חולשות מתקדמות

תרגול 6 – הנדסה לאחור – חורף תשפ"א

INTEGER ERRORS

- Integer Overflow (taken from OpenSSH 3.3 CVE-2002-0639)

```
int nresp = packet_get_int();
if (nresp > 0) {
response = xmalloc(nresp*sizeof(char*));
for (i = 0; i < nresp; i++)
    response[i] = packet_get_string(NULL);
}
```

INTEGER ERRORS

- Integer Coercion Error

```
DataPacket *packet;
int numHeaders;
PacketHeader *headers;
sock=AcceptSocketConnection();
ReadPacket(packet, sock);
numHeaders =packet->headers;
if (numHeaders > 100) {
    ExitError("too many headers!");
}
headers = malloc(numHeaders * sizeof(PacketHeader);
ParsePacketHeaders(packet, headers);
```

FORMAT STRING VULNERABILITIES

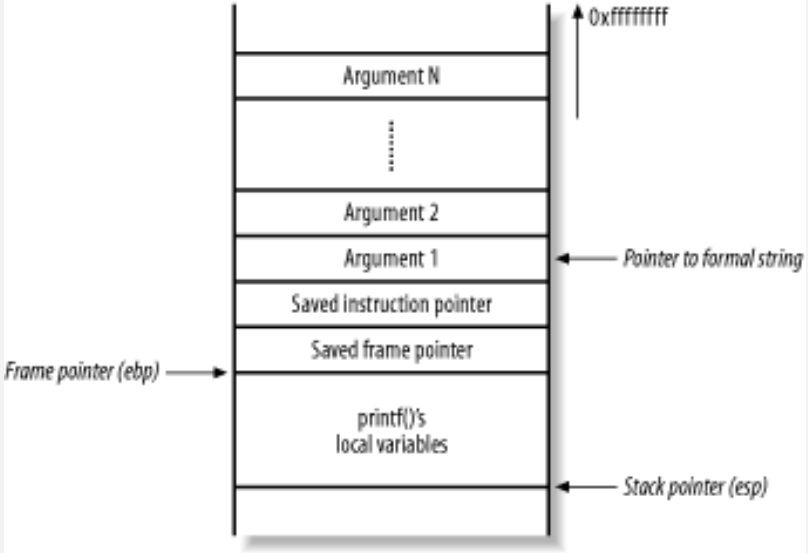
- מה הבעיה בקוד הבא?

```
1 int main(){
2     char* buffer[20];
3     printf(“Enter your Name:\n”);
4     scanf(“%19s”, buffer);
5     printf(“Welcome:\n“);
6     printf((buffer);
7 }
```

- מה יקרה אם נכניס את הקלט הבא: "%x%x%x"?

FORMAT STRING VULNERABILITIES

- תזכורת: מצב המחסנית בקריאה לprintf:



- לכן, באמצעות החולשה הזו אנחנו יכולים להדליף מידע מהמחסנית
- בנוסף לכך, אנחנו יכולים לכתוב לזיכרון באמצעות הפרמטר %n
- במקרים מסוימים אנחנו אפילו יכולים לשלוט על הכתובת אליה אנחנו כותבים לקבל WWW

HEAP OVERFLOW

- בדומה לstack overflow, עם ההבדל שכעת הbuffer שאותו אנחנו דורסים נמצא על הheap ולא על המחסנית
- אנחנו יכולים להשתמש בחולשה זו על מנת לדרוס את הheader של הבלוק הבא בזיכרון ולגרום לחולשת WWW (כמו שראיתם בהרצאה)

```
#define BUFSIZE 256
int main(int argc, char **argv) {
    char *buf1 = (char *) malloc(BUFSIZE);
    char *buf2 = (char *) malloc(BUFSIZE);
    strcpy(buf1, argv[1]);
    free(buf2);
}
```

USE AFTER FREE

- חולשה הנגרמת מטיפול לא נכון בהקצאות זיכרון
- בפרט, שימוש במצביע כלשהו שכבר שוחרר
- לדוגמה:

```
1 char* ptr = (char*)malloc (SIZE);
2     ...
3 if (err) {
4     abrt = 1;
5     free(ptr);
6 }
7 ...
8 if (abrt) {
9     logError("operation aborted before commit", ptr);
10 }
```

TRY IT YOURSELF

- באתר הקורס מופיע לכם קובץ הרצה וקוד המקור עבור תכנית כלשהי
- תכנית זו מכילה את אחת מהחולשות שראינו בתרגול
- המטרה שלכם היא לגרום לכך שהפונקציה win_exercise ע"י הכנסת קלט לתכנית (בלי שום שינוי לקבצים שקיבלתם)
- בהצלחה!