TRIDIUM

NS2022

ACCELERATING INNOVATION

Security Best Practices

Bill Smith

Lead Software Architect - Tridium

TRIDIUM

Overview

- Tools of the Trade
  - Threat Modeling
  - Code Coverage/Unit Tests
  - Code Reviews
  - Static Code Analysis
  - Third Party Components
  - Penetration Testing
- Assessing Risk
  - CVSS
  - Beyond CVSS
- Lessons Learned

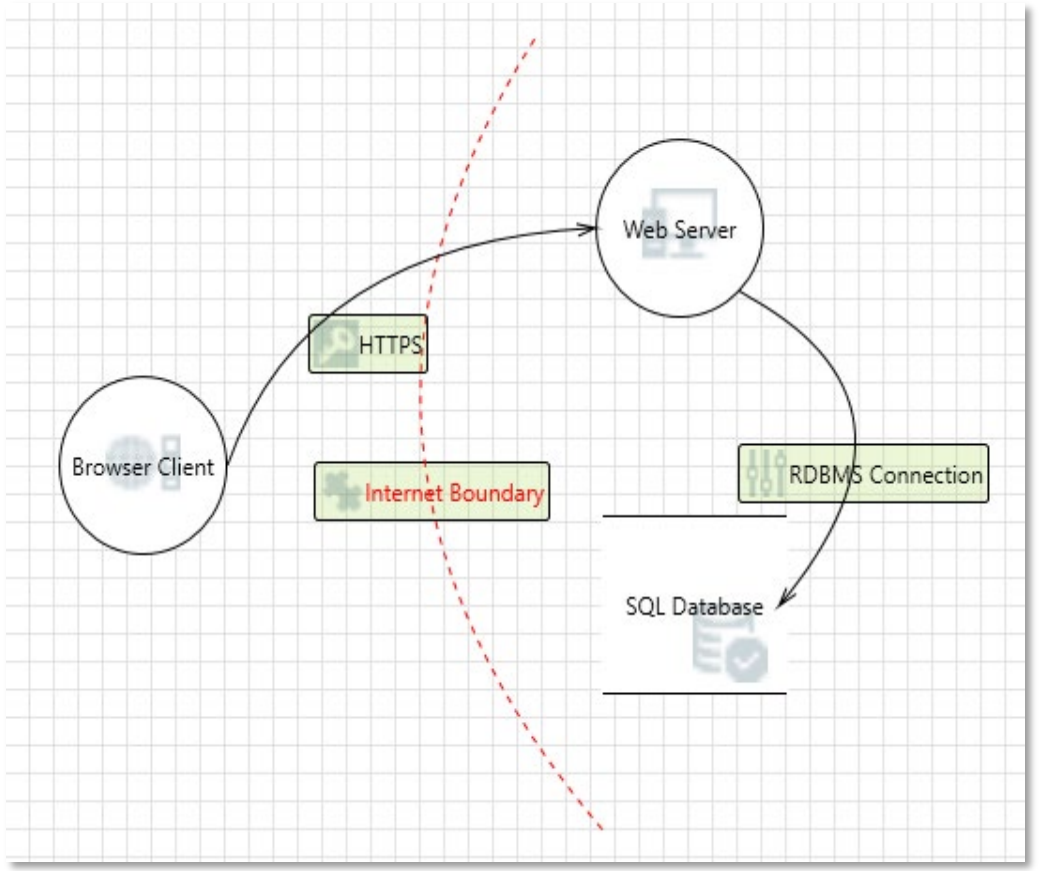
TRIDIUM

Tools of the Trade

- Threat Modeling
- Code Coverage/Unit Tests
- Code Reviews
- Static Code Analysis
- Third Party Components
- Pen Testing

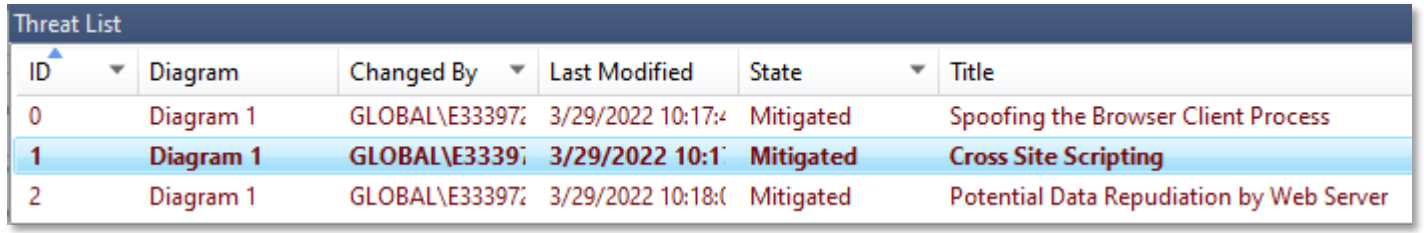
Threat Modeling

- MS Threat Modeling Tool is the tool of choice for us
- Threat model diagram derived from network diagram
- Auto generates risks based on interactions
- Risks outside the automatic ones can be added

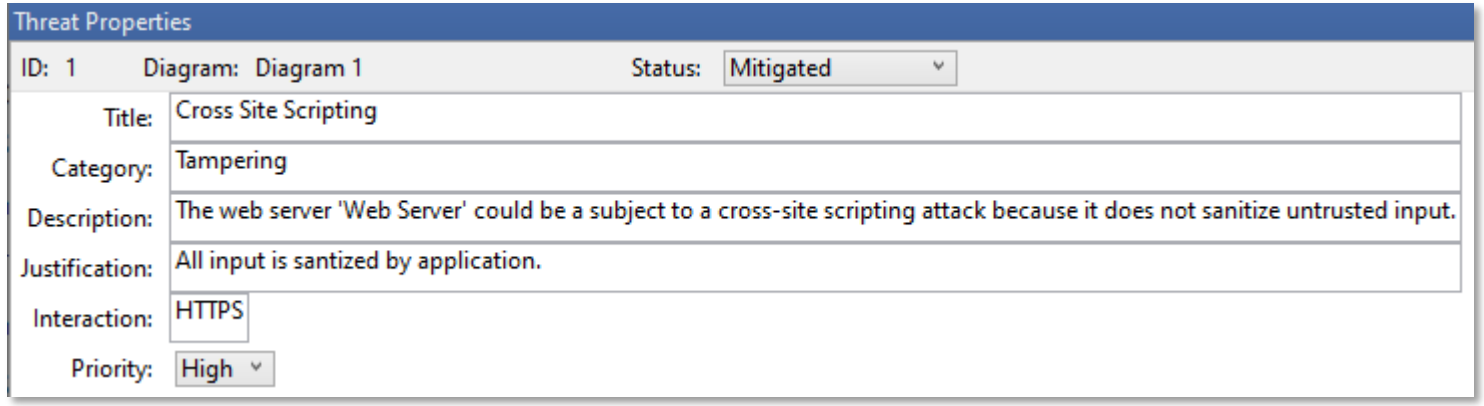


Threat Modeling

- Threat List shows list of identified threats.



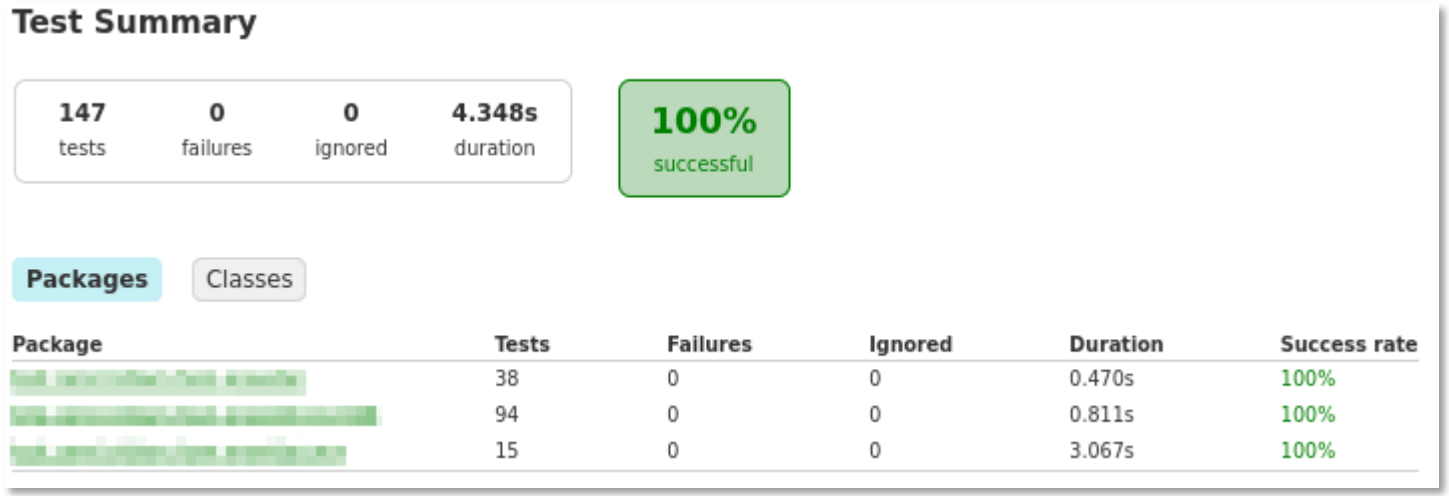
- Threat properties provide status and justification of identified threat.

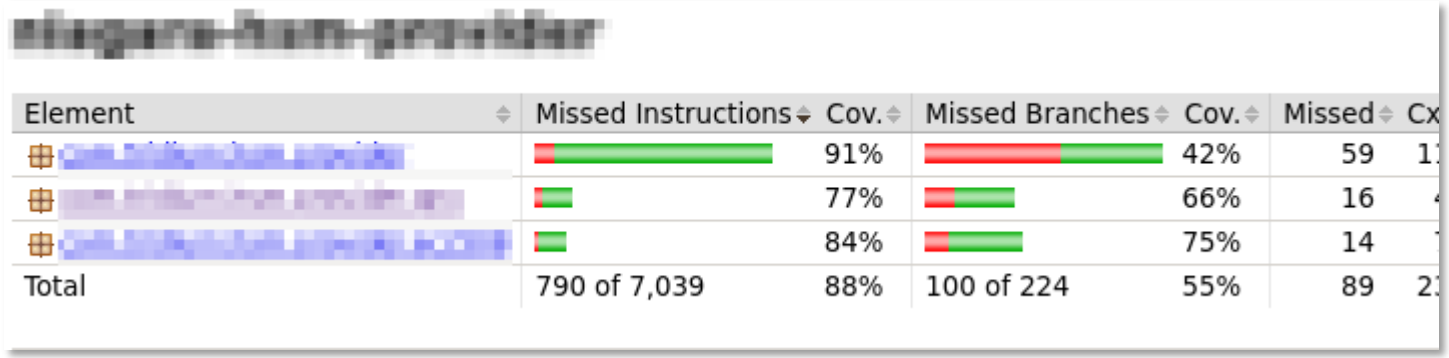


niagara SUMMIT

Code Coverage/Unit Tests

- Unit Test Tools
  - JUnit
  - TestNG
  - Jasmine/Karma
- Code Coverage Tools
  - JaCoCo
  - SonarQube
  - Istanbul





niagara SUMMIT

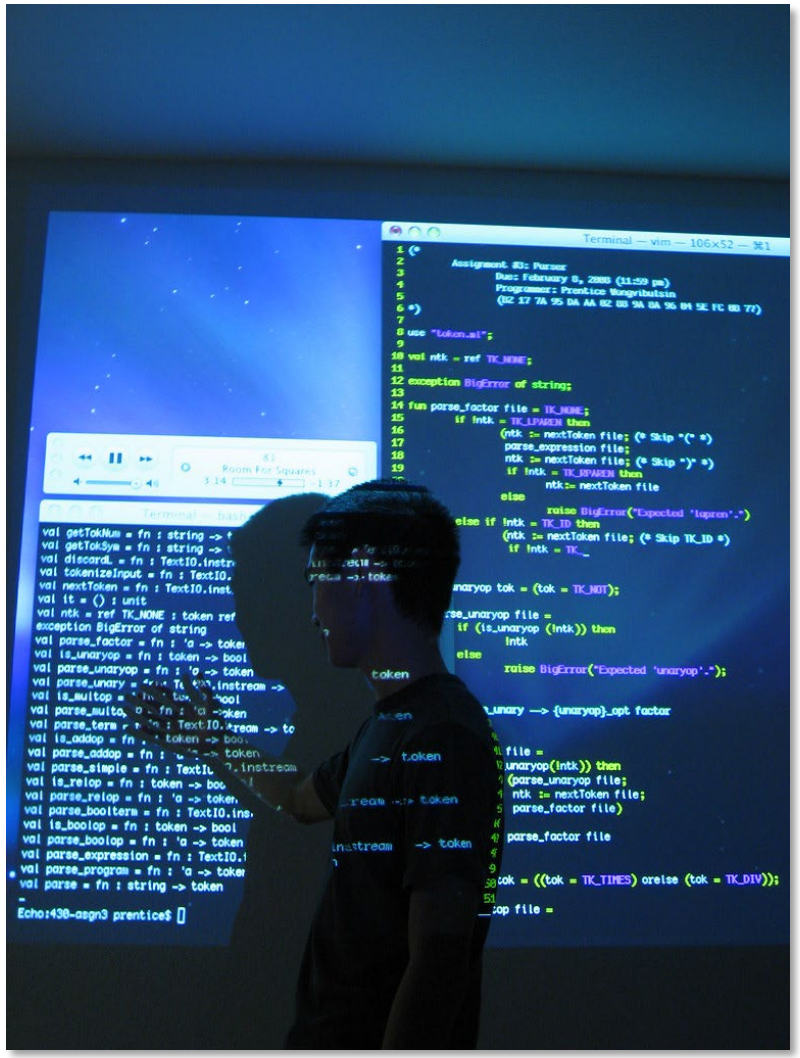
Code Reviews

Some things to consider:

- Coding Standards
- Logging of Sensitive Data
- Input Validation
- Returning Privileged Information
- Hardcoded Credentials

Some Niagara specific things:

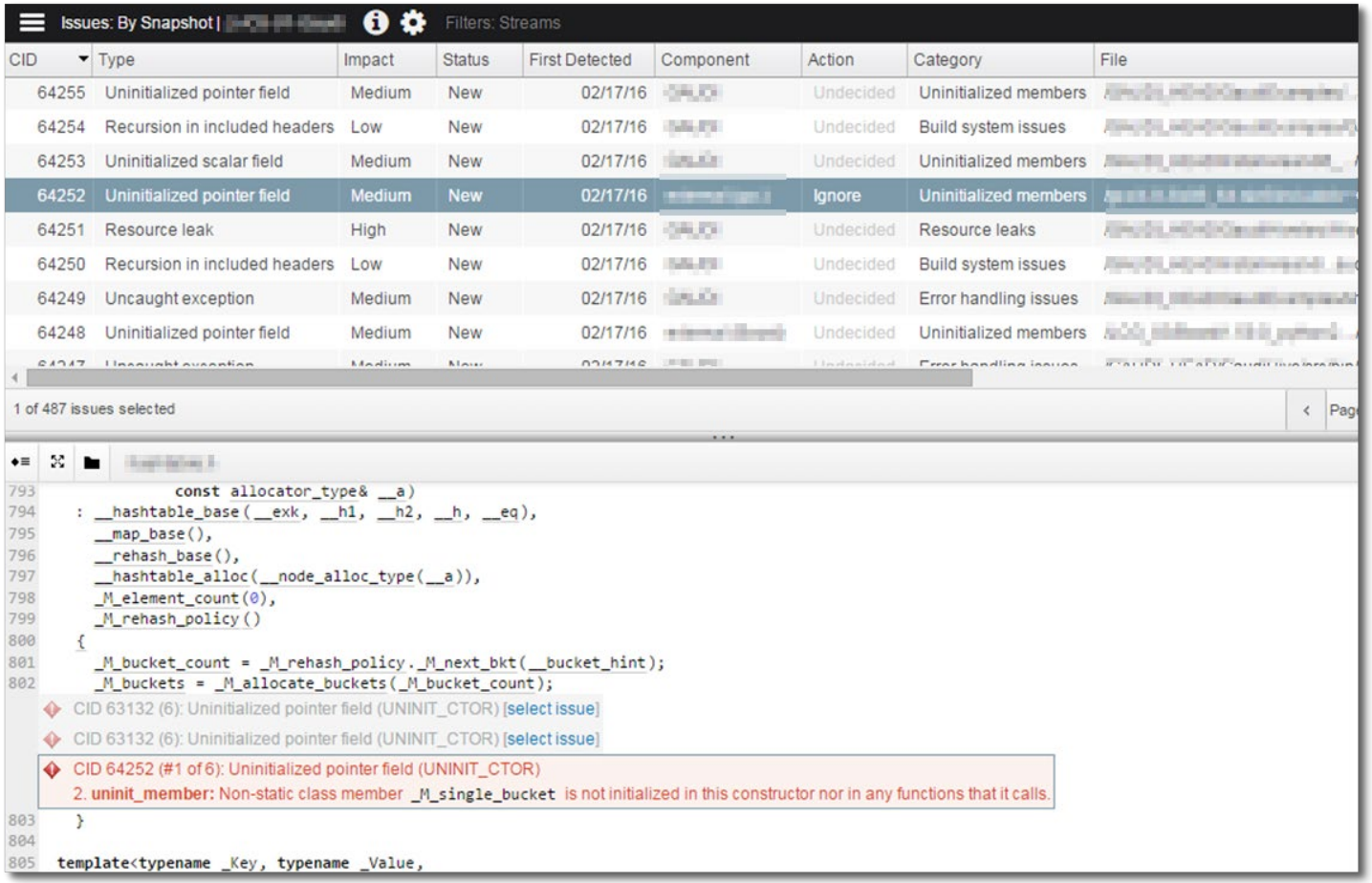
- Permissions Model
- Security Audit Log
- Security Facet
- Security Dashboard Card



niagara SUMMIT

Static Code Analysis

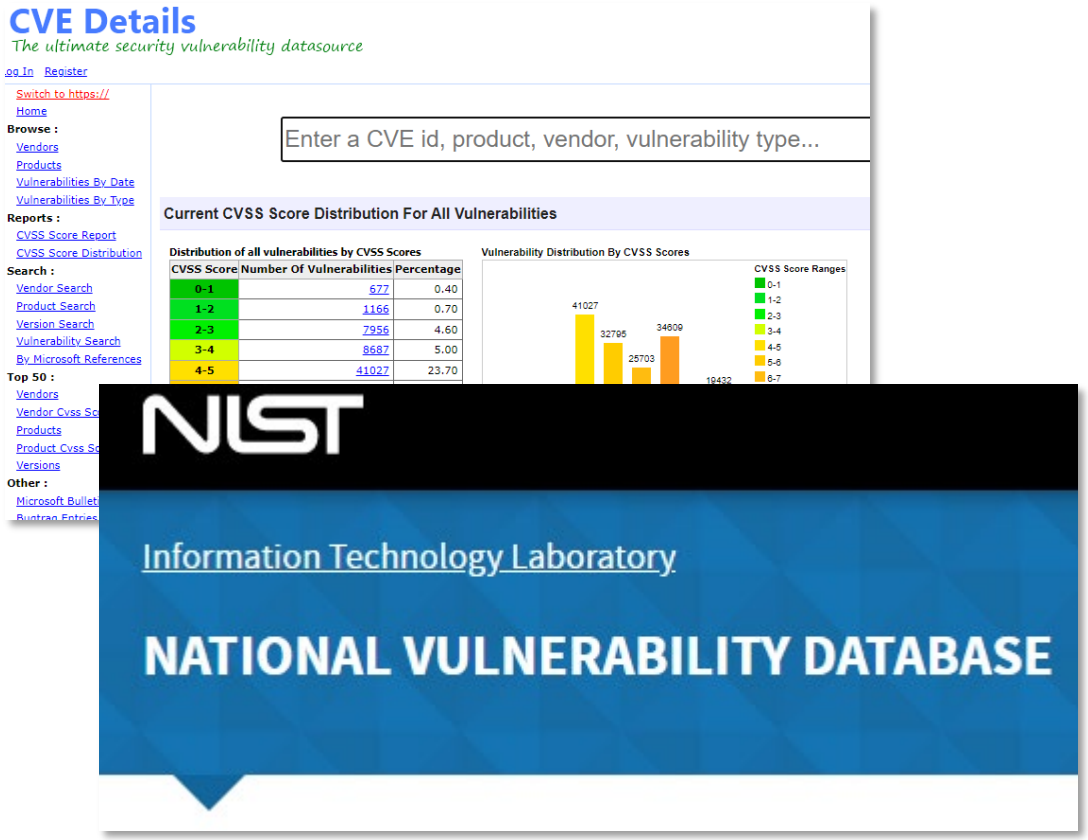
- Tools
  - Coverity
  - SonarQube
- Functions
  - Security
  - Quality



niagara SUMMIT

Third Party Components

- Tools
  - Black Duck Hub
  - OWASP Dependency Checker
- Other Resources
  - https://www.cvedetails.com/
  - https://cve.mitre.org/cve/
  - https://nvd.nist.gov/

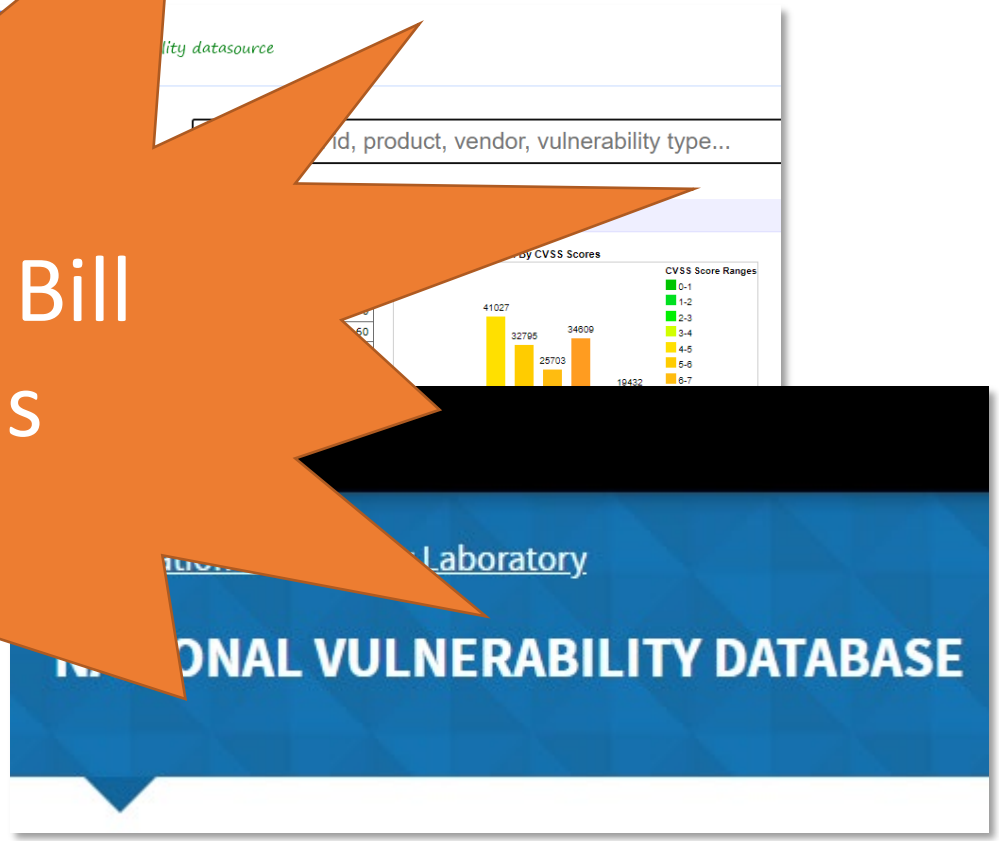


niagara SUMMIT

Third Party Components

- Tools
  - Black Duck Hu
  - OWASP Depend
- Other Resource
  - https
  - https://cve
  - https:/

Validate Your Bill of Materials First!!!



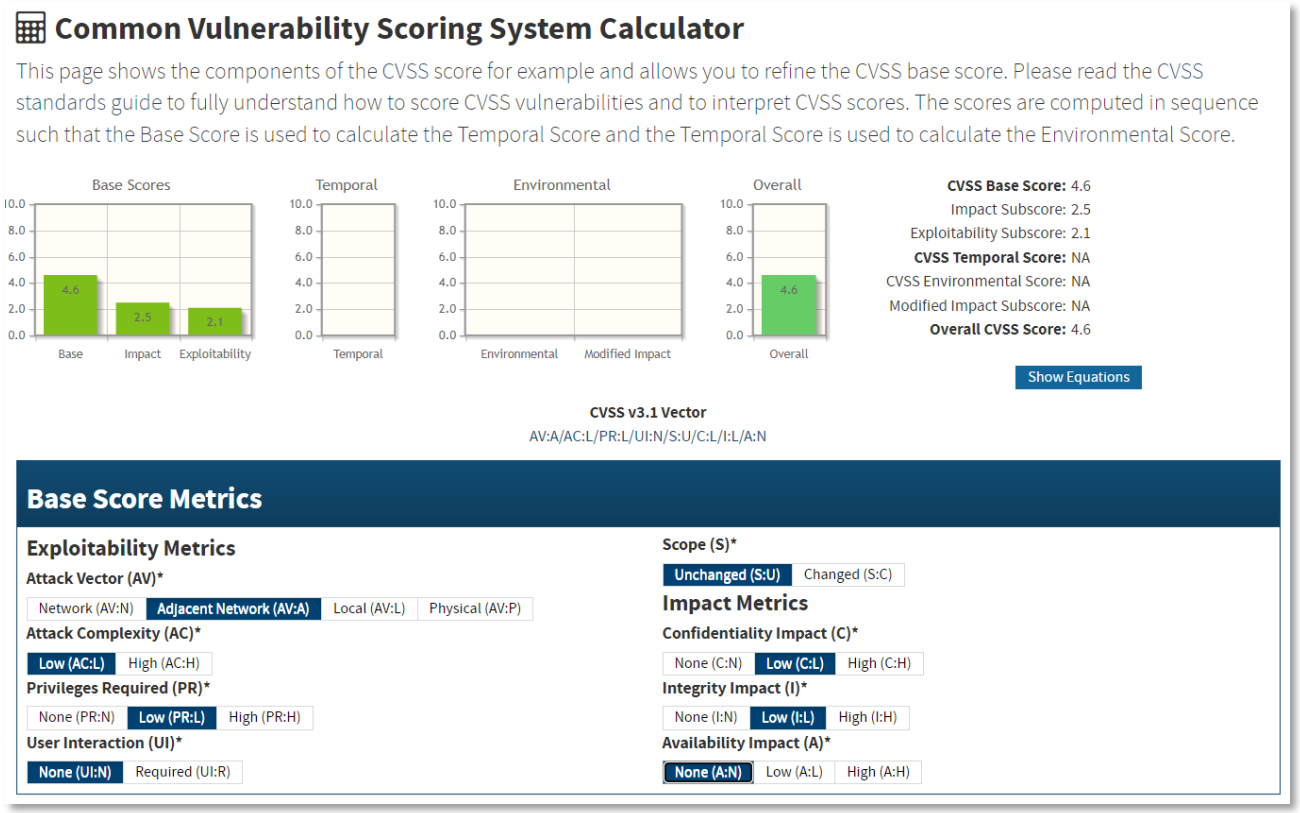
niagara SUMMIT

Penetration Testing

- Tools
  - BurpSuite
  - Metasploit
  - FuzzDB
  - Nmap
  - Qualys

Assessing Risk

- Primary method is CVSS (Common Vulnerability Scoring System)
- NIST Calculator (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator)
- Environmental scoring can help, but…



niagara SUMMIT

Contrived Example

Contrived Example

Are these REALLY the same?

Beyond CVSS

- Consider other factors in addition to CVSS, examples:
  - Fire/Life Safety
  - Alternative mitigations
  - Number of customers impacted
  - Risk of destabilizing product
  - Cost to fix

Lessons Learned

- Relationship with engineering teams should be symbiotic, NOT adversarial
- BREAK THE BUILD can be very counter productive
- Understand WHY something is being done, don't just be a checkbox
- OWN and EMBRACE findings and tackle them with pride

Questions?

bsmith@tridium.com

https://www.linkedin.com/in/bill-smith-vmi91/

TRIDIUM

References/Citations

- *"Tools" by zzpza is marked with CC BY 2.0. To view the terms, visit https://creativecommons.org/licenses/by/2.0/?ref=openverse*
- *MS Threat Modeling Tool, visit https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool*
- *TestNG, visit https://testng.org/doc/*
- *"Code on the Wall" by Nat W is marked with CC BY-SA 2.0. To view the terms, visit https://creativecommons.org/licenses/by-sa/2.0/?ref=openverse*
- *BurpeSuite, visit https://portswigger.net/burp*
- *Metasploit, visit https://www.metasploit.com/*
- *Fuzzdb, visit https://github.com/fuzzdb-project/fuzzdb*
- *NMAP, visit https://nmap.org/*
- *CVE Details, visit https://www.cvedetails.com/*
- *CVE Mitre List, visit https://cve.mitre.org/cve/*
- *"Aaaagh!" by Finizio is marked with CC BY-ND 2.0. To view the terms, visit https://creativecommons.org/licenses/by-nd/2.0/?ref=openverse*
- *NIST Calculator, visit https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator*
- *Water Fountain 3" by joshme17 is marked with CC BY 2.0. To view the terms, visit https://creativecommons.org/licenses/by/2.0/?ref=openverse*
- *"Drip." by Instant Vantage is marked with CC BY-SA 2.0. To view the terms, visit https://creativecommons.org/licenses/by-sa/2.0/?ref=openverse*
- *"File:Johnny-automatic-scales-of-justice.svg" by johnny_automatic is marked with CC0 1.0. To view the terms, visit https://creativecommons.org/publicdomain/zero/1.0/deed.en?ref=openverse*

TRIDIUM