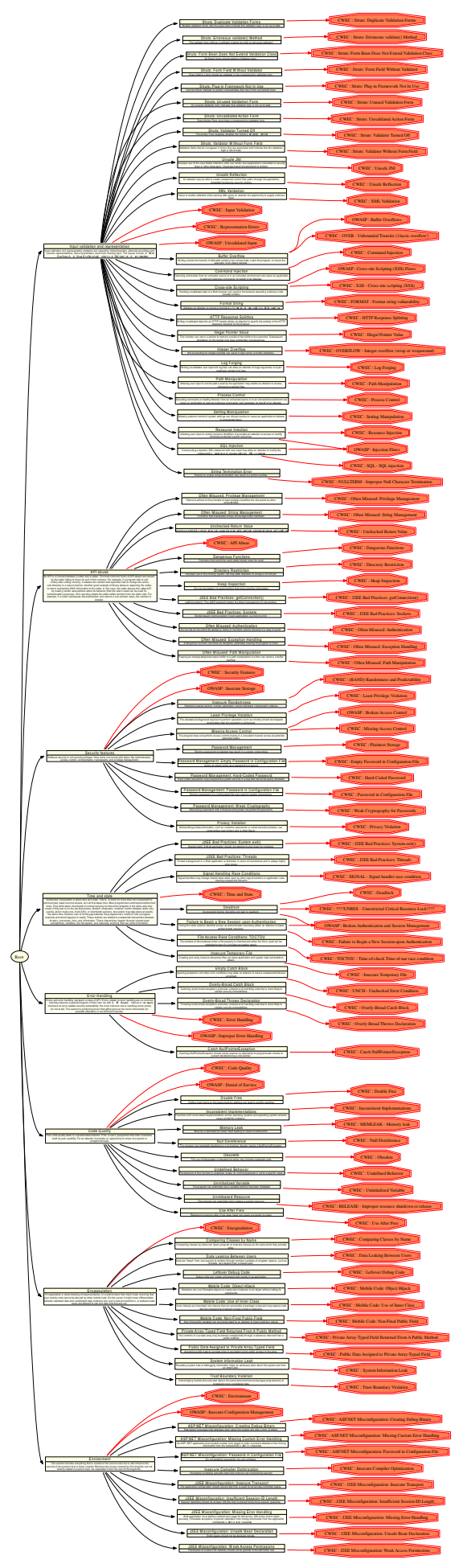
Root
Input validation and representation
Strsts: Duplicate Validation Forms
CWE: Strsts: Duplicate Validation Forms
Strsts: Erroneous validate() Method
CWE: Strsts: Erroneous validate() Method
Strsts: Form Bean Does Not Extend Validation Class
CWE: Strsts: Form Bean Does Not Extend Validation Class
Strsts: Form Field Without Validator
CWE: Strsts: Form Field Without Validator
Strsts: Plug-in Framework Not In Use
CWE: Strsts: Plug-in Framework Not In Use
Strsts: Unused Validation Form
CWE: Strsts: Unused Validation Form
Strsts: Unvalidated Action Form
CWE: Strsts: Unvalidated Action Form
Strsts: Validator Turned Off
CWE: Strsts: Validator Turned Off
Strsts: Validator Without Form Field
CWE: Strsts: Validator Without Form Field
Unsafe JNI
CWE: Unsafe JNI
Unsafe Reflection
CWE: Unsafe Reflection
XML Validation
CWE: XML Validation
CWE: Input Validation
CWE: Representation Errors
OWASP: Unvalidated Input
Buffer Overflow
OWASP: Buffer Overflows
CWE: OVER - Unbounded Transfer (Classic overflow)
Command Injection
CWE: Command Injection
Cross-site Scripting
OWASP: Cross-site Scripting (XSS) Flaws
CWE: XSS - Cross-site scripting (XSS)
Format String
CWE: FORMAT - Format string vulnerability
HTTP Response Splitting
CWE: HTTP Response Splitting
Illegal Pointer Value
CWE: Illegal Pointer Value
Integer Overflow
CWE: OVERFLOW - Integer overflow (wrap or wraparound)
Log Forging
CWE: Log Forging
Path Manipulation
CWE: Path Manipulation
Process Control
CWE: Process Control
Setting Manipulation
CWE: Setting Manipulation
Resource Injection
CWE: Resource Injection
SQL Injection
OWASP: Injection Flaws
CWE: SQL - SQL injection
Sizing Declaration Error
CWE: NULLTERM - Improper Null Character Termination
API abuse
Often Misused: Privilege Management
CWE: Often Misused: Privilege Management
Often Misused: String Management
CWE: Often Misused: String Management
Unchecked Return Value
CWE: Unchecked Return Value
CWE: API Abuse
Dangerous Functions
CWE: Dangerous Functions
Directory Restriction
CWE: Directory Restriction
Heap Inspection
CWE: Heap Inspection
J2EE Bad Practices: getConnection()
CWE: J2EE Bad Practices: getConnection()
J2EE Bad Practices: Sockets
CWE: J2EE Bad Practices: Sockets
Often Misused: Authentication
CWE: Often Misused: Authentication
Often Misused: Exception Handling
CWE: Often Misused: Exception Handling
Often Misused: File Manipulation
CWE: Often Misused: File Manipulation
Security Features
CWE: Security Features
OWASP: Insecure Storage
CWE: (RAND) Randomness and Predictability
Insecure Randomness
CWE: Insecure Randomness
Least Privilege Violation
CWE: Least Privilege Violation
OWASP: Broken Access Control
Least Privilege Violation
CWE: Broken Access Control
Missing Access Control
CWE: Missing Access Control
Missing Access Control
CWE: Missing Access Control
Plaintext Storage
CWE: Plaintext Storage
Password Management
CWE: Password Management
Password Management: Empty Password in Configuration File
CWE: Empty Password in Configuration File
Password Management: Hard-Coded Password
CWE: Hard-Coded Password
Password Management: Password in Configuration File
CWE: Password in Configuration File
Password Management: Weak Cryptography
CWE: Weak Cryptography for Passwords
Privacy Violation
CWE: Privacy Violation
Time and state
J2EE Bad Practices: System.exit()
CWE: J2EE Bad Practices: System.exit()
J2EE Bad Practices: Threads
CWE: J2EE Bad Practices: Threads
Signal Handling Race Conditions
CWE: SIGNAL - Signal handler race condition
CWE: Time and State
Deadlock
CWE: Deadlock
Failure to Release a Resource after Authentication
CWE: ???UNRES - Unrestricted Critical Resource Lock(???)
OWASP: Broken Authentication and Session Management
File Access Race Conditions: TOCTOU
CWE: Failure to Begin a New Session upon Authentication
Insecure Temporary File
CWE: TOCTOU - Time-of-check Time-of-use race condition
Insecure Temporary File
CWE: Insecure Temporary File
Empty Catch Block
CWE: UNCH - Unchecked Error Condition
Overly Broad Catch Block
CWE: Overly Broad Catch Block
Overly Broad Throws Declaration
CWE: Overly Broad Throws Declaration
Error Handling
CWE: Error Handling
OWASP: Improper Error Handling
Catch NullPointerException
CWE: Catch NullPointerException
Code quality
CWE: Code Quality
OWASP: Denial of Service
Double Free
CWE: Double Free
Inconsistent Implementations
CWE: Inconsistent Implementations
Memory Leak
CWE: MEMLEAK - Memory leak
Null Dereference
CWE: Null Dereference
Obsolete
CWE: Obsolete
Undefined Behavior
CWE: Undefined Behavior
Uninitialized Variable
CWE: Uninitialized Variable
Unreleased Resource
CWE: RELEASE - Improper resource shutdown or release
Use After Free
CWE: Use After Free
Encapsulation
CWE: Encapsulation
Comparing Classes by Name
CWE: Comparing Classes by Name
Data Leaking Between Users
CWE: Data Leaking Between Users
Leftover Debug Code
CWE: Leftover Debug Code
Mobile Code: Object Hijack
CWE: Mobile Code: Object Hijack
Mobile Code: Use of Inner Class
CWE: Mobile Code: Use of Inner Class
Mobile Code: Non-Final Public Field
CWE: Mobile Code: Non-Final Public Field
Private Array-Typed Field Returned From A Public Method
CWE: Private Array-Typed Field Returned From A Public Method
Public Data Assigned to Private Array-Typed Field
CWE: Public Data Assigned to Private Array-Typed Field
System Information Leak
CWE: System Information Leak
Trust Boundary Violation
CWE: Trust Boundary Violation
Environment
CWE: Environment
OWASP: Insecure Configuration Management
ASP.NET Misconfiguration: Creating Debug Binary
CWE: ASP.NET Misconfiguration: Creating Debug Binary
ASP.NET Misconfiguration: Missing Custom Error Handling
CWE: ASP.NET Misconfiguration: Missing Custom Error Handling
ASP.NET Misconfiguration: Password in Configuration File
CWE: ASP.NET Misconfiguration: Password in Configuration File
Insecure Compiler Optimization
CWE: Insecure Compiler Optimization
J2EE Misconfiguration: Insecure Transport
CWE: J2EE Misconfiguration: Insecure Transport
J2EE Misconfiguration: Insufficient Session-ID Length
CWE: J2EE Misconfiguration: Insufficient Session-ID Length
J2EE Misconfiguration: Missing Error Handling
CWE: J2EE Misconfiguration: Missing Error Handling
J2EE Misconfiguration: Unsafe Bean Declaration
CWE: J2EE Misconfiguration: Unsafe Bean Declaration
J2EE Misconfiguration: Weak Access Permissions
CWE: J2EE Misconfiguration: Weak Access Permissions