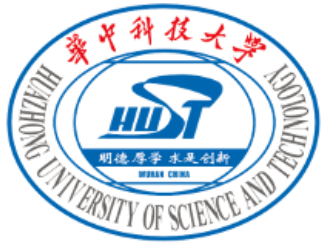


华中科技大学
HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

网络空间安全学院

未初始化变量漏洞

未初始化变量漏洞

- 未初始化栈变量
  - 定义栈局部变量
  - 首次使用前未进行相应的初始化
  - e.g., int va;
- 未初始化堆变量
  - 定义堆上动态分配的变量
  - 分配后未进行相应的初始化
  - e.g., void * pa = malloc(0x20);


```
int sum;

for (int i = 0; i < 100; i++) {
        sum += i;
}

printf("%d\n", sum);
```

未初始化栈变量漏洞利用

- 泄露栈上敏感信息，如上一个函数残留的敏感数据

```
char * secretstr = "This is a secret string";

void leave_secret()
{
        char secret[0x40];
        printf("secret is @: %p\n", &secret);
        memcpy(secret, secretstr, 0x40);
}
```

```
void vuln()
{
        char buffer[0x50];
        printf("buffer is @: %p\n", &buffer);
        printf("buffer content is: %s\n", buffer);
}

int main()
{
        leave_secret();
        vuln();
        return 0;
}
```

```
± % ./uninit-stack-leak
secret is @: 0x7fffb974c8e0
buffer is @: 0x7fffb974c8e0
secret is: This is a secret string
```

未初始化堆变量漏洞利用

- 泄露堆上残留指针与敏感数据

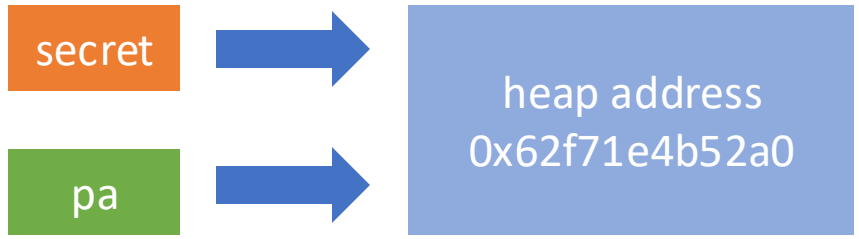
```
char * secretstr = "This is a secret string";

void leave_secret()
{
        char * secret;
        secret = malloc(0x40);
        memcpy(secret+0x20, secretstr, 0x20);
        printf("secret is @: %p\n", secret);
        free(secret);
}
```

```
± % ./uninit-stack-heap
secret is @: 0x62f71e4b52a0
pa is @: 0x62f71e4b52a0
secret: This is a secret string
```

```
void vuln()
{
        char * pa;
        pa = malloc(0x40);
        printf("pa is @: %p\n", pa);
        printf("secret: %s\n", (char *)pa+0x20);
}

int main()
{
        leave_secret();
        vuln();
        return 0;
}
```



未初始化堆变量漏洞利用

- 覆盖堆上敏感数据

```
char * passwd = NULL;
char * passwdstr = "I am a password";
char * fakepasswd = "I don't eat beef";
void leave_secret()
{
        size_t * pa;
        pa = malloc(0x40);
        passwd = malloc(0x20);
        pa[7] = passwd;
        memcpy(passwd, passwdstr, 0x20);
        printf("pa is @: %p\n", pa);
        printf("passwd is: %s\n", passwd);
        free(pa);
}
```

```
void vuln()
{
        size_t * pb;
        pb = malloc(0x40);
        memcpy(pb[7], fakepasswd, 0x20);
        printf("pb is @: %p\n", pb);
        printf("passwd is: %s\n", passwd);
}

int main()
{
        leave_secret();
        vuln();
        return 0;
}
```


```
± % ./uninit-stack-heap-1
pa is @: 0x58e1601dd2a0
passwd is: I am a password
pb is @: 0x58e1601dd2a0
passwd is: I don't eat beef
```