
937 - OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities
931 - OWASP Top Ten 2013 Category A3 - Cross-Site Scripting (XSS)
79 - Improper Neutralization of Input During Web Page Generation
938 - OWASP Top Ten 2013 Category A10 - Unvalidated Redirects and Forwards
601 - URL Redirection to Untrusted Site
643 - Improper Neutralization of Data within XPath Expressions
652 - Improper Neutralization of Data within XQuery Expressions
74 - Improper Neutralization of Special Elements in Output Used by a Downstream Component
77 - Improper Neutralization of Special Elements used in a Command
929 - OWASP Top Ten 2013 Category A1 - Injection
78 - Improper Neutralization of Special Elements used in an OS Command
88 - Improper Neutralization of Argument Delimiters in a Command
89 - Improper Neutralization of Special Elements used in an SQL Command
564 - Use of Hibernate with HQL/SQL Query String Containing External Input
90 - Improper Neutralization of Special Elements used in an LDAP Query
91 - XML Injection
936 - OWASP Top Ten 2013 Category A8 - Cross-Site Request Forgery (CSRF)
352 - Cross-Site Request Forgery
935 - OWASP Top Ten 2013 Category A7 - Missing Function Level Access Control
285 - Improper Authorization
256 - Plaintext Storage of a Password
287 - Improper Authentication
384 - Session Fixation
522 - Insufficiently Protected Credentials
930 - OWASP Top Ten 2013 Category A2 - Broken Authentication and Session Management
523 - Unprotected Transport of Credentials
613 - DEPRECATED: Insufficient Session Expiration
620 - Unverified Password Change
640 - Weak Password Recovery Mechanism for Forgotten Password
311 - Missing Encryption of Sensitive Data
312 - Cleartext Storage of Sensitive Information
319 - Cleartext Transmission of Sensitive Information
325 - Missing Cryptographic Step
934 - OWASP Top Ten 2013 Category A6 - Sensitive Data Exposure
326 - Inadequate Encryption Strength
327 - Use of a Broken or Risky Cryptographic Algorithm
328 - Use of Weak Hash
320 - Key Management Errors
22 - Improper Limitation of a Pathname to a Restricted Directory
639 - Authorization Bypass Through User-Controlled Key
932 - OWASP Top Ten 2013 Category A4 - Insecure Direct Object References
706 - Use of Incorrectly-Resolved Name or Reference
99 - Improper Control of Resource Identifiers
209 - Generation of Error Message Containing Sensitive Information
215 - Insertion of Sensitive Information Into Debugging Code
933 - OWASP Top Ten 2013 Category A5 - Security Misconfiguration
548 - Exposure of Information Through Directory Listing
16 - Configuration
2 - 7PK - Environment