netSPI
RISK COMPLIANCE SECURITY

CorrelatedVM™ Overview

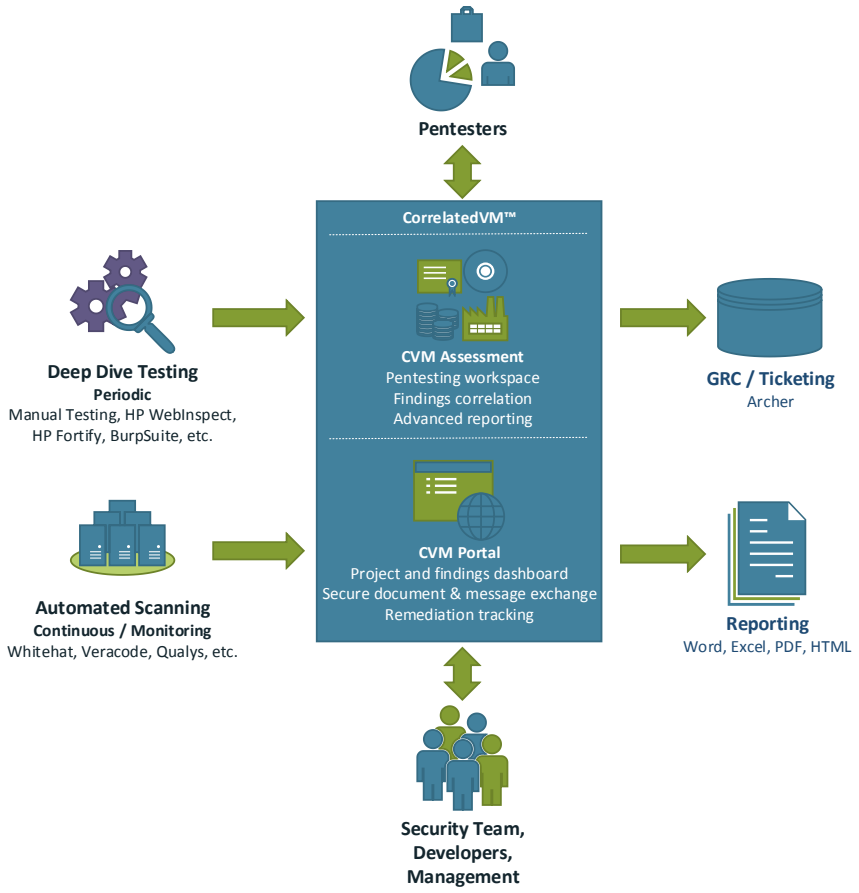
Business Problem

- Does your security assessment program include?
  - Multiple tools
  - Manual testing
  - Integration with asset management
  - Customized reporting
  - Remediation tracking
  - Vulnerability trending
- How do you manage your vulnerability dataset?
  - Spreadsheets
  - Natively within an assessment product

CorrelatedVM™ Overview

- CorrelatedVM™ is a vulnerability management framework tool developed by NetSPI designed to
  - Aggregate & correlate findings from multiple testing tools and from multiple testing layers
  - Manage vulnerability data
  - Produce quality, relative reports
- CorrelatedVM™ supports the following inputs
  - Code reviews
  - Application assessments
  - Database and operating system assessments
  - Penetration tests
  - Network assessments
  - Manual findings

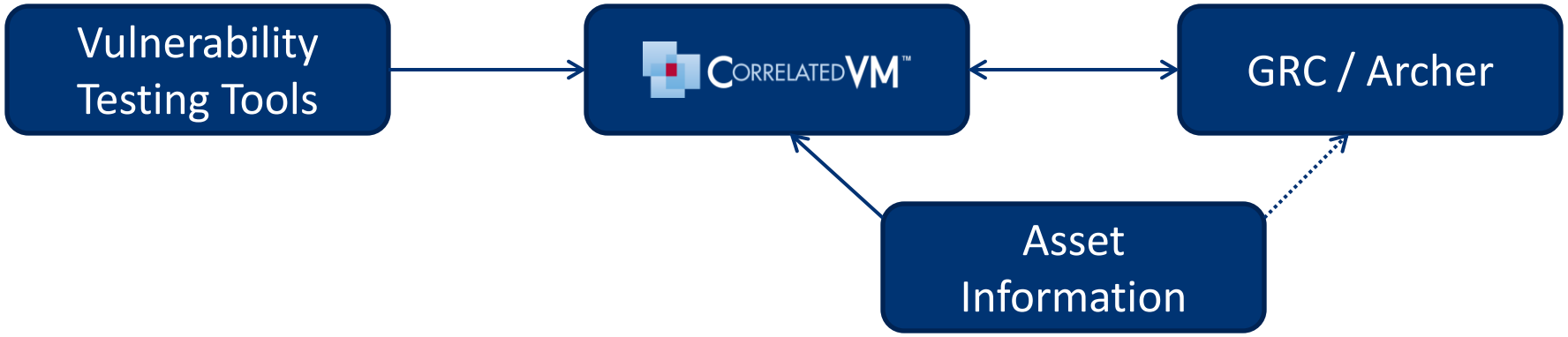
CorrelatedVM™ Architecture



*The rich client **CVM Assessment** software is designed by pentesters for pentesters; and the web based **CVM Portal**, is for software security stake holders, from developers up to the CISO. This built-in workflow will dramatically lower the risks associated with hosting or deploying vulnerable software on your network.*

CorrelatedVM's ability to bring elegant order to the uniquely challenging and sometimes outright disorderly vulnerability management efforts has been demonstrated in hundreds of organizations, on thousands of engagements, and for some of the most business-critical applications running on some of the most secure networks in the world.

CorrelatedVM™ Integrated with GRC / Archer



Benefits

- Automation for remediation assignments & due dates
- Customization of vulnerability descriptions, recommendations, severities, etc.
- Grouping and filtering of findings
- Updates to existing records with use of the unique key
- Findings reports can be attached to remediation plans

netSPI
RISK COMPLIANCE SECURITY

CVM Assessment Screen Shots

Asset Information

CorrelatedVM™ Assessment 5.0.67.168

File Edit Tools Administration Window Help

NetSPI CorrelatedVM™ Demo System
- Bailey Bros. Building and Loan Associatior
  - Assets
  - Asset Groups
  - Contacts
  - 2010 Q3 Demo Project
    - Containers
      - nCircle CSV2 (C:\Demofiles\I
      - Nessus (C:\Demofiles\Nessus
      - WebInspect XML (C:\Demofil
    - 2010 Q3 Demo Project Workspac
  - 2010 Q4 Demo Project
  - New Project
- Callahan Auto Parts
- Happy-Go-Lucky Toy Company
- Network Security Professionals
- Opti-Grab Inc
- TEST

Workspace - 520451 - 2010 Q3 Demo Project Workspace

- High
  - OpenSSH X11 Cookie Local Aut
  - PHP HTMLEntities HTMLSp
  - PHP MySQL Extension Optic
  - SQL Injection
    - 15.216.12.12 - This is the
      - SQL Injection (confirmed)
      - SQL Injection (confirmed)
      - SQL Injection (confirmed)
- Medium
- Low
- None
- Information
- Ignore

Workspace | Asset | Finding | Verification | Master Finding | Severity | Description | Remediation Instr | Verification Instr | Reports

Asset metadata

Asset	
Asset ID	366850
Asset Name	ecommerce web server
Asset Description	UAT web service
Asset IP Address	15.216.12.12
Asset Host Name	Barney
Asset DNS Name	zero.webappsecurity.com
Asset Aliases	uat.webappsecurity.com
Asset Environment	UAT
Asset Owner	John Smith
Asset Location	Back Up Data Center
Asset Product	Linux / Apache / PHP
Asset Application	Storefront.net
Asset Contact 1	John Smith
Asset Contact 2	Jane Johnson
Asset Contact 3	Tim Olson
Asset Contact 4	
Asset Contact 5	
Asset Contact	Mary Hatch Bailey (mary.bailey@bbbla.com)
Asset Tier	Tier1
Asset Type Provided	UAT
Asset Type	FreeBSD 5.5
Asset Function	Web Server
Asset is Virtual	False
Asset CVSS Environmental Metrics	CDP:H/TD:ND/CR:L/IR:M/AR:H

Services

Port	Proto	Name
22	tcp	ssh
53	tcp	domain
53	udp	domain
80	tcp	http
123	udp	ntp
443	tcp	https
8001	tcp	vcom-tunnel

Vulnerabilities

Port	Severity	Entry Point	Vulnerability
80	High	Unknown	SQL Injection
443	High	No	PHP HTMLEntities HTMLSpecialChars Buffer Overflow Vulnerabilities
22	High	Unknown	OpenSSH X11 Cookie Local Authentication Bypass Vulnerability
443	High	No	PHP MySQL Extension Option Handling Error Vulnerability
53	Medium	Unknown	DNS Cache Snooping
80	Medium	Unknown	HTTP TRACE or TRACK Cross-Site Scripting
80	Medium	Unknown	Backup File
80	Medium	No	Cross-Site Scripting
80	Medium	Unknown	CVS Content Files Found
443	Medium	No	Deprecated SSL Protocol Usage
80	Medium	Unknown	Logins Sent Over Unencrypted Connection
80	Medium	Unknown	Microsoft ASP.NET or ASP Unicode Conversion Cross-Site Scripting
80	Medium	Unknown	Microsoft ASP.NET Request Filtering Bypass Cross-Site Scripting Vulnerability
443	Medium	No	SSL Server Supports Weak Encryption

Connected to MSP01CPTSQL01P:CVMNETSPIUAT as NETSPI\speter [Administrator]

Remediation Tracking

CorrelatedVM™ Assessment 5.0.67.168 - [Workspace - 520451 - 2010 Q3 Demo Project Workspace]

File Edit Tools Administration Window Help

- NetSPI CorrelatedVM™ Demo System
  - Bailey Bros. Building and Loan Associatior
    - Assets
    - Asset Groups
    - Contacts
    - 2010 Q3 Demo Project
      - Containers
      - 2010 Q3 Demo Project Workspac
    - 2010 Q4 Demo Project
    - New Project
  - Callahan Auto Parts
  - Happy-Go-Lucky Toy Company
  - Network Security Professionals
  - Opti-Grab Inc
  - TEST

- High
  - OpenSSH X11 Cookie Local Auth
  - PHP HTMLEntities HTMLSp
  - PHP MySQL Extension Optic
  - SQL Injection
    - 15.216.12.12 - ecommerce
      - SQL Injection (confirmed)
      - SQL Injection (confirmed)
      - SQL Injection (confirmed)
- Medium
  - Backup File
  - Cross-Site Scripting
  - CVS Content Files Found
  - Deprecated SSL Protocol U
  - DNS Cache Snooping
  - HTTP TRACE or TRACK Cro
  - IIS Global Server Variables
  - Logins Sent Over Unencrypt
  - Microsoft Active Server Pag
  - Microsoft ASP.NET or ASP
  - Microsoft ASP.NET Request
  - Password in Query Data
  - PHP MB_Send_Mail TO Argu
  - SSL Server Supports Weak
  - Usable Remote Name Serve
- Low
- None
- Information
- Ignore

Workspace | Asset | Finding | Verification | Master Finding | Severity | Description | Remediation Instr | Verification Instr | Reports

Affected	
Affected URL	http://zero.webappsecurity.com/login1.asp
Affected Source	
Affected Source Line	
Asset	
Asset ID	366850
Asset	15.216.12.12 - ecommerce web server - Barney - zero.webapp
Container	
Container ID	536061
Container Name	WebInspect XML (C:\Demofiles\WebInspect.xml) Monday, Ju
Container Source	C:\Demofiles\WebInspect.xml
Identification	
Finding ID	239aae39-cd95-e011-b27a-001e4f120021
Finding Name	SQL Injection (confirmed)
Finding Description	
Master Finding ID	877
Intermediate Finding ID	8754
Port	
Port ID	140
Port Number	80
Port Protocol	tcp
Port Name	http
State	
Finding Assessment State	New
Finding Remediation State	Assigned
Finding Remediation Notes	This will require a coding change
Finding Remediation Contact	Mary Hatch Bailey (mary.bailey@bbbla.com)
Estimated Remediation Date	11/11/2011
Actual Remediation Date	
Estimated Remediation Hours	16
Actual Remediation Hours	
Remediation Resource Type	Internal

Connected to MSP01CPTSQL01P:CVMNETSPIUAT as NETSPI\speter [Administrator]

Customized Severities

CorrelatedVM™ Assessment 5.0.67.168 - [Workspace - 520451 - 2010 Q3 Demo Project Workspace]

File Edit Tools Administration Window Help

NetSPI CorrelatedVM™ Demo Sy
- Bailey Bros. Building and Loa
  - Assets
  - Asset Groups
  - Contacts
  - 2010 Q3 Demo Project
    - Containers
    - 2010 Q3 Demo Proje
  - 2010 Q4 Demo Project
  - New Project
- Callahan Auto Parts
- Happy-Go-Lucky Toy Compa
- Network Security Professiona
- Opti-Grab Inc
- TEST

- High
  - OpenSSH X11 Cookie Local A
  - PHP HTMLEntities HTML
  - PHP MySQL Extension Op
  - SQL Injection
    - 15.216.12.12 - ecomme
      - SQL Injection (confirme
      - SQL Injection (confirme
      - SQL Injection (confirme
- Medium
  - Backup File
  - Cross-Site Scripting
  - CVS Content Files Found
  - Deprecated SSL Protocol
  - DNS Cache Snooping
  - HTTP TRACE or TRACK
  - IIS Global Server Variable
  - Logins Sent Over Unencr
  - Microsoft Active Server P
  - Microsoft ASP.NET or AS
  - Microsoft ASP.NET Requ
  - Password in Query Data
  - PHP MB_Send_Mail TO A
  - SSL Server Supports Wea
  - Usable Remote Name Ser
- Low
- None
- Information
- Ignore

Workspace | Asset | Finding | Verification | Master Finding | Severity | Description | Remediation Instr | Verification Instr | Reports

Default Project Type

Severity: Critical

Business Impact: SQL injection can allow an attacker to extract, modify, add, or delete information from database servers, the ability to remotely execute system commands, or in some circumstances provides the means to take control of the server hosting the database.

Similar...

☑ Override Severity for Project Type "New ASV Project Type"

Severity Properties for Project Type "New ASV Project Type"

Severity: High

Business Impact: SQL injection can allow an attacker to extract, modify, add, or delete information from database servers, the ability to remotely execute system commands, or in some circumstances provides the means to take control of the server hosting the database.

Similar...

Categories
- ☐ Configuration
- ☐ Patch/Version
- ☑ Code Change

Connected to MSP01CPTSQL01P:CVMNETSPIUAT as NETSPI\speter [Administrator]

Robust Reporting

CorrelatedVM™ Assessment 5.0.67.168 - [Workspace - 520451 - 2010 Q3 Demo Project Workspace]

File Edit Tools Administration Window Help

NetSPI CorrelatedVM™ Demo Sy
Bailey Bros. Building and Loa
Assets
Asset Groups
Contacts
2010 Q3 Demo Project
Containers
2010 Q3 Demo Proje
2010 Q4 Demo Project
New Project
Callahan Auto Parts
Happy-Go-Lucky Toy Compa
Network Security Professiona
Opti-Grab Inc
TEST

High
OpenSSH X11 Cookie Local A
PHP HTMLEntities HTML
PHP MySQL Extension O
SQL Injection
15.216.12.12 - ecomme
SQL Injection (confirm
SQL Injection (confirm
SQL Injection (confirm
Medium
Backup File
Cross-Site Scripting
CVS Content Files Found
Deprecated SSL Protocol
DNS Cache Snooping
HTTP TRACE or TRACK
IIS Global Server Variable
Logins Sent Over Unencr
Microsoft Active Server P
Microsoft ASP.NET or AS
Microsoft ASP.NET Requ
Password in Query Data
PHP MB_Send_Mail TO A
SSL Server Supports Wea
Usable Remote Name Ser
Low
None
Information
Ignore

Workspace | Asset | Finding | Verification | Master Finding | Severity | Description | Remediation Instr | Verification Instr | Reports

Report Type
Remediation Report
Generate...

Include Severities
- [x] Urgent
- [x] Critical
- [x] High
- [x] Medium
- [x] Low
- [ ] None
- [ ] Information
- [ ] Ignore

Include Finding Assessment States
- [x] Final
- [x] Entry Point
- [x] In Progress
- [x] New
- [ ] False Positive
- [ ] Duplicate

Asset Group Filter
- [x] WebApplications
- [ ] Group 2
- [ ] Group 3

Include Finding Remediation States
- [x] New
- [x] Assigned
- [x] Closed
- [ ] Verified

Set Precedent Workspaces...
Spell Check Workspace

Connected to MSP01CPTSQL01P:CVMNETSPIUAT as NETSPI\speter [Administrator]

netSPI
RISK COMPLIANCE SECURITY

CVM Portal Screen Shots

Project Dashboards

CorrelatedVM - Windows Internet Explorer

https://correlatedvm.netspi.com/dashboard

CorrelatedVM by netSPI

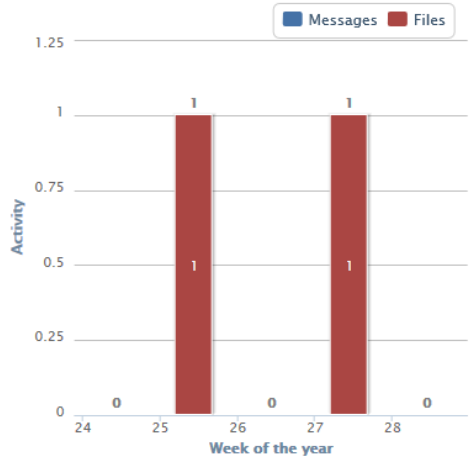
Welcome Seth Peter | Contact Us

PROJECT STATS

Latest Projects

Acme-2013-ACR	83%
ACME-2013-WAPen-Attack	71%

Project Activity



NOTIFICATIONS

- Gaurav Gaur uploaded code fullcalendar-1.5.4_2.zip on July 03 for project Acme-2013-ACR
- Seth Peter uploaded attachment Acme-Test-Project-9000-Preliminary_Report.docx on June 18 for project ACME-2013-WAPen-Attack
- Gaurav Gaur uploaded code fullcalendar-1.5.4_2__3_.zip on June 03 for project Acme-2013-ACR
- Gaurav Gaur uploaded attachment Acmesample_(3).docx on June 03 for project Acme-2013-ACR
- Ryan Wakeham [Demo] posted a message on May 29 for project ACME-2013-WAPen-Attack
- Gaurav Gaur uploaded code fullcalendar-1.5.4_2.zip on May 23 for project Acme-2013-ACR
- Gaurav Demo posted a message on May 20 for project Acme-2013-ACR
- Gaurav Gaur uploaded attachment Acmesample.docx on May 10 for project Acme-2013-ACR
- Gaurav Demo posted a message on May 10 for project Acme-2013-ACR
- Gaurav Demo posted a message on April 11 for project

CALENDAR

Jul 8 — 12 2013 | month | week

Mon 7/8	Tue 7/9	Wed 7/10	Thu 7/11	Fri 7/12

Dynamic Charts

CorrelatedVM - Windows Internet Explorer

https://correlatedvm.netspi.com/findings/17b1f18b

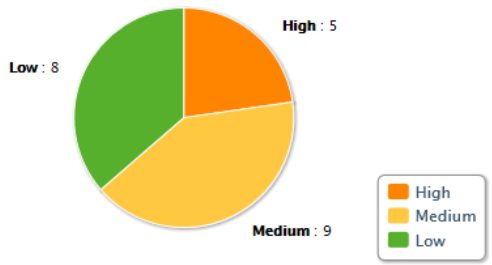
CorrelatedVM by netSPI

Welcome Seth Peter Contact Us

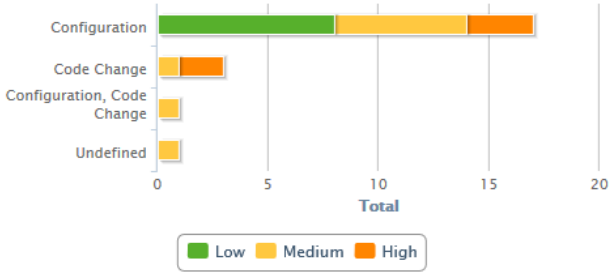
- Dashboard
- Projects
- Findings
- Company Information
- Users
- Share Files with NetSPI
- Calendar
- Feedback
- Sign Out

SUMMARY OF ACME-2013-WAPEN-ATTACK FINDINGS

Summary by Vulnerability Level



Summary by Severity Level and Vulnerability Category



Summary by Finding and Instance

Detailed Findings

369890	15.216.12.12-zero.webappsecurity.com	Localstart.asp Brute Force exposure	80	http	New	High	Configuration	+
369893	15.216.12.12-zero.webappsecurity.com	SQL Injection	80	http	Partially Remediated	High	Code Change	+

Vulnerability Details

SQL injection is a method of attack that takes advantage of input variables that have not been validated, thus allowing the manipulation of SQL queries processed by the backend database server. It is often presented in web-based forms, queries within URLs, and XML requests.

Business Impact

SQL injection may allow an attacker to extract, modify, add, or delete information from database servers, causing the confidentiality and integrity of the information stored in the database to be compromised. Depending on the SQL implementation, the attacker may also be able to execute system commands on the affected host. In some circumstances this provides the means to take control of the server hosting the database, leading to the complete compromise of the confidentiality, integrity, and availability of the affected host.

OWASP Category

A1-Injection

Recommendation

Employ a layered approach to security that includes using parameterized queries when accepting user input. Strictly define the data type (for instance, a string, an alphanumeric character, etc.) that the application will accept and harden the database server to prevent data from being accessed inappropriately.
Also, ensure that all data used by the application is put through a data input filter that removes potentially harmful characters. Best practice recommends the use of white lists using regular expressions.
Disable detailed error messages that could give an attacker information about database names, table names, versions and type of databases being used. Replace the error message with a generic error asking the user to contact the IT department or send an e-mail to the web administrator.
A non-privileged service account should be used to run the database server, and the database user in use should not have administrative privileges to the database. Following the principle of least privilege when assigning permissions for the service account and database user helps limit the impact of a successful SQL injection attack.

References

- http://en.wikipedia.org/wiki/Sql_injection,
- http://en.wikipedia.org/wiki/SQL_injection,
- http://msdn.microsoft.com/msdnmag/issues/04/09/SQLInjection/default.aspx,
- http://msdn2.microsoft.com/en-us/library/ms161953.aspx,
- http://www.owasp.org/index.php/Avoiding_SQL_Injection,
- http://www.owasp.org/index.php/Blind_SQL_Injection,
- http://www.owasp.org/index.php/SQL_injection,
- http://www.owasp.org/index.php/Testing_for_SQL_Injection_%28OWASP-DV-005%29

Finding Details

AffectedUrl http://zero.webappsecurity.com/forgot1.asp?get=security_audit%2540netspi.com'+and++(select+count(*)+from+spitable)+=1+or+'1'='0

Remediated

AffectedUrl http://zero.webappsecurity.com/login1.asp

Additional Details

Download This Info

netSPI
RISK COMPLIANCE SECURITY

Contact us:

www.netspi.com

612-465-8880