Computer Security: Principles and Practice, 2nd Edition Chapter 11

**Chapter 11 – Software Security**

|  |  |
| --- | --- |
|  | 1. “Failure to Preserve SQL Query Structure” is in the Insecure Interaction Between Components CWE/SANS software error category. 2. Defensive programming is a form of design intended to ensure the continuing function of a piece of software in spite of unforeseeable usage of the software. 3. Program input refers to any source of data that originates outside the program and whose value is not explicitly known by the programmer when the code was written. 4. Two key areas of concern for any input are the size of the input and the meaning and interpretation of the input. 5. A number of widely used standard C library routines compound the problem of buffer overflow by not providing any means of limiting the amount of data transferred to the space available in the buffer. 6. Program input data may be broadly classified as textual or binary. 7. In the SQL injection attack the user supplied input is used to construct a SQL request to retrieve information from a database. 8. Cross-site scripting attacks are most commonly seen in scripted Web applications. 9. A variant where the attacker includes malicious script content in data supplied to a site is the XSS reflection vulnerability. 10. The process of transforming input data that involves replacing alternate, equivalent encodings by one common value is called canonicalization. 11. The major advantage of fuzzing is its simplicity and its freedom from assumptions about the expected input to any program, service, or function. 12. A race condition occurs when multiple processes and threads compete to gain uncontrolled access to some resource. 13. UNIX related systems provide the chroot system function to limit a program’s view of the file system to just one carefully configured section that is known as a chroot jail. 14. If privileges are greater than those already available to the attacker the result is a privilege escalation. 15. The principle of least privilege strongly suggests that programs should execute with the least amount of privileges needed to complete their function. |