XML Injection Mutation for Web Services Vulnerability Testing Based on SOAP Messages

Bimal Varghese Simi Stephen

Department of Computer Science and Engineering
Federal Institute of Science and Technology
Mookkannoor

March 5, 2015

Outline

Introduction

Web Service

- Common way of implementing SOA.
- Widely used in the Internet.
- Quality and Reliability of Web Service must be heavily tested.

Introduction

Vulnerabilities in WS

- Multiple Components in WS

Vulnerabilities in WS

- Multiple Components in WS
    - WSDL

Vulnerabilities in WS

- Multiple Components in WS
  - WSDL
  - SOAP

Vulnerabilities in WS

- Multiple Components in WS
  - WSDL
  - SOAP
  - XML

Vulnerabilities in WS

- Multiple Components in WS
  - WSDL
  - SOAP
  - XML
  - UDDI

Vulnerabilities in WS

- Multiple Components in WS
    - WSDL
    - SOAP
    - XML
    - UDDI

Vulnerabilities in WS

- Multiple Components in WS
  - WSDL
  - SOAP
  - XML
  - UDDI
- Vulnerability refers to flaws in the service that threaten the security of the computer system

Vulnerabilities in WS

- Multiple Components in WS
  - WSDL
  - SOAP
  - XML
  - UDDI
- Vulnerability refers to flaws in the service that threaten the security of the computer system
- Some types of Web service vulnerability faults might not be effectively revealed by traditional testing approaches

Introduction

Mutation Operators

- Testing based on SOAP message.
- An extended Regular Tree Grammar(RTG) model
  - $<$ E; N; DT; P; A; $n_s >$
  - E :finite set of elements.
  - N :finite set of non Terminals.
  - DT :finite set of Data types.
  - P :finite set of production rules.
  - A :2 tuple $< n, type >$
    1. n :number of parameters.
    2. type: parameter type.
- A mutation operator is r= $f(n_1, n_2, ...n_i)$ where f is a function, i $\geq$1, each $n_1, n_2, ...n_i \epsilon N$ and has an arbitrary data type and r outputs mutated $n_1, n_2, ..n_i$ with the same data type.

Introduction

Mutation Operators

- Regular Mutation
  - Small modification of the legitimate input

Mutation Operators

- Regular Mutation
  - Small modification of the legitimate input
- Worst Input Mutation
  - Use Farthest neighbor sequence from the legitimate input.

Contd. . .

- Many program faults result in failures manifesting in contiguous areas of the input domain.
- if previously executed test cases have not revealed a failure, new test cases should be as far from the already executed non-failure test cases as possible
- For Testing, a Web Service Vulnerability Testing System (WSVTS) is created

Advantages

- Have the greatest possible test coverage.
- Typical representation for triggering faults.
- Low redundancy.

Introduction

XML Injection

- XML is the default way by which web service communicates.
- Also used in storing data with dynamic tag values.
- Tampering an XML will compromise the security of the web service.
- One of the most serious xml vulnerability is the XML injection.
- Can compromise data and even the security of the entire system itself.

Introduction

Work Completed

- Web service Testing Tool is Created.
- Tool is able to identify the available Method names, their parameters, types, and their return values from the wsdl file.
- It is able to generate SOAP message for available Web methods dynamically.
- It can also invoke the web method and display the result in xml format.
- Can inject *xml injection vulnerability* code into SOAP message.

Introduction

GUI Screens

Main Form

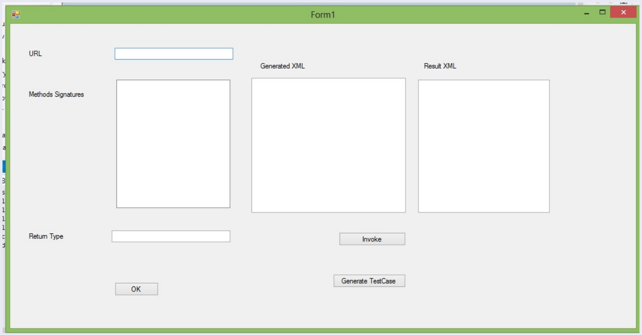
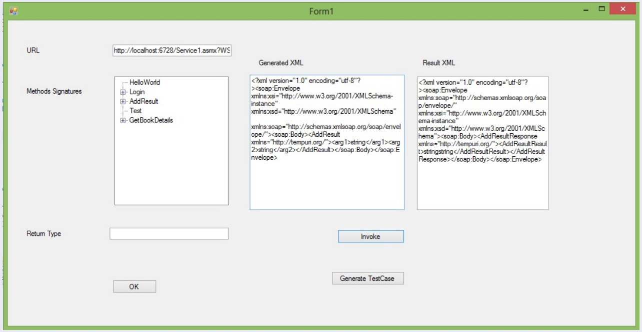


Figure: Main Form

GUI Screens

Main Form



http://localhost:6728/Service1.asmx?WS

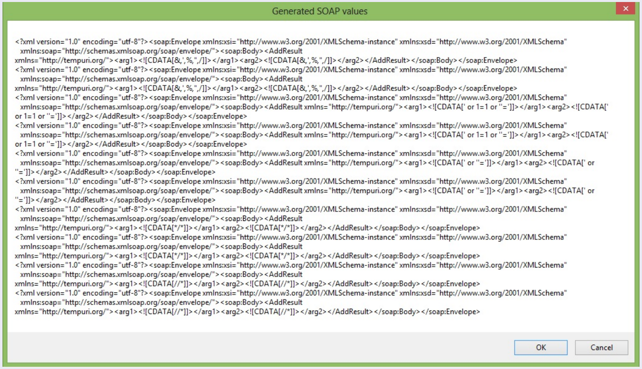
```
<?xml version="1.0" encoding="utf-8"?
><soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"

xmlns:soap="http://schemas.xmlsoap.org/soap/envel
ope/"><soap:Body><AddResult
xmlns="http://tempuri.org/"><arg1>string</arg1><arg
2>string</arg2></AddResult></soap:Body></soap:E
nvelope>
```

```
<?xml version="1.0" encoding="utf-8"?
><soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soa
p/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSch
ema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSc
hema"><soap:Body><AddResultResponse
xmlns="http://tempuri.org/"><AddResultResul
t>stringstring</AddResultResult></AddResult
Response></soap:Body></soap:Envelope>
```

Figure: Main Form

GUI Screens

Test Cases

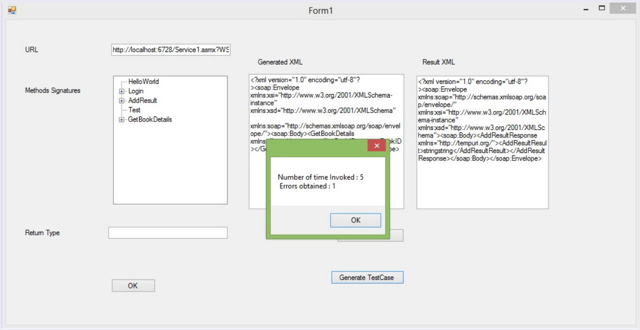


```
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><AddResult
xmlns="http://tempuri.org/"><arg1><![CDATA[&,',%,",/]]></arg1><arg2><![CDATA[&,',%,",/]]></arg2></AddResult></soap:Body></soap:Envelope>
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><AddResult
xmlns="http://tempuri.org/"><arg1><![CDATA[&,',%,",/]]></arg1><arg2><![CDATA[&,',%,",/]]></arg2></AddResult></soap:Body></soap:Envelope>
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><AddResult xmlns="http://tempuri.org/"><arg1><![CDATA[' or 1=1 or ''=']]></arg1><arg2><![CDATA['
or 1=1 or ''=']]></arg2></AddResult></soap:Body></soap:Envelope>
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><AddResult xmlns="http://tempuri.org/"><arg1><![CDATA[' or 1=1 or ''=']]></arg1><arg2><![CDATA['
or 1=1 or ''=']]></arg2></AddResult></soap:Body></soap:Envelope>
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><AddResult xmlns="http://tempuri.org/"><arg1><![CDATA[' or ''=']]></arg1><arg2><![CDATA[' or
''=']]></arg2></AddResult></soap:Body></soap:Envelope>
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><AddResult xmlns="http://tempuri.org/"><arg1><![CDATA[' or ''=']]></arg1><arg2><![CDATA[' or
''=']]></arg2></AddResult></soap:Body></soap:Envelope>
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><AddResult
xmlns="http://tempuri.org/"><arg1><![CDATA[*/*]]></arg1><arg2><![CDATA[*/*]]></arg2></AddResult></soap:Body></soap:Envelope>
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><AddResult
xmlns="http://tempuri.org/"><arg1><![CDATA[*/*]]></arg1><arg2><![CDATA[*/*]]></arg2></AddResult></soap:Body></soap:Envelope>
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><AddResult
xmlns="http://tempuri.org/"><arg1><![CDATA[//*]]></arg1><arg2><![CDATA[//*]]></arg2></AddResult></soap:Body></soap:Envelope>
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><AddResult
xmlns="http://tempuri.org/"><arg1><![CDATA[//*]]></arg1><arg2><![CDATA[//*]]></arg2></AddResult></soap:Body></soap:Envelope>
```

Figure: Main Form

GUI Screens

Results



http://localhost:6728/Service1.asmx?WS

HelloWorld
Login
AddResult
Test
GetBookDetails

```
<?xml version="1.0" encoding="utf-8"?
><soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"

xmlns:soap="http://schemas.xmlsoap.org/soap/envel
ope/"><soap:Body><GetBookDetails
xmlns                                    okID
></G                                     pe>
```

```
<?xml version="1.0" encoding="utf-8"?
><soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soa
p/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSch
ema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSc
hema"><soap:Body><AddResultResponse
xmlns="http://tempuri.org/"><AddResultResul
t>stringstring</AddResultResult></AddResult
Response></soap:Body></soap:Envelope>
```

Number of time Invoked : 5
Errors obtained : 1

Figure: Result Form

To be completed

- Proper analysis of output.
- Proper formatting of XML for display.
- Display output for test case invocation.
- Fix display issues is showing the results.
- Clean the code.

Demo

Thank You