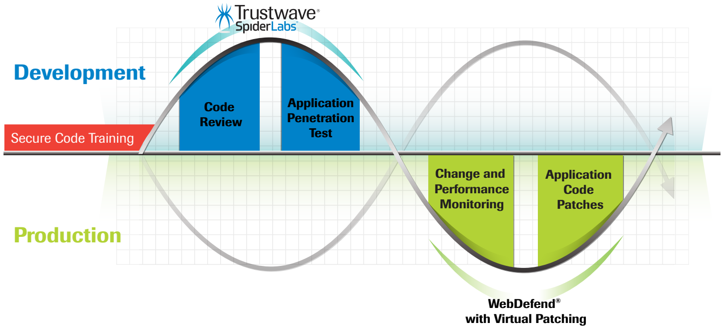
Trustwave®

360 Application Security

Poorly coded applications put your organization at risk. As more organizations develop applications to streamline internal processes and improve customer experiences, large amounts of unprotected, confidential information are left within the application layer. Without security at the core of the software development life cycle (SDLC) you put your data, operations and customer satisfaction at risk.

Trustwave's 360 Application Security program ensures security is at the very foundation of software development and ongoing operations. By taking a holistic approach, our application security life cycle support greatly enhances your ability to produce and manage stable, secure applications. The program is also part of our unique, unified security approach that allows layered security products to share intelligence and events that uncover threats that single, point products miss.



The 360 Application Security program delivers the following key offerings:

Secure Development Training

- Online
- Instructor-Led

Services

- Application Code Review
- Application Penetration Testing

Web Application Firewall

- On Premise Appliance
- Managed Service
- ModSecurity Open Source Rules and Support

The program is customized to your organization and can be used in conjunction with all major software development methodologies (e.g., Agile, RAD, Waterfall, Spiral, Microsoft and others).

Key Benefits

Defend applications from cyber threats with Trustwave's holistic application security program.

Build More Secure Applications.
We educate your developers on the latest best practices for secure application development with expert-led online and classroom training.

Reduce Application Vulnerabilities.
Our holistic application security life cycle approach reduces vulnerabilities from design to production, resulting in stable and secure applications.

Flexible Application Protection
We offer flexible delivery options — online, onsite, on premise or managed — helping you improve your application security posture across your entire business.

Secure Development Training

Online Training

Recommended as a prerequisite to our instructor-led training, our comprehensive, online training teaches your application developers about application security in the design, code and testing phases – with over (30) classes available today.

Instructor-Led Training

We provide customized training for your developers, taught worldwide, including at OWASP™ conferences and onsite at your location.

Specific examples from application penetration tests and code reviews conducted as part of the 360 Application Security program can be included within the training class, allowing your staff to learn from real-world, business-relevant coding problems to immediately put their knowledge to use.

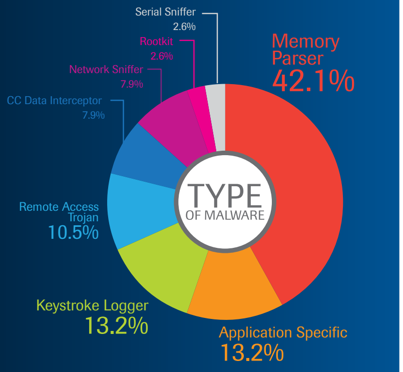
Services

Application Code Review

Custom applications require custom security. During the Trustwave application code review, SpiderLabs application security experts manually inspect all relevant application source code to:

- Pinpoint deficiencies in security controls, line by line
- Identify development errors that lead to vulnerabilities and violate best practices
- Evaluate the tools and commercial applications used to create and run the front-end and back-end services

Application-specific malware ranks as the second most frequented targeted attack found in investigations – targeting sensitive data in memory, storage or by tricking the application to pass the data directly to the malware during processing.



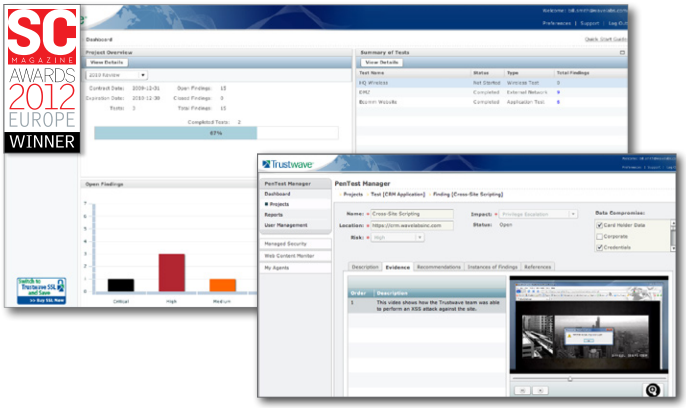
Source: Trustwave 2012 Global Security Report

At the completion of the review, your team receives an extensive report detailing areas that should be considered to maintain a secure system. We ensure your developers receive actionable, instructive information specific to the application rather than generic information provided by automated tools.

Application Penetration Testing

Performed by SpiderLabs' security experts, our Application Penetration Testing provides human driven attack sequences to determine the effectiveness of its security controls and tests an application from a variety of authenticated and unauthenticated user perspectives to highlight the risks posed by exploitable vulnerabilities.

Results are delivered via our award-winning PenTest Manager, which provides rich evidence of each identified vulnerability – with step-by-step screenshots and video as each vulnerability is exploited. In addition, PenTest Manager offers detailed reporting, remediation tracking and test scheduling.



Dashboard

Project Overview

2010 Review

Contract Date: 2009-12-31 Open Findings: 15
Expiration Date: 2010-12-30 Closed Findings: 0
Tests: 3 Total Findings: 15
Completed Tests: 2
67%

Summary of Tests

Test Name	Status	Type	Total Findings
HQ Wireless	Not Started	Wireless Test	0
DMZ	Completed	External Network	9
Ecomm Website	Completed	Application Test	6

PenTest Manager
Projects › Test [CRM Application] › Finding [Cross-Site Scripting]

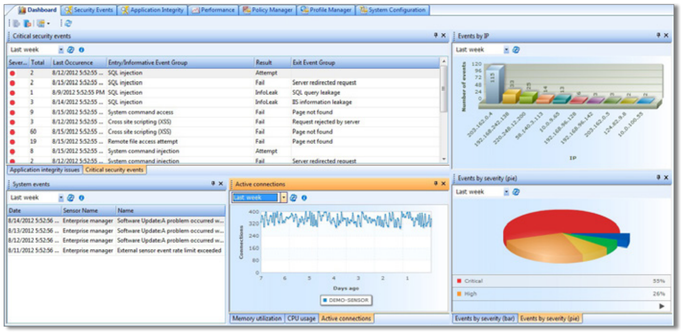
Name: * Cross-Site Scripting
Location: * https://crm.wavelabsinc.com
Risk: * High
Impact: * Privilege Escalation
Status: Open
Data Compromise:
☑ Card Holder Data
□ Corporate
☑ Credentials

Order	Description
1	This video shows how the Trustwave team was able to perform an XSS attack against the site.

PenTest Manager: Centralized Dashboard and Video Evidence Reporting

Web Application Firewall (WAF)

Our Web application firewall solutions provide operational assurance and are available as an on premise appliance, managed service or as rules and support for an open source solution– giving you full flexibility to select the platform that best meets your needs.



Sever...	Total	Last Occurence	Entry/Informative Event Group	Result	Exit Event Group
●	2	8/12/2012 5:52:55 ...	SQL injection	Attempt	
●	2	8/15/2012 5:52:55 ...	SQL injection	Fail	Server redirected request
●	1	8/9/2012 5:52:55 PM	SQL injection	InfoLeak	SQL query leakage
●	3	8/14/2012 5:52:55 ...	SQL injection	InfoLeak	IIS information leakage
●	9	8/15/2012 5:52:55 ...	System command access	Fail	Page not found
●	3	8/12/2012 5:52:55 ...	Cross site scripting (XSS)	Fail	Request rejected by server
●	60	8/15/2012 5:52:55 ...	Cross site scripting (XSS)	Fail	Page not found
●	19	8/15/2012 5:52:55 ...	Remote file access attempt	Fail	Page not found
●	8	8/15/2012 5:52:55 ...	System command injection	Attempt	
●	2	8/12/2012 5:52:55 ...	System command injection	Fail	Server redirected request

Date	Sensor Name	Name
8/14/2012 5:52:56 ...	Enterprise manager	Software Update:A problem occurred w...
8/13/2012 5:52:56 ...	Enterprise manager	Software Update:A problem occurred w...
8/12/2012 5:52:56 ...	Enterprise manager	Software Update:A problem occurred w...
8/11/2012 5:52:56 ...	Enterprise manager	External sensor event rate limit exceeded

WebDefend: Intuitive, Instructive Console

WebDefend – On Premise Appliance

WebDefend is a highly scalable, real-time WAF that offers customized, behavior-based security for each protected application and is integrated with our award-winning Trustwave SIEM, which correlates and consolidates attack information from many sources beyond Web applications. WebDefend provides virtual patching to protect your vulnerable applications from attack, without having to wait for the next release cycle. Only WebDefend uses a patent-pending profiling system and multiple, collaborative detection engines to ensure the flow of mission-critical traffic while supplying complete protection for applications to keep your confidential information safe from targeted attacks.

WebDefend – Managed Service

As a managed service, your WebDefend WAF is configured and tuned by our SpiderLabs experts who have conducted your Application Penetration Tests and Code Reviews and have intimate knowledge of your applications, ensuring the utmost protection.

ModSecurity – Open Source Rules and Support

Trustwave is the primary custodian of ModSecurity, providing the 17,000+ and growing rules set and commercial support. ModSecurity is a customizable, open source solution that supports Apache, Microsoft Internet Information Services (IIS) and Nginx. Trustwave's SpiderLabs, with a legacy of providing threat intelligence to the security community, is committed to supporting ModSecurity and its diverse and widespread user base.

Trustwave®

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations — ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers — manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide. For more information: https://www.trustwave.com.

Corporate Headquarters
70 West Madison St.
Suite 1050
Chicago, IL 60602 USA

P: 312.873.7500
F: 312.443.8028

EMEA Headquarters
Westminster Tower
3 Albert Embankment
London SE1 7SP UK

P: +44 (0) 845 456 9611
F: +44 (0) 845 456 9612

LAC Headquarters
Rua Cincinato Braga,
340 nº 71 Edificio Delta Plaza
Bairro Bela Vista - São Paulo - SP
CEP: 01333-010 - BRASIL

P: +55 (11) 4064-6101

APAC Headquarters
Level 7/Suite 3
100 Walker Street
North Sydney NSW 2060 Australia

P: +61 2 9089 8870
F: +61 2 9089 8989