AN TOÀN ỨNG DỤNG WEB VÀ CƠ SỞ DỮ LIỆU

Giới thiệu môn học

Giảng viên: ThS. Ninh Thị Thu Trang
Khoa: An toàn thông tin
Email: Trangntt2@ptit.edu.vn

Nội dung

Phần I – An toàn ứng dụng web

1. Tổng quan về bảo mật các ứng dụng Web
2. Các dạng tấn công lên các ứng dụng Web
3. Các biện pháp bảo mật máy chủ, ứng dụng và trình duyệt web
4. Bảo mật trong phát triển và triển khai ứng dụng web

Phần II – An toàn cơ sở dữ liệu

5. Tổng quan về an toàn cơ sở dữ liệu
6. Các cơ chế bảo mật cơ sở dữ liệu
7. Sao lưu, khôi phục dự phòng, kiểm toán và giám sát hoạt động CSDL

Tài liệu tham khảo

1. Hoàng Xuân Dậu, Bài giảng an toàn ứng dụng web và cơ sở dữ liệu, Học viện Công nghệ BCVT, 2017.
2. Bryan Sullivan, Vincent Liu, Web Application Security, A Beginner's Guide, McGraw-Hill, 2012.
3. Alfred Basta, Melissa Zgola, *Database Security*, Cengage Learning, 2012.
4. Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, John Wiley & Sons, 2011.
5. Ron Ben Natan, Implementing Database Security and Auditing, Elsevier Inc., 2005.
6. Mike Shema, Hacking Web Apps: Detecting and Preventing Web Application Security Problems, Elsevier Inc., 2012.
7. Roberta Bragg, Mark Rhodes-Ousley and Keith Strassberg, Network Security: The Complete Reference, McGraw-Hill Osborne Media, 2013.

Đánh giá môn học

- Điểm chuyên cần 10%. Điểm CC<5 sẽ **Không đủ ĐKDT**
  - Vắng 1 buổi không phép (v) trừ 1 điểm.
  - Đi muộn (m)/Về sớm (s) trừ 0.5 điểm
  - Vắng có lý do (p) trừ 0.5 điểm. Xin phép bằng cách gửi email trước giờ học.
  - Nếu tổng p+v>4 thì CC=0
  - Phát biểu xây dựng bài tốt cộng 0.5 điểm/lần.
  - Thiếu 1 bài thực hành -2đ
  - Không tham gia vòng loại PTIT CTF -1đ. Vượt qua vòng loại +1đ, Giải phong trào và giải KK +2đ, giải Ba +3đ, giải Nhì +4đ, giải Nhất +5đ
  - **CC>10 thì có thể chuyển sang điểm KT, BTL.**

Đánh giá môn học

- Kiểm tra: 10%
  - Kiểm tra trắc nghiệm trên hệ thống *lmsattt.ptit.edu.vn*
  - Mỗi bài thực hành hoàn thành tốt +1đ. Đăng ký lại lịch thực hành trên lms.

  Hạn đăng ký hết ngày **31/8**.
- Bài tập lớn: 20%
  - Mỗi nhóm SV nộp file báo cáo không quá 25 trang, deadline là **23:59 ngày 1/11.** Tên file đặt **Lopx_Nhomy.pdf**
  - Các nhóm báo cáo phải có slide và demo. Sau khi nhóm báo cáo, GV sẽ vấn đáp từng SV về đề tài của nhóm.
  - Chấm điểm bài tập nhóm bắt đầu từ **03/11.**
  - Điểm pdf+ppt 20%, demo 40%, vấn đáp 40%
- Thi: 60% - Trắc nghiệm

Danh sách đề tài bài tập lớn

STT	Tên đề tài	Yêu cầu
1	Tìm hiểu về mật khẩu sử dụng một lần OTP	Nghiên cứu phương pháp sinh và chuyển giao OTP. Cài đặt 1 trang web đơn giản có khả năng sinh và gửi OTP cho người dùng qua điện thoại di động/email.
2	Tìm hiểu khái quát về tường lửa ứng dụng web (Web Application Firewall).	Tìm hiểu về kiến trúc, hoạt động, tạo luật và cài đặt tường lửa ứng dụng web ModSecurity. Cài đặt và demo chạy thử ModSecurity bảo vệ website chống lại các dạng tấn công XSS và SQL Injection.
3	Tìm hiểu về hệ quản trị CSDL MySQL	Kiến trúc, các thành phần, tính năng và các cơ chế bảo mật của MySQL. Cài đặt và quản trị MySQL (tạo CSDL, thêm bảng, xoá bảng, thêm/sửa dữ liệu, tạo backup CSDL)
4	Tìm hiểu về các công cụ rà quét điểm yếu và lỗ hổng website thông dụng	Cài đặt và chạy thử 1 công cụ và thực hiện quét (chẳng hạn như Abbey Scan, Acunetix, Arachni), tạo báo cáo và phân tích lỗ hổng của 5 website trên mạng Internet.
5	Tìm hiểu về hệ quản trị CSDL Microsoft SQL Server 2016	Nghiên cứu kiến trúc, các thành phần, tính năng và các cơ chế bảo mật của Microsoft SQL Server 2016. Cài đặt và quản trị Microsoft SQL Server 2016 (tạo CSDL, thêm bảng, xoá bảng, thêm/sửa dữ liệu, tạo backup CSDL)
6	Tìm hiểu về CAPTCHAR và các phương pháp tạo CAPTCHAR.	Nghiên cứu về các kỹ thuật tạo Captchar. Xây dựng 1 trang web tích hợp khả năng tạo và kiểm tra CAPTCHAR.
7	Tìm hiểu về chuỗi cân bằng tải các máy chủ web (web server load balancing cluster).	Các dạng và thuật toán cân bằng tải chuỗi máy chủ web . Cài đặt thử nghiệm và demo 1 web cluster (phục vụ cùng 1 website) gồm 2-3 máy ảo sử dụng tính năng Network Load Balancing của MS Windows Servers.
8	Tìm hiểu về hệ quản trị CSDL MongoDB	Tìm hiểu kiến trúc, các thành phần, tính năng và các cơ chế bảo mật của MongoDB. Cài đặt và quản trị MongoDB (sử dụng các lệnh tạo CSDL, tạo collection, tạo document, nhập dữ liệu vào collection, lập chỉ số, tìm kiếm).

Danh sách đề tài bài tập lớn

STT	Tên đề tài	Yêu cầu
9	Tìm hiểu về nền tảng xử lý song song Apache Spark:	Giới thiệu, kiến trúc, hoạt động. Cài đặt và thử nghiệm Apache Spark.
10	Tìm hiểu về hệ quản trị CSDL Oracle	kiến trúc, các thành phần, tính năng và các cơ chế bảo mật của Oracle. Cài đặt và quản trị Oracle (tạo CSDL, thêm bảng, xoá bảng, thêm/sửa dữ liệu, tạo backup CSDL)
11	Tìm hiểu về hệ quản trị CSDL PostgreSQL	kiến trúc, các thành phần, tính năng và các cơ chế bảo mật của PostgreSQL. Cài đặt và quản trị PostgreSQL(tạo CSDL, thêm bảng, xoá bảng, thêm/sửa dữ liệu, tạo backup CSDL)
12	Tìm hiểu và so sánh các công cụ và phần mềm kiểm tra bảo mật cơ sở dữ liệu phổ biến như IBM Guardium, Imperva SecureSphere, McAfee Database Security	Cài đặt và chạy thử 1 công cụ (có thể dùng công cụ mã nguồn mở ngoài 3 công cụ gợi ý) và thực hiện quét, tạo báo cáo và phân tích lỗ hổng.
13	Tìm hiểu về lỗ hổng IIS Directory Traversal	Tìm hiểu cách thức tin tặc khai thác tấn công; trình bày giải pháp (cách fix) lỗ hổng này. Có demo tấn công trên hệ thống giả lập tự xây dựng
14	Tìm hiểu về lỗ hổng IIS Remote Code Execution	Tìm hiểu cách thức tin tặc khai thác tấn công; trình bày giải pháp (cách fix) lỗ hổng này. Có demo tấn công trên hệ thống giả lập tự xây dựng
15	Tìm hiểu về lỗ hổng Apache File Inclusion	Tìm hiểu cách thức tin tặc khai thác tấn công; trình bày giải pháp (cách fix) lỗ hổng này. Có demo tấn công trên hệ thống giả lập tự xây dựng
16	Học máy trong phân tích log: Sử dụng học máy để phân tích log hệ thống nhằm phát hiện tấn công web	Nghiên cứu các kỹ thuật học máy trong việc phân tích log server để phát hiện tấn công; có demo đối với phát hiện một loại tấn công cụ thể ví dụ SQL Injection

Một số lỗi thường gặp khi làm báo cáo

1. Báo cáo không có bìa, không làm mục lục tự động, không trích dẫn tài liệu tham khảo.
2. Báo cáo đi copy nội dung về không chỉnh sửa: dùng từ “bạn”, dùng nguyên văn của google translate, font chữ không đồng nhất…
3. Bố cục các mục không logic, lý thuyết A nhưng demo B…
4. Slide quá nhiều chữ, font chữ và cỡ chữ khó nhìn…
5. Demo quá đơn giản. Nếu được, mỗi bạn trong nhóm nên có 1 phần demo của riêng mình.

Quy định gửi email

- Email: Trangntt2@ptit.edu.vn
- Tiêu đề email: ATW-2023
- Viết email cần có phần chào hỏi, giới thiệu bản thân.
- Các vấn đề phải gửi qua email: xin nghỉ học, xin đổi lịch thực hành, làm rõ nội dung bài tập nhóm…
- Các vấn đề trao đổi khác có thể tạo topic trên nhóm Facebook hoặc hỏi trực tiếp trên lớp.