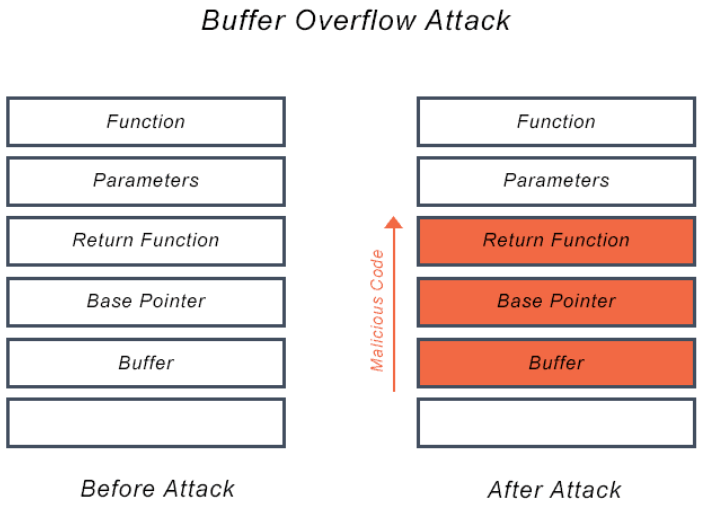
Non Top-10 Vulnerabilities

1. Buffer Overflow

Attackers use buffer overflows to corrupt the execution stack of a web application. By sending carefully crafted input to a web application, an attacker can cause the web application to execute arbitrary code – effectively taking over the machine.

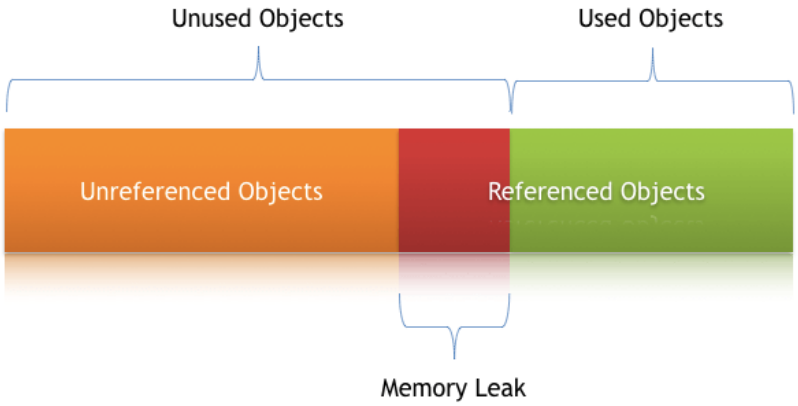


2. Improper pointer subtraction

The subtraction of one pointer from another in order to determine size is dependant on the assumption that both pointers exist in the same memory chunk.

3. Memory Leak

A memory leak is an unintentional form of memory consumption whereby the developer fails to free an allocated block of memory when no longer needed. The consequences of such an issue depend on the application itself.



4. Password Plaintext Storage

Storing a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource. Developers sometimes believe that they cannot defend the application from someone who has access to the configuration, but this attitude makes an attacker's job easier. Good password management guidelines require that a password never be stored in plaintext.

5. Insecure Transport

If an application uses SSL to guarantee confidential communication with client browsers, the application configuration should make it impossible to view any access controlled page without SSL. However, it is not an uncommon problem that the configuration of the application fails to enforce the use of SSL on pages that contain sensitive data.