# MANAGED VULNERABILITY SCANNING

## Web Application Security

### About SensePost

SensePost is an independent and objective organisation specialising in information security consulting, training, security assessment services and IT Vulnerability Management.

SensePost is about security. Specifically - information security. Even more specifically - measuring information security.

We've made it our mission to develop a set of competencies and services that provide our customers with insight into the security posture of their information and information systems.

### Why SensePost

Over more than a decade in service to the biggest and best organisations in the world, SensePost has built a reputation based on trust. Trust our integrity and objectivity, and trust that we will provide the highest available level of technical expertise.

### Contact Us


**Web**: www.sensepost.com

**Tel**: +27 12 460 0880

**Fax**: +27 12 460 0885

**Mail**: info@sensepost.com

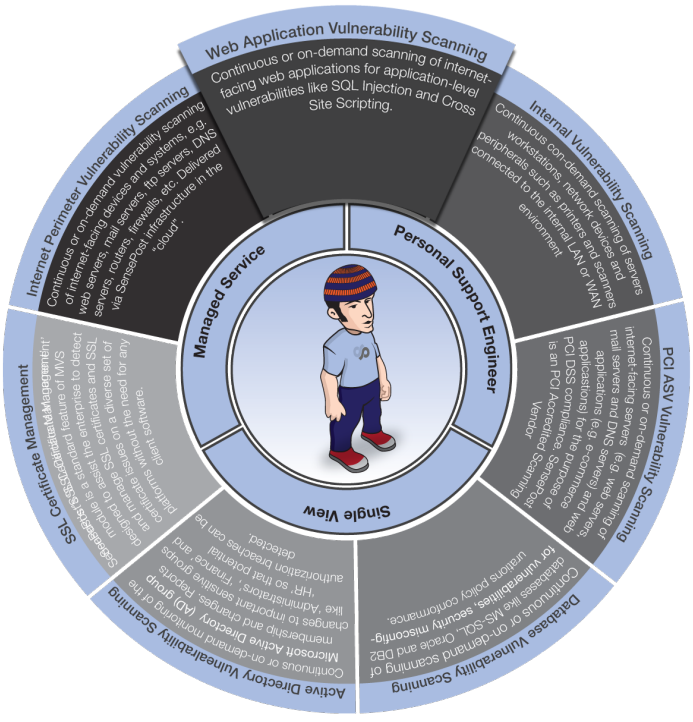

### Introduction

SensePost Managed Vulnerability Scanning (MVS) is a fully Managed Vulnerability Scanning service supported by SensePost and designed for the enterprise. Requiring no client software and accessible from any location via a powerful and easy-to-use web interface, MVS deploys a collection of specialised scanners to discover and analyse vulnerabilities across all the different components of a network.

Many corporations, large and small maintain a large number of web sites on the Internet. Most of these have been created using some form of data-driven back-end and therefore really fall more into the realm of 'application' than 'website'. Web-based applications, written in Java, Python, ASP.NET, etc., have revolutionised the way we do business. Flexible and easily developed, such applications allow business to reach their users and customers wherever they are. However, such convenience comes at a price. Web-based applications represent both an attractive and a convenient target for attack and, because many applications also connect to key business systems, a compromised application can often have extremely serious implications.

As such sites are often already in production, there is no opportunity to address the issue during development, and so a requirement for post-production vulnerability assessment starts to emerge.

SensePost MVS offers a continuous Web Application Vulnerability Scanning service, aimed at companies with multiple and distributed web application implementations. The service provides continuous Web Application Vulnerability management that subjects all target applications to regular, repeated application vulnerability scans that are designed to find high impact, easily overlooked vulnerabilities that can be leveraged by malicious automated applications such as worms, or batched and unfocused attacks.



# MANAGED VULNERABILITY SCANNING

## Web Application Security

**Features and Benefits**

- Automatically and continuously detects and reports potentially damaging Web Application vulnerabilities in any Internet-facing sites and applications;
- Fulfils the requirement for Web Application Vulnerability Management for the Payment Card Industry (PCI) Data Security Standards (DSS);
- Fulfils the requirement for PCI Approved Scanning Vendor (ASV) quarterly scanning as prescribed by the PCI DSS;
- Provides a single complete and comprehensive view of the enterprise vulnerability posture from inside and outside, for both Vulnerability Management and PCI compliance purposes;
- A fully managed service, requiring no installation, configuration, or maintenance. No in-house security skills or experience are required;
- Full business-hours support by experienced security consultants, penetration testers and programmers, with additional support available on request;
- Personalised reports in the form of dashboards can be presented to specific groups and users according to their role in the Vulnerability Management process;
- A powerful drill-down feature allows for quick and easy access to very detailed security information or high-level management metrics;
- Automatic tagging and inventory of hosts enables easy and automatic classification for searching and reporting into groups, according to function, location, sensitivity or other attributes; and
- Multiple report formats allow for easy integration and distribution of vulnerability and remediation information.

**Automated Web Application Vulnerability Assessment**

SensePost MVS provides supervised automated Web Application scans consisting of vulnerability checks, grouped into classes as prescribed by Web Application Security Consortium (WASC). The classes consists of:

**Command Execution**

- Buffer Overflow;
- Format String Attack;
- LDAP Injection;
- OS Commanding;
- SQL Injection;
- SSI Injection; and
- XPath Injection.

**Information Disclosure**

- Directory Indexing;

- Information Leakage;
- Path Traversal; and
- Predictable Resource Location.

**Client-Side**

- Content Spoofing;
- Cross-site Scripting (XSS); and
- HTTP Response Splitting.

Scans run automatically without client intervention and fully customised reports can be viewed via a web interface or delivered automatically via email.

**Powerful, Flexible Reports**

Each user on the system has a unique dashboard customised for their role within the Vulnerability Management Process. Dashboards can consist of any number of widgets, called 'Blizzards', which can easily be added or customised. Examples of standard Blizzards include:

- Important new issues discovered since the previous scan;
- Most critical hosts and applications;
- Most critical security issues;
- Trends of total issues, new issues and unresolved issues;
- Summary of application frameworks (e.g. Joomla, Wordpress, etc);
- Summary of applications with login forms and applications run on secure (SSL) channels; and
- Web Application security issues affecting PCI compliance.

Pre-configured templates allow for role-specific dashboards with the relevant widgets to be easily assigned to specific users.

# Web Application Security

## Differentiators

- A fully Managed Service. No installation, configuration or maintenance required;
- Each client is assigned a Personal Support Engineer who is an experienced security analyst and penetration tester;
- Provides a comprehensive overview of enterprise risk posture with specific dashboards for specific users and groups;
- Over 50 specialised report widgets are available to each user. New widgets, dashboards and tests can be seamlessly added;
- Highly configurable and customisable via your Personal Support Engineer to meet individual requirements; and
- Unlimited users. Unlimited scanning.

## Screenshots

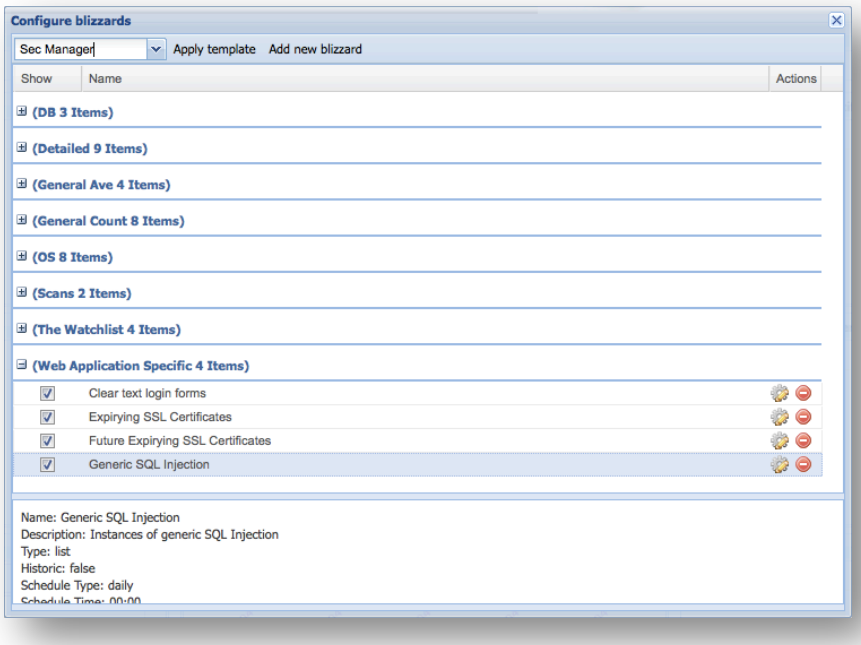



Figure 1 Adding WebApp Blizzards to a user desktop

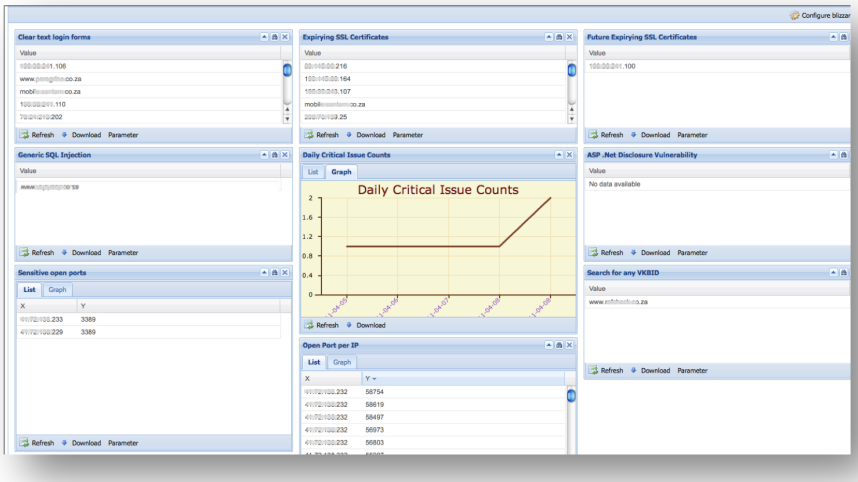



Figure 2 A custom Web Application desktop

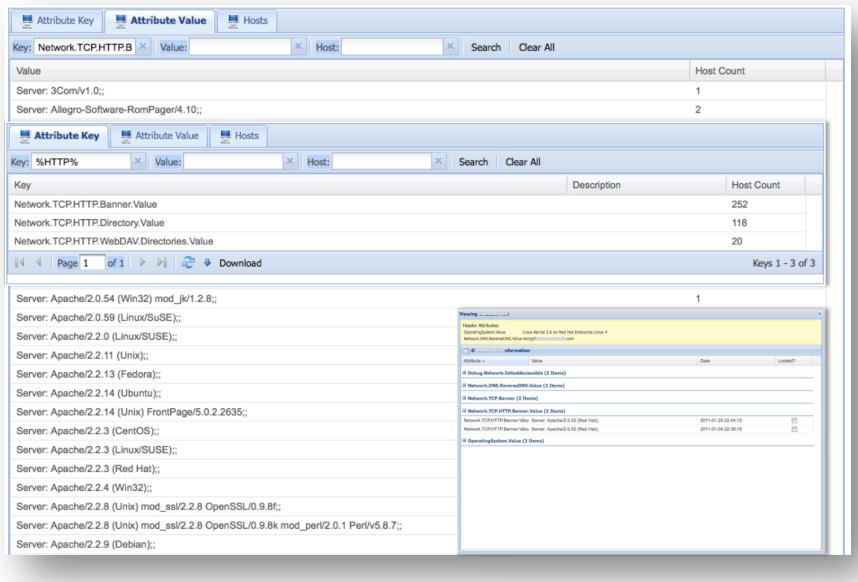



Figure 3 Querying Web Server Attributes

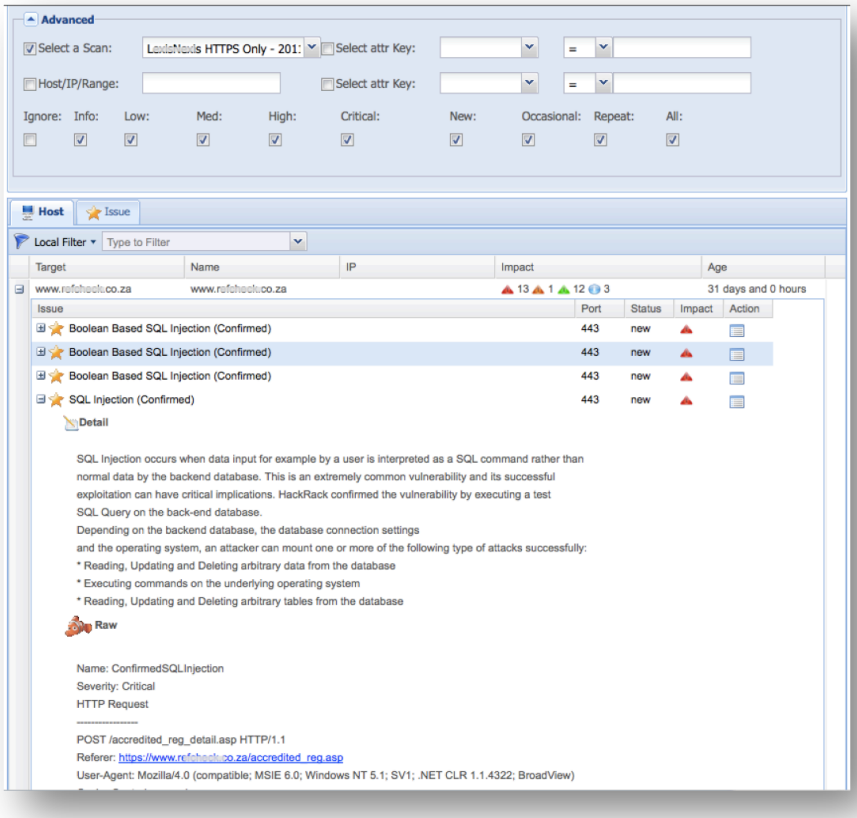



Figure 4 Web Application Vulnerability Report

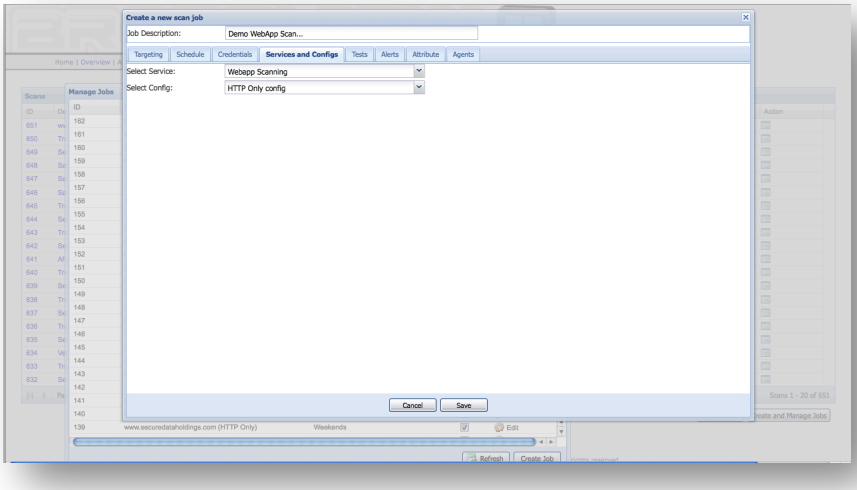



Figure 5 Configuring a Web Application Vulnerability Scan