



Lecture 2:

1-Example: Buffer overflow - a common and persistent vulnerability

A Vulnerable Password Checking Program



 `#include <stdio.h>`
`#include <strings.h>`


```
int main(int argc, char *argv[]) {
    int allow_login = 0;
    char pwdstr[12];
    char targetpwd[12] = "MyPwd123";
    gets(pwdstr);
    if (strncmp(pwdstr, targetpwd, 12) == 0)
        allow_login = 1;

    if (allow_login == 0)
        printf("Login request rejected");
    else
        printf("Login request allowed");
}
```

The output:


Attacker Code Execution

We type a correct password (MyPwd123) of less than 12 characters:




The login request is allowed.

Now let us type "BadPasswd" when we are asked to provide the password:



The login request is rejected.

Quiz and answer:



Stack Access Quiz

Check the lines of code, when executed, accesses addresses in the stack frame for main():

```
int main(int argc, char *argv[]) {
    ☐ int allow_login = 0;
    ☐ char pwdstr[12];
    ☒ char targetpwd[12] = "MyPwd123";
    ☒ gets(pwdstr);
    ☒ if (strncmp(pwdstr, targetpwd, 12) == 0)
        ☒ allow_login = 1;

    ☒ if (allow_login == 0)
        ☐ printf("Login request rejected");
    ☐ else
        ☐ printf("Login request allowed");
}
```

2-**Shell Code**: creates a shell which allows it to execute any code the attacker wants.

3-**Return-to-libc**: the return address is overwritten to point to a standard library function.

4-**Heap** :does not have a return address So you cannot hijack the control flow of the program


5-**OpenSSL Heartbleed** Vulnerability: classified as a **buffer over-read**

6-OpenSSL Heartbleed Vulnerability: From **Heartbeat to Heartbleed.**

7-**NVD**: National Vulnerability Database

8-**Defense Against Buffer Overflow Attacks**: Examples of safe languages: **Java, C#**

9-Quiz:



Strongly vs. Weakly Typed Language Quiz

Strongly typed languages help reduce software vulnerabilities. Determine which of the following options apply to strongly typed languages and which are for weakly typed. (Use 's' or 'w').

- ☒ S Any attempt to pass data of incompatible type is caught at compile time or generates an error at runtime.
- ☒ W An array index operation $b[k]$ may be allowed even though k is outside the range of the array.
- ☒ S It is impossible to do "pointer arithmetic" to access arbitrary area of memory.

10-Use **automatic tools** to analyze code for potential unsafe functions.

Analysis Tools Can flag potentially unsafe functions

11-**Stack Canaries**:

- When a return address is stored in a stack frame, a **random canary** value is written just before it.
- Any attempt to rewrite the address using buffer overflow will result in the canary being rewritten and an **overflow will be detected.**

12-**ASLR** :Address Space Layout Randomization

- Use **non-executable stack** coupled with ASLR
- randomizes** stack, heap, libc.
- This makes it harder for the attacker to find important locations ● (example: libc function address).

بالتوفيق للجميع