

## TRIPWIRE WEBAPP360 HIGHLIGHTS

- ◆ Continuous, real-time assessment of web applications in production environments
- ◆ Leverages Tripwire's appliance-based architecture, eliminating the high cost of deployment associated with software-based solutions
- ◆ Licensed to support unlimited users, eliminating a common frustration among enterprise customers of standalone web application scanners

# TRIPWIRE WEBAPP360

## ENTERPRISE WEB APPLICATION SCANNING FOR PRODUCTION ENVIRONMENTS

Online systems such banking, health-care, e-commerce, and customer support portals increasingly collect and provide access to extremely sensitive data and internal systems that need to be protected, and all are internet-facing web applications—the primary target of opportunistic hackers.

Over the past several years, web application vulnerabilities such as Cross-Site Scripting (XSS) and SQL Injection attacks have made up an increasing percentage of newly discovered vulnerabilities and actual reported intrusions. Enterprises have struggled to find solutions that take into account not only the web applications themselves but also the underlying operating systems, databases and other IT infrastructure. Enterprises also require scalability and manageability to support their production systems across their large networks. Tripwire® WebApp360 is the solution, providing a highly scalable, easily managed solution that is designed to test production web applications and their underlying infrastructure.

### TRIPWIRE WEBAPP360 DELIVERS:

- » Complete web application infrastructure assessment, including web applications, underlying operating systems, and adjacent applications in production environments

- » Comprehensive security risk analysis, combining web application coverage with network, operating system, and infrastructure exposure intelligence
- » Leverages Tripwire's appliance-based architecture, eliminating the high cost of deployment and maintenance associated with other solutions
- » Fully integrated with Tripwire IP360, Tripwire Focus and Tripwire Suite360 Intelligence Hub to provide customers with unprecedented visibility into their overall IT security risks

Built on the world's leading security risk management system, Tripwire IP360, Tripwire WebApp360 is uniquely designed to address the needs of global enterprises. It provides a fully integrated and comprehensive view of all vulnerabilities and risks—from web applications to the IT systems supporting them. Leveraging Tripwire IP360's appliance-based architecture, Tripwire WebApp360 is a true enterprise solution that cost-effectively deploys and scales to enterprises of all sizes and complexity.

When combined with Tripwire IP360, Tripwire Configuration Compliance Manager and Tripwire Suite360 Intelligence Hub, enterprises can now have a fully integrated, highly scalable and manageable solution for security risk and compliance management. Enterprises can finally obtain a single

solution that leads to unprecedented visibility and management of IT risk and compliance.

## ADDITIONAL BENEFITS

- » Normalized risk scoring using Tripwire's unified risk metric and CVSS v2
- » Granular role-based access controls enable re-use of existing Tripwire IP360 roles and creation of new roles specific to management of web properties
- » Support for HTTP virtual hosts provides assessment of multiple web sites hosted on a single server

## SAMPLE VULNERABILITY CHECKS

### » Cross-Site Scripting (XSS)

Vulnerabilities Cross-Site Scripting vulnerabilities allow attackers to inject arbitrary HTML or other code into web applications and their served web pages, potentially compromising the security of a visiting client's browser. Tripwire WebApp360 uses dynamic testing for various types of persistent and non-persistent Cross-Site Scripting vulnerabilities to ensure that your web applications are not compromised.

### » Injection Vulnerability SQL

Injection vulnerabilities allow attackers to inject SQL commands through web pages, making changes to stored data or executing commands that were not intended by the application's developers. Tripwire WebApp360 ensures that your web application will not permit code execution or changes to stored data without appropriate authorization.

The screenshot shows the Tripwire WebApp360 interface. At the top, there is a 'Host Properties' section with fields like Network, Web Applications, IP Address, NetBios Name, Asset Value, and Operating System. Below this is a 'Host Composite' section titled 'Vulnerabilities' with a table showing various security issues and their last scan dates. The table includes rows for Numeric Cross-Site Script (XSS) Vulnerability, Apache HTDigest Realm Command Line Argument Buffer Overflow Vulnerability, Apache 'mod\_proxy\_ftp' Undefined Charset UTF-7 Cross-Site Scripting Vulnerability, OpenSSH Duplicated Block Remote Denial of Service Vulnerability, Apache HTTP Server 'mod\_status' Cross-Site Scripting Vulnerability, Basic SQL Injection Vulnerability, and HTML Tag Insertion Vulnerability. The last scan dates for these items range from 2012-03-12 to 2012-03-13. At the bottom of the interface, there is a large list of additional vulnerabilities with their corresponding last scan dates.

Vulnerabilities	Last Scan
Numeric Cross-Site Script (XSS) Vulnerability	2012-03-12
Apache HTDigest Realm Command Line Argument Buffer Overflow Vulnerability	2012-03-12
Apache 'mod_proxy_ftp' Undefined Charset UTF-7 Cross-Site Scripting Vulnerability	2012-03-12
OpenSSH Duplicated Block Remote Denial of Service Vulnerability	2012-03-12
Apache HTTP Server 'mod_status' Cross-Site Scripting Vulnerability	2012-03-12
Basic SQL Injection Vulnerability	2012-03-12
HTML Tag Insertion Vulnerability	2012-03-12

Vulnerabilities	Last Scan
Windows Best Practices (Windows Default Configuration) Vulnerability	2012-03-13
Microsoft IIS 7.0, Oracle Forms Vulnerability	2012-03-13
Numeric Cross-Site Scripting (XSS) Vulnerability	2012-03-13
PortMapper Available	2012-03-13
PortMapper RPC Listener	2012-03-13
RPC Listen Available	2012-03-13
Self-Signed TLS/SSL Certificate Present	2012-03-13
SSH Protocol Available	2012-03-13
SSL Server Supports Weak Encryption	2012-03-13
SSL/TLS Certificate Common Name Mismatch	2012-03-13
Sun Java Library Available	2012-03-13
URL Injections Vulnerability	2012-03-13
Web Server HTTP TRACE Method Supported	2012-03-13

◆ FIG. 1 Tripwire WebApp360 reports and analytics provide a comprehensive view of IT security risk.

### » Web Page Implementation Flaws

Securing the production implementation of your web applications is just as important as the web application code itself. Tripwire WebApp360 ensures that fundamental design flaws have not been introduced to your web applications during production implementation, such as password submissions via insecure input fields.

### » Web Application Infrastructure

Web application security must take into account the web application itself as well as the underlying infrastructure such as web servers, operating systems, and adjacent applications. Tripwire WebApp360 is the only solution that provides a real time, continuous security assessment of both web applications and their related infrastructure.

*"With WebApp360, (Tripwire) enhances the value of their enterprise-wide risk assessment to include on-going production scanning of these critical web-based applications, complementing the penetration testing that may have been done during development and enabling their ongoing security."*

**PETER CHRISTY, PRINCIPAL, INTERNET RESEARCH GROUP**



◆ Tripwire is a leading global provider of risk-based security and compliance management solutions that enable organizations to effectively connect security to the business. Tripwire delivers foundational security controls like security configuration management, file integrity monitoring, log and event management, vulnerability management, and security business intelligence with performance reporting and visualization. ◆

LEARN MORE AT [WWW.TRIPWIRE.COM](http://WWW.TRIPWIRE.COM) OR FOLLOW US @TRIPWIREINC ON TWITTER.