

**ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN  
PHÁT HIỆN LỖI VÀ LỖ HỔNG BẢO MẬT PHẦN MỀM**

**Chuyên ngành đào tạo: An toàn thông tin  
Bậc đào tạo: Đại học**

*(Ban hành kèm theo Quyết định Số 640/QĐ-ĐHTB, ngày 14/12/2019)*

**1. Tên học phần: PHÁT HIỆN LỖI VÀ LỖ HỔNG BẢO MẬT PHẦN MỀM**

**2. Số tín chỉ: 2 (2,0,4)**

**3. Trình độ: Cho sinh viên năm thứ ba**

**4. Phân bổ thời gian**

**- Lên lớp:**

Lý thuyết: 30 tiết

Thực hành: 0 tiết

**- Tự học: 30 x 2 = 60 giờ**

**5. Điều kiện tiên quyết:**

**6. Mục tiêu của học phần**

**6.1. Kiến thức**

Học phần này sẽ giúp sinh viên nắm được các lỗ hổng bảo mật cơ bản trong phần mềm cũng như một số các lỗi lập trình thường gặp có thể gây ra các lỗ hổng bảo mật như: buffer overflow, Vulnerable CGI program,.. Đồng thời, học phần này cũng sẽ giới thiệu một số các kỹ thuật, công cụ để phát hiện các lỗi bảo mật như: packet sniffing, port scanning,..

**6.2. Kỹ năng**

Sinh viên biết phân biệt các loại lỗ hổng bảo mật và biết sử dụng công cụ để phát hiện ra lỗi bảo mật.

**6.3. Về năng lực tự chủ và tự chịu trách nhiệm.**

- Có thái độ nghiêm túc trong học tập;

- Có đạo đức, lương tâm nghề nghiệp; có trách nhiệm với công việc, dám làm, dám chịu trách nhiệm

- Có ý thức tổ chức kỷ luật, chủ động trong quá trình học tập.

**7. Mô tả các nội dung học phần**

Học phần mô tả cho sinh viên hiểu được khái niệm về lỗ hổng bảo mật, lỗ hổng bảo mật phần mềm; Đưa ra các loại lỗi thường gặp khi lập trình làm gây ra lỗ hổng, cách nhận biết và phân biệt nó; Giới thiệu các công cụ phát hiện lỗi bảo mật.

**8. Nhiệm vụ của sinh viên**

- Dự lớp: Sinh viên phải tham gia tối thiểu 80% số tiết học trên lớp.

- Có đầy đủ điểm thường xuyên, điểm đánh giá nhận thức, làm bài tập ở nhà theo yêu cầu của giảng viên.

- Có đủ 2 bài kiểm tra định kỳ và bài tập lớn.
- Tham gia dự kỳ thi kết thúc học phần.
- Nghiên cứu tài liệu trước khi lên lớp.

## 9. Tài liệu học tập

### - Giáo trình chính:

[1]. Giáo trình Phát hiện lỗi và lỗ hổng bảo mật phần mềm – Trường Đại học Thái Bình

### - Sách tham khảo:

[1] Giáo trình An toàn và bảo mật thông tin – Trường Đại học Bách khoa Hà Nội.

[2] Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges - Chair: Marietje Schaake

## 10. Tiêu chuẩn đánh giá sinh viên

### 10.1. Tiêu chí đánh giá:

| STT | Điểm thành phần  | Quy định   | Trọng số | Ghi chú |
|-----|--|--|----------|---------|
| 1   | Điểm thường xuyên, đánh giá nhận thức, thái độ thảo luận, chuyên cần, làm bài tập ở nhà. | - Số tiết dự học/Tổng số tiết: 10%.<br>- Số bài tập đã làm/Tổng số bài tập được giao: 10%. | 10%      |         |
| 2   | Điểm kiểm tra định kỳ 2 lý thuyết 45'. Điểm tiểu luận.                                   | - 2 bài kiểm tra lý thuyết 1 tiết trên lớp.<br>- 1 bài tiểu luận                           | 30%      |         |
| 3   | Thi kết thúc học phần  | - Thi lý thuyết (60')  | 60%      |         |

### 10.2. Cách tính điểm:

- Sinh viên không tham gia đủ 80% số tiết học trên lớp không được thi lần đầu.
- Điểm thành phần để điểm lẻ đến một chữ số thập phân.
- Điểm kết thúc học phần làm tròn đến phần nguyên.

## 11. Thang điểm: 10

## 12. Nội dung chi tiết học phần

| Chương | Nội dung  | LT | TH |
|--------|---|----|----|
| 1      | <b>Chương 1: Tổng quan về bảo mật và an toàn thông tin</b><br>1. Khái quát về an toàn thông tin<br>2. Khái quát về bảo mật thông tin<br>3. Các yêu cầu đảm bảo An toàn thông tin<br>4. An toàn phần mềm | 3  | 0  |
| 2      | <b>Chương 2: Lỗ hổng bảo mật</b><br>1. Khái niệm lỗ hổng bảo mật<br>2. Nguyên nhân gây ra lỗ hổng<br>3. Sự khác biệt giữa lỗ hổng và rủi ro<br>4. Quản lý lỗ hổng, các phương pháp phát hiện lỗ hổng    | 9  | 0  |
| 3      | <b>Chương 3: Lỗ hổng phần mềm</b><br>1. Khái niệm về lỗ hổng phần mềm   | 12 | 0  |

| Chương | Nội dung   | LT | TH |
|--------|--|----|----|
|        | 2. Cách thức khai thác phần mềm trên máy tính<br>3. Các loại lỗ hổng bảo mật<br>4.1. Buffer overflow<br>4.2. CGI program |    |    |
| 4      | <b>Chương 4: Các công cụ phát hiện lỗi bảo mật</b><br>1. Packet sniffer<br>2. Port scanning                              | 6  | 0  |

### 13. Hình thức và nội dung từng tuần:

| HTTCDH                      | Nội dung  | Thời gian (tiết) | Yêu cầu SV chuẩn bị và địa chỉ tư liệu  | Ghi chú |
|-----------------------------|---|------------------|---|---------|
| <b>Nội dung 1: (Tuần 1)</b> |   |                  |   |         |
| Lý thuyết                   | <b>Chương 1: Tổng quan về bảo mật và an toàn thông tin</b><br>1. Khái quát về an toàn thông tin<br>2. Khái quát về bảo mật thông tin<br>3. Các yêu cầu đảm bảo An toàn thông tin<br>4. An toàn phần mềm | 3                | - Chuẩn bị tài liệu giáo trình môn học<br>- Nghiên cứu và đọc giáo trình Tài liệu [1], [2]      |         |
| <b>Nội dung 2: (Tuần 2)</b> |   |                  |   |         |
| Lý thuyết                   | <b>Chương 2: Lỗ hổng bảo mật</b><br>1. Khái niệm lỗ hổng bảo mật<br>2. Nguyên nhân gây ra lỗ hổng<br>3. Sự khác biệt giữa lỗ hổng và rủi ro   | 3                | - Chuẩn bị tài liệu giáo trình môn học<br>- Nghiên cứu và đọc giáo trình Tài liệu [1], [2], [3] |         |
| <b>Nội dung 3: (Tuần 3)</b> |   |                  |   |         |
| Lý thuyết                   | <b>Chương 2: Lỗ hổng bảo mật</b><br>4. Quản lý lỗ hổng, các phương pháp phát hiện lỗ hổng   | 3                | - Chuẩn bị tài liệu giáo trình môn học<br>- Nghiên cứu và đọc giáo trình Tài liệu [1], [3]      |         |
| <b>Nội dung 4: (Tuần 4)</b> |   |                  |   |         |
| Lý thuyết                   | 4. Quản lý lỗ hổng, các phương pháp phát hiện lỗ hổng <tiếp>  | 3                | - Chuẩn bị tài liệu giáo trình môn học<br>- Nghiên cứu  |         |

| HTTCDH                      | Nội dung   | Thời gian (tiết) | Yêu cầu SV chuẩn bị và địa chỉ tư liệu   | Ghi chú |
|-----------------------------|--|------------------|--|---------|
|                             |  |                  | và đọc giáo trình Tài liệu [1], [3]  |         |
| <b>Nội dung 5: (Tuần 5)</b> |  |                  |  |         |
| Lý thuyết                   | <b>Chương 3: Lỗ hổng phần mềm</b><br>1. Khái niệm về lỗ hổng phần mềm<br>2. Cách thức khai thác phần mềm trên máy tính                   | 3                | - Chuẩn bị tài liệu giáo trình môn học<br>- Nghiên cứu và đọc giáo trình Tài liệu [1] Tài liệu [2] |         |
| <b>Nội dung 6: (Tuần 6)</b> |  |                  |  |         |
| Lý thuyết                   | <b>Chương 3: Lỗ hổng phần mềm</b><br>3. Các loại lỗ hổng bảo mật<br>3.1 . Buffer overflow  | 3                | - Chuẩn bị tài liệu giáo trình môn học<br>- Nghiên cứu và đọc giáo trình Tài liệu [1], [3]         |         |
| <b>Nội dung 7:(Tuần 7)</b>  |  |                  |  |         |
| Lý thuyết                   | <b>Chương 3: Lỗ hổng phần mềm</b><br>3. Các loại lỗ hổng bảo mật<br>3.2. CGI program   | 2                | - Chuẩn bị tài liệu giáo trình môn học<br>- Nghiên cứu và đọc giáo trình Tài liệu [1], [3]         |         |
| Kiểm tra                    | Kiểm tra 1 tiết  | 1                |  |         |
| <b>Nội dung 8:(Tuần 8)</b>  |  |                  |  |         |
| Lý thuyết                   | <b>Chương 3: Lỗ hổng phần mềm</b><br>Sinh viên thảo luận – Tìm hiểu thêm các loại lỗ hổng bảo mật; Đưa ra so sánh giữa các loại lỗ hổng. | 3                | - Chuẩn bị tài liệu giáo trình môn học<br>- Nghiên cứu và đọc giáo trình Tài liệu [1], [3]         |         |
| <b>Nội dung 9: (Tuần 9)</b> |  |                  |  |         |
| Lý thuyết                   | <b>Chương 4: Các công cụ phát hiện lỗi bảo mật</b><br>1. Packet sniffer  | 3                | - Chuẩn bị tài liệu giáo trình môn học<br>- Nghiên cứu và đọc giáo trình Tài liệu [1], [3]         |         |

| HTTCDH                        | Nội dung   | Thời gian (tiết) | Yêu cầu SV chuẩn bị và địa chỉ tư liệu   | Ghi chú |
|-------------------------------|--|------------------|--|---------|
| <b>Nội dung 10: (Tuần 10)</b> |  |                  |  |         |
| Lý thuyết                     | <b>Chương 4: Các công cụ phát hiện lỗi bảo mật</b><br>2. Port scanning | 2                | - Chuẩn bị tài liệu giáo trình môn học<br>- Nghiên cứu và đọc giáo trình Tài liệu [1], [3] |         |
| Kiểm tra                      | - Kiểm tra đánh giá môn học  | 1                |  |         |

**TRƯỞNG KHOA**  
(Đã ký)

**TRƯỞNG BỘ MÔN**  
(Đã ký)