JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Validation of Results

VULNERABILITY MANAGEMENT

Validating of Results

- CVSS Scores are helpful, but they alone don’t tell you how a vulnerability affects *your* systems

- Some vulnerabilities are:
  - False Positives
  - Documented Exceptions
  - Informational Results

False Positives

- Scanners can often report that a vulnerability exists even if it doesn’t
- How often this occurs is known as the *false positive error rate*
- Vulnerabilities are validated and verified
  - Check if a patch is missing
  - Attempt to exploit erroneous code
  - Verify the system configuration

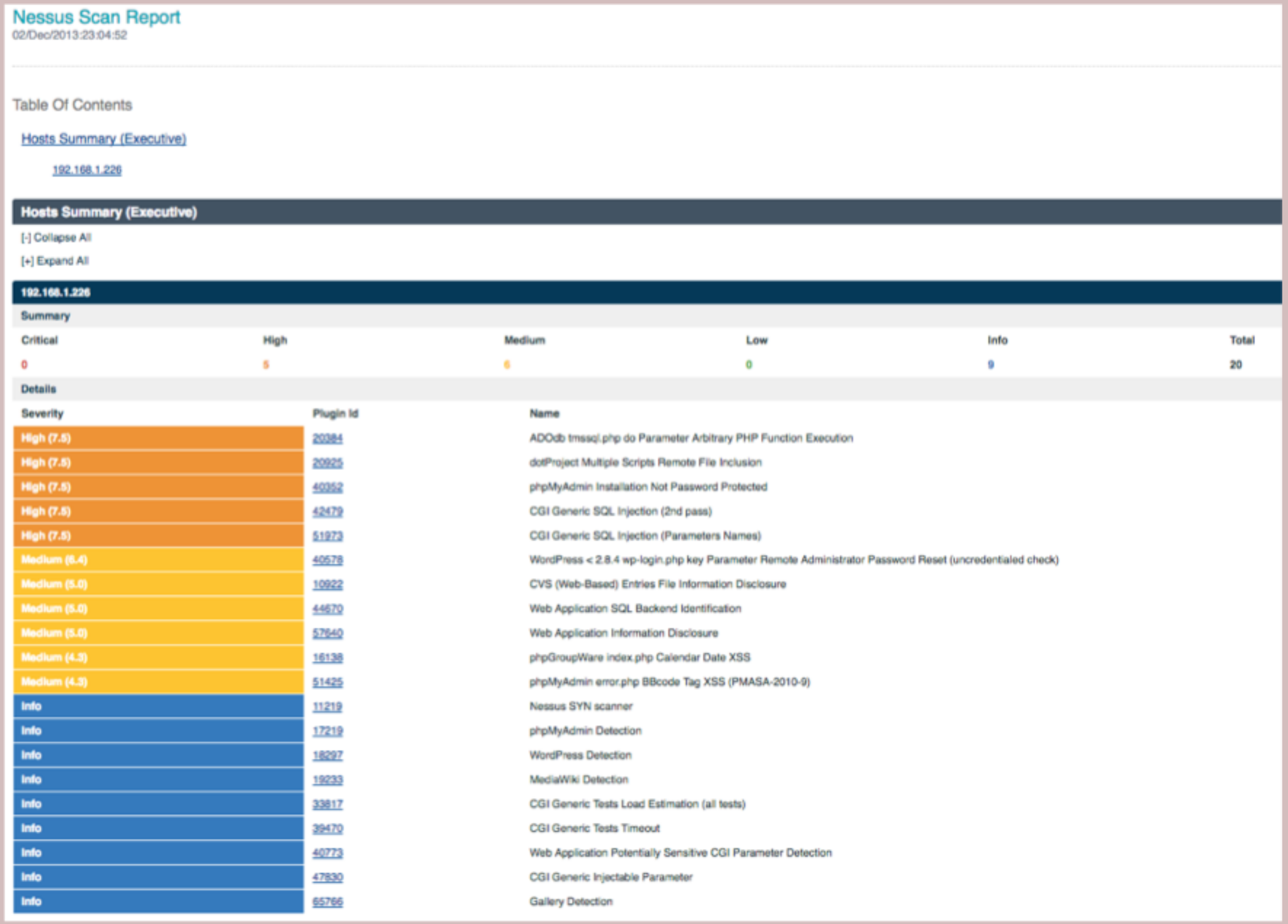
Documented Exceptions

- Accepted vulnerabilities that are known, but will not be fixed by the organization
- Once this risk is accepted by management, they should be documented in the scanner to prevent future reporting of them

Informational Results

- Not everything reported by the scanner is considered a vulnerability
- Some are reported as ”informational”
- Typical “informational” items are configurations that would allow an attacker to perform reconnaissance

Informational Results



Nessus Scan Report
02/Dec/2013:23:04:52

Table Of Contents

Hosts Summary (Executive)

192.168.1.226

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

192.168.1.226

Summary

Critical	High	Medium	Low	Info	Total
0	5	6	0	9	20

Details

Severity	Plugin Id	Name
High (7.5)	20384	ADOdb tmssql.php do Parameter Arbitrary PHP Function Execution
High (7.5)	20925	dotProject Multiple Scripts Remote File Inclusion
High (7.5)	40352	phpMyAdmin Installation Not Password Protected
High (7.5)	42479	CGI Generic SQL Injection (2nd pass)
High (7.5)	51973	CGI Generic SQL Injection (Parameters Names)
Medium (6.4)	40578	WordPress < 2.8.4 wp-login.php key Parameter Remote Administrator Password Reset (uncredentialed check)
Medium (5.0)	10922	CVS (Web-Based) Entries File Information Disclosure
Medium (5.0)	44670	Web Application SQL Backend Identification
Medium (5.0)	57640	Web Application Information Disclosure
Medium (4.3)	16138	phpGroupWare index.php Calendar Date XSS
Medium (4.3)	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
Info	11219	Nessus SYN scanner
Info	17219	phpMyAdmin Detection
Info	18297	WordPress Detection
Info	19233	MediaWiki Detection
Info	33817	CGI Generic Tests Load Estimation (all tests)
Info	39470	CGI Generic Tests Timeout
Info	40773	Web Application Potentially Sensitive CGI Parameter Detection
Info	47830	CGI Generic Injectable Parameter
Info	65766	Gallery Detection

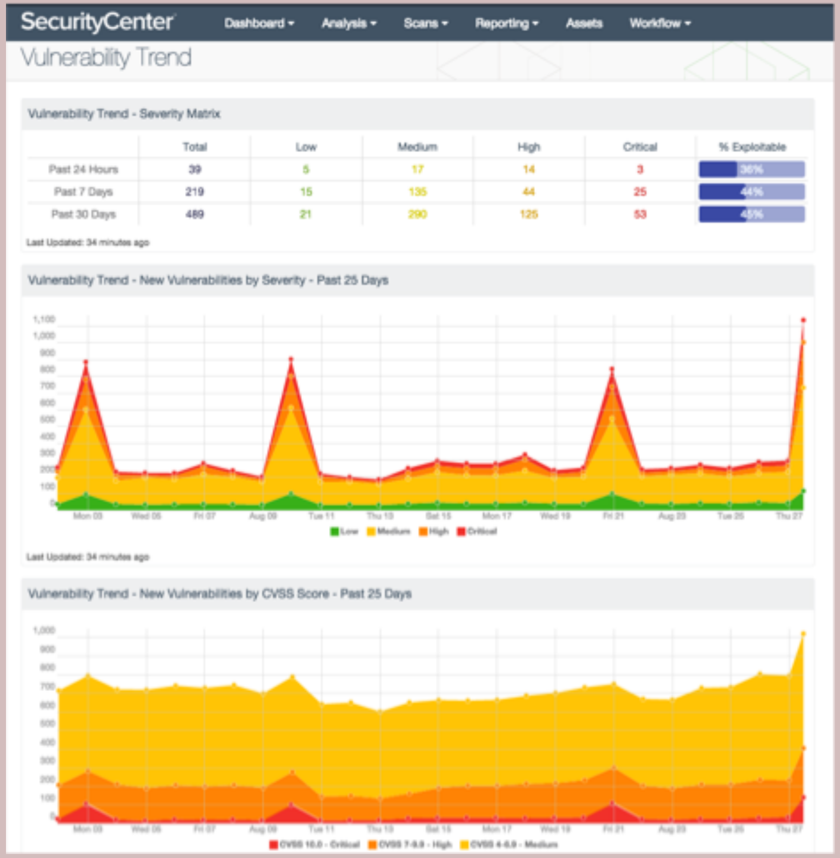
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Compare Results with Other Information Sources

- Logs from servers, network devices, applications, and other sources
- Configuration management systems
- Security Information and Event Monitoring (SIEM)

Conduct Trend Analysis

- Trend analysis also allows the analyst to ensure the vulnerability management program is working effectively



Vulnerability Trend

Vulnerability Trend - Severity Matrix

	Total	Low	Medium	High	Critical	% Exploitable
Past 24 Hours	39	5	17	14	3	36%
Past 7 Days	219	15	135	44	25	44%
Past 30 Days	489	21	290	125	53	45%

Last Updated: 34 minutes ago

Vulnerability Trend - New Vulnerabilities by Severity - Past 25 Days

Last Updated: 34 minutes ago

Vulnerability Trend - New Vulnerabilities by CVSS Score - Past 25 Days