Testing Solutions to Tackle Application Security Checkpoint Technologies SQGNE

Jimmie Parson– Checkpoint Technologies

Agenda

- Welcome, Introductions
- Checkpoint Technologies – Quick Corporate Overview
- Why do we need Application Security?
- High Level Discussion of HP’s Fortify and Web Inspect
- Q & A

checkpoint TECHNOLOGIES Software Quality. Assured.

Welcome and Introductions

- Thanks everyone for attending today!
  - From Checkpoint Technologies, we have…

Jimmie Parson
Sr. Technical Engineer
813-818-8324 x133 (office)
www.checkpointech.com

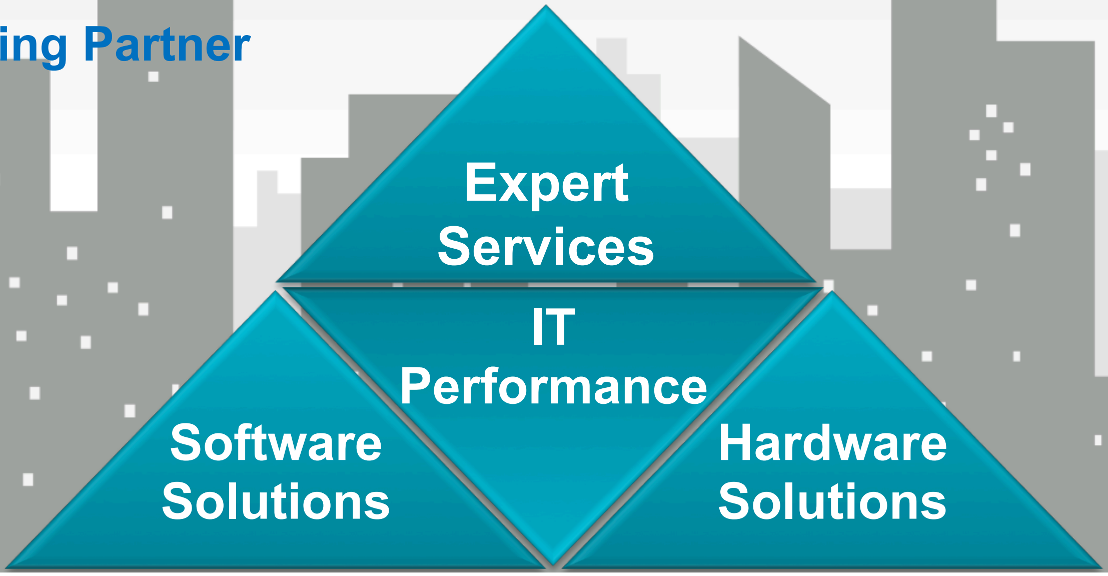
checkpoint TECHNOLOGIES Software Quality. Assured.

Checkpoint Technologies

Corporate Overview

About Checkpoint Technologies….

- ✓ Incorporated in January, 2003
- ✓ Experts in Quality Assurance, Security and Software Testing!
- ✓ HP Software Gold Partner & Authorized Training Partner
- ✓ HP Authorized Software Support Partner
- ✓ Partner of Perfecto Mobile, Mobile Labs, and Turnkey Solutions
- ✓ QAI Training Partner



Professional Services

Staff Augmentation

- Long-term contract services, on-site and remote
- QA leads, manual testers, automation experts, etc.

Consulting

- Assessment, installation, configuration, analysis, etc.
- Long-term and short-term, on-site and remote

Outsourcing

- U.S. based functional and performance testing
- Software testing performed at our test lab by expert resources

Training

- HP Authorized Training Partner
- On-site, virtual, or public
- Structured classroom format using HP materials

Mentoring

- Customized training essential to your team - in your environment
- Cost-effective $$$

Now…On to the Presentation!

Security Overview

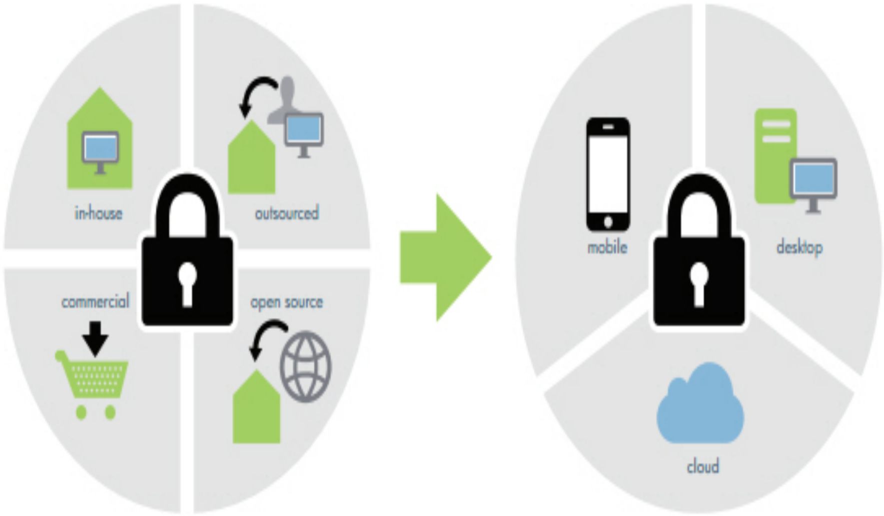
checkpoint TECHNOLOGIES Software Quality. Assured.

Why do we need Application Security?

- More and more each day, the world is embracing:
  - Online transactions, conducting research, storing information, social media
- How many of you have heard in the news (or been affected by) a data breach:
  - (Retail) LARGE Retailer – CEO Resigns (analysts forecast a total cost of approximately $1 billion)
  - (Healthcare) N.Y. Presbyterian & Columbia Medical Center – Largest HIPAA enforcement fine to date of $4.8 million due to compromised patient records
  - (Banking) First American Bank, Casino (Las Vegas Sands Corp)
- Bottom Line:
  - No industry/organization is Safe - Lose your Data, Lose

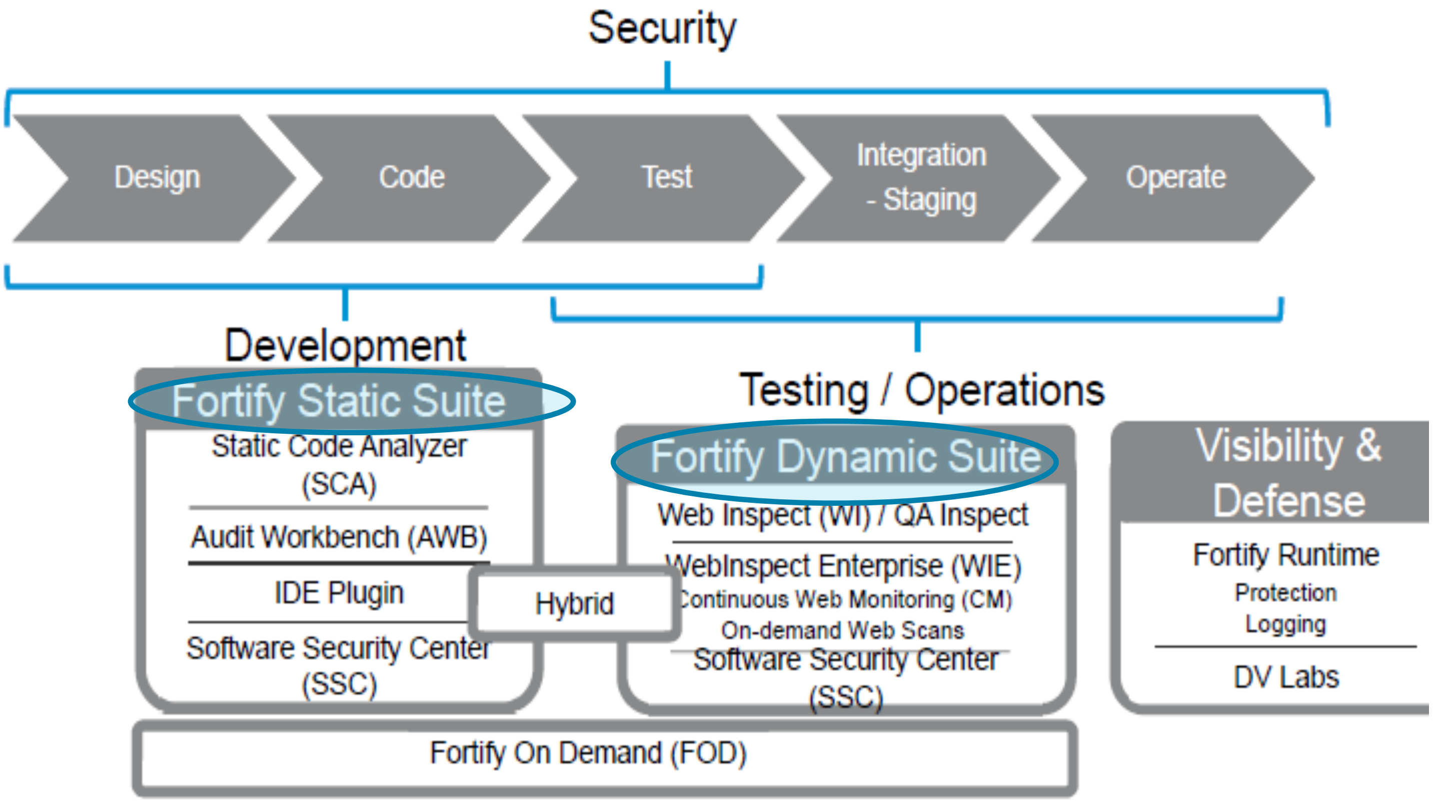
Application Security Discussion

Risk is Everywhere!



Vulnerability risks can be present in software no matter how it's created or deployed.

Software Security Assurance (SSA & SDLC)



Security

Design

Code

Test

Integration - Staging

Operate

Development

Fortify Static Suite

Static Code Analyzer (SCA)

Audit Workbench (AWB)

IDE Plugin

Software Security Center (SSC)

Hybrid

Testing / Operations

Fortify Dynamic Suite

Web Inspect (WI) / QA Inspect

WebInspect Enterprise (WIE)

Continuous Web Monitoring (CM)

On-demand Web Scans

Software Security Center (SSC)

Visibility & Defense

Fortify Runtime

Protection

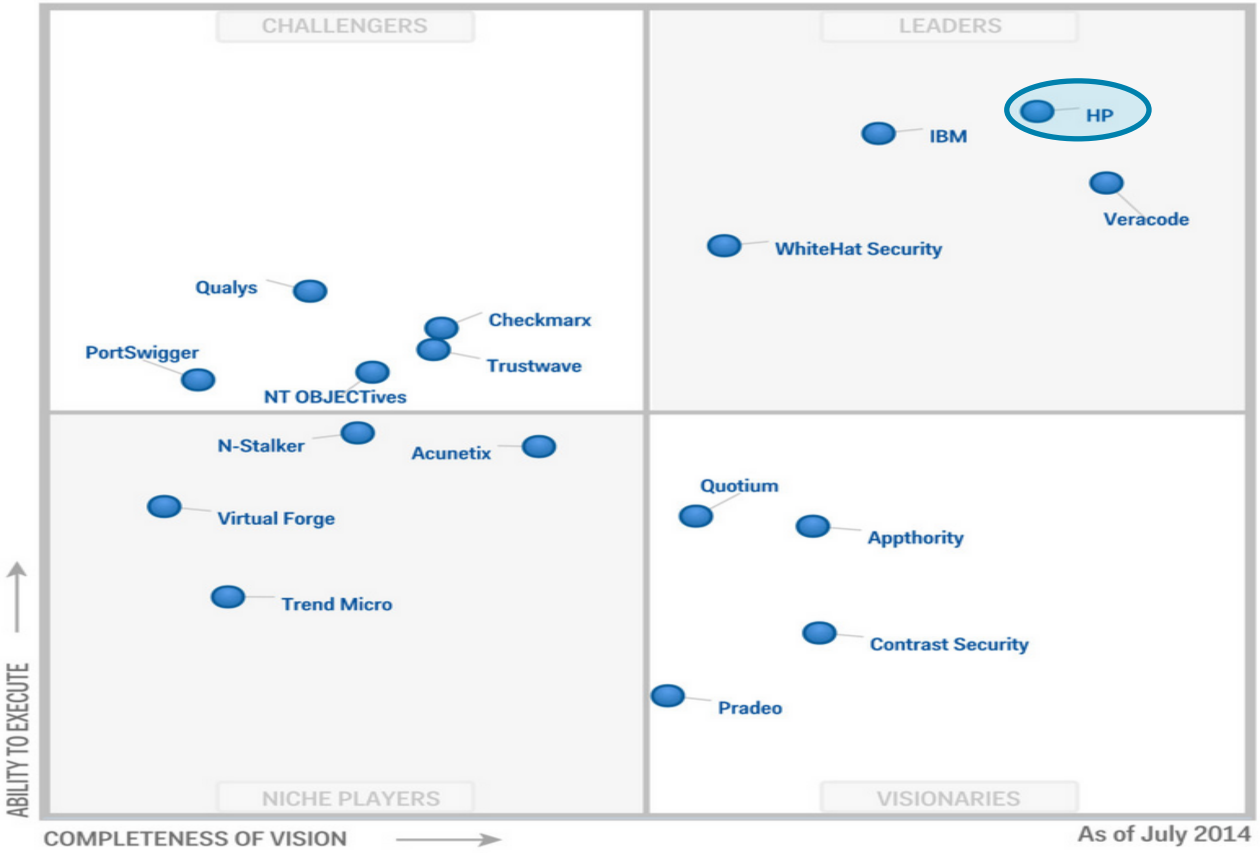
Logging

DV Labs

Fortify On Demand (FOD)

Follow the Leader!

Figure 1. Magic Quadrant for Application Security Testing



Source: Gartner (July 2014)

checkpoint
TECHNOLOGIES
Software Quality. Assured.

HP Fortify/Web Inspect Discussion

Security Testing - Key Features of Fortify

- Engage in security testing with HP’s Fortify SSC (Software Security Center)
  - Quickly gain an accurate picture of risk in your applications, no matter if they’re developed in-house or by vendors.

- Engage in Static Analysis, also known as Static Application Security Testing (SAST),

− Detects more types of potential vulnerabilities than any other detection method

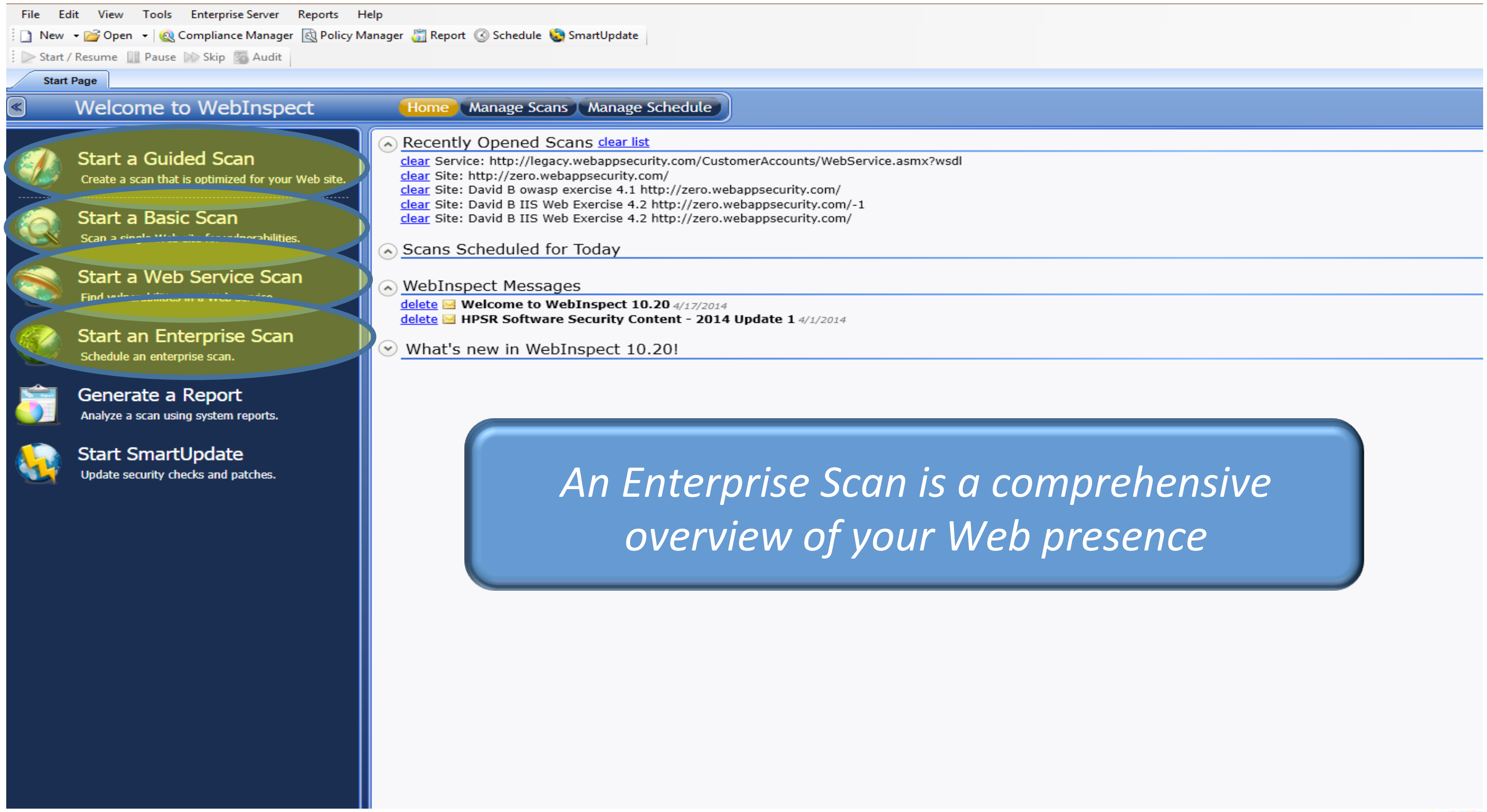
− Pinpoints the root cause of vulnerabilities with line-of-code detail

− Helps you identify critical issues during development when they are easiest and least expensive to fix

Key Features of WebInspect

- Dynamic Analysis, also known as Dynamic Application Security Testing (DAST), available from HP Web Inspect.
  - Engage in dynamic security testing for web apps from Dev thru Production
  - Automated and configurable web application security and penetration testing tool that mimics real-world hacking techniques and attacks
  - Easily manage, view and share security-test results and histories
  - Security test web APIs and web services that support your business
- Demonstrate compliance with various regulatory agencies
  - Run compliance reports for all major regulatory standards, including PCI, SOX, ISO, and HIPAA

Main WebInspect Screen



Start a Guided Scan
Create a scan that is optimized for your Web site.

Start a Basic Scan
Scan a single Web site for vulnerabilities.

Start a Web Service Scan
Find vulnerabilities in a Web service.

Start an Enterprise Scan
Schedule an enterprise scan.

Generate a Report
Analyze a scan using system reports.

Start SmartUpdate
Update security checks and patches.

Recently Opened Scans clear list

clear Service: http://legacy.webappsecurity.com/CustomerAccounts/WebService.asmx?wsdl
clear Site: http://zero.webappsecurity.com/
clear Site: David B owasp exercise 4.1 http://zero.webappsecurity.com/
clear Site: David B IIS Web Exercise 4.2 http://zero.webappsecurity.com/-1
clear Site: David B IIS Web Exercise 4.2 http://zero.webappsecurity.com/

Scans Scheduled for Today

WebInspect Messages

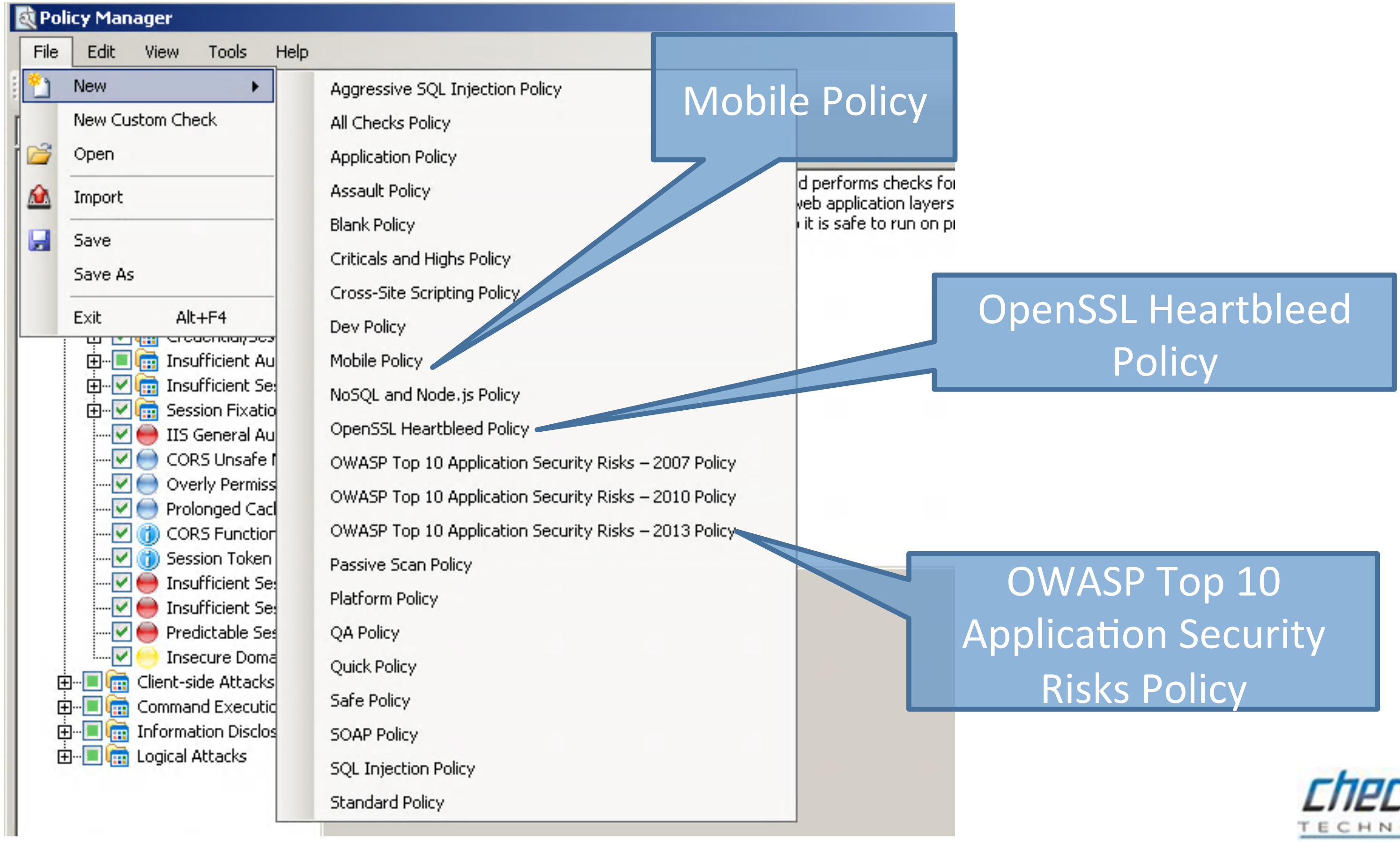
delete Welcome to WebInspect 10.20 4/17/2014
delete HPSR Software Security Content - 2014 Update 1 4/1/2014

What's new in WebInspect 10.20!

An Enterprise Scan is a comprehensive overview of your Web presence

checkpoint TECHNOLOGIES
Software Quality. Assured.

WebInspect Policy Manager

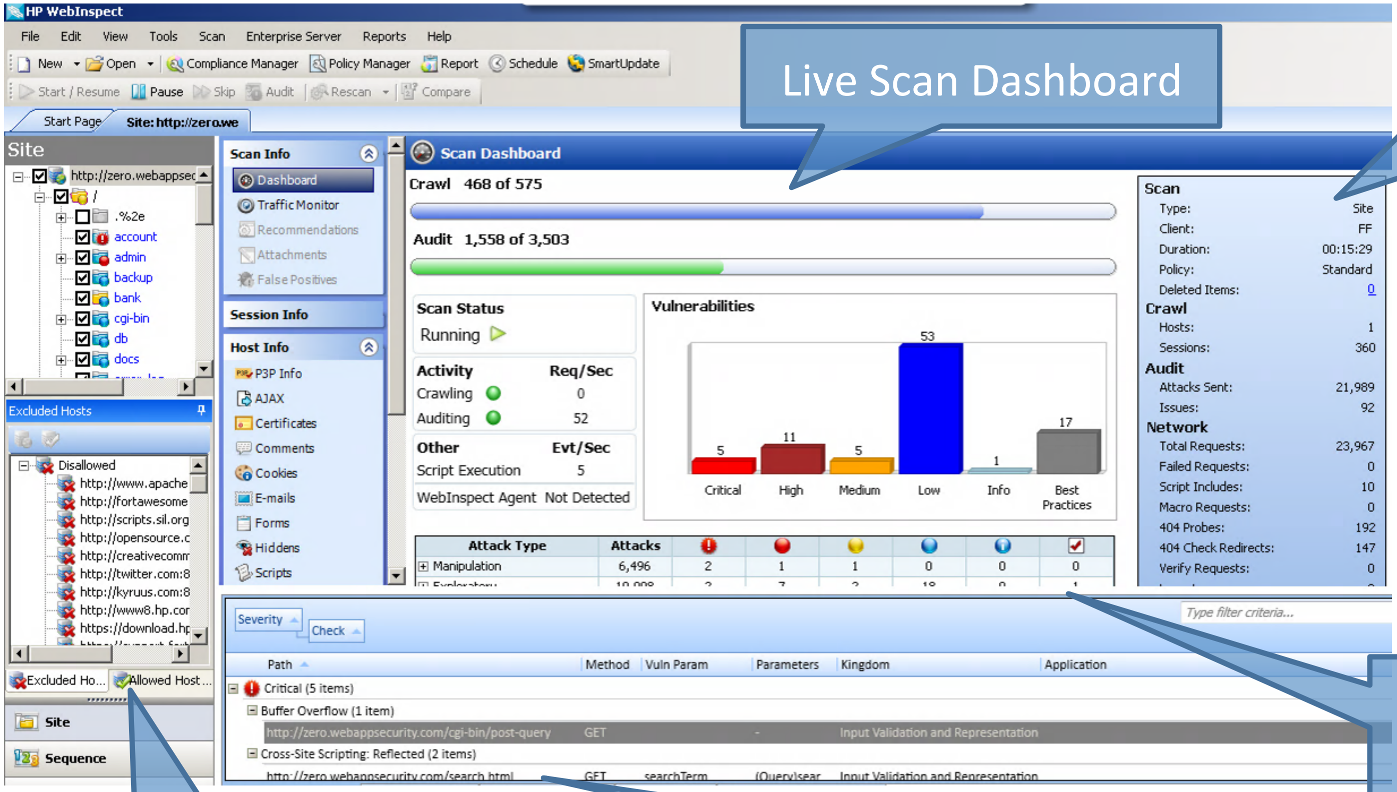


Mobile Policy

OpenSSL Heartbleed Policy

OWASP Top 10 Application Security Risks Policy

Web Inspect Live Scan Visualization



Crawl 468 of 575

Audit 1,558 of 3,503

Scan Status
Running

Activity	Req/Sec
Crawling ●	0
Auditing ●	52

Other	Evt/Sec
Script Execution	5
WebInspect Agent	Not Detected

Scan	
Type:	Site
Client:	FF
Duration:	00:15:29
Policy:	Standard
Deleted Items:	0
Crawl	
Hosts:	1
Sessions:	360
Audit	
Attacks Sent:	21,989
Issues:	92
Network	
Total Requests:	23,967
Failed Requests:	0
Script Includes:	10
Macro Requests:	0
404 Probes:	192
404 Check Redirects:	147
Verify Requests:	0

Attack Type	Attacks	●	●	●	●	●	✓
⊞ Manipulation	6,496	2	1	1	0	0	0
⊞ Exploratory	10,998	2	7	2	18	0	1

Path	Method	Vuln Param	Parameters	Kingdom	Application
⊟ Critical (5 items)					
⊟ Buffer Overflow (1 item)					
http://zero.webappsecurity.com/cgi-bin/post-query	GET		-	Input Validation and Representation	
⊟ Cross-Site Scripting: Reflected (2 items)					
http://zero.webappsecurity.com/search.html	GET	searchTerm	(Query)sear	Input Validation and Representation	

Live Scan Dashboard

Live Scan Statistics

Detailed Attack Table

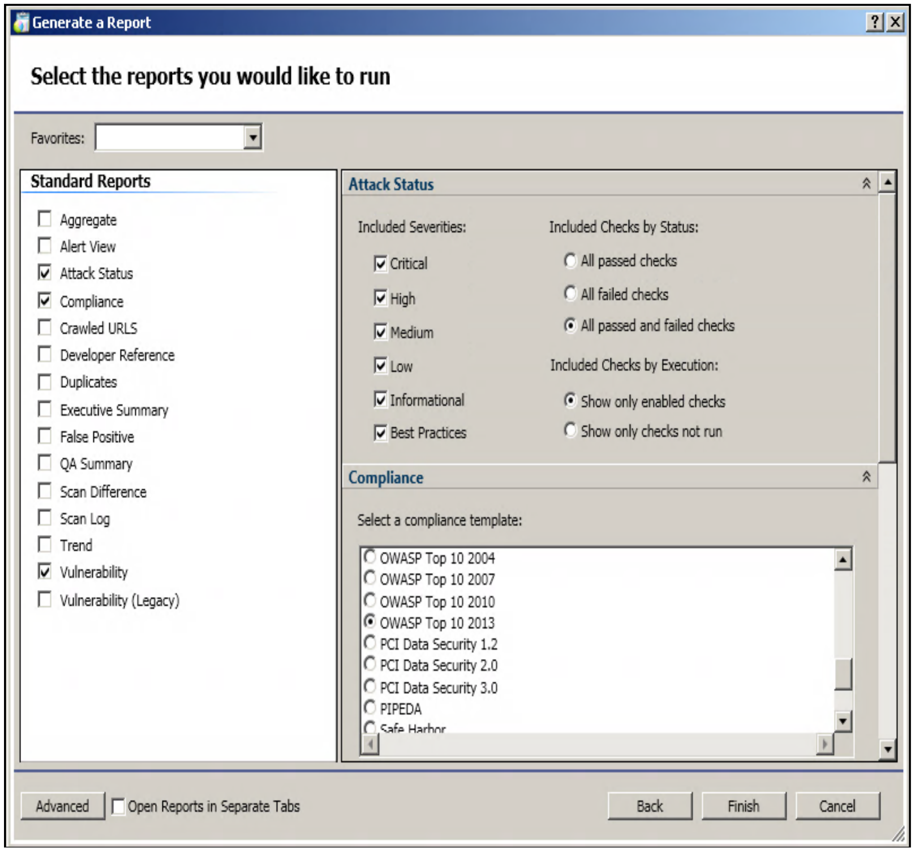
Excluded & Allowed Hosts

Vulnerabilities Found in Application

checkpoint
TECHNOLOGIES
Software Quality. Assured

Generating Reports

The WebInspect Report Wizard allows you to easily select the report types and detail you want included in your reports…



Generate a Report

Select the reports you would like to run

Favorites:

Standard Reports

- ☐ Aggregate
- ☐ Alert View
- ☑ Attack Status
- ☑ Compliance
- ☐ Crawled URLS
- ☐ Developer Reference
- ☐ Duplicates
- ☐ Executive Summary
- ☐ False Positive
- ☐ QA Summary
- ☐ Scan Difference
- ☐ Scan Log
- ☐ Trend
- ☑ Vulnerability
- ☐ Vulnerability (Legacy)

Attack Status

Included Severities:

- ☑ Critical
- ☑ High
- ☑ Medium
- ☑ Low
- ☑ Informational
- ☑ Best Practices

Included Checks by Status:

- ○ All passed checks
- ○ All failed checks
- ● All passed and failed checks

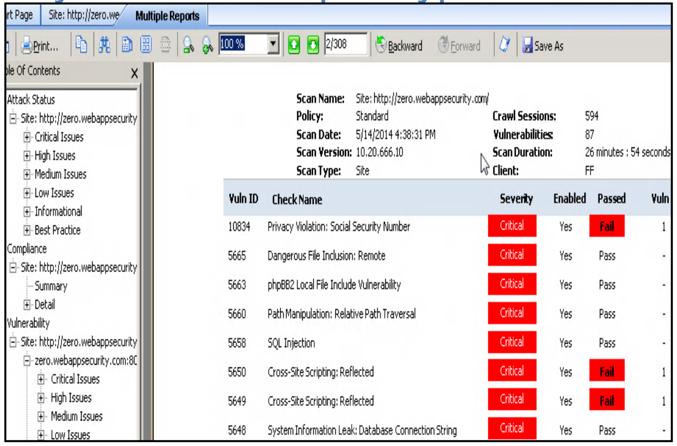
Included Checks by Execution:

- ● Show only enabled checks
- ○ Show only checks not run

Compliance

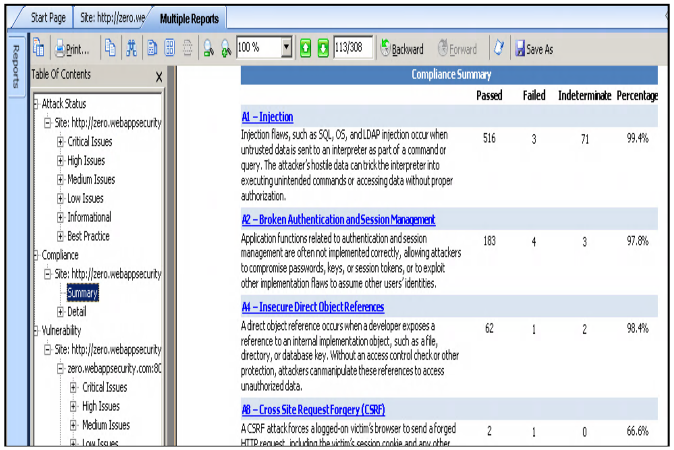
Select a compliance template:

- ○ OWASP Top 10 2004
- ○ OWASP Top 10 2007
- ○ OWASP Top 10 2010
- ● OWASP Top 10 2013
- ○ PCI Data Security 1.2
- ○ PCI Data Security 2.0
- ○ PCI Data Security 3.0
- ○ PIPEDA
- ○ Safe Harbor



Scan Name:	Site: http://zero.webappsecurity.com/		
Policy:	Standard	**Crawl Sessions:**	594
Scan Date:	5/14/2014 4:38:31 PM	**Vulnerabilities:**	87
Scan Version:	10.20.666.10	**Scan Duration:**	26 minutes : 54 seconds
Scan Type:	Site	**Client:**	FF

Vuln ID	Check Name	Severity	Enabled	Passed	Vuln
10834	Privacy Violation: Social Security Number	Critical	Yes	Fail	1
5665	Dangerous File Inclusion: Remote	Critical	Yes	Pass	-
5663	phpBB2 Local File Include Vulnerability	Critical	Yes	Pass	-
5660	Path Manipulation: Relative Path Traversal	Critical	Yes	Pass	-
5658	SQL Injection	Critical	Yes	Pass	-
5650	Cross-Site Scripting: Reflected	Critical	Yes	Fail	1
5649	Cross-Site Scripting: Reflected	Critical	Yes	Fail	1
5648	System Information Leak: Database Connection String	Critical	Yes	Pass	-



Compliance Summary

	Passed	Failed	Indeterminate	Percentage
A1 – Injection				
Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.	516	3	71	99.4%
A2 – Broken Authentication and Session Management				
Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.	183	4	3	97.8%
A4 – Insecure Direct Object References				
A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers canmanipulate these references to access unauthorized data.	62	1	2	98.4%
A8 – Cross Site Request Forgery (CSRF)				
A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other	2	1	0	66.6%

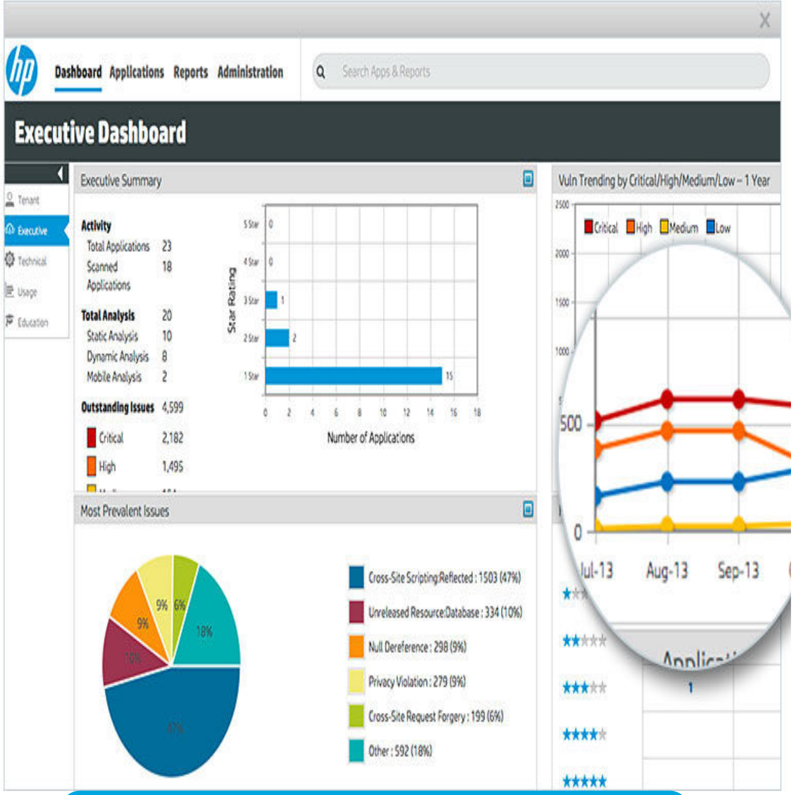
checkpoint TECHNOLOGIES Software Quality. Assured.

Fortify on Demand

- What if we don't have in house resources and or expertise in Security Testing?
  - HP Fortify on Demand offers a simple cost-effective cloud-based approach with no application security experience required.
  - Start small and quickly scale to hundreds of apps. This flexible solution can assess them all; web, mobile and client in-house, 3rd party or commercial off-the-shelf.

  - It's as easy as 1, 2, 3!
    - 1) **Initiate:** Upload your source code or point us at your URL and receive a comprehensive application layer test that encompasses static and dynamic analysis.
    - 2) **Test:** Our SaaS expert team will conduct a thorough audit of your application for security vulnerabilities.
    - 3) **Review:** Review detailed and correlated results, prioritized by severity & exploitability. Issues identified include line of code-level details with suggestions on how to fix.

HP Fortify On Demand



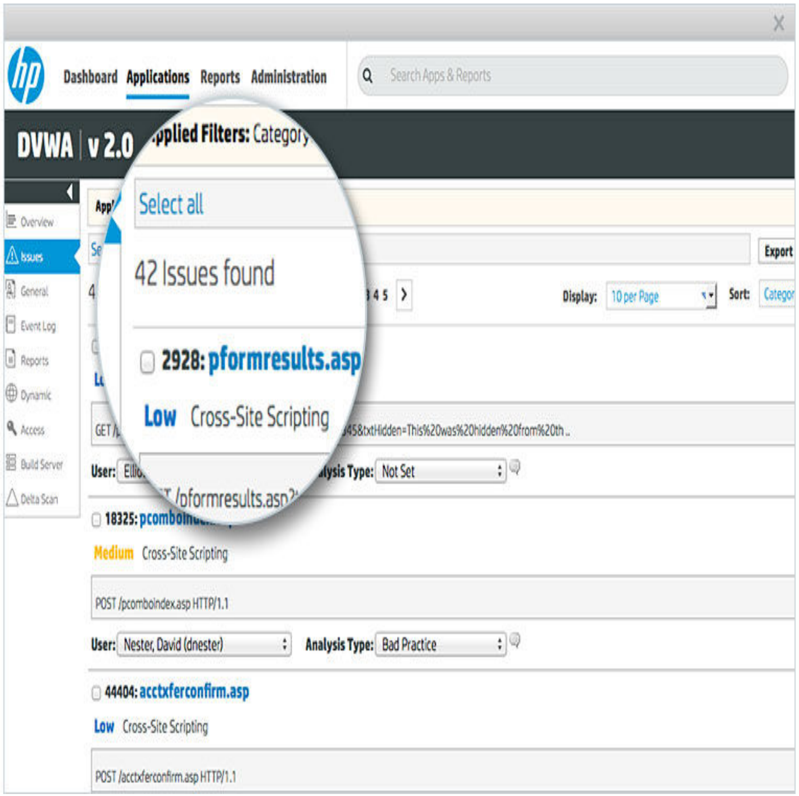
Executive Dashboard

Activity

Total Applications	23
Scanned Applications	18
Total Analysis	20
Static Analysis	10
Dynamic Analysis	8
Mobile Analysis	2
Outstanding Issues	4,599
🟥 Critical	2,182
🟧 High	1,495

- Cross-Site Scripting:Reflected : 1503 (47%)
- Unreleased Resource:Database : 334 (10%)
- Null Dereference : 298 (9%)
- Privacy Violation : 279 (9%)
- Cross-Site Request Forgery : 199 (6%)
- Other : 592 (18%)

Executive Dashboard: Charts the applications by risk category and star rating



DVWA | v 2.0

Applied Filters: Category

42 Issues found

Display: 10 per Page

□ **2928: pformresults.asp**

Low Cross-Site Scripting

GET /pformresults.asp? 45&txtHidden=This%20was%20hidden%20from%20th...

User: Ellio Analysis Type: Not Set

□ **18325: pcomboindex.asp**

Medium Cross-Site Scripting

POST /pcomboindex.asp HTTP/1.1

User: Nester, David (dnester) Analysis Type: Bad Practice

□ **44404: acctxferconfirm.asp**

Low Cross-Site Scripting

POST /acctxferconfirm.asp HTTP/1.1

Issues: Provides Remediation Advice

checkpoint TECHNOLOGIES Software Quality. Assured.

Q&A

Thank You

Jimmie Parson
Sr. Technical Engineer
813-818-8324 x133 (office)
www.checkpointech.com

Perform Better with
Checkpoint Technologies and HP