HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

Bản số: …

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Giới thiệu
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Trung tá, TS, Phan Việt Anh

HÀ NỘI, THÁNG 12 NĂM 2021

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

PHÊ DUYỆT
Ngày tháng 12 năm 2021
P.CHỦ NHIỆM KHOA

2// PGS.TS Tạ Minh Thanh

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Giới thiệu
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Ngày tháng 12 năm 2021
CHỦ NHIỆM BỘ MÔN

2// TS, Nguyễn Việt Hùng

HÀ NỘI, THÁNG 12 NĂM 2021

MỞ ĐẦU

Mục đích:

- - Nắm sơ lược về Học phần, các chính sách riêng của giáo viên, địa chỉ giáo viên.
- -Ý thức đươc tầm quan trọng và ý nghĩa của lập trình phần mềm an toàn
- -Thảo luận các nội dung đã học

Yêu cầu:

- - Đọc trước bài giảng
- - Chú ý nghe giảng

Nội dung bài giảng

Thời gian: 4 tiết (1-4)

Nội dung	Thời gian
Giới thiệu về lập trình phần mềm an toàn	**45'**
Một số hậu quả trong thực tế do lỗi phần mềm	**45'**
Nội dung môn học	**45'**
Trình bày và thảo luận nguyên nhân, hậu quả một số lỗi phần mềm trong thực tế	**45'**

KẾT LUẬN

Trong bài giảng này sinh viên đã được giới thiệu về các nội dung như sau:

Giới thiệu về lỗ hổng phần mềm, các thiệt hại có thể xảy ra trong thực tế do lỗi phần mềm. Sự cần thiết phải xây dựng phần mềm an toàn.

HƯỚNG DẪN NGHIÊN CỨU

1. Tiếp tục tìm hiểu các tài liệu trong tâm
   J. Viega and G. McGraw, "Building Secure Software: How to Avoid Security Problems the Right Way", Addison-Wesley, 2001.
2. Cài đặt thử nghiệm theo yêu cầu lý thuyết

Ngày tháng 12 năm 2021

NGƯỜI BIÊN SOẠN

2// TS Phan Việt Anh

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

Bản số: …

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Lỗ hổng phần mềm
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Trung tá, TS, Phan Việt Anh

HÀ NỘI, THÁNG 12 NĂM 2021

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

PHÊ DUYỆT
Ngày tháng 12 năm 2021
P.CHỦ NHIỆM KHOA

2// PGS.TS Tạ Minh Thanh

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Lỗ hổng phần mềm
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Ngày tháng 12 năm 2021
CHỦ NHIỆM BỘ MÔN

2// TS, Nguyễn Việt Hùng

HÀ NỘI, THÁNG 12 NĂM 2021

MỞ ĐẦU

Mục đích:

- - Giới thiệu cho học viên về lỗ hổng phần mềm và các hậu quả có thể xảy ra.
- - Tìm hiểu các loại lỗ hổng thường gặp.
- - Giới thiệu một mô hình xây dựng phần mềm an toàn

Yêu cầu:

- Đọc trước bài giảng
- Chú ý nghe giảng

Nội dung bài giảng

Thời gian: 4 tiết (5-8)

Nội dung	Thời gian
Ví dụ về lỗ hổng	**45'**
Các lỗ hổng từ bên ngoài	**45'**
Các lỗ hổng thường gặp và khả năng bị khai thác	**45'**
Xây dựng an toàn với mô hình BSIMM	**45'**

KẾT LUẬN

Trong bài giảng này sinh viên đã được giới thiệu về các nội dung như sau:

Một số ví dụ về lỗ hổng phần mềm. Các lỗ hổng thường gặp và khả năng bị khai thác. Tìm hiểu về phương pháp triển khai an toàn phần mềm với mô hình BSIMM

HƯỚNG DẪN NGHIÊN CỨU

1. Tiếp tục tìm hiểu các tài liệu trong tâm
   [TL1] J. Viega and G. McGraw, "Building Secure Software: How to Avoid Security Problems the Right Way", Addison-Wesley, 2001.
   [TL3] David Basin, Patrick Schaller, Michael Schlapfer, "Applied Information Security: A Hands-on Approach", Springer, 2011.
2. Cài đặt thử nghiệm theo yêu cầu lý thuyết

Ngày tháng 12 năm 2021

NGƯỜI BIÊN SOẠN

2// TS Phan Việt Anh

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

Bản số: …

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Lỗi bộ nhớ
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Trung tá, TS, Phan Việt Anh

HÀ NỘI, THÁNG 12 NĂM 2021

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

PHÊ DUYỆT
Ngày tháng 12 năm 2021
P.CHỦ NHIỆM KHOA

2// PGS.TS Tạ Minh Thanh

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Lỗi bộ nhớ
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Ngày tháng 12 năm 2021
CHỦ NHIỆM BỘ MÔN

2// TS, Nguyễn Việt Hùng

HÀ NỘI, THÁNG 12 NĂM 2021

MỞ ĐẦU

Mục đích:

- Hướng dẫn học viên tìm hiểu các lỗ hổng về lỗi bộ nhớ đối với ngôn ngữ lập trình bậc thấp.

Yêu cầu:

- Đọc trước bài giảng
- Chú ý nghe giảng

Nội dung bài giảng

Thời gian: 4 tiết (9-12)

Nội dung	Thời gian
Giới thiệu lỗi bộ nhớ	**45'**
Ngôn ngữ bậc thấp và thực thi	**45'**
Ngôn ngữ C và Assembler x86	**45'**
Tràn bộ nhớ	**45'**

KẾT LUẬN

Trong bài giảng này sinh viên đã được giới thiệu về các nội dung như sau:

Quá trình biên dịch và thực thi với một số ngôn ngữ bậc thấp. Nguy cơ lỗi do quản lý bộ nhớ trong ngôn ngữ bậc thấp.

HƯỚNG DẪN NGHIÊN CỨU

1. Tiếp tục tìm hiểu các tài liệu trong tâm
   [TL2] M. Howard and D. LeBlanc, "Writing Secure Code", Microsoft Press, second edition, 2003, Springer, 2011.
   [TL4] Fred Long et al. "The Oracle/CERT Secure Coding Standard for Java", Addison-Wesley, 2011
2. Cài đặt thử nghiệm theo yêu cầu lý thuyết

Ngày tháng 12 năm 2021

NGƯỜI BIÊN SOẠN

2// TS Phan Việt Anh

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

Bản số: …

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Lỗi bộ nhớ
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Trung tá, TS, Phan Việt Anh

HÀ NỘI, THÁNG 12 NĂM 2021

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

PHÊ DUYỆT
Ngày tháng 12 năm 2021
P.CHỦ NHIỆM KHOA

2// PGS.TS Tạ Minh Thanh

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Lỗi bộ nhớ
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Ngày tháng 12 năm 2021
CHỦ NHIỆM BỘ MÔN

2// TS, Nguyễn Việt Hùng

HÀ NỘI, THÁNG 12 NĂM 2021

MỞ ĐẦU

Mục đích:

- - Giới thiệu cho sinh viên lỗi bộ nhớ trên stack và heap
- - Hướng dẫn phương pháp tấn công và hậu quả tiềm ẩn với lỗi bộ nhớ heap và stack.

Yêu cầu:

- Đọc trước bài giảng
- Chú ý nghe giảng

Nội dung bài giảng

Thời gian: 4 tiết (13-16)

Nội dung	Thời gian
Lỗi biến trên stack	**45'**
Khai thác mã thực thi - Shell code - Chuyển hướng luồng thực thi	**45'**
Tràn vùng đệm trên heap - Một số trường hợp tấn công heap - Phương pháp chung tấn công heap	**45'**
Thảo luận	**45'**

KẾT LUẬN

Trong bài giảng này sinh viên đã được giới thiệu về các nội dung như sau:

Lỗi bộ nhớ heap. Khả năng và các nguy cơ tiềm ẩn của lỗi bộ nhớ heap.

HƯỚNG DẪN NGHIÊN CỨU

1. Tiếp tục tìm hiểu các tài liệu trong tâm
   [TL2] M. Howard and D. LeBlanc, "Writing Secure Code", Microsoft Press, second edition, 2003, Springer, 2011.
   [TL4] Fred Long et al. "The Oracle/CERT Secure Coding Standard for Java", Addison-Wesley, 2011
2. Cài đặt thử nghiệm theo yêu cầu lý thuyết

Ngày tháng 12 năm 2021

NGƯỜI BIÊN SOẠN

2// TS Phan Việt Anh

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

Bản số: …

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Lỗi bộ nhớ
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Trung tá, TS, Phan Việt Anh

HÀ NỘI, THÁNG 12 NĂM 2021

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

PHÊ DUYỆT
Ngày tháng 12 năm 2021
P.CHỦ NHIỆM KHOA

2// PGS.TS Tạ Minh Thanh

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Lỗi bộ nhớ
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Ngày tháng 12 năm 2021
CHỦ NHIỆM BỘ MÔN

2// TS, Nguyễn Việt Hùng

HÀ NỘI, THÁNG 12 NĂM 2021

MỞ ĐẦU

Mục đích:

- Thực hành viết chương trình bằng ngôn ngữ C có lỗ hổng tràn bộ nhớ trên stack và heap

Yêu cầu:

- - Đọc trước bài giảng
- - Chú ý nghe giảng
- - Làm bài tập trong sách tham khảo, giáo viên giao

Nội dung bài giảng

Thời gian: 4 tiết (17-20)

Nội dung	Thời gian
Thực hành Viết các chương trình minh họa các tình huống khác nhau có thể xảy ra tràn bộ nhớ trên stack và heap.	**45'**
Thực hành Viết các chương trình minh họa các tình huống khác nhau có thể xảy ra tràn bộ nhớ trên stack và heap.	**45'**
Thực hành Viết các chương trình minh họa các tình huống khác nhau có thể xảy ra tràn bộ nhớ trên stack và heap.	**45'**
Thực hành Viết các chương trình minh họa các tình huống khác nhau có thể xảy ra tràn bộ nhớ trên stack và heap.	**45'**

KẾT LUẬN

Trong bài giảng này sinh viên đã được giới thiệu về các nội dung như sau:

Viết chương trình minh họa và khai thác lỗi tràn bộ nhớ heap và stack

HƯỚNG DẪN NGHIÊN CỨU

1. Tiếp tục tìm hiểu các tài liệu trong tâm
2. Cài đặt thử nghiệm theo yêu cầu lý thuyết

Ngày tháng 12 năm 2021

NGƯỜI BIÊN SOẠN

2// TS Phan Việt Anh

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

Bản số: …

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Lỗi bộ nhớ
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Trung tá, TS, Phan Việt Anh

HÀ NỘI, THÁNG 12 NĂM 2021

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

PHÊ DUYỆT
Ngày tháng 12 năm 2021
P.CHỦ NHIỆM KHOA

2// PGS.TS Tạ Minh Thanh

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Lỗi bộ nhớ
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Ngày tháng 12 năm 2021
CHỦ NHIỆM BỘ MÔN

2// TS, Nguyễn Việt Hùng

HÀ NỘI, THÁNG 12 NĂM 2021

MỞ ĐẦU

Mục đích:

- - Giới thiệu cho sinh viên một số loại lỗ hổng liên quan đến sử dụng con trỏ, kiểu dữ liệu
- - Phương pháp hạn chế lỗi bộ nhớ khi lập trình, và phương pháp bảo vệ bộ nhớ.

Yêu cầu:

- Đọc trước bài giảng
- Chú ý nghe giảng

Nội dung bài giảng

Thời gian: 4 tiết (21-24)

Nội dung	Thời gian
Các lỗi bộ nhớ khác - Lỗi ngoài luồng, Tràn số, con trỏ, - Nhầm lẫn kiểu dữ liệu	**45'**
Các biện pháp phòng chống lỗi bộ nhớ - Phát hiện giả mạo - Bảo vệ chế độ bộ nhớ	**45'**
- Đa dạng hóa chương trình - Tránh lỗi trong lập trình	**45'**
Thảo luận	**45'**

KẾT LUẬN

Trong bài giảng này sinh viên đã được giới thiệu về các nội dung như sau:

Tìm hiểu một số loại lỗi bộ nhớ khác như tràn số, sử dụng con trỏ, hoặc nhầm lẫn kiểu dữ liệu. Các biện pháp phòng chống lỗi bộ nhớ trong soạn thảo chương trình.

HƯỚNG DẪN NGHIÊN CỨU

1. Tiếp tục tìm hiểu các tài liệu trong tâm
   [TL2] M. Howard and D. LeBlanc, "Writing Secure Code", Microsoft Press, second edition, 2003, Springer, 2011.
   [TL4] Fred Long et al. "The Oracle/CERT Secure Coding Standard for Java", Addison-Wesley, 2011
2. Cài đặt thử nghiệm theo yêu cầu lý thuyết

Ngày tháng 12 năm 2021

NGƯỜI BIÊN SOẠN

2// TS Phan Việt Anh

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

Bản số: …

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Các lỗ hổng CVE
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Trung tá, TS, Phan Việt Anh

HÀ NỘI, THÁNG 12 NĂM 2021

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

PHÊ DUYỆT
Ngày tháng 12 năm 2021
P.CHỦ NHIỆM KHOA

2// PGS.TS Tạ Minh Thanh

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Các lỗ hổng CVE
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Ngày tháng 12 năm 2021
CHỦ NHIỆM BỘ MÔN

2// TS, Nguyễn Việt Hùng

HÀ NỘI, THÁNG 12 NĂM 2021

MỞ ĐẦU

Mục đích:

- Giới thiệu cho sinh viên nắm được một số lỗ hổng CVE phổ biến.
- Giới thiệu cho sinh viên kiểu tấn công dựa trên nhập dữ liệu đầu vào để chèn lệnh (injection).

Yêu cầu:

- Đọc trước bài giảng
- Chú ý nghe giảng

Nội dung bài giảng

Thời gian: 4 tiết (25-28)

Nội dung	Thời gian
Xếp hạng các kiểu lỗ hổng	**45'**
Tấn công chèn mã lệnh	**45'**
Chèn siêu ký tự vào các lệnh shell	**45'**
Các biến môi trường	**45'**

KẾT LUẬN

Trong bài giảng này sinh viên đã được giới thiệu về các nội dung như sau:

Giới thiệu 10 loại lỗ hổng CVE phổ biến. Kiểu tấn công chèn mã lệnh sử dụng shell, và thay đổi biến môi trường.

HƯỚNG DẪN NGHIÊN CỨU

1. Tiếp tục tìm hiểu các tài liệu trong tâm
   [TL1] J. Viega and G. McGraw, "Building Secure Software: How to Avoid Security Problems the Right Way", Addison-Wesley, 2001.
   [TL6] The OWASP web application security project
2. Cài đặt thử nghiệm theo yêu cầu lý thuyết

Ngày tháng 12 năm 2021

NGƯỜI BIÊN SOẠN

2// TS Phan Việt Anh

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

Bản số: …

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Các lỗ hổng CVE
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Trung tá, TS, Phan Việt Anh

HÀ NỘI, THÁNG 12 NĂM 2021

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

PHÊ DUYỆT
Ngày tháng 12 năm 2021
P.CHỦ NHIỆM KHOA

2// PGS.TS Tạ Minh Thanh

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Các lỗ hổng CVE
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Ngày tháng 12 năm 2021
CHỦ NHIỆM BỘ MÔN

2// TS, Nguyễn Việt Hùng

HÀ NỘI, THÁNG 12 NĂM 2021

MỞ ĐẦU

Mục đích:

- Hướng dẫn học viên tìm hiểu về phương pháp tấn công SQL Injection và phương pháp phòng chống.

Yêu cầu:

- Đọc trước bài giảng
- Chú ý nghe giảng

Nội dung bài giảng

Thời gian: 4 tiết (29-32)

Nội dung	Thời gian
Tấn công chèn vào lệnh SQL	**45'**
Một số ví dụ tấn công SQL trong thực tế và hậu quả	**45'**
Phân loại - Cách thức và động cơ tấn công - Các dạng mã SQL được chèn vào	**45'**
Phòng tránh và phát hiện tấn công SQL Injection	**45'**

KẾT LUẬN

Trong bài giảng này sinh viên đã được giới thiệu về các nội dung như sau:

Giới thiệu phương pháp tấn công chèn lệnh SQL. Các kiểu tấn công SQL Injection và cách phòng chống.

HƯỚNG DẪN NGHIÊN CỨU

1. Tiếp tục tìm hiểu các tài liệu trong tâm
   [TL1] J. Viega and G. McGraw, "Building Secure Software: How to Avoid Security Problems the Right Way", Addison-Wesley, 2001.
   [TL6] The OWASP web application
2. Cài đặt thử nghiệm theo yêu cầu lý thuyết

Ngày tháng 12 năm 2021

NGƯỜI BIÊN SOẠN

2// TS Phan Việt Anh

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

Bản số: …

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Các lỗ hổng CVE
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Trung tá, TS, Phan Việt Anh

HÀ NỘI, THÁNG 12 NĂM 2021

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

PHÊ DUYỆT
Ngày tháng 12 năm 2021
P.CHỦ NHIỆM KHOA

2// PGS.TS Tạ Minh Thanh

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Các lỗ hổng CVE
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Ngày tháng 12 năm 2021
CHỦ NHIỆM BỘ MÔN

2// TS, Nguyễn Việt Hùng

HÀ NỘI, THÁNG 12 NĂM 2021

MỞ ĐẦU

Mục đích:

- Hướng dẫn thực hành khai thác, và phòng tránh lỗ hổng dựa trên nhập dữ liệu đầu vào.

Yêu cầu:

- Đọc trước bài giảng
- Chú ý nghe giảng

Nội dung bài giảng

Thời gian: 4 tiết (33-36)

Nội dung	Thời gian
Thực hành khai thác và phòng tránh lỗ hổng dựa trên nhập dữ liệu đầu vào	**45'**
Thực hành khai thác và phòng tránh lỗ hổng dựa trên nhập dữ liệu đầu vào	**45'**
Thực hành khai thác và phòng tránh lỗ hổng dựa trên nhập dữ liệu đầu vào	**45'**
Thực hành khai thác và phòng tránh lỗ hổng dựa trên nhập dữ liệu đầu vào	**45'**

KẾT LUẬN

Trong bài giảng này sinh viên đã được giới thiệu về các nội dung như sau:

Các bài tập thực hành tấn công và khắc phục lỗi chèn dữ liệu đầu vào

HƯỚNG DẪN NGHIÊN CỨU

1. Tiếp tục tìm hiểu các tài liệu trong tâm
2. Cài đặt thử nghiệm theo yêu cầu lý thuyết

Ngày tháng 12 năm 2021

NGƯỜI BIÊN SOẠN

2// TS Phan Việt Anh

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

Bản số: …

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Phát triển phần mềm
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Trung tá, TS, Phan Việt Anh

HÀ NỘI, THÁNG 12 NĂM 2021

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

PHÊ DUYỆT
Ngày tháng 12 năm 2021
P.CHỦ NHIỆM KHOA

2// PGS.TS Tạ Minh Thanh

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Phát triển phần mềm
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Ngày tháng 12 năm 2021
CHỦ NHIỆM BỘ MÔN

2// TS, Nguyễn Việt Hùng

HÀ NỘI, THÁNG 12 NĂM 2021

MỞ ĐẦU

Mục đích:

- Giới thiệu về quy trình phát triển phần mềm an toàn. Phân tích các mối rủi ro trong từng giai đoạn phát triển

Yêu cầu:

- Đọc trước bài giảng
- Chú ý nghe giảng

Nội dung bài giảng

Thời gian: 4 tiết (37-40)

Nội dung	Thời gian
Vòng đời phát triển phần mềm an toàn Kiểm tra và sửa mã nguồn	**45'**
Phân tích các mối rủi ro kiến trúc Kiểm tra xâm nhập	**45'**
- Kiểm tra bảo mật dựa trên rủi ro - Các trường hợp lạm dụng	**45'**
Yêu cầu bảo mật Các hành động bảo mật	**45'**

KẾT LUẬN

Trong bài giảng này sinh viên đã được giới thiệu về các nội dung như sau:

Các giai đoạn của vòng đời phát triển phần mềm an toàn.

HƯỚNG DẪN NGHIÊN CỨU

1. Tiếp tục tìm hiểu các tài liệu trong tâm
   [TL1] J. Viega and G. McGraw, "Building Secure Software: How to Avoid Security Problems the Right Way", Addison-Wesley, 2001.
2. Cài đặt thử nghiệm theo yêu cầu lý thuyết

Ngày tháng 12 năm 2021

NGƯỜI BIÊN SOẠN

2// TS Phan Việt Anh

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

Bản số: …

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: An toàn ứng dụng Web
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Trung tá, TS, Phan Việt Anh

HÀ NỘI, THÁNG 12 NĂM 2021

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

PHÊ DUYỆT
Ngày tháng 12 năm 2021
P.CHỦ NHIỆM KHOA

2// PGS.TS Tạ Minh Thanh

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: An toàn ứng dụng Web
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Ngày tháng 12 năm 2021
CHỦ NHIỆM BỘ MÔN

2// TS, Nguyễn Việt Hùng

HÀ NỘI, THÁNG 12 NĂM 2021

MỞ ĐẦU

Mục đích:

- Giới thiệu cho sinh viên các vấn đề có thể mất an toàn đối với ứng dụng web, cách phòng chống

Yêu cầu:

- Đọc trước bài giảng
- Chú ý nghe giảng

Nội dung bài giảng

Thời gian: 4 tiết (41-44)

Nội dung	Thời gian
Giới thiệu	**45'**
Giao thức HTTP	**45'**
Xác thực	**45'**
Cookie và session	**45'**

KẾT LUẬN

Trong bài giảng này sinh viên đã được giới thiệu về các nội dung như sau:

Các vấn đề mất an toàn đối với ứng dụng web

HƯỚNG DẪN NGHIÊN CỨU

1. Tiếp tục tìm hiểu các tài liệu trong tâm
   [TL6] The OWASP web application security project
2. Cài đặt thử nghiệm theo yêu cầu lý thuyết

Ngày tháng 12 năm 2021

NGƯỜI BIÊN SOẠN

2// TS Phan Việt Anh

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

Bản số: …

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Kiểm tra mã nguồn và phân tích chương trình
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Trung tá, TS, Phan Việt Anh

HÀ NỘI, THÁNG 12 NĂM 2021

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

PHÊ DUYỆT
Ngày tháng 12 năm 2021
P.CHỦ NHIỆM KHOA

2// PGS.TS Tạ Minh Thanh

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Kiểm tra mã nguồn và phân tích chương trình
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Ngày tháng 12 năm 2021
CHỦ NHIỆM BỘ MÔN

2// TS, Nguyễn Việt Hùng

HÀ NỘI, THÁNG 12 NĂM 2021

MỞ ĐẦU

Mục đích:

- Giới thiệu cho sinh viên một số kỹ thuật phân tích tĩnh để phát hiện các lỗ hổng trong chương trình

Yêu cầu:

- Đọc trước bài giảng
- Chú ý nghe giảng

Nội dung bài giảng

Thời gian: 4 tiết (45-48)

Nội dung	Thời gian
Tổng quan	**45'**
Các lỗ hổng và phân tích	**45'**
Sử dụng phân tích tĩnh	**45'**
Một số phương pháp phân tích tĩnh đơn giản - Kiểm tra kiểu dữ liệu - Kiểm tra quy cách viết mã nguồn	**45'**

KẾT LUẬN

Trong bài giảng này sinh viên đã được giới thiệu về các nội dung như sau:

Phương pháp và công cụ phân tích tĩnh để phát hiện lỗ hổng phần mềm

HƯỚNG DẪN NGHIÊN CỨU

1. Tiếp tục tìm hiểu các tài liệu trong tâm
   [TL5] B. Chess and J. West, "Secure Programming with Static Analysis", Addison-Wesley, 2007
2. Cài đặt thử nghiệm theo yêu cầu lý thuyết

Ngày tháng 12 năm 2021

NGƯỜI BIÊN SOẠN

2// TS Phan Việt Anh

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

Bản số: …

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Kiểm tra mã nguồn và phân tích chương trình
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Trung tá, TS, Phan Việt Anh

HÀ NỘI, THÁNG 12 NĂM 2021

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

PHÊ DUYỆT
Ngày tháng 12 năm 2021
P.CHỦ NHIỆM KHOA

2// PGS.TS Tạ Minh Thanh

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Kiểm tra mã nguồn và phân tích chương trình
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Ngày tháng 12 năm 2021
CHỦ NHIỆM BỘ MÔN

2// TS, Nguyễn Việt Hùng

HÀ NỘI, THÁNG 12 NĂM 2021

MỞ ĐẦU

Mục đích:

- Hướng dẫn các phương pháp phân tích động để kiểm tra chương trình
- Yêu cầu đối với sinh viên

Yêu cầu:

- Đọc trước bài giảng
- Chú ý nghe giảng

Nội dung bài giảng

Thời gian: 4 tiết (49-52)

Nội dung	Thời gian
Tìm hiểu chương trình	**45'**
Kiểm thử chương trình và kiểm tra tài nguyên	**45'**
Phát hiện lỗi	**45'**
Phân tích động	**45'**

KẾT LUẬN

Trong bài giảng này sinh viên đã được giới thiệu về các nội dung như sau:

Phương pháp và một số môi trường giả lập để phân tích động phát hiện lỗi phần mềm

HƯỚNG DẪN NGHIÊN CỨU

1. Tiếp tục tìm hiểu các tài liệu trong tâm
   [TL5] B. Chess and J. West, "Secure Programming with Static Analysis", Addison-Wesley, 2007
2. Cài đặt thử nghiệm theo yêu cầu lý thuyết

Ngày tháng 12 năm 2021

NGƯỜI BIÊN SOẠN

2// TS Phan Việt Anh

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

Bản số: …

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Kiểm tra mã nguồn và phân tích chương trình
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Trung tá, TS, Phan Việt Anh

HÀ NỘI, THÁNG 12 NĂM 2021

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

PHÊ DUYỆT
Ngày tháng 12 năm 2021
P.CHỦ NHIỆM KHOA

2// PGS.TS Tạ Minh Thanh

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Kiểm tra mã nguồn và phân tích chương trình
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Ngày tháng 12 năm 2021
CHỦ NHIỆM BỘ MÔN

2// TS, Nguyễn Việt Hùng

HÀ NỘI, THÁNG 12 NĂM 2021

MỞ ĐẦU

Mục đích:

- Thực hành phương pháp phân tích tĩnh và động để phát hiện lỗ hổng chương trình.

Yêu cầu:

- Đọc trước bài giảng
- Chú ý nghe giảng

Nội dung bài giảng

Thời gian: 4 tiết (53-56)

Nội dung	Thời gian
Thực hành Sử dụng một số công cụ để phân tích tĩnh chương trình	**45'**
Thực hành Sử dụng một số công cụ để phân tích tĩnh chương trình	**45'**
Thực hành Dùng một số môi trường giả lập để phân tích, tìm hiểu hoạt động của chương trình	**45'**
Thực hành Dùng một số môi trường giả lập để phân tích, tìm hiểu hoạt động của chương trình	**45'**

KẾT LUẬN

Trong bài giảng này sinh viên đã được giới thiệu về các nội dung như sau:

Thực hành phân tích chương trình theo phương pháp động và tĩnh

HƯỚNG DẪN NGHIÊN CỨU

1. Tiếp tục tìm hiểu các tài liệu trong tâm
2. Cài đặt thử nghiệm theo yêu cầu lý thuyết

Ngày tháng 12 năm 2021

NGƯỜI BIÊN SOẠN

2// TS Phan Việt Anh

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

Bản số: …

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Hướng dẫn ôn tập và thi
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Trung tá, TS, Phan Việt Anh

HÀ NỘI, THÁNG 12 NĂM 2021

HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA CÔNG NGHỆ THÔNG TIN

PHÊ DUYỆT
Ngày tháng 12 năm 2021
P.CHỦ NHIỆM KHOA

2// PGS.TS Tạ Minh Thanh

BÀI GIẢNG

Môn học: Lập trình phần mềm an toàn
Bài: Hướng dẫn ôn tập và thi
Đối tượng: BĐATTT 54
Năm học: 2021-2022

Ngày tháng 12 năm 2021
CHỦ NHIỆM BỘ MÔN

2// TS, Nguyễn Việt Hùng

HÀ NỘI, THÁNG 12 NĂM 2021

MỞ ĐẦU

Mục đích:

- Ôn tập và giải đáp các thắc mắc của sinh viên. Hướng dẫn và thống nhất cách thức làm bài thi hết môn

Yêu cầu:

- Đọc trước bài giảng
- Chú ý nghe giảng

Nội dung bài giảng

Thời gian: 4 tiết (57-60)

Nội dung	Thời gian
Thử nghiệm bảo vệ phần mềm	**45'**
Thử nghiệm bảo vệ dữ liệu truyền trên mạng	**45'**
Câu hỏi và trả lời	**45'**
Câu hỏi và trả lời	**45'**

KẾT LUẬN

Trong bài giảng này sinh viên đã được giới thiệu về các nội dung như sau:

Ôn tập các nội dung đã học

HƯỚNG DẪN NGHIÊN CỨU

1. Tiếp tục tìm hiểu các tài liệu trong tâm
2. Cài đặt thử nghiệm theo yêu cầu lý thuyết

Ngày tháng 12 năm 2021

NGƯỜI BIÊN SOẠN

2// TS Phan Việt Anh