

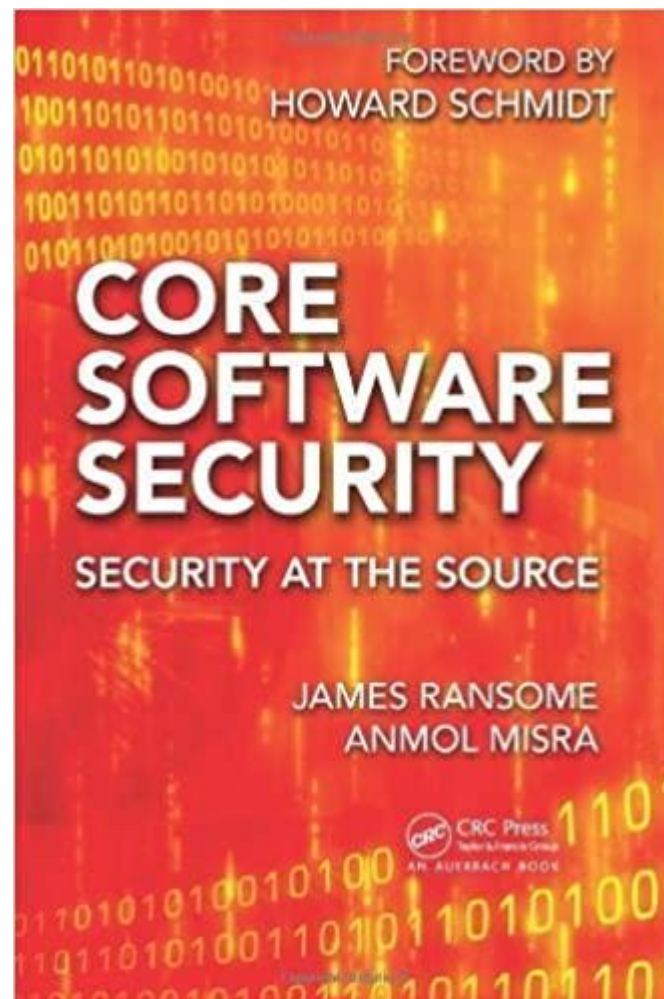
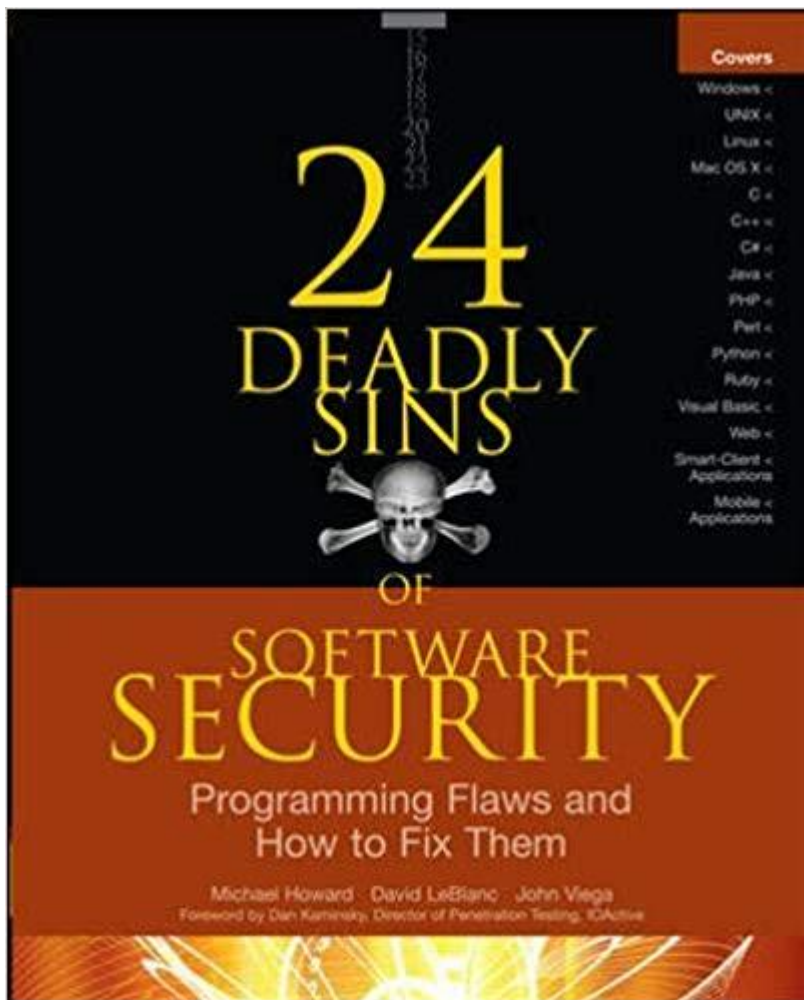
AN TOÀN PHẦN MỀM

Bài 01. Mở đầu

Nội dung học phần "An toàn phần mềm"

1. Lỗ hổng phần mềm, khai thác lỗ hổng phần mềm
(và cách phòng tránh lỗ hổng phần mềm)
2. Lập trình ứng dụng web an toàn
3. Lập trình sử dụng mật mã an toàn
4. Kiểm thử, phát hiện lỗ hổng phần mềm
5. Bảo vệ phần mềm
6. Quy trình phát triển phần mềm an toàn

Tài liệu tham khảo



HỌC VIỆN KỸ THUẬT MẬT MÃ

Lương Thế Dũng, Phạm Duy Trung

GIÁO TRÌNH

KỸ THUẬT LẬP TRÌNH AN TOÀN

2013

1

Lỗ hổng phần mềm

2

Phân loại lỗ hổng phần mềm

3

Các chủ đề xê-mi-na

1

Lỗ hổng phần mềm

2

Phân loại lỗ hổng phần mềm

3

Các chủ đề xê-mi-na

Khái niệm

- **Lỗ hổng phần mềm** là một **điểm yếu** hoặc là một **lỗi** trong phần mềm mà **có thể bị khai thác** bởi một kẻ tấn công để làm thay đổi hoạt động bình thường của phần mềm
- Thuật ngữ
 - Lỗ hổng = Vulnerability
 - Điểm yếu = Weakness
 - Lỗi = Bug

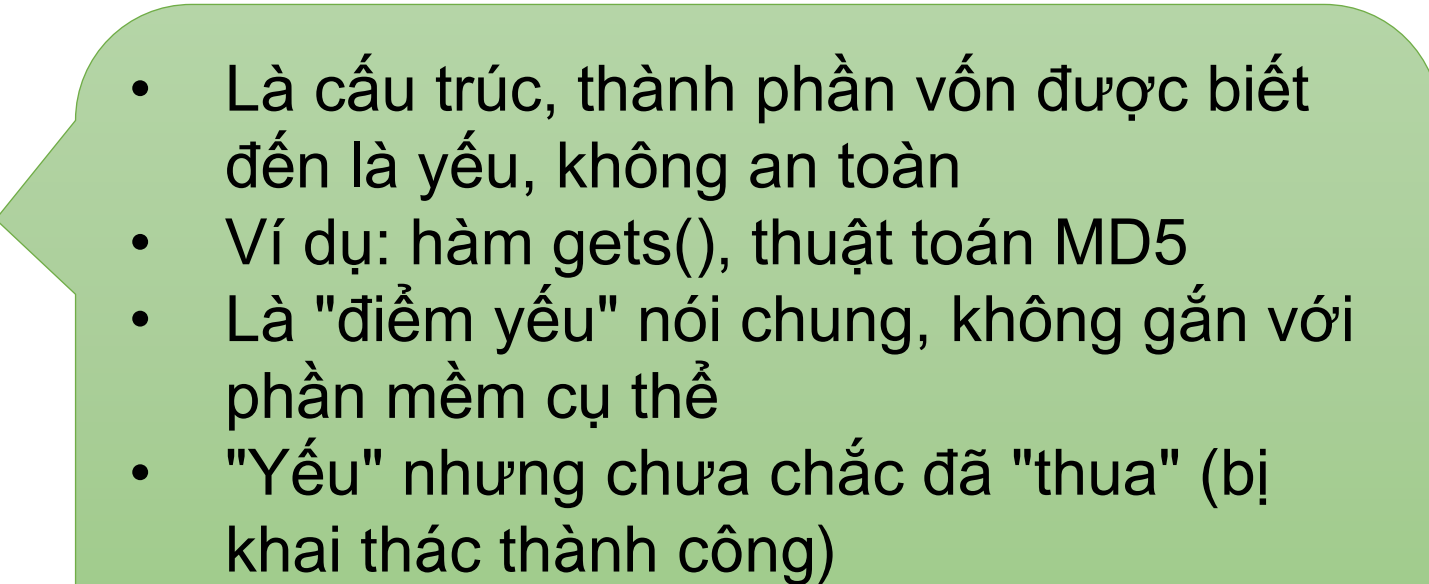
Khái niệm

- **Lỗ hổng phần mềm** là một **điểm yếu** hoặc là một **lỗi** trong phần mềm mà **có thể bị khai thác** bởi một kẻ tấn công để làm thay đổi hoạt động bình thường của phần mềm
- Thuật ngữ
 - Lỗ hổng = Vulnerability
 - Điểm yếu = Weakness
 - Lỗi = Bug

Là sai sót trong thiết kế, lập trình phát triển phần mềm. Ví dụ:

```
int a;  
while (a!=0)  
    scanf ("%d", a);
```

Khái niệm

- **Lỗ hổng phần mềm** là một **điểm yếu** hoặc là một **lỗi** trong phần mềm mà **có thể bị khai thác** bởi một kẻ tấn công để làm thay đổi hoạt động bình thường của phần mềm
 - Thuật ngữ
 - Lỗ hổng = Vulnerability
 - Điểm yếu = Weakness
 - Lỗi = Bug
- 
- Là cấu trúc, thành phần vốn được biết đến là yếu, không an toàn
 - Ví dụ: hàm gets(), thuật toán MD5
 - Là "điểm yếu" nói chung, không gắn với phần mềm cụ thể
 - "Yếu" nhưng chưa chắc đã "thua" (bị khai thác thành công)

Khái niệm

- **Lỗ hổng phần mềm** là một **điểm yếu** hoặc là một **lỗi** trong phần mềm mà **có thể bị khai thác** bởi một kẻ tấn công để làm thay đổi hoạt động bình thường của phần mềm
- Thuật ngữ
 - Lỗ hổng = Vulnerability
 - Điểm yếu = Weakness
 - Lỗi = Bug

- Là điểm yếu đã được kiểm chứng là có thể bị khai thác thành công
- Gắn với sản phẩm cụ thể
- Ví dụ: "Lỗ hổng MS08-067 của Windows"

Common Weakness Enumeration



- Website: <https://cwe.mitre.org/>
- Là cơ sở dữ liệu về các dạng điểm yếu của phần mềm
- Được phát triển bởi cộng đồng
- Cho mục đích phát triển, kiểm thử an toàn phần mềm

2019 CWE Top 10

Rank	ID	Name	Score
[1]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	75.56
[2]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.69
[3]	CWE-20	Improper Input Validation	43.61
[4]	CWE-200	Information Exposure	32.12
[5]	CWE-125	Out-of-bounds Read	26.53
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24.54
[7]	CWE-416	Use After Free	17.94
[8]	CWE-190	Integer Overflow or Wraparound	17.35
[9]	CWE-352	Cross-Site Request Forgery (CSRF)	15.54
[10]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.10

Thông tin về mỗi CWE

- Mô tả
- Ví dụ, bao gồm ví dụ thực tế
- Khả năng khai thác
- Hậu quả
- Cách phát hiện
- Cách khắc phục
- ...

Presentation Filter: Basic ▼

- Description
- Extended Description
- Relationships
- Modes Of Introduction
- Applicable Platforms
- Common Consequences
- Likelihood Of Exploit
- Demonstrative Examples
- Potential Mitigations
- Memberships
- Notes

Common Vulnerabilities and Exposures



- Là cơ sở dữ liệu về các lỗ hổng phần mềm và phần cứng đã được biết đến
- Mỗi lỗ hổng được gán một định danh duy nhất, tạo thuận lợi cho việc đối chiếu thông tin giữa các công cụ và dịch vụ an toàn thông tin khác nhau
- CVE-2019-16057: Lỗ hổng command injection trong thiết bị D-link được MITRE đánh giá mức độ nguy hiểm 10/10

Ví dụ về sự không thống nhất

- Cùng 1 file nhưng mỗi AV định danh một kiểu

Acronis	ⓘ Suspicious
AhnLab-V3	ⓘ Malware/Gen.Generic.C2865...
Alibaba	ⓘ Keygen:Win32/Generic.99dde...
SecureAge APEX	ⓘ Malicious
Avast	ⓘ Win32:Malware-gen
AVG	ⓘ Win32:Malware-gen



Common Vulnerabilities and Exposures

- Sử dụng mã định danh CVE đảm bảo mọi người "nói cùng ngôn ngữ"
- CVE cung cấp thông tin về từng lỗ hổng:
 - Sản phẩm có lỗ hổng
 - Bản chất lỗ hổng
 - Các tham chiếu tới các báo cáo về lỗ hổng

Nhiệm vụ bất khả thi



- Do tính chất phức tạp của phần mềm, việc loại trừ hoàn toàn lỗi hổng là không thể!
- Các hãng phần mềm lớn (Microsoft, Adobe,...) đã áp dụng triệt để quy trình phát triển phần mềm an toàn nhưng sản phẩm của họ vẫn có lỗi hổng.

Ví dụ về lỗ hổng và khai thác lỗ hổng

Cảnh báo e-mail mạo danh Thủ tướng phát tán mã độc-Công ...

<https://www.24h.com.vn> › Công nghệ thông tin - Translate this page

Jun 8, 2015 - Tin tức đang **mạo danh email** của **Thủ tướng** để **phát tán mã độc** ... Trong e-mail **gửi** đến không có nội dung mà chỉ có một file Word đính kèm ...

Cảnh báo e-mail mạo danh Thủ tướng phát tán mã độc ...

hanoimoi.com.vn › ban-in › Khoa-hoc › canh-bao-e-m... ▼ Translate this page

Cảnh báo e-mail **mạo danh Thủ tướng phát tán mã độc** ... Trong e-mail **gửi** đến không có nội dung mà chỉ có một file Word đính kèm giống với tiêu đề của thư.

Cảnh báo e-mail mạo danh Thủ tướng phát tán mã độc - Dân trí

<https://dantri.com.vn> › Sức mạnh số ▼ Translate this page

Jun 6, 2015 - Cảnh báo e-mail **mạo danh Thủ tướng phát tán mã độc** ... Trong e-mail **gửi** đến không có nội dung mà chỉ có một file Word đính kèm giống với ...

Ví dụ về lỗ hổng và khai thác lỗ hổng

Thấy gì từ Hội nghị TW 11



Hộp thư đến x



hongsam btctw pham <phamhongsam btctw@gmail.com>

tôi liet. btctw, yemvpctn, bcc: tôi



Thấy gì từ Hội nghị TW
11.doc

327 KB



Ví dụ về lỗ hổng và khai thác lỗ hổng

- thuhuyenvpcp@gmail.com
→ "Thông báo kết luận của Thủ tướng Nguyễn Tấn Dũng tại cuộc họp 03.6 về Luật ĐU'QT"
- phamhongsambtctw@gmail.com
→ "Thấy gì từ Hội nghị TW 11"
- vanphongbcy@gmail.com
→ "Kế hoạch nghỉ hè 2015"

CVE-2012-0158

(MS12-027)

Lỗ hổng của Microsoft Office!

Ví dụ về lỗ hổng và khai thác lỗ hổng

Vụ tấn công của WannaCry – Wikipedia tiếng Việt

[https://vi.wikipedia.org › wiki › Vụ_tấn_công_của_Wa...](https://vi.wikipedia.org/wiki/Vụ_tấn_công_của_WannaCry) ▼ Translate this page

WannaCry (tạm dịch là "Muốn khóc") còn được gọi là WannaDecryptor 2.0, là một phần mềm độc hại **mã độc** tổng tiền tự lan truyền trên các máy tính sử dụng ...

Bối cảnh và diễn biến · Các định dạng file mà ... · Hậu quả · Thủ phạm

Mã độc WannaCry: cơ chế hoạt động và cách phòng chống ...

antoanthongtin.vn › Detail ▼ Translate this page

Sep 20, 2017 - **WannaCry** là một loại **mã độc** tổng tiền (ransomware), với các tên gọi khác nhau như WannaCrypt0r 2.0 hay WCry. Phần mềm độc hại này mã ...

Cảnh báo về mã độc WannaCry - VNISA - VIETNAM ...

[https://vnisa.org.vn › canh-bao-ve-ma-doc-wannacry](https://vnisa.org.vn/canh-bao-ve-ma-doc-wannacry) ▼ Translate this page

Mã độc tổng tiền **WannaCry** đang lây lan trên toàn cầu, theo Cảnh sát châu Âu (Europol) hiện tại có ít nhất 200.000 nạn nhân của **WannaCry** tại 150 quốc gia và ...

Ví dụ về lỗ hổng và khai thác lỗ hổng

Payment will be raised on
5/16/2017 00:47:55

Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55

Time Left
06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
GMT from Monday to Friday

 **bitcoin**
ACCEPTED HERE

Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

Ví dụ về lỗ hổng và khai thác lỗ hổng

- Equation Group (NSA) → The Shadow Brokers → CVE-2017-0144 → WannaCry
- CVE-2017-0144 (MS17-010) là lỗ hổng của Windows, cụ thể là của dịch vụ SMB của Microsoft trên Windows
- CWE-20: Improper Input Validation

Zero-day vulnerability?

1

Lỗi hỏng phần mềm

2

Phân loại lỗi hỏng phần mềm

3

Các chủ đề xê-mi-na

Phân loại

- Phân loại: là việc phân chia một tập hợp thành các tập hợp con theo một tiêu chí phân loại nhất định
- Tiêu chí phân loại: là một đặc điểm của các phần tử được chọn để phân biệt các phần tử với nhau
- Ví dụ tiêu chí phân loại: Giới tính, Điểm trung bình, Độ tuổi, Cân nặng,...

Phân loại lỗi hỏng phần mềm

□ Tiêu chí phân loại

- Theo nguyên nhân xuất hiện
- Theo thời điểm xuất hiện (trong quy trình phát triển phần mềm)
- Theo mức độ nguy hiểm
 - Định tính
 - Định lượng

Phân loại theo nguyên nhân xuất hiện

- Lỗ hổng do kiểm tra dữ liệu:
 - Buffer Overflow,
 - Format String,
 - XSS,
 - SQL Injection...
- Lỗ hổng khác:
 - Race condition,
 - Sử dụng các thành tố mật mã không an toàn...

Phân loại theo thời điểm xuất hiện

Nghiên cứu sơ bộ (Preliminary Investigation)

Phân tích yêu cầu (Analysis)

Thiết kế hệ thống (Design of the System)

Xây dựng phần mềm (Software Construction)

Thử nghiệm hệ thống (System Testing)

Thực hiện, triển khai (System Implementation)


Bảo trì, nâng cấp (System Maintenance)

Giai đoạn Phân tích (đặc tả) yêu cầu

- Lỗi hỏng xuất hiện do không có yêu cầu về tính năng an toàn
- Ví dụ: không yêu cầu cơ chế chống spam ở trang "Liên hệ"

Nội dung

☐ Tôi không phải là người máy


reCAPTCHA
Bảo mật - Điều khoản

Gửi liên hệ

Giai đoạn Thiết kế

- Lỗi hỏng xuất hiện do:
 - Thiết kế luồng thực thi không an toàn
 - Lựa chọn hoặc cho phép lựa chọn các thành tố không an toàn
- Ví dụ: tấn công Padding Oracle lên chế độ CBC của mã khối

	1	2	3	4	5	6	7	8
Encrypted Input	0xF8	0x51	0xD6	0xCC	0x68	0xFC	0x95	0x37
	↓	↓	↓	↓	↓	↓	↓	↓
	TRIPLE DES							
	↓	↓	↓	↓	↓	↓	↓	↓
Intermediary Value	0x39	0x73	0x23	0x22	0x07	0x6a	0x26	0x3b
	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Initialization Vector	0x00	0x00	0x00	0x00	0x00	0x00	0x24	0x3f
	↓	↓	↓	↓	↓	↓	↓	↓
Decrypted Value	0x39	0x73	0x23	0x22	0x07	0x26	0x02	0x02

VALID PADDING



	1	2	3	4	5	6	7	8
Encrypted Input	0xF8	0x51	0xD6	0xCC	0x68	0xFC	0x95	0x37
	↓	↓	↓	↓	↓	↓	↓	↓
	TRIPLE DES							
	↓	↓	↓	↓	↓	↓	↓	↓
Intermediary Value	0x39	0x73	0x23	0x22	0x07	0x6a	0x26	0x3b
	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Initialization Vector	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x3f
	↓	↓	↓	↓	↓	↓	↓	↓
Decrypted Value	0x39	0x73	0x23	0x22	0x07	0x6a	0x26	0x02

INVALID PADDING



Giai đoạn Xây dựng (lập trình)

- Lỗi hỏng xuất hiện do sử dụng các hàm, các cấu trúc không an toàn, do không kiểm tra thỏa đáng dữ liệu đầu vào
- Ví dụ:
 - buffer overflow
 - format string
 - race condition
 - integer overflow...

Định tính mức độ nguy hiểm

- **Lỗi hỏng loại C (Mức thấp):** cho phép tấn công từ chối dịch vụ (DoS)
- **Lỗi hỏng loại B (Mức trung bình):** cho phép người dùng cục bộ leo thang đặc quyền hoặc truy cập trái phép.
- **Lỗi hỏng loại A (Mức cao):** cho phép người dùng từ xa có thể truy nhập trái phép vào hệ thống

Định lượng mức độ nguy hiểm

- Common Vulnerability Scoring System,
<https://www.first.org/cvss/>
- Có 3 nhóm đại lượng đặc trưng cho mỗi lỗ hổng
 - Base Metric Group
 - Temporal Metric Group
 - Environmental Metric Group

Base Metric Group

Exploitability Metrics

Attack Vector

Attack Complexity

Privileges Required

User Interaction

Impact Metrics

Confidentiality Impact

Integrity Impact

Availability Impact

Scope

Temporal Metric Group

Exploit Code Maturity

Remediation Level

Report Confidence

Environmental Metric Group

Modified Base Metrics

Confidentiality Requirement

Integrity Requirement

Availability Requirement

Định lượng mức độ nguy hiểm

- Mỗi đại lượng đều có thể đo được và nhận một giá trị nhất định
- Có công thức để tính điểm chung cho lỗ hổng từ giá trị của các đại lượng: <https://www.first.org/cvss/calculator/3.0>
- Thang điểm: 0.0 đến 10.0; điểm càng cao càng nguy hiểm

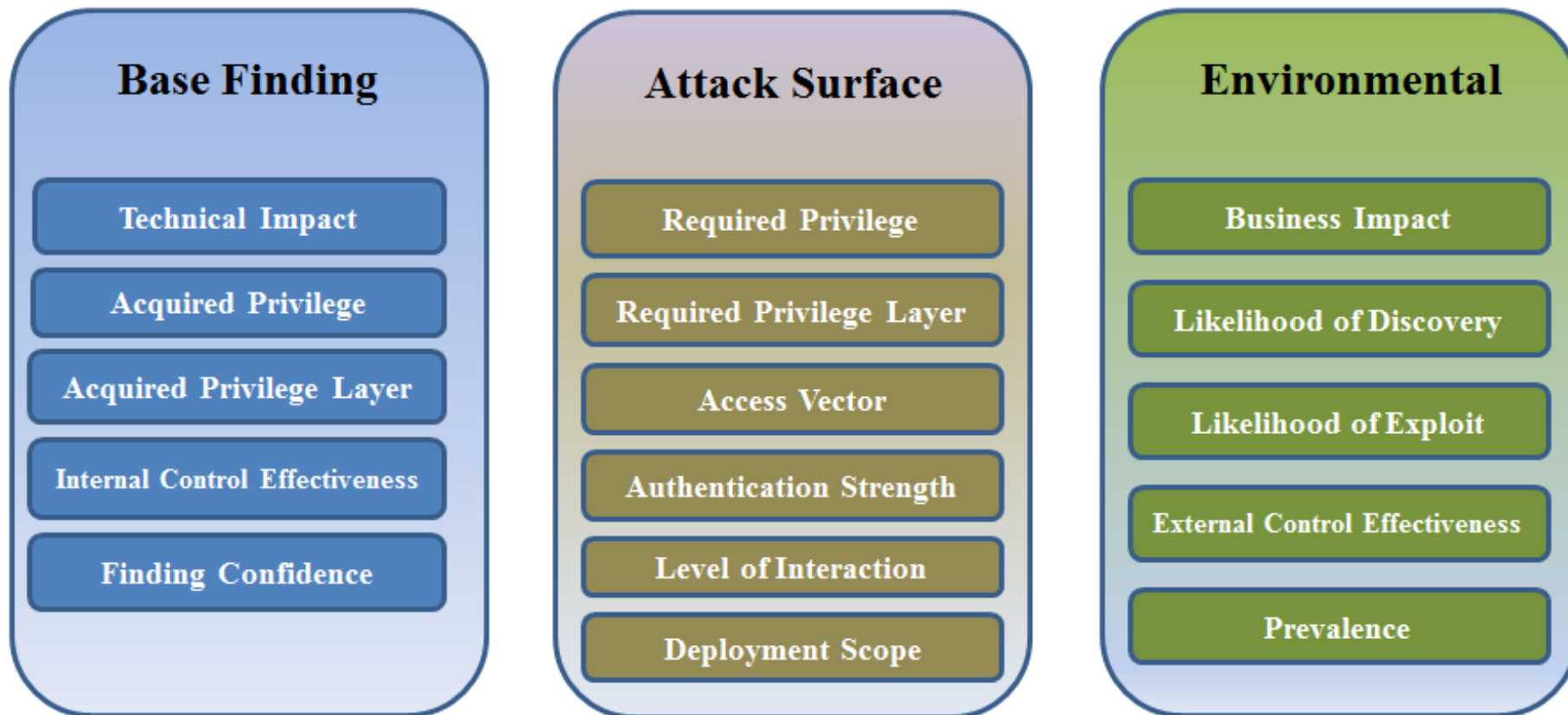
Định lượng mức độ nguy hiểm

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

Common Weakness Scoring System

- CWSS Metric Groups

https://cwe.mitre.org/cwss/cwss_v1.0.1.html



1

Lỗi hỏng phần mềm

2

Phân loại lỗi hỏng phần mềm

3

Các chủ đề xê-mi-na

Nội dung học phần "An toàn phần mềm"

1. Lỗi hỏng phần mềm, khai thác lỗi hỏng phần mềm (và cách phòng tránh lỗi hỏng phần mềm)
2. Lập trình ứng dụng web an toàn
3. Lập trình sử dụng mật mã an toàn
4. Kiểm thử, phát hiện lỗi hỏng phần mềm
5. Bảo vệ phần mềm
6. Quy trình phát triển phần mềm an toàn

Xê-mi-na Lập trình ứng dụng web an toàn

- Chủ đề

- Regular Expression và ứng dụng trong lọc dữ liệu
- SSO và quản lý người dùng khi sử dụng SSO
- Lập trình ứng dụng web an toàn với Laravel
- Lập trình ứng dụng web an toàn với Spring
- Lập trình ứng dụng web an toàn với ASP.NET
- Lập trình ứng dụng web an toàn với Joomla (hoặc WordPress)

- Yêu cầu

- "an toàn" = xác thực, phân quyền, cấp quyền, phòng chống tấn công (CSRF, XSS, SQLi) bằng các tính năng có sẵn trong framework
- Cấu trúc tối thiểu: tổng quan → hỗ trợ gì an toàn → sử dụng thế nào (không áp dụng cho Regular Expression và SSO).

Xê-mi-na Kiểm thử, phát hiện lỗi hồng phần mềm

- Chủ đề
 - Kiểm thử mã nguồn web
 - Kiểm thử mã nguồn C/C++
 - Kiểm thử fuzzing với AFL
 - Kiểm thử fuzzing với libFuzzer
- Yêu cầu:

Yêu cầu chung

- Lớp trưởng phân công nhiệm vụ
- Mỗi chủ đề trong xê-mi-na phải có Nhóm báo cáo, Nhóm phản biện và 01 người Chủ trì.
 - Nhóm báo cáo gửi tài liệu báo cáo cho Nhóm phản biện và người Chủ trì chậm nhất 02 ngày trước ngày xê-mi-na.
 - Mỗi thành viên Nhóm phản biện gửi ý kiến phản biện (bằng văn bản in) cho người Chủ trì ở đầu buổi xê-mi-na.
 - Người Chủ trì là điều phối việc báo cáo, phát biểu phản biện và hỏi đáp trong quá trình xê-mi-na, sau cùng đưa ra kết luận đánh giá. Tổng hợp và gửi tài liệu xê-mi-na cho giảng viên.
- Trong suốt học phần, mỗi người tham gia ít nhất 01 Nhóm báo cáo và 01 Nhóm phản biện.

Dự kiến thời gian xê-mi-na

- Thứ 7, 27/06: Lập trình ứng dụng web an toàn (1-3)
- Thứ 7, 04/07: Lập trình ứng dụng web an toàn (4-6)
- Thứ 7, 11/07: Kiểm thử, phát hiện lỗi hỏng phần mềm

