NANYANG TECHNOLOGICAL UNIVERSITY

Tutorial 2: Risk Analysis with CVSS

presented by

Li Yi
Assistant Professor
SCSE

N4-02b-64
yi_li@ntu.edu.sg

COPYRIGHT STATEMENT

- All course materials, including but not limited to, lecture slides, handout and recordings, are for your own educational purposes only. **All the contents of the materials are protected by copyright, trademark or other forms of proprietary rights.**
- All rights, title and interest in the materials are owned by, licensed to or controlled by the University, unless otherwise expressly stated. **The materials shall not be uploaded, reproduced, distributed, republished or transmitted in any form or by any means, in whole or in part, without written approval from the University.**
- You are also not allowed to take any photograph, film, audio record or other means of capturing images or voice of any contents during lecture(s) and/or tutorial(s) and reproduce, distribute and/or transmit any form or by any means, in whole or in part, without the written permission from the University.
- Appropriate action(s) will be taken against you including but not limited to disciplinary proceeding and/or legal action if you are found to have committed any of the above or infringed the University's copyright.

Common Vulnerability Scoring Scheme

CVSS

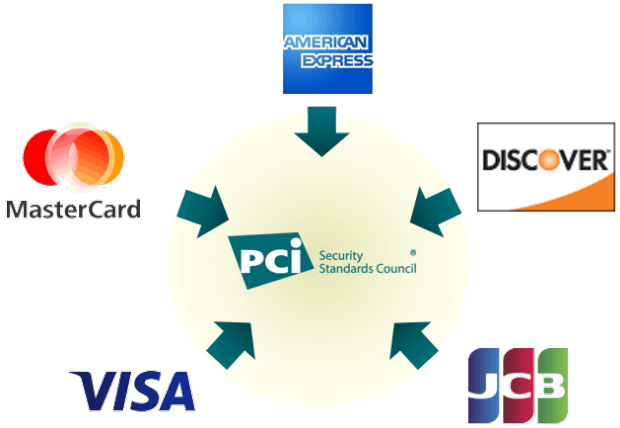
- CVSS starts from the vulnerabilities when organizing impact assessment
  - http://www.first.org/cvss/
  - http://web.nvd.nist.gov/view/vuln/search (US National Vulnerability Database)
- Impact of a vulnerability may change over time
- Impact of a vulnerability may depend on the specific environment a system is deployed in
- Not all sources of vulnerability reports are equally reliable

Benefits

- Objectivity over subjectivity. Example: avoid arguments like, "it's severe!", "no, it's not!", "yes, it is!"
- Standardized vulnerability scores for organizations. An organization can leverage a single vulnerability management policy defining the maximum allowable time to validate and remediate a given vulnerability
- Transparency for users. Users may be confused when a vulnerability is assigned an arbitrary score by a third party. With CVSS, the individual characteristics used to derive a score are transparent
- Helps prioritize risk. Especially when the environmental score is computed, the vulnerability becomes contextual & specific to each organization

Used as Industrial Standard

- In September 2007, CVSS v2.0 was adopted as part of the Payment Card Industry Data Security Standard (PCI DSS)
- In order to comply with PCI DSS, merchants processing credit cards must demonstrate that none of their computing systems has a vulnerability with a CVSS score greater than or equal to 4.0



Vulnerability categorization

To assist customers in prioritizing the solution or mitigation of identified issues, ASVs must assign a severity level to each identified vulnerability or mis-configuration.

The designation of each severity level must allow an easy comparison between levels. Therefore, a severity ranking that is easy to understand must be presented, such as with levels Low Priority, Medium Priority, and Urgent.

Wherever possible, the ASV must use the CVSS base score for the severity level.

Compliance determination

Reports must indicate compliance determination at two levels: component and (global) customer level.

The following statements provide the necessary guidance to ASVs to determine compliance at component level and customer level.

Component compliance determination

Generally, to be considered compliant, a component must not contain any vulnerability that has been assigned a CVSS base score equal to or higher than 4.0.

Source: Sohttps://www.pcisecuritystandards.org/pdfs/pci_dss_asv_tech_op_req.pdf

CVSS v2.0 – Scoring Scheme

Basic metrics		Temporal metrics	Environmental metrics	
Access vector	Confidentiality impact	Exploitability	Collateral damage potential	Confidentiality requirement
Access complexity	Integrity impact	Remediation level	Target distribution	Integrity requirement
Authentication	Availability impact	Report confidence		Availability requirement

From these individual ratings the CVSS severity is computed

CVSS – Basic Metrics

- Basic metric group: collects generic aspects of a vulnerability
  - Access vector: consider from where the vulnerability can be exploited (local or remote attacker?)
  - Access complexity: how complex an exploit would have to be (related to exploitability in DREAD)
  - Authentication: how many times an attacker would have to be authenticated during an attack; related to exposure
  - Ratings also consider the standard impact categories confidentiality, integrity, and availability

CVSS – Temporal Metrics

- Temporal metrics group: captures current state of exploits and countermeasures (may change overtime)
  - Exploitability captures the state of exploits available; related to reproducibility in DREAD
  - Remediation level: to which extent are fixes addressing the vulnerability available?
  - Report confidence: quality of source announcing the vulnerability

CVSS – Environmental Metrics

- Environmental metrics group: rates impacts on the assets of a given organisation
  - Collateral damage potential: damage outside the IT system, like loss of life, loss of productivity, or loss of physical assets
  - Target distribution: number of potential targets within the organisation
  - Environmental metrics: IT assets rated according to confidentiality, integrity, and availability
- These metrics allow the scoring analyst to promote or demote the importance of a vulnerable system according to her business risk

CVSS v2.0 vs CVSS v3.0

CVSS v2.0

Basic metrics		Temporal metrics	Environmental metrics	
Access vector	Confidentiality impact	Exploitability	Collateral damage potential	Confidentiality requirement
Access complexity	Integrity impact	Remediation level	Target distribution	Integrity requirement
Authentication	Availability impact	Report confidence		Availability requirement

CVSS v3.0

Basic metrics		Temporal metrics	Environmental metrics	
Exploitability	**Impact**			
Attack vector	Confidentiality impact	Exploit code maturity	Base Modifiers	Confidentiality requirement
Attack complexity	Integrity impact	Remediation level		Integrity requirement
Privileges Required	Availability impact	Report confidence		Availability requirement
User interaction				
Scope				

Access Vector and Access Complexity

- The Access Vector (from v2.0) has been renamed to Attack Vector, but still generally reflects the "remoteness" of the attacker relative to the vulnerable component
- But now, it also distinguishes between
  - Local attacks which require local system access (such as with an attack against a desktop application) and
  - Physical attacks which require physical access to the platform in order to exploit a vulnerability (such as with a firewire or USB)
- Access Complexity (from v2.0) didn't consider factors that are not under control by attacker such as user interaction requirements

Privilege Required

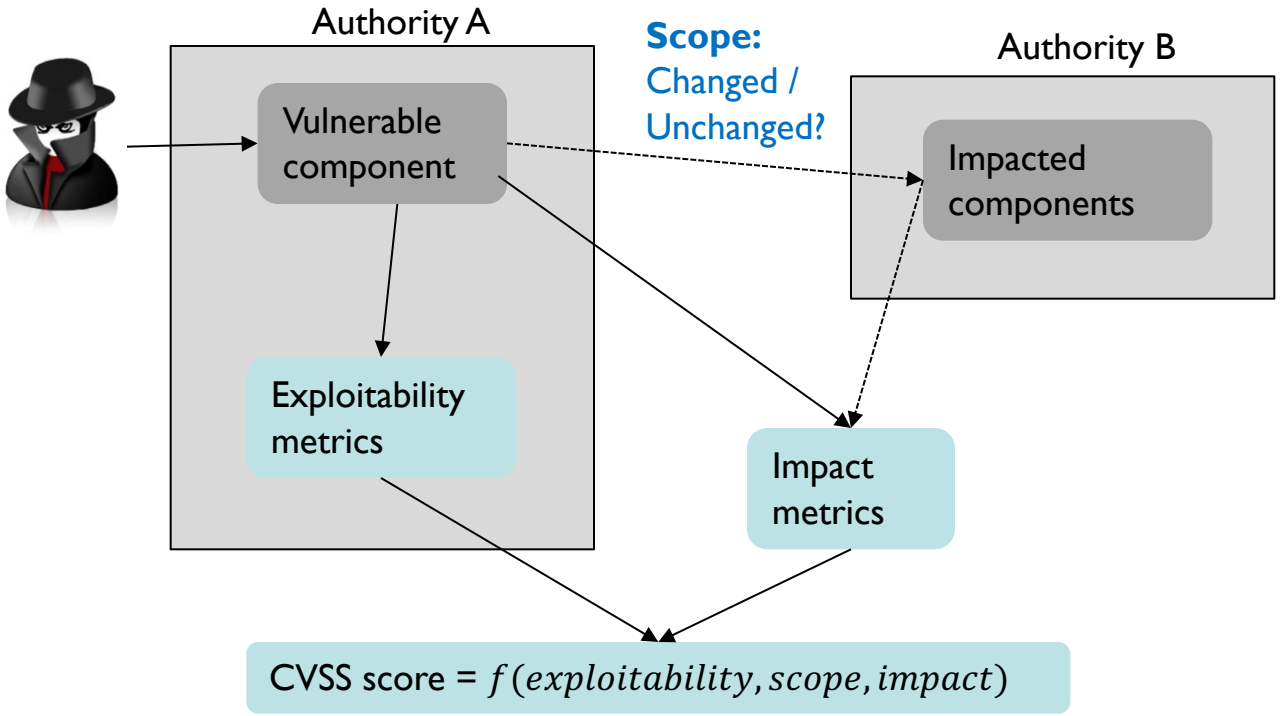
- The new metric, Privileges Required, replaces the Authentication metric of v2.0
- Instead of measuring the *number of times* an attacker must separately authenticate to a system, Privileges Required captures the *level of access* required for a successful attack

Scope, vulnerable component, and impacted component

- In v2.0 vulnerabilities are scored relative to the host (operating system, server)
- Presented difficulties for vendors when scoring vulnerabilities that would fully compromise their software, but only partially affect the host
- This led one application vendor to adopt a "Partial+" impact metric convention
- CVSS v3.0 addresses this issue with updates to where the impact metrics are scored and a new metric called Scope

Scope, vulnerable component, and impacted component

Therefore, an important conceptual change in CVSS v3.0 is the ability to score vulnerabilities that exist in one software component but impact a separate software, hardware, or networking component



Other Changes

- Temporal metrics: the influence of Temporal metrics has been reduced in v3.0, relative to v2.0. Exploitability has been renamed to Exploit Code Maturity to better represent what the metric is measuring
- Environmental metrics: Target Distribution and Collateral Damage Potential have been replaced by *modified factors* which accommodates mitigating controls or control weaknesses that may exist within the user's environment that could reduce or raise the impact of a successfully exploited vulnerability
- Qualitative rating scale: discussed earlier

Who scores?

- Anyone can create a CVSS score
- Two scorers can give different scores
- As new things are learnt, score can change
- Base and temporal – know vulnerable component
- Environmental – know component's deployment
- For some vulnerability, environmental metrics for one customer might be different than for another customer

CVSS – Scoring

- Each item on the score sheet has a fixed number of possible answers
- For example, the access vector can be "undefined", "local" or "remote"
- From the ratings given, the CVSS severity score is being calculated
- Score calculator is available at https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

phpMyAdmin Reflected Cross-site Scripting Vulnerability (CVE-2013-1937)

- Reflected XSS in the `tbl_gis_visualization.php` page in phpMyAdmin v3.5.8 or earlier versions
- These allow remote attackers to inject arbitrary client script via the two `visualizationSettings` parameters
- A successful exploit requires an attacker to perform reconnaissance of the system running the vulnerable phpMyAdmin software to determine a valid database name and obtain a valid session token
- The attacker constructs a URL to the web server running the vulnerable phpMyAdmin software that contains this database name and token

phpMyAdmin Reflected Cross-site Scripting Vulnerability (CVE-2013-1937)

- One of the two injectable parameters is added to the URL with its value set to the malicious code
- The attacker distributes this URL and entices a victim to click
- If a victim clicks on the URL, the malicious code will execute in the victim's web browser
- The malicious code is only able to access information associated with the website running the vulnerable phpMyAdmin software due to Same Origin Policy (SOP) restrictions in web browsers
- phpMyAdmin, by default, sets the `HttpOnly` flag on its cookies, preventing JavaScript from accessing cookies which limits the overall impact of this attack
- Fix: https://github.com/phpmyadmin/phpmyadmin/commit/79089c9bc02c82c15419fd9d6496b8781ae08a5a#diff-aa46e83ff38fe840e2b5647be8475334
- Learn more at: https://nvd.nist.gov/vuln/detail/CVE-2013-1937

Image courtesy of NVD (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator)

CVSS Score Calculator at NVD

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) | High (AC:H)

Privileges Required (PR)*

None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*

None (UI:N) | Required (UI:R)

Scope (S)*

Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*

None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*

None (A:N) | Low (A:L) | High (A:H)

* - All base metrics are required to generate a base score.

Temporal Score Metrics

Exploit Code Maturity (E)

Not Defined (E:X) | Unproven that exploit exists (E:U) | Proof of concept code (E:P) | Functional exploit exists (E:F) | High (E:H)

Remediation Level (RL)

Not Defined (RL:X) | Official fix (RL:O) | Temporary fix (RL:T) | Workaround (RL:W) | Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:X) | Unknown (RC:U) | Reasonable (RC:R) | Confirmed (RC:C)

Environmental Score Metrics

Exploitability Metrics

Attack Vector (MAV)

Not Defined (MAV:X) | Network (MAV:N) | Adjacent Network (MAV:A) | Local (MAV:L) | Physical (MAV:P)

Impact Metrics

Confidentiality Impact (MC)

Not Defined (MC:X) | None (MC:N) | Low (MC:L) | High (MC:H)

Impact Subscore Modifiers

Confidentiality Requirement (CR)

Not Defined (CR:X) | Low (CR:L) | Medium (CR:M) | High (CR:H)

CVSS for XSS – why is XSS a medium risk?

phpMyAdmin Reflected Cross-site Scripting Vulnerability (CVE-2013-1937)

- Reflected XSS in the `tbl_gis_visualization.php` page in phpMyAdmin 3.5.8 or before
- These allow remote attackers to inject arbitrary client script via the two `visualizationSettings` parameters
- A successful exploit requires an attacker to perform reconnaissance of the system running the vulnerable phpMyAdmin software to determine a valid database name and obtain a valid session token
- The attacker constructs a URL to the web server running the vulnerable phpMyAdmin software that contains this database name and token

phpMyAdmin Reflected Cross-site Scripting Vulnerability (CVE-2013-1937)

- One of the two injectable parameters is added to the URL with its value set to the malicious code
- The attacker distributes this URL and entices a victim to click
- If a victim clicks the URL, the malicious code will execute in the victim's web browser
- The malicious code is only able to access information associated with the website running the vulnerable phpMyAdmin software due to Same Origin Policy (SOP) restrictions in web browsers
- phpMyAdmin, by default, sets the HttpOnly flag on its cookies, preventing JavaScript from accessing cookies which limits the overall impact of this attack

CVSS v2 Base Score: 4.3

Metric	Value
Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality Impact	None
Integrity Impact	Partial
Availability Impact	None

Image courtesy of CVSS (https://www.first.org/cvss/examples)

Scoring tip from CVSS v2.0 Specs

- TIP #2: When scoring a vulnerability, consider the direct impact to the target host only
- For example, consider a cross-site scripting vulnerability: the impact to a user's system could be much greater than the impact to the target host. However, this is an indirect impact
- This cross-site scripting vulnerabilities should be scored with no impact to confidentiality or availability, and partial impact to integrity

Scoring Guide from CVSS v3.0

https://www.first.org/cvss/cvss-v30-user_guide_v1.5.pdf

- In CVSS v2.0, specific guidance was necessary to produce non-zero scores for cross-site scripting (XSS) vulnerabilities
- Because vulnerabilities were scored relative to the host operating system that contained the vulnerability

Scoring Guide from CVSS v3.0

https://www.first.org/cvss/cvss-v30-user_guide_v1.5.pdf

- This is one key reason why Scope was designed – where impacts are suffered not by the vulnerable component (e.g. web server), but by a component whose privileges are managed by a separate authority (e.g. browser).
- Under CVSS v3.0, XSS does not have to be constrained to the limited or non-existent impacts to the server, and can now be scored for impacts that are realized at the client.
- A reflected XSS vulnerability that allowed an attacker to deliver a malicious link to a victim and execute JavaScript in their browser might be scored:

`AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N`

CVSS v3.0 Base Score: 6.1

- User interaction requirement was captured
- Scope changed was captured

Metric	Value	Comments
Attack Vector	Network	The vulnerability is in the web application and reasonably requires network interaction with the server.
Attack Complexity	Low	Although an attacker needs to perform some reconnaissance of the target system, a valid session token can be easily obtained and many systems likely use well-known or default database names.
Privileges Required	None	An attacker requires no privileges to mount an attack.
User Interaction	Required	A successful attack requires the victim to visit the vulnerable component, e.g. by clicking a malicious URL.
Scope	Changed	The **vulnerable component** is the web server running the phpMyAdmin software. The **impacted component** is the victim's browser.
Confidentiality Impact	Low	Information maintained in the victim's web browser can be read and sent to the attacker. This is constrained to information associated with the web site running phpMyAdmin, and cookie data is excluded because the HttpOnly flag is enabled by default by phpMyAdmin. If the HttpOnly flag is not set, the Confidentiality Impact will become High if the attacker has access to sufficient cookie data to hijack the victim's session.
Integrity Impact	Low	Information maintained in the victim's web browser can be modified, but only information associated with the web site running phpMyAdmin.
Availability Impact	None	The malicious code can deliberately slow the victim's system, but the effect is usually minor and the victim can easily close the browser tab to terminate it.

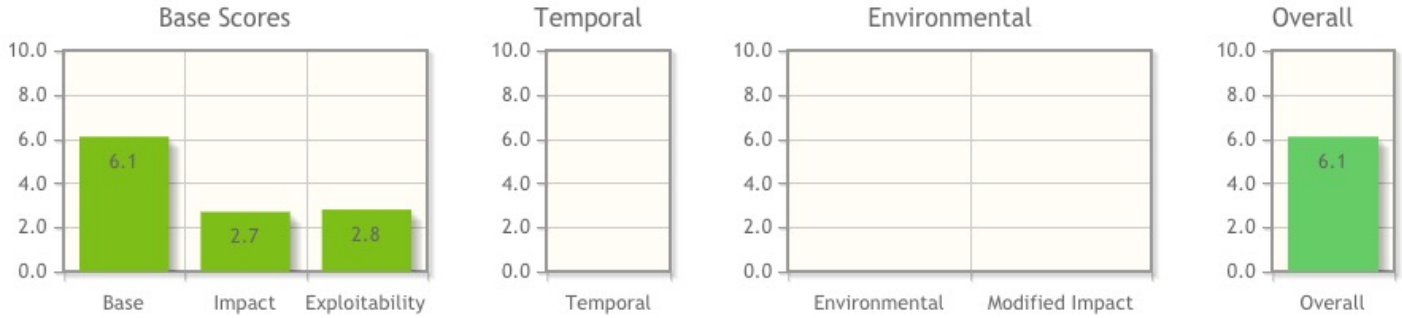
Image courtesy of CVSS (https://www.first.org/cvss/examples)

CVSS Score Calculator at NVD

Common Vulnerability Scoring System Calculator CVE-2013-1937

Source: NIST

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read th
standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed
such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environme



CVSS Base Score: 6.1
Impact Subscore: 2.7
Exploitability Subscore: 2.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 6.1

Show Equations

- Publish vector, which details each metric
  - E.g., CVSS 3.1 vector: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
- Even better: publish the vector URL (easy for users to revise)

Qualitative Representation

- CVSS provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity
- Some organizations created systems to map CVSS v2.0 Base scores to qualitative ratings
- CVSS v3.0 now provides a standard mapping from numeric scores to the severity rating terms – None, Low, Medium, High and Critical
- This helps organizations properly assess and prioritize their vulnerability management processes

Qualitative Severity Rating Scale

Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

- Help organizations properly assess and prioritize their vulnerability management processes
- Scores don't matter, actions associated with the ratings matter

Still a Medium Risk

- No impact on availability
- Confidential impact is considered low, due to indirect impact on confidentiality
- The rationale is that the remediation of the vulnerability is to solve it at its source (remove the possibility of XSS by having better input filtering). Improving data confidentiality won't solve the XSS issue
- Hence, still a medium risk even though attack complexity is low and no privilege required
- Up to organizations to apply Environmental metrics according to their business risks