- Automotive
  - Unauthorized Access to Vehicle Design Data
    - Financial Gain through Intellectual Property Theft
      - Design and Engineering Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
  - Compromise of Engineering and Simulation Systems
    - Disruption of Automotive Manufacturing and Safety Standards
      - Engineering and Simulation Platforms
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-319: Cleartext Transmission of Sensitive Information
  - Data Exposure in Supply Chains
    - Financial Gain through Intellectual Property Theft
      - Supply Chain Management and Vendor Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-319: Cleartext Transmission of Sensitive Information
  - Data Exposure in Research & Development
    - Technological Advancement through Industrial Espionage
      - Research & Development Networks and Data Repositories
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-319: Cleartext Transmission of Sensitive Information
  - Disruption of Automotive Production Systems
    - Disruption of Automotive Manufacturing and Supply Chains
      - Automated Manufacturing and Production Control Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-319: Cleartext Transmission of Sensitive Information
  - Compromise of Industrial Control Systems (ICS)
    - Disruption of Automotive Manufacturing and Supply Chains
      - Industrial Control Systems (ICS) and Smart Manufacturing Platforms
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
  - Unauthorized Modification of Vehicle Software and Firmware
    - Disruption of Automotive Safety and Security
      - Vehicle Software and Embedded Firmware Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
  - Abuse of Smart Manufacturing and AI-driven Automation Systems
    - Influence over Smart Manufacturing Processes
      - IoT and AI-Driven Smart Manufacturing Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
  - Injection of Malicious Code into Supplier-Embedded Software
    - Disruption of Automotive Safety and Supply Chains
      - Supplier-Embedded Software and Firmware Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
  - Compromise of Dealer Management Systems (DMS)
    - Financial Gain through Data Theft and Fraud
      - Dealer Management Systems (DMS)
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
  - Unauthorized Access to Customer Financing and Sales Data
    - Financial Gain through Fraud and Identity Theft
      - Customer Financing and Sales Data Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
  - Compromise of Dealership Payment Systems
    - Financial Gain through Payment Fraud and Data Theft
      - Dealership Payment Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
  - Unauthorized Access to Dealership Management Platforms
    - Unauthorized Access for Data Theft and Financial Fraud
      - Dealership Management and Financial Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
  - Unauthorized Access to Vehicle Inventory Systems
    - Disruption of Operations
      - Digital Inventory Management Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
  - Unauthorized Manipulation of Vehicle Diagnostic and Tuning Systems
    - Disruption of Operations
      - Vehicle Diagnostic and Tuning Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
  - Abuse of Remote Vehicle Maintenance and OTA (Over-The-Air) Update Services
    - Disruption of Vehicle Operations and Safety
      - Remote Vehicle Maintenance and Over-the-Air Update Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
  - Unauthorized Modifications to Vehicle Software
    - Manipulation of Vehicle Performance
      - Vehicle Software and Control Systems
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)
  - Unauthorized Access to Vehicle Diagnostic and Service Data
    - Technological Advantage through Theft of Proprietary Data
      - Vehicle Service and Customization Platforms
        - CWE-521: Weak Password Requirements
        - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
        - CWE-287: Improper Authentication
        - CWE-284: Improper Access Control
        - CWE-639: Authorization Bypass Through User-Controlled Key
        - CWE-863: Incorrect Authorization
        - CWE-311: Missing Encryption of Sensitive Data
        - CWE-778: Insufficient Logging
        - CWE-502: Deserialization of Untrusted Data
        - CWE-918: Server-Side Request Forgery (SSRF)
        - CWE-20: Improper Input Validation
        - CWE-94: Improper Control of Generation of Code (Code Injection)
        - CWE-434: Unrestricted Upload of File with Dangerous Type
        - CWE-319: Cleartext Transmission of Sensitive Information
        - CWE-601: URL Redirection to Untrusted Site (Open Redirect)
        - CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)

Presented with xmind