BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ

Thi ngày 05/01/2022

ĐỀ THI KẾT THÚC HỌC PHẦN
Môn học: Phát hiện lỗi và lỗ hổng phần mềm
Khóa đào tạo: AT14
Thi lần thứ: 1 Thời gian: 90 phút

ĐỀ SỐ 1

(dành cho thí sinh có SỐ BÁO DANH LẺ)

Câu 1 (3 điểm). Trình bày khái niệm lỗ hổng dư 1 (off-by-one); chỉ ra ví dụ về lỗ hổng dư 1 và khai thác lỗ hổng dư 1.

Câu 2 (2 điểm). Cho đoạn mã C sau:

```
#include <stdio.h>
void sub(int a, int b, int *s){
     *s = a - b;
}
int main(){
     int a, b, t;
     scanf("%d", &a, &b);
     sub(a, b, &t);
     printf("%d", t);
     return 0;
}
```

Anh/chị hãy trình bày stack frame của hàm "sub" khi nó được gọi và trình bày hoạt động của hàm trên stack frame đó. Yêu cầu: có vẽ hình minh họa stack frame của hàm được chỉ định; trên hình vẽ thể hiện các tham số hình thức của hàm; khi trình bày hoạt động thì chỉ ra các tham số thực sự tương ứng với các tham số hình thức.

Câu 3 (2 điểm). Anh/chị hãy trình bày khái niệm lỗ hổng chuỗi định dạng (format string); giải thích cơ chế khai thác lỗ hổng chuỗi định dạng để ghi một giá trị tùy ý vào một địa chỉ tùy ý.

Câu 4 (3 điểm). Khi dịch ngược một chương trình, người ta thu được đoạn giả mã C như sau:

```
int __cdecl vun()
{
     int result;   // eax@8
     char buf;     // [sp+8h] [bp-20h]@1
     int v2;       // [sp+18h] [bp-10h]@4
     int v3;       // [sp+1Ch] [bp-Ch]@1

     v3 = 6000;
     puts("FLAG's PRIZE: 6001$");
     printf("Your money: %d$\n", 6000);
     puts("YOU BET ... ");
     read(0, &buf, 0xFu);
     if ( strchr(&buf, '-') )
     {
          puts("BYE BYE HACKER ...");
          exit(0);
     }
```

```
    v2 = strtoul(&buf, 0, 0);
    if (v2 > v3)
    {
        puts("YOU THINK I AM STUPID???");
        exit(0);
    }
    v3 -= v2;
    printf("You money: %d$\n", v3);
    if ( v3 <= 6000 )
        result = puts("Good bye loser");
    else
        result = system("cat flag");
    return result;
}

int __cdecl main()
{
    vun();
    return 0;
}
```

Anh/chị hãy:

a) Trình bày hoạt động của chương trình

b) Phân tích, chỉ ra lỗ hổng trong chương trình

c) Trình bày cách thức để khiến chương trình thực thi câu lệnh "cat flag".

***Ghi chú**: - Sinh viên KHÔNG được sử dụng tài liệu khi làm bài.*

*- **Tham số hình thức** là biến được liệt kê trong danh sách **tham số** (thường nằm tại phần đầu của định nghĩa chương trình con). Còn **tham số thực** sự là giá trị cụ thể của biến đó tại thời gian chạy.*

BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ

Thi ngày 05/01/2022

ĐỀ THI KẾT THÚC HỌC PHẦN
Môn học: Phát hiện lỗi và lỗ hổng phần mềm
Khóa đào tạo: AT14
Thi lần thứ: 1 Thời gian: 90 phút

ĐỀ SỐ 2

(dành cho thí sinh có SỐ BÁO DANH CHẴN)

Câu 1 (3 điểm). Anh/chị hãy trình bày khái niệm lỗ hổng trường hợp đua (race condition); chỉ ra ví dụ về lỗ hổng trường hợp đua và khai thác lỗ hổng trường hợp đua.

Câu 2 (2 điểm). Cho đoạn mã C sau:

```
#include <stdio.h>
#include <string.h>
int safecopy(char *src, char des[], int dsize){
     if(src==NULL || strlen(src)>=dsize)
          return -1;
     strcpy(des, src);
     return 0;
}
int main(int argc, char *argv[]){
     char buf[60];
     //argv[0] là đường dẫn đã được dùng để gọi chương trình này
     safecopy(argv[0], buf, sizeof(buf));
     return 0;
}
```

Anh/chị hãy trình bày stack frame của hàm "check" khi nó được gọi và trình bày hoạt động của hàm trên stack frame đó. Yêu cầu: có vẽ hình minh họa stack frame của hàm được chỉ định; trên hình vẽ thể hiện các tham số hình thức của hàm; khi trình bày hoạt động thì chỉ ra các tham số thực sự tương ứng với các tham số hình thức.

Câu 3 (2 điểm). Anh/chị hãy trình bày khái niệm lỗ hổng chuỗi định dạng (format string); giải thích cơ chế khai thác lỗ hổng chuỗi định dạng để đọc dữ liệu dạng chuỗi từ một địa chỉ tùy ý.

Câu 4 (3 điểm) Khi dịch ngược một chương trình, người ta thu được đoạn giả mã C sau:

```
int __cdecl vun()
{
     int result;   // eax@8
     char buf;     // [sp+8h] [bp-20h]@1
     int v2;       // [sp+18h] [bp-10h]@4
     int v3;       // [sp+1Ch] [bp-Ch]@1

     v3 = 4000;
     puts("FLAG's PRIZE: 4001$");
     printf("Your money: %d$\n", 4000);
     puts("YOU BET ... ");
     read(0, &buf, 0xFu);
     if ( strchr(&buf, '-') )
     {
```

```
          puts("BYE BYE HACKER ...");
          exit(0);
     }
     v2 = strtoul(&buf, 0, 0);
     if (v2 > v3)
     {
          puts("YOU THINK I AM STUPID???");
          exit(0);
     }
     v3 -= v2;
     printf("You money: %d$\n", v3);
     if ( v3 <= 4000 )
          result = puts("Good bye loser");
     else
          result = system("cat flag");
     return result;
}

int __cdecl main()
{
     vun();
     return 0;
}
```

Anh/chị hãy:

a) Trình bày hoạt động của chương trình

b) Phân tích, chỉ ra lỗ hổng trong chương trình

c) Trình bày cách thức để khiến chương trình thực thi câu lệnh "cat flag".

***Ghi chú**: - Sinh viên KHÔNG được sử dụng tài liệu khi làm bài.*

*- **Tham số hình thức** là biến được liệt kê trong danh sách **tham số** (thường nằm tại phần đầu của định nghĩa chương trình con). Còn **tham số thực** sự là giá trị cụ thể của biến đó tại thời gian chạy.*