks, enabling to block them while managing alerts to the organization's Information Security Center/Manager.

WebSniper's features enable the Information Security Department to manage the definitions of the WebSniper installed on the web servers in a controlled manner, and to determine rules in accordance with the organization's policy; rules that will enable to prevent such or other exposures according to a scale of severity, or based on procedures that have been predefined by the organization.



Protecting from old and new attacks:

- Brute force
- Directory indexing
- Format string attack
- Insufficient anti-automation
- Path traversal
- SQL injection
- Cross site scripting
- XPath injection
- SSI injection
- HTTP response splitting
- LDAP injection
- Session fixation
- Buffer overflow
- Unicode
- Information leakage
- OS Commanding
- Format string attack
- Predictable resource location
- Denial of service

Additionally:

- Quick, easy assimilation
- A significantly lower cost than that of competitors' information security products
- Complete statistics and the presentation of data in a broad range of cross-sections
- A user-friendly interface
- A central data base for administering several servers

Our advantages over competitors:

- Lower price (Hardware or Software solution)
- Fast & easy installation
- Approaching to all customers size
- Effectively handles client-side security
- Removing the attack instead of blocking it



For further information, please contact us: