CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')	The program allocates or initializes a resource such as a pointer, object, or variable using one type, but it later accesses that resource using a type that is incompatible with the original type.
CWE-824	Access of Uninitialized Pointer	The program accesses or uses a pointer that has not been initialized.
CWE-770	Allocation of Resources Without Limits or Throttling	The software allocates a reusable resource or group of resources on behalf of an actor without imposing any restrictions on the size or number

		of resources that can be allocated, in violation of the intended security policy for that actor.
CWE-670	Always-Incorrect Control Flow Implementation	The code contains a control flow path that does not reflect the algorithm that the path is intended to implement, leading to incorrect behavior any time this path is navigated.
CWE-294	Authentication Bypass by Capture-replay	A capture-replay flaw exists when the design of the software makes it possible for a malicious user to sniff network traffic and bypass authenticati on by replaying it to the server

		in question to the same effect as the original message (or with minor changes).
CWE-290	Authentication Bypass by Spoofing	This attack-focused weakness is caused by improperly implemented authentication schemes that are subject to spoofing attacks.
CWE-639	Authorization Bypass Through User-Controlled Key	The system's authorization functionality does not prevent one user from gaining access to another user's data or record by modifying the key value identifying the data.
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	The program copies an input buffer to an output

		buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow.
CWE-312	Cleartext Storage of Sensitive Information	The application stores sensitive information in cleartext within a resource that might be accessible to another control sphere.
CWE-319	Cleartext Transmission of Sensitive Information	The software transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	The program contains a code sequence that can run concurrently with other code, and the code sequence requires temporary, exclusive access to a shared resource, but a timing window exists in which the shared resource can be modified by another code sequence that is operating concurrently .
CWE-352	Cross-Site Request Forgery (CSRF)	The web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally

		provided by the user who submitted the request.
CWE-502	Deserialization of Untrusted Data	The application deserializes untrusted data without sufficiently verifying that the resulting data will be valid.
CWE-425	Direct Request ('Forced Browsing')	The web application does not adequately enforce appropriate authorization on all restricted URLs, scripts, or files.
CWE-369	Divide By Zero	The product divides a value by zero.
CWE-415	Double Free	The product calls free() twice on the same memory address, potentially leading to modification

		of unexpected memory locations.
CWE-494	Download of Code Without Integrity Check	The product downloads source code or an executable from a remote location and executes the code without sufficiently verifying the origin and integrity of the code.
CWE-834	Excessive Iteration	The software performs an iteration or loop without sufficiently limiting the number of times that the loop is executed.
CWE-668	Exposure of Resource to Wrong Sphere	The product exposes a resource to the wrong control sphere, providing unintended actors with inappropriate access to

		the resource.
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.
CWE-610	Externally Controlled Reference to a Resource in Another Sphere	The product uses an externally controlled name or reference that resolves to a resource that is outside of the intended control sphere.
CWE-552	Files or Directories Accessible to External Parties	The product makes files or directories accessible to unauthorized actors, even though they should not be.
CWE-209	Generation of Error Message Containing Sensitive Information	The software

		generates an error message that includes sensitive information about its environment, users, or associated data.
CWE-287	Improper Authentication	When an actor claims to have a given identity, the software does not prove or insufficiently proves that the claim is correct.
CWE-295	Improper Certificate Validation	The software does not validate, or incorrectly validates, a certificate.
CWE-273	Improper Check for Dropped Privileges	The software attempts to drop privileges but does not check or incorrectly checks to see if the

		drop succeeded.
CWE-754	Improper Check for Unusual or Exceptional Conditions	The software does not check or incorrectly checks for unusual or exceptional conditions that are not expected to occur frequently during day to day operation of the software.
CWE-913	Improper Control of Dynamically-Managed Code Resources	The software does not properly restrict reading from or writing to dynamically -managed code resources such as variables, objects, classes, attributes, functions, or executable instructions or statements.

CWE-94	Improper Control of Generation of Code ('Code Injection')	The software constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.
CWE-116	Improper Encoding or Escaping of Output	The software prepares a structured message for communication with another component, but encoding or escaping of the data is either missing or done incorrectly.

		As a result, the intended structure of the message is not preserved.
CWE-924	Improper Enforcement of Message Integrity During Transmission in a Communication Channel	The software establishes a communication channel with an endpoint and receives a message from that endpoint, but it does not sufficiently ensure that the message was not modified during transmission.
CWE-178	Improper Handling of Case Sensitivity	The software does not properly account for differences in case sensitivity when accessing or determining the properties of a resource,

		leading to inconsistent results.
CWE-755	Improper Handling of Exceptional Conditions	The software does not handle or incorrectly handles an exceptional condition.
CWE-665	Improper Initialization	The software does not initialize or incorrectly initializes a resource, which might leave the resource in an unexpected state when it is accessed or used.
CWE-20	Improper Input Validation	The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely

		and correctly.
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	The software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.
CWE-59	Improper Link Resolution Before File Access ('Link Following')	The software attempts to access a file based on

		the filename, but it does not properly prevent that filename from identifying a link or shortcut that resolves to an unintended resource.
CWE-667	Improper Locking	The software does not properly acquire or release a lock on a resource, leading to unexpected resource state changes and behaviors.
CWE-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	The software constructs a string for a command to executed by a separate component in another control sphere, but it does not

		properly delimit the intended arguments, options, or switches within that command string.
CWE-1236	Improper Neutralization of Formula Elements in a CSV File	The software saves user-provided information into a Comma-Separated Value (CSV) file, but it does not neutralize or incorrectly neutralizes special elements that could be interpreted as a command when the file is opened by spreadsheet software.
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	The software does not neutralize or incorrectly neutralizes user-controllable

		input before it is placed in output that is used as a web page that is served to other users.
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	The software constructs all or part of a command, data structure, or record using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify how it is parsed or interpreted when it is sent to a downstream component.
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	The software constructs all or part of a command

		using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component.
CWE-917	Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression La	The software constructs all or part of an expression language (EL) statement in a framework such as a Java Server Page (JSP) using externally-influenced input from an upstream component, but it does not neutralize or

		incorrectly neutralizes special elements that could modify the intended EL statement before it is executed.
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	The software constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component.
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	The software constructs all or part of an SQL

		command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.
CWE-281	Improper Preservation of Permissions	The software does not preserve permissions or incorrectly preserves permissions when copying, restoring, or sharing objects, which can cause them to have less restrictive permissions

		than intended.
CWE-269	Improper Privilege Management	The software does not properly assign, modify, track, or check privileges for an actor, creating an unintended sphere of control for that actor.
CWE-212	Improper Removal of Sensitive Information Before Storage or Transfer	The product stores, transfers, or shares a resource that contains sensitive information, but it does not properly remove that information before the product makes the resource available to unauthorized actors.
CWE-404	Improper Resource Shutdown or Release	The program does not release or incorrectly releases a

		resource before it is made available for re-use.
CWE-307	Improper Restriction of Excessive Authentication Attempts	The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks.
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	The software performs operations on a memory buffer, but it can read from or write to a memory location that is outside of the intended boundary of the buffer.
CWE-920	Improper Restriction of Power Consumption	The software

		operates in an environment in which power is a limited resource that cannot be automatically replenished, but the software does not properly restrict the amount of power that its operation consumes.
CWE-776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	The software uses XML documents and allows their structure to be defined with a Document Type Definition (DTD), but it does not properly control the number of recursive definitions of entities.

CWE-1021	Improper Restriction of Rendered UI Layers or Frames	The web application does not restrict or incorrectly restricts frame objects or UI layers that belong to another application or domain, which can lead to user confusion about which interface the user is interacting with.
CWE-611	Improper Restriction of XML External Entity Reference	The software processes an XML document that can contain XML entities with URIs that resolve to documents outside of the intended sphere of control, causing the product to embed incorrect documents into its output.

CWE-662	Improper Synchronization	The software utilizes multiple threads or processes to allow temporary access to a shared resource that can only be exclusive to one process at a time, but it does not properly synchronize these actions, which might cause simultaneous accesses of this resource by multiple threads or processes.
CWE-129	Improper Validation of Array Index	The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the

		index to ensure the index references a valid position within the array.
CWE-354	Improper Validation of Integrity Check Value	The software does not validate or incorrectly validates the integrity check values or "checksums " of a message. This may prevent it from detecting if the data has been modified or corrupted in transmissio n.
CWE-1284	Improper Validation of Specified Quantity in Input	The product receives input that is expected to specify a quantity (such as size or length), but it does not validate or incorrectly

		validates that the quantity has the required properties.
CWE-347	Improper Verification of Cryptographic Signature	The software does not verify, or incorrectly verifies, the cryptographic signature for data.
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	The software receives input from an upstream component that specifies attributes that are to be initialized or updated in an object, but it does not properly control modifications of attributes of the object prototype.
CWE-326	Inadequate Encryption Strength	The software stores or transmits sensitive data using an

		encryption scheme that is theoretically sound, but is not strong enough for the level of protection required.
CWE-838	Inappropriate Encoding for Output Context	The software uses or specifies an encoding when generating output to a downstream component, but the specified encoding is not the same as the encoding that is expected by the downstream component.
CWE-829	Inclusion of Functionality from Untrusted Control Sphere	The software imports, requires, or includes executable functionality (such as a library) from a source that is

		outside of the intended control sphere.
CWE-459	Incomplete Cleanup	The software does not properly "clean up" and remove temporary or supporting resources after they have been used.
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	The product acts as an intermediary HTTP agent (such as a proxy or firewall) in the data flow between two entities such as a client and server, but it does not interpret malformed HTTP requests or responses in ways that are consistent with how the messages

		will be processed by those entities that are at the ultimate destination.
CWE-863	Incorrect Authorization	The software performs an authorization check when an actor attempts to access a resource or perform an action, but it does not correctly perform the check. This allows attackers to bypass intended access restrictions.
CWE-682	Incorrect Calculation	The software performs a calculation that generates incorrect or unintended results that are later used in security-critical

		decisions or resource management.
CWE-131	Incorrect Calculation of Buffer Size	The software does not correctly calculate the size to be used when allocating a buffer, which could lead to a buffer overflow.
CWE-697	Incorrect Comparison	The software compares two entities in a security-relevant context, but the comparison is incorrect, which may lead to resultant weaknesses.
CWE-681	Incorrect Conversion between Numeric Types	When converting from one data type to another, such as long to integer, data can be

		omitted or translated in a way that produces unexpected values. If the resulting values are used in a sensitive context, then dangerous behaviors may occur.
CWE-276	Incorrect Default Permissions	During installation, installed file permissions are set to allow anyone to modify those files.
CWE-732	Incorrect Permission Assignment for Critical Resource	The product specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.
CWE-669	Incorrect Resource Transfer Between Spheres	The product does not properly transfer a

		resource/behavior to another sphere, or improperly imports a resource/behavior from another sphere, in a manner that provides unintended control over that resource.
CWE-704	Incorrect Type Conversion or Cast	The software does not correctly convert an object, resource, or structure from one type to a different type.
CWE-335	Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)	The software uses a Pseudo-Random Number Generator (PRNG) but does not correctly manage seeds.
CWE-407	Inefficient Algorithmic Complexity	An algorithm in a product

		has an inefficient worst-case computational complexity that may be detrimental to system performance and can be triggered by an attacker, typically using crafted manipulations that ensure that the worst case is being reached.
CWE-1333	Inefficient Regular Expression Complexity	The product uses a regular expression with an inefficient, possibly exponential worst-case computational complexity that consumes excessive CPU cycles.
CWE-1188	Insecure Default Initialization of Resource	The software initializes or

		sets a resource with a default that is intended to be changed by the administrator, but the default is not secure.
CWE-922	Insecure Storage of Sensitive Information	The software stores sensitive information without properly limiting read or write access by unauthorized actors.
CWE-532	Insertion of Sensitive Information into Log File	Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information.
CWE-331	Insufficient Entropy	The software uses an algorithm or

		scheme that produces insufficient entropy, leaving patterns or clusters of values that are more likely to occur than others.
NVD-CWE-noinfo	Insufficient Information	There is insufficient information about the issue to classify it; details are unkown or unspecified.
CWE-613	Insufficient Session Expiration	According to WASC, "Insufficient Session Expiration is when a web site permits an attacker to reuse old session credentials or session IDs for authorizatio n."
CWE-345	Insufficient Verification of Data Authenticity	The software does not sufficiently verify the origin or

		authenticity of data, in a way that causes it to accept invalid data.
CWE-522	Insufficiently Protected Credentials	The product transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval.
CWE-190	Integer Overflow or Wraparound	The software performs a calculation that can produce an integer overflow or wraparound, when the logic assumes that the resulting value will always be larger than the original value. This

		can introduce other weaknesses when the calculation is used for resource management or execution control.
CWE-191	Integer Underflow (Wrap or Wraparound)	The product subtracts one value from another, such that the result is less than the minimum allowable integer value, which produces a value that is not equal to the correct result.
CWE-436	Interpretation Conflict	Product A handles inputs or steps differently than Product B, which causes A to perform incorrect actions

		based on its perception of B's state.
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')	The program contains an iteration or loop with an exit condition that cannot be reached, i.e., an infinite loop.
CWE-306	Missing Authentication for Critical Function	The software does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources.
CWE-862	Missing Authorization	The software does not perform an authorization check when an actor attempts to access a resource or perform an action.

CWE-311	Missing Encryption of Sensitive Data	The software does not encrypt sensitive or critical information before storage or transmissio n.
CWE-909	Missing Initialization of Resource	The software does not initialize a critical resource.
CWE-401	Missing Release of Memory after Effective Lifetime	The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.
CWE-772	Missing Release of Resource after Effective Lifetime	The software does not release a resource after its effective lifetime has ended, i.e., after the

		resource is no longer needed.
CWE-476	NULL Pointer Dereference	A NULL pointer dereference occurs when the application dereferences a pointer that it expects to be valid, but is NULL, typically causing a crash or exit.
CWE-203	Observable Discrepancy	The product behaves differently or sends different responses under different circumstances in a way that is observable to an unauthorized actor, which exposes security-relevant information about the state of the product, such as

		whether a particular operation was successful or not.
CWE-193	Off-by-one Error	A product calculates or uses an incorrect maximum or minimum value that is 1 more, or 1 less, than the correct value.
CWE-672	Operation on a Resource after Expiration or Release	The software uses, accesses, or otherwise operates on a resource after that resource has been expired, released, or revoked.
CWE-346	Origin Validation Error	The software does not properly verify that the source of data or communication is valid.

NVD-CWE-Other	Other	NVD is only using a subset of CWE for mapping instead of the entire CWE, and the weakness type is not covered by that subset.
CWE-125	Out-of-bounds Read	The software reads data past the end, or before the beginning, of the intended buffer.
CWE-787	Out-of-bounds Write	The software writes data past the end, or before the beginning, of the intended buffer.
CWE-617	Reachable Assertion	The product contains an assert() or similar statement that can be triggered by an attacker, which leads

		to an application exit or other behavior that is more severe than necessary.
CWE-763	Release of Invalid Pointer or Reference	The application attempts to return a memory resource to the system, but calls the wrong release function or calls the appropriate release function incorrectly.
CWE-565	Reliance on Cookies without Validation and Integrity Checking	The application relies on the existence or values of cookies when performing security-critical operations, but it does not properly ensure that the setting is valid for the associated user.

CWE-918	Server-Side Request Forgery (SSRF)	The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.
CWE-384	Session Fixation	Authenticating a user, or otherwise establishing a new user session, without invalidating any existing session identifier gives an attacker the opportunity to steal authenticated sessions.
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition	The software checks the

		state of a resource before using that resource, but the resource's state can change between the check and the use in a way that invalidates the results of the check. This can cause the software to perform invalid actions when the resource is in an unexpected state.
CWE-252	Unchecked Return Value	The software does not check the return value from a method or function, which can prevent it from detecting unexpected states and conditions.

CWE-674	Uncontrolled Recursion	The product does not properly control the amount of recursion which takes place, consuming excessive resources, such as allocated memory or the program stack.
CWE-400	Uncontrolled Resource Consumption	The software does not properly control the allocation and maintenance of a limited resource, thereby enabling an actor to influence the amount of resources consumed, eventually leading to the exhaustion of available resources.
CWE-427	Uncontrolled Search Path Element	The product uses a fixed

		or controlled search path to find resources, but one or more locations in that path can be under the control of unintended actors.
CWE-428	Unquoted Search Path or Element	The product uses a search path that contains an unquoted element, in which the element contains whitespace or other separators. This can cause the product to access resources in a parent path.
CWE-434	Unrestricted Upload of File with Dangerous Type	The software allows the attacker to upload or transfer files of dangerous

		types that can be automatically processed within the product's environment.
CWE-426	Untrusted Search Path	The application searches for critical resources using an externally-supplied search path that can point to resources that are not under the application's direct control.
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')	A web application accepts a user-controlled input that specifies a link to an external site, and uses that link in a Redirect. This simplifies phishing attacks.

CWE-416	Use After Free	Referencing memory after it has been freed can cause a program to crash, use unexpected values, or execute code.
CWE-327	Use of a Broken or Risky Cryptographic Algorithm	The use of a broken or risky cryptographic algorithm is an unnecessary risk that may result in the exposure of sensitive information.
CWE-338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	The product uses a Pseudo-Random Number Generator (PRNG) in a security context, but the PRNG's algorithm is not cryptographically strong.
CWE-134	Use of Externally-Controlled Format String	The software uses a function

		that accepts a format string as an argument, but the format string originates from an external source.
CWE-470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	The application uses external input with reflection to select which classes or code to use, but it does not sufficiently prevent the input from selecting improper classes or code.
CWE-798	Use of Hard-coded Credentials	The software contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication,

		outbound communication to external components, or encryption of internal data.
CWE-706	Use of Incorrectly-Resolved Name or Reference	The software uses a name or reference to access a resource, but the name/reference resolves to a resource that is outside of the intended control sphere.
CWE-330	Use of Insufficiently Random Values	The software uses insufficiently random numbers or values in a security context that depends on unpredictable numbers.
CWE-916	Use of Password Hash With Insufficient Computational Effort	The software generates a hash for a password,

		but it uses a scheme that does not provide a sufficient level of computatio nal effort that would make password cracking attacks infeasible or expensive.
CWE-908	Use of Uninitialized Resource	The software uses or accesses a resource that has not been initialized.
CWE-640	Weak Password Recovery Mechanism for Forgotten Password	The software contains a mechanism for users to recover or change their passwords without knowing the original password, but the mechanism is weak.
CWE-521	Weak Password Requirements	The product does not require that users

		should have strong passwords, which makes it easier for attackers to compromise user accounts.
CWE-91	XML Injection (aka Blind XPath Injection)	The software does not properly neutralize special elements that are used in XML, allowing attackers to modify the syntax, content, or commands of the XML before it is processed by an end system.