ÔN TẬP CUỐI KỲ

Môn học: Lập trình An toàn và khai thác lỗ hổng phần mềm

Câu 1: SDLC là viết tắt của từ khóa nào?

A. System development life cycle
B. Software development life cycle
C. Software development life conditions
D. Khác

Câu 2: Trong quy trình phát triển phần mềm, việc lập trình được thực hiện ở giai đoạn nào?

A. Implementation
B. Design
C. Deployment
D. Analysis

Câu 3: Mô hình Waterfall không còn được sử dụng để phát triển phần mềm do đã lỗi thời?

A. True
B. False

Câu 4: Nhận định đúng về mô hình Waterfall ban đầu?

A. Ít tài liệu
B. Thích hợp với các dự án có nhiều sự thay đổi
C. Thuộc nhóm mô hình phát triển phần mềm Agile
D. Không có sự quay lui

Câu 5: Nhóm toàn các mô hình phát triển thuộc nhóm Agile?

A. RUP, Waterfall, Lean
B. Waterfall, Scrum, Lean
C. Scrum, Lean, RUP
D. Lean, Scrum, XP

Câu 6: Kí hiệu C trong mẫu thiết kế phần mềm MVC tương ứng với thành phần nào của phần mềm?

A. Code: các tệp tin code của phần mềm
B. Container: môi trường triển khai của phần mềm
C. Controller: xử lý chức năng, trung gian giữa dữ liệu và giao diện
D. Em hông biết :(

Câu 7: Khi cần hiện thực chức năng đăng ký nhận thông báo, có thể sử dụng design pattern nào?

A. Observer
B. Singleton
C. Server-client
D. Không nên dùng design pattern

Câu 8: Nhận định nào **đúng**?

A. Git là hệ thống quản lý phiên bản tập trung
B. Git và Github là một
C. Khi 1 file đang được chỉnh sửa, Git sẽ khóa truy cập vào file
D. Không câu nào đúng

Câu 9: Cho biết tác dụng của lệnh sau: **git clone https://github.com/user1/test.git .**

A. Sao chép thư mục hiện hành

B. Tải về 1 repository từ URL về thư mục hiện hành
C. Tạo 1 git repository tại thư mục hiện hành
D. Xóa các thư mục của git tại thư mục hiện hành

Câu 10: Kiểm thử an toàn thông tin (security testing) được xếp vào nhóm?
A. Kiểm thử phi chức năng
B. Kiểm thử đơn vị
C. Kiểm thử chức năng
D. Kiểm thử tích hợp

Câu 11: Nhận định **sai** về định dạng JSON?
A. Các file có đuôi .json
B. Dựa trên kiểu dữ liệu của Javascript
C. Cho phép comment
D. Có thể nhúng trong định dạng YAML

Câu 12: CI/CD là gì?
A. Continuous Integration/Continuous Development
B. Continuous Integration/Continuous Delivery
C. Continuous Implementation/Continuous Delivery
D. Continuous Implementation/Continuous Development

Câu 13: Cho biến **char buf[25]**. Cách gọi hàm nào dưới đây có thể gây ra lỗ hổng buffer overflow?
A. read(stdin, buf, 25)
B. scanf("%s", buf)
C. fgets(buf, 50, stdin)
D. 2 câu fgets và scanf

Câu 14: Biện pháp phòng tránh buffer overflow?
A. Dùng option -fno-stack-protector
B. Dùng ASLR
C. Cả 2 cách đều đúng
D. Cả 2 cách đều sai

Câu 15: Format string nào cho phép ghi dữ liệu vào bộ nhớ?
A. %s
B. %w
C. %n
D. %d

Câu 16: Điều nào **đúng** về kỹ thuật tấn công ROP?
A. Xảy ra trong trường hợp chỉ có thể làm tràn buffer 1 byte
B. Tìm và sử dụng một số gadget kết thúc bằng lệnh ret
C. Có thể bị chặn nếu bật cơ chế ngăn thực thi code trên stack
D. Khai thác lỗ hổng integer overflow

Câu 17: Biết addr g2 < g3 < g1 < g4, cần thực thi luồng g1 -> g2 -> g3 -> g4, thứ tự địa chỉ các gadget tính từ đầu payload?
A. g1 -> g2 -> g3 -> g4
B. g4 -> g3 -> g2 -> g1
C. g2 -> g3 -> g1 -> g4
D. g4 -> g1 -> g3 -> g2

Câu 18: Nhận định đúng khi sử dụng Data Execution Prevention (DEP)?

A. Code trên stack thực thi được
B. Không có vùng nhớ có cả quyền ghi và thực thi
C. Cờ NX của file thực thi là DISABLED
D. Cả 3 ý trên đều đúng

Câu 19: Giả sử A gọi B, hàm B có chuỗi buf nằm ngay dưới ô nhớ lưu ebp cũ của A và có thể ghi dư thêm 1 byte, ta có thể làm gì?
A. Điều hướng thay vì A > B > A thì A > B sau đó đi đến đoạn code tùy ý
B. Không làm được gì ngoài lỗi Segmentation Fault
C. Tạo stack frame giả cho A sử dụng
D. Em không rõ :(

Câu 20: Với Return-to-libc, để điều hướng đến hàm system(), mở shell với tham số "/bin/sh" trong hệ thống 64 bit, ta cần làm gì?
A. Ghi đè ret addr thành địa chỉ system() và đưa chuỗi tham số vào stack
B. Ghi đè ret addr thành địa chỉ system() và đưa chuỗi tham số vào rdi
C. Ghi đè ret addr thành địa chỉ system() và đưa chuỗi tham số vào rax
D. Chỉ ghi đè ret addr thành địa chỉ system(), tham số mặc định là "/bin/sh"