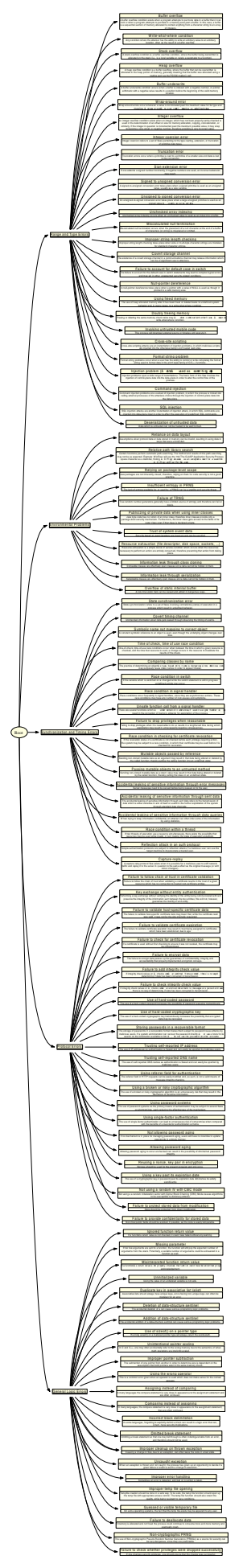
Blue
Protocol Error Codes
Buffer overflow
Buffer overflow condition arises when a program attempts to perform data in a buffer that is larger than the allocated memory. Attackers exploit this condition to execute malicious code on the host or to cause a denial of service.
Write-what-where condition
Write-what-where condition arises when a program allows an attacker to write a value to an arbitrary memory location.
Stack overflow
A stack overflow condition is a buffer overflow condition that occurs when a program writes to memory outside of the allocated stack. It is a common cause of program crashes and security vulnerabilities.
Heap overflow
A heap overflow condition is a buffer overflow condition that occurs when a program writes to memory outside of the allocated heap. It is a common cause of program crashes and security vulnerabilities.
Buffer underrun
Buffer underrun condition occurs when a program attempts to read data from a buffer that is smaller than the allocated memory. Attackers can exploit this condition to read sensitive data or cause a denial of service.
Buffer underflow
Buffer underflow condition occurs when a program attempts to read data from a buffer that is smaller than the allocated memory. Attackers can exploit this condition to read sensitive data or cause a denial of service.
Buffer access error
Buffer access error occurs when a program attempts to access an invalid or out-of-bounds memory location.
Integer to unsigned conversion error
Integer to unsigned conversion error occurs when a program attempts to convert an integer value to an unsigned integer value.
Unsigned to signed conversion error
Unsigned to signed conversion error occurs when a program attempts to convert an unsigned integer value to a signed integer value.
Unchecked array indexing
Unchecked array indexing occurs when a program does not check the validity of an array index before accessing the array.
Miscalculated null termination
Miscalculated null termination occurs when a program does not properly terminate a string with a null character.
Unknown image source
Unknown image source error occurs when a program does not recognize the source of an image.
Invalid image dimensions
Invalid image dimensions error occurs when a program does not recognize the dimensions of an image.
Failure to connect to proxy server
Failure to connect to proxy server error occurs when a program fails to connect to a proxy server.
Not-secure cleartext
Not-secure cleartext error occurs when a program transmits sensitive data in cleartext.
Invalid field length
Invalid field length error occurs when a program receives a field with an invalid length.
Invalid Trailing Padding
Invalid Trailing Padding error occurs when a program receives a message with an invalid padding.
Unknown extended trailer code
Unknown extended trailer code error occurs when a program receives a message with an unknown extended trailer code.
Cross site scripting
Cross site scripting allows an attacker to execute malicious scripts in a web browser on behalf of a user.
Further cross scripting
Further cross scripting allows an attacker to execute malicious scripts in a web browser on behalf of a user.
Cookie poisoning
Cookie poisoning is a type of cross site scripting attack in which an attacker injects malicious code into a web page that is then stored in the user's cookies. The code can then be executed by the user's browser when they visit the page.
Cookie injection
Cookie injection