**별첨2) 104개 애플리케이션 취약점**

|  |  |  |
| --- | --- | --- |
| **카테고리** | **문제유형** | |
| Range and  Type Errors | 1. Buffer overflow 2. “Write-what-where” condition 3. Stack overflow 4. Heap overflow 5. Buffer underwrite 6. Wrap-around error 7. Integer overflow 8. Integer coercion error 9. Truncation error 10. Sign extension error 11. Signed to unsigned conversion error 12. Unsigned to signed conversion error 13. Unchecked array indexing 14. Miscalculated null termination 15. Improper string length checking 16. Convert storage channer | 1. Failure to account for default case in switch 2. Null-pointer dereference 3. Using freed memory 4. Doubly freeing memory 5. Invoking untrusted mobile code 6. Cross-site scripting 7. Format string problem 8. Injection problem(“data” used as something else) 9. Command Injection 10. Log Injection 11. Reflection Injection 12. SQL Injection 13. Deserialization of untrusted data |
| Environmental Problem | 1. Reliance on data layout 2. Relative path library search 3. Relying on package-level scope 4. Insufficient entropy in PRNG 5. Failure of TRNG 6. Publicizing of private data when using inner classes 7. Trust of system event data | 1. Resource exhaustion (file descriptor, disk space, sockets, …) 2. Information leak through class cloning 3. Information leak through serialization 4. Overflow of static internal buffer |
| Synchronization & Timing Errors | 1. State synchronization error 2. Covert timing channel 3. Symbolic name not mapping to correct object 4. Time of check, time of use race condition 5. Comparing classes by name 6. Race condition in switch 7. Race condition in signal handler 8. Unsafe function call from a signal handler 9. Failure to drop privileges when reasonable 10. Race condition in checking for certificate revocation | 1. Passing mutable objects to an untrusted method 2. Mutable object returned 3. Accidental leaking of sensitive information through error message 4. Accidental leaking of sensitive information through sent data 5. Accidental leaking of sensitive information through data queries 6. Race condition within a thread 7. Reflection attak in an auto protocol 8. Capture-replay |
| **카테고리** | **문제유형** | |
| Protocol Errors | 1. Failure to follow chain of trust in certificate validation 2. Key exchange without entity authentication 3. Failure to validate host-specific certificate data 4. Failure to validate certificate expiration 5. Failure to check for certificate revocation 6. Failure to encrypt data 7. Failure to add integrity check value 8. Failure to check integrity check value 9. Use of hard-coded password 10. Use of hard-coded cryptographic key 11. Storing passwords in a recoverable format 12. Trusting self-reported IP address 13. Trusting self-reported DNS name | 1. Using referrer field for authentication 2. Using a broken or risky cryptographic algorithm 3. Using password systems 4. Using single-factor authentication 5. Not allowing password aging 6. Allowing password aging 7. Reusing a nonce, key pair in encryption 8. Using a key past its expiration date 9. Not using a random IV with CBC mode 10. Failure to protect stored data from modification 11. Failure to provide confidentiality for stored data |
| Generic  Logic Errors | 1. Ignore function return value 2. Missing parameter 3. Misinterpreted function return value 4. Uninitialized variable 5. Duplicate key in associative list (alist) 6. Deletion of data-structure sentinel 7. Addition of data-structure sentinel 8. Use of sizeof() on a pointer type 9. Unintentional pointer scaling 10. Improper pointer subtraction 11. Assigning instead of comparing 12. Comparing instead of assigning 13. Incorrect block delimitation | 1. Omitted break statement 2. Improper cleanup on thrown exception 3. Uncaught exception 4. Improper error handling 5. Improper temp file opening 6. Guessed or visible temporary file 7. Failure to deallocate data 8. Non-cryptographic PRNG 9. Failure to check whether privileges were dropped successfully |