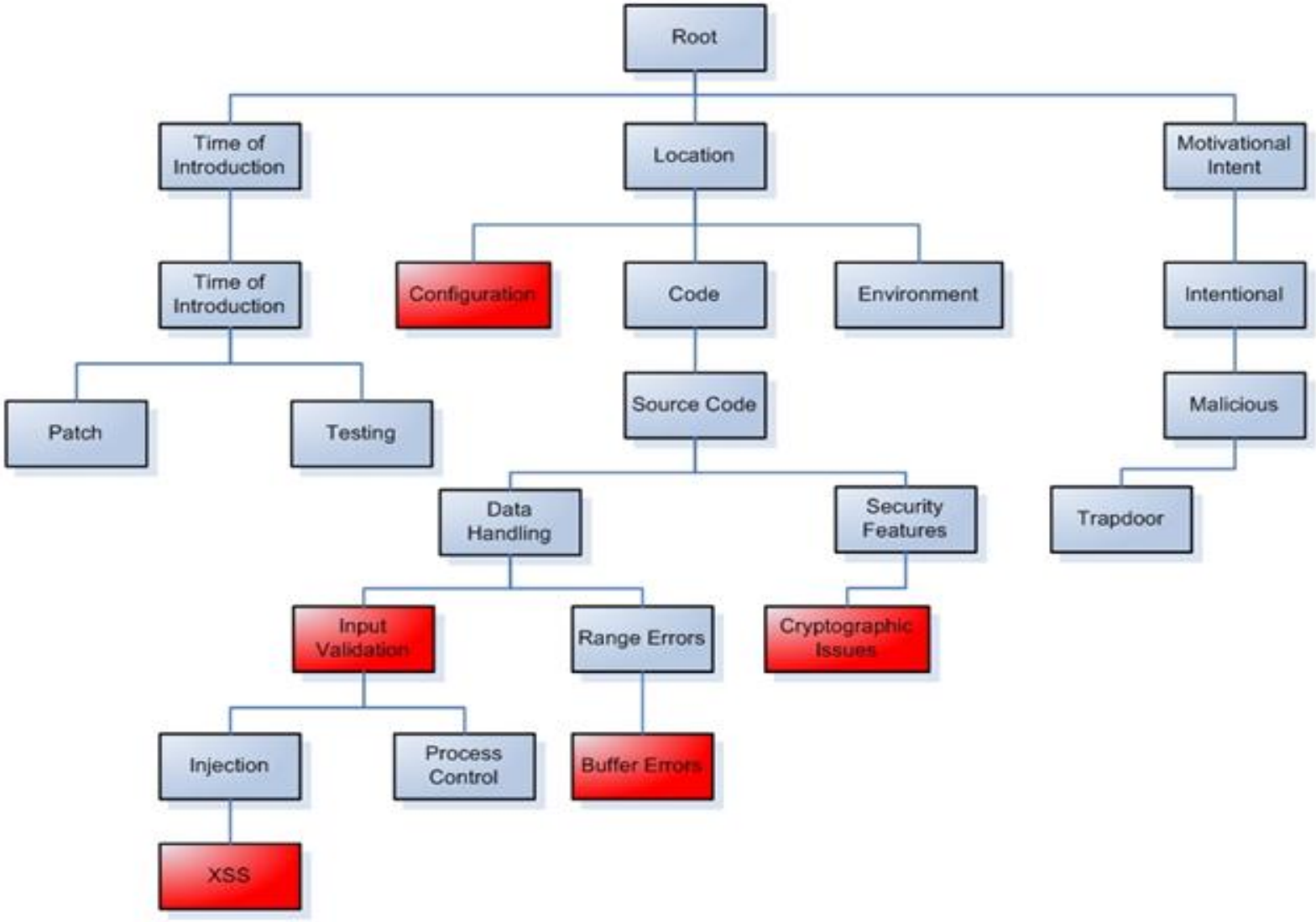
Системы классификации уязвимостей сервисов

- NVD (National Vulnerability Database) – Национальная база данных уязвимостей правительства США предназначена для автоматизации управления уязвимостями и их соответствием программному обеспечению, в составе:
  - ✓ CVE (Common Vulnerabilities and Exposures) – список известных уязвимостей, имеющий строгое структурирование по описательным критериям;
  - ✓ CWE (Common Weakness Enumeration) – словарь категорий уязвимостей в программных продуктах;
  - ✓ CPE (Common Platform Enumeration) – система идентификации программных продуктов;
  - ✓ CVSS (Common Vulnerability Scoring System) – система оценки степени опасности различных уязвимостей;
- BID;
- OSVDB;
- Secunia;
- ISS X-Force;
- Отдельные классификации различных сканеров уязвимостей.

Структура CWE



Представление данных в реестре CWE (фрагмент)

- Path Equivalence: Windows 8.3 Filename - *(58)*
- Symbolic Name not Mapping to Correct Object - *(386)*

Improper Access Control - (284)

- Improper Authentication - *(287)*
  - Authentication Bypass Issues - *(592)*
    - Authentication Bypass Using an Alternate Path or Channel - *(288)*
      - *Direct Request ('Forced Browsing') - (425)*
    - Authentication Bypass by Alternate Name - *(289)*
    - Authentication Bypass by Assumed-Immutable Data - *(302)*
    - Authentication Bypass by Capture-replay - *(294)*
    - Authentication Bypass by Primary Weakness - *(305)*
    - Authentication Bypass by Spoofing - *(290)*
      - Trusting Self-reported DNS Name - *(292)*
      - Trusting Self-reported IP Address - *(291)*
        - *Modification of Assumed-Immutable Data (MAID) - (471)*
        - *Use of Less Trusted Source - (348)*
      - Using Referer Field for Authentication - *(293)*
    - Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created - *(593)*
  - Channel Accessible by Non-Endpoint ('Man-in-the-Middle') - *(300)*
  - Improper Restriction of Excessive Authentication Attempts - *(307)*
  - Incorrect Implementation of Authentication Algorithm - *(303)*
  - Insufficiently Protected Credentials - *(522)*
    - J2EE Misconfiguration: Plaintext Password in Configuration File - *(555)*
    - Missing Password Field Masking - *(549)*
    - Password in Configuration File - *(260)*
      - ASP.NET Misconfiguration: Password in Configuration File - *(13)*
      - Empty Password in Configuration File - *(258)*
    - Plaintext Storage of a Password - *(256)*
    - Storing Passwords in a Recoverable Format - *(257)*

Пример описания уязвимостей в NVD

```
</entry>
 <entry id="CVE-2011-2173">
  <vuln:vulnerable-configuration id="http://nvd.nist.gov/">
   <cpe-lang:logical-test negate="false" operator="OR">
    <cpe-lang:fact-ref name="cpe:/a:ibm:websphere_portal:6.0.1.7" />
    <cpe-lang:fact-ref name="cpe:/a:ibm:websphere_portal:7.0.0.1" />
   </cpe-lang:logical-test>
  </vuln:vulnerable-configuration>
  <vuln:vulnerable-software-list>
   <vuln:product>cpe:/a:ibm:websphere_portal:6.0.1.7</vuln:product>
   <vuln:product>cpe:/a:ibm:websphere_portal:7.0.0.1</vuln:product>
  </vuln:vulnerable-software-list>
  <vuln:cve-id>CVE-2011-2173</vuln:cve-id>
  <vuln:published-datetime>2011-05-26T12:55:06.613-04:00</vuln:published-datetime>
  <vuln:last-modified-datetime>2011-05-27T00:00:00.000-04:00</vuln:last-modified-datetime>
  <vuln:cvss>
   <cvss:base_metrics>
    <cvss:score>4.0</cvss:score>
    <cvss:access-vector>NETWORK</cvss:access-vector>
    <cvss:access-complexity>LOW</cvss:access-complexity>
    <cvss:authentication>SINGLE_INSTANCE</cvss:authentication>
    <cvss:confidentiality-impact>NONE</cvss:confidentiality-impact>
    <cvss:integrity-impact>NONE</cvss:integrity-impact>
    <cvss:availability-impact>PARTIAL</cvss:availability-impact>
    <cvss:source>http://nvd.nist.gov</cvss:source>
    <cvss:generated-on-datetime>2011-05-27T09:17:00.000-04:00</cvss:generated-on-datetime>
   </cvss:base_metrics>
  </vuln:cvss>
  <vuln:cwe id="CWE-399" />
  <vuln:references xml:lang="en" reference_type="UNKNOWN">
   <vuln:source>CONFIRM</vuln:source>
   <vuln:reference href="http://www.ibm.com/support/docview.wss?uid=swg24029452"
xml:lang="en">http://www.ibm.com/support/docview.wss?uid=swg24029452</vuln:reference>
  </vuln:references>
  <vuln:references xml:lang="en" reference_type="UNKNOWN">
   <vuln:source>AIXAPAR</vuln:source>
   <vuln:reference href="http://www-01.ibm.com/support/docview.wss?uid=swg1PM33432" xml:lang="en">PM33432</vuln:reference>
  </vuln:references>
  <vuln:summary>The implementation of OutputMediator objects in IBM WebSphere Portal 6.0.1.7, and 7.0.0.1 before CF002, allows remote authenticated users to
cause a denial of service (memory consumption) via requests.</vuln:summary>
 </entry>
```