Vấn đề phát triển phần mềm

Vấn đề phát triển phần mềm

- Các phương pháp tấn công vào lỗi do quá trình lập trình
- Quy trình phát triển phần mềm

Lỗi lập trình

- Lỗi bỏ quên
- Lỗi nhầm lẫn
- Lỗi do không có kiến thức về vấn đề

Các lỗi

- Lỗi vượt giới hạn
  - Lỗi tràn bộ đệm
  - Lỗi tràn số
- Lỗi tấn chèn mã
  - SQL injection
  - Command injection
- Lỗi kiểm soát, thông báo lỗi

Các lỗi (t)

- Cross site attack
- Use of Magic URLs and Hidden Form Fields
- Improper Use of SSL and TLS
- Store sensitive data

Tràn bộ đệm

- Nguyên lý tổ chức bộ nhớ
- Cách gọi chương trình
- Tình huống lỗi
  - Nhập liệu, nhận dữ liệu
  - Tham số dòng lệnh
- Hậu quả
  - Không thực hiện đúng, dừng dịch vụ
  - Cơ sở khai thác các lệnh khác

Tràn bộ đệm (t)

```
#include <stdio.h>
void DontDoThis(char* input) {
    char buf[16];
    strcpy(buf, input);
    printf("%s\n", buf);
}
int main(int argc, char* argv[]) {
    DontDoThis(argv[1]);
    return 0;
}
```

Lỗi tràn số

- **Signed int to Larger unsigned int**
  - This combines the two behaviors: (char)-1 (0xff) becomes 4,294,967,295 (0xffffffff) when cast to an unsigned long.
- **Unsigned int to Same-Size signed int**
  - As with the cast from signed to unsigned, the bit pattern is preserved, and the meaning of the value may change, depending on whether the uppermost (sign) bit is a 1 or 0.

Lỗi tràn số (t)

- **Unsigned int to Larger signed int**
- This behaves very much the same as casting from an unsigned int to a larger unsigned int. The value first zero-extends to an unsigned int the same size as the larger value, then is cast to the signed type. The value of the number is maintained, and won't usually cause programmer astonishment.

Lỗi tràn số (t)

- **Signed int to Larger signed int**
  - (char)0x7f -> 0x0000007f
  - , but (char)0x80 -> 0xffffff80.
- **Signed int to Same-Size unsigned int**
  - (char)0xff (-1) -> 0xff when cast to an unsigned char, but -1 # 255.

Lỗi định dạng

```
#include <stdio.h>
int main(int argc, char* argv[]) {
    if(argc > 1)
        printf(argv[1]);
    return 0;
    }
```

Lỗi định dạng

- printf(user_input); is wrong, and
- printf("%s", user_input); is correct.

Lỗi chèn mã SQL inject

- Do việc sử dụng xây dựng câu lệnh SQL trực tiếp
  - Chèn vượt qua điều kiện kiểm tra
  - Chèn thêm các lệnh không mong muốn (multi command)

Lỗi chèn mã SQL injection (t)

- Giải pháp
  - Kiểm tra đầy đủ dữ liệu đầu vào (theo định kiểu)
  - Thay thế các ký tự trong trường hợp cộng chuỗi
  - Không sử dụng phương pháp cộng chuỗi mà sử dụng
    - Stored procedure
    - Inline parameter

Lỗi chèn mã – command injection

- Do thực hiện một số lệnh với các dữ liệu đầu vào với mô hình qua biên dịch lại

```
char buf[1024];
snprintf(buf, "system lpr -P %s", user_input,
   sizeof(buf)-1);
system(buf);
```

Kiểm soát lỗi

- Lỗi do quá trình thực hiện chương trình
  - Thông báo lỗi quá chi tiết
  - Không bắt lỗi
  - Xử lý không hết các tình huống trả về
  - Hàm trả về không đủ thông tin

Kiểm soát lỗi (t)

- Thực hiện
  - Thông báo lỗi đủ người dùng hiểu, và xử lý tại thời điểm đó
  - Xử lý kiểm lỗi cho các lệnh có nguy cơ: dữ liệu, thiết bị khác, kết nối
  - Xử lý các thông tin trả về đầy đủ
  - Xây dựng hàm tường minh

Lỗi XSS

- Lỗi do việc vào trang web không vào chính xác trang mình cần
  - Lỗi phishing
  - Lỗi link và hiển thị thực tế
  - Lỗi do dữ liệu nhập vào thu thập thông tin

Lỗi XSS (t)

- Vấn đề
  - Người dùng cẩn thận khi sử dụng các link được chia sẽ
  - Kiểm tra dữ liệu đầu vào loại các thẻ nhạy cảm
  - Cấu hình dịch vụ

Lỗi về hidden value

- Sử dụng các biên hidden lưu truyền dữ liệu
  - Dữ liệu nhạy cảm
  - Dữ liệu không kiểm tra lại
- Sử dụng url thay thế các biến hidden

Chiến lược về mật khẩu

- Chiến lược tạo lập và lưu trữ mật khẩu

Bảo vệ thông tin

- Thông tin truyền
- Thông tin lưu trữ

Phát triển phần mềm

- Quy trình
  - Có quy trình thiết kế đầy đủ
  - Có định hướng về phát hiện lỗi và giải quyết lỗi
  - Quy trình test có thể hiện các vấn đề lỗi
  - Framework, quy tắc lập trình

Vấn đề phát triển phần mềm

- Các phương pháp tấn công vào lỗi do quá trình lập trình
- Quy trình phát triển phần mềm