An essential component of many buffer overflow attacks is the transfer of execution to code, known as **shellcode,** supplied by the attacker and often saved in the buffer being overflowed.

The possibility of overwriting the saved frame pointer and return address forms the core of a stack overflow. **True**

A **stack frame** is a structure where data are usually saved on the stack.

Shellcode is not specific to a particular processor architecture. **False**

A stack buffer overflow attack is also referred to as **stack smashing**.

The x86 Assembly Language Instruction NOP means **no operation or do nothing instruction.**

**Environment variables** are a collection of string values inherited by each process from its parent that can affect the way a running process behaves.

A stead reduction in memory available on the heap to the point where it is completely exhausted is known as a **memory leak.**

The difference between defensive programming and normal practices is that everything is assumed. **False**

To counter XSS attacks a defensive programmer needs to explicitly identify any assumptions as to the form of input and to verify that any input data conform to those assumptions before any use of the data. **False**

Programmers often make assumptions about the type of inputs a program will receive. **True**

There is a problem anticipating and testing for all potential types of non-standard inputs that might be exploited by an attacker to subvert a program. **True**

Incorrect handling of program **input** is one of the most common failings in software security.

Bots starting from a given HTTP link and then following all links on the provided website in a recursive way is called **spidering.**

**Application-based** bandwidth attacks attempt to take advantage of the disproportionally large resource consumption at a server.

The attacker needs access to a high volume network connection for a SYN spoof attack. **False**

A denial-of-service attack is an attempt to compromise availability by hindering or blocking completely the provision of some service. **True**

In a **DNS amplification** attack, the attacker creates a series of DNS requests containing the spoofed source address for the target system.

The SYN spoofing attack targets the table of TCP connections on the server. **True**

A SIP flood attack exploits the fact that a single INVITE request triggers considerable resource consumption. **True**