**SOAP parameter Tampering**

**Description 1**

An attacker sends a SOAP message where the field values are other than what the server is likely to expect in order to precipitate non-standard server behavior. In a SOAP message, parameters take the form of values within XML elements. The server will have an XML schema that indicates certain restrictions on these parameter values. For example, the server may expect a parameter to be a string with fewer than 10 characters, or a number less than 100. In a SOAP parameter tampering attack, an attacker either violates this schema, or takes advantage of flexibility within the scheme (for example, a lack of a character limit) to provide parameters that a server might not expect. Examples of unexpected parameters include oversized data, data with different data types, inserting metacharacters within data, and sending contextually inappropriate data (for example, sending a non-existent product name in a product name field or using an out-of-order sequence number). Results of this attack can include **information disclosure, denial of service, or even execution of arbitrary code**. [1]

**Description 2**

Usually each SOAP request contains some sort of parameter that is passed to the application logic. If the application logic doesn't check what type of parameters are passed a classical buffer overflow within the application logic can easily occur if the parameters are out of bound. A simple example is a string value whose range of values is exceeded.

NOTE: This attack is not web application specific. All applications processing user input might be vulnerable to this attack. [2]

**Example.** Let us assume that the attacked web service expects an integer value between 0 to 15. Which equals a variable size of 4 bits**. If an attacker passes an integer smaller than 0 or greater than 15 a buffer overflow will occur if the application logic does not handle this exception**. In Listing 1, the passed value is 20.

<?xml version=”1.0” encoding=”UTF-8”?>

**<soap:Envelope** xmlns:soap=”http://schemas.xmlsoap.org/soap/envelope/” xmlns:ns=”http://example.org/soap/”**>**

**<soap:Body>**

**<soap:Value>**20**</soap:Value>**

**</soap:Body>**

**</soap:Envelope>**

**Description 3**

An attacker modifies the parameters of the SOAP message that is sent from the service consumer to the service provider to initiate a SQL injection attack. On the service provider side, the SOAP message is parsed and parameters are not properly validated before being used to access a database in a way that does not use parameter binding, thus **enabling the attacker to control the structure of the executed SQL query. This pattern describes a SQL injection attack with the delivery mechanism being a SOAP message.**

**Reference**

**[1]** [**https://capec.mitre.org/data/definitions/280.html**](https://capec.mitre.org/data/definitions/280.html)

**[2]** [**http://www.ws-attacks.org/SOAP\_Parameter\_DOS**](http://www.ws-attacks.org/SOAP_Parameter_DOS)

**[3]** [**https://capec.mitre.org/data/definitions/110.html**](https://capec.mitre.org/data/definitions/110.html)