**Weak XML Schema: Type Any Development Mitigation SOP**

When a XML Schema allows the <any> element, it provides a means for XML injections to occur. The <any> element can be included in a valid XML document, and an attacker can add nodes in to the XML document not declared in the schema or overwrite any previous written nodes.

**Defense Against Weak XML Schema: Type Any**

To prevent being vulnerable to this exploit, replace the <any> element with a concretely defined elements. By removing the <any> element, it removes the capability of the document to not contain any additional elements that are not declared in the XML schema.

**Example**

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"  >

  <xs:element name="cart" >

    <xs:complexType>

      <xs:sequence>

     <xs:element name="itemID" maxOccurs="1" />

     <xs:element name="price" maxOccurs="1" />

     <xs:element name="description" maxOccurs="1"/>

        <xs:any minOccurs="0"/>

      </xs:sequence>

    </xs:complexType>

  </xs:element>

  <xs:element name="description" type="xs:string"/>

  <xs:element name="name" type="xs:string"/>

  <xs:element name="price" type="xs:decimal"/>

  <xs:element name="code" type="xs:string"/>

</xs:schema>

**Explanation**

For the above example, the <any> element is used to extend the XML document and allows to overwrite previous nodes.

**Recommendation**

To prevent being vulnerable to this exploit, explicitly define elements instead of using the <any> element.

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"  >

  <xs:element name="cart" >

    <xs:complexType>

      <xs:sequence>

    <xs:element name="itemID" maxOccurs="1" />

    <xs:element name="price" maxOccurs="1" />

    <xs:element name="description" maxOccurs="1"/>

      </xs:sequence>

    </xs:complexType>

  </xs:element>

  <xs:element name="description" type="xs:string"/>

  <xs:element name="name" type="xs:string"/>

  <xs:element name="price" type="xs:decimal"/>

  <xs:element name="code" type="xs:string"/>

</xs:schema>