WS-Attacker

A Modular Framework for Web Services Penetration Testing

Christian Mainka

27. Januar 2011

HelloName is chosen as the operation to be tested. The table at the bottom gives a form based input possibility for all request parameters and in this case, *name* is set to *Hello*.

1.2 Submitting a Test Request

Next step is to do a test request: Figure 2 shows the test request and the corresponding response. The request contains a "HelloName" element as first body child and the response holds the corresponding element "HelloNameResult". This request is very important as attack plugins will use its response for comparing it with the responses of the attack request. This allows to check, what has really changed due to attack modifications.

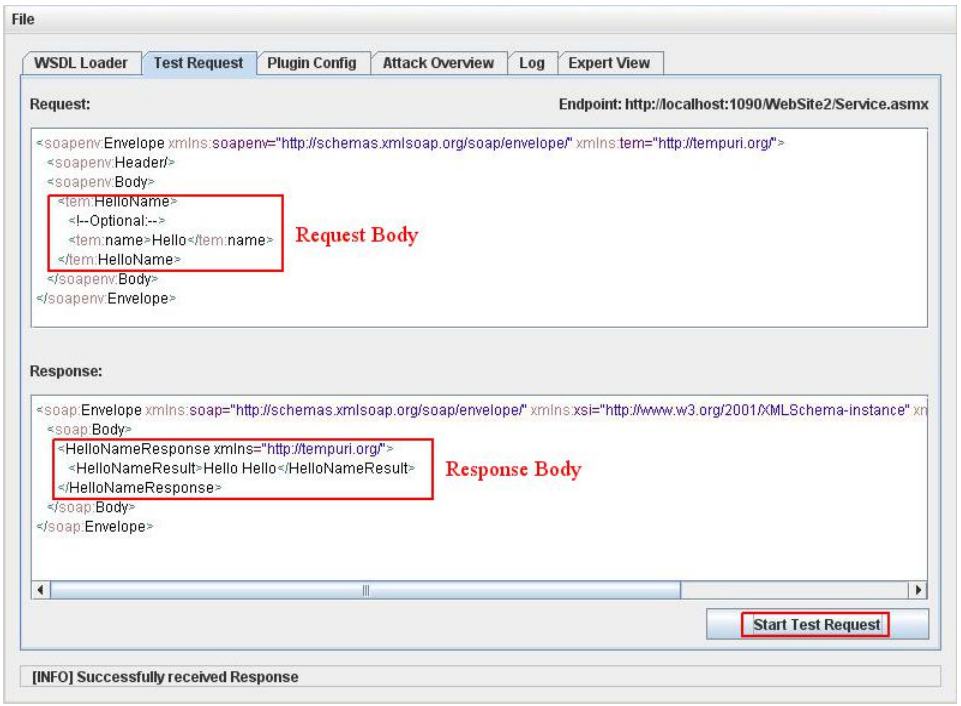

Figure 2: Submitting a test request

1.3 Attack Plugin Configuration

The next step is to configure the plugins. In this case, the automatic mode is used for SOAPAction Spoofing (Figure 3) and the WS-Addressing Spoofing plugin detects the

endpoint URL (Your IP) automatically (Figure 4), too – there is nothing to configure manually. The tree on the left shares different views on the plugins. *Active Plugins* contains all plugins which will be used for attacking the server, *All Plugins* contains all plugins ordered by their category and *Alphabetical Sorted* shows all plugins in an alphabetical order.

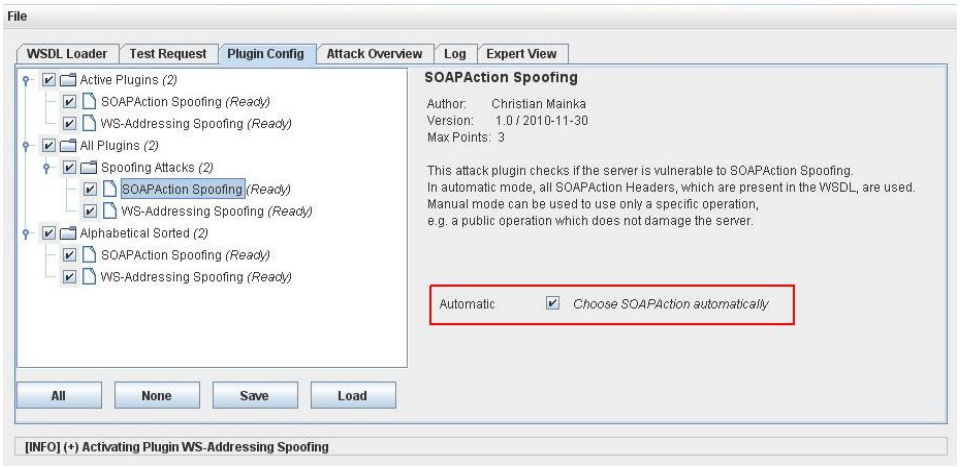

Figure 3: Plugin configuration for SOAPAction Spoofing

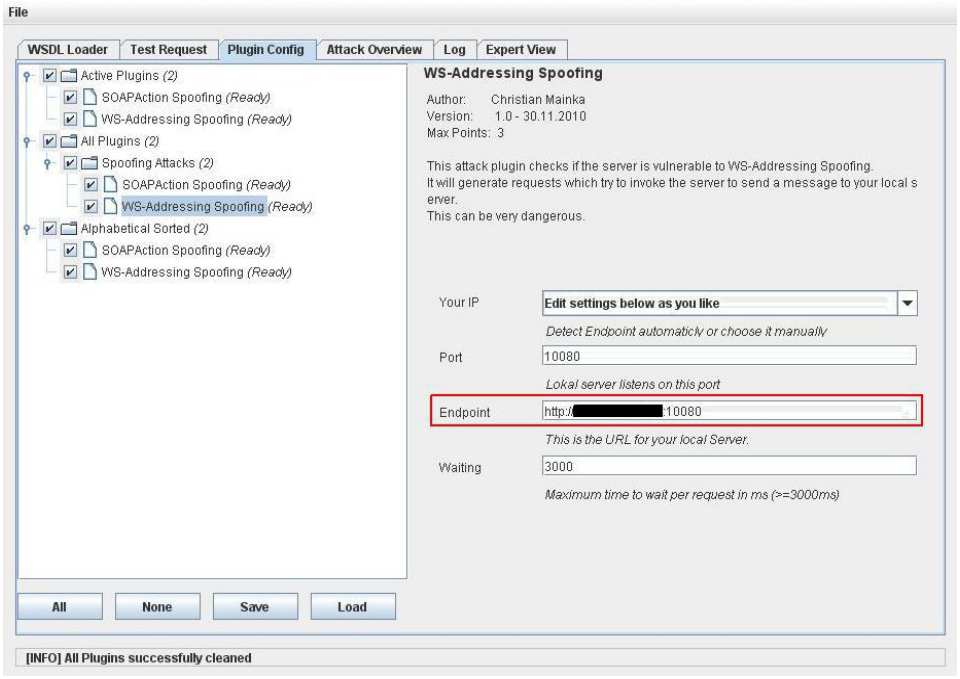

Figure 4: Plugin configuration for WS-Addressing Spoofing

1.4 Starting the Attacks

The last step is to start the attack. Figure 5 shows the overview of a finished attack run. Active plugins are displayed on the top, their results at the bottom. The slider in the top part allows to filter the results by their level. The user can choose to see only the most *important* results, or see even the request content at the *tracing* level.

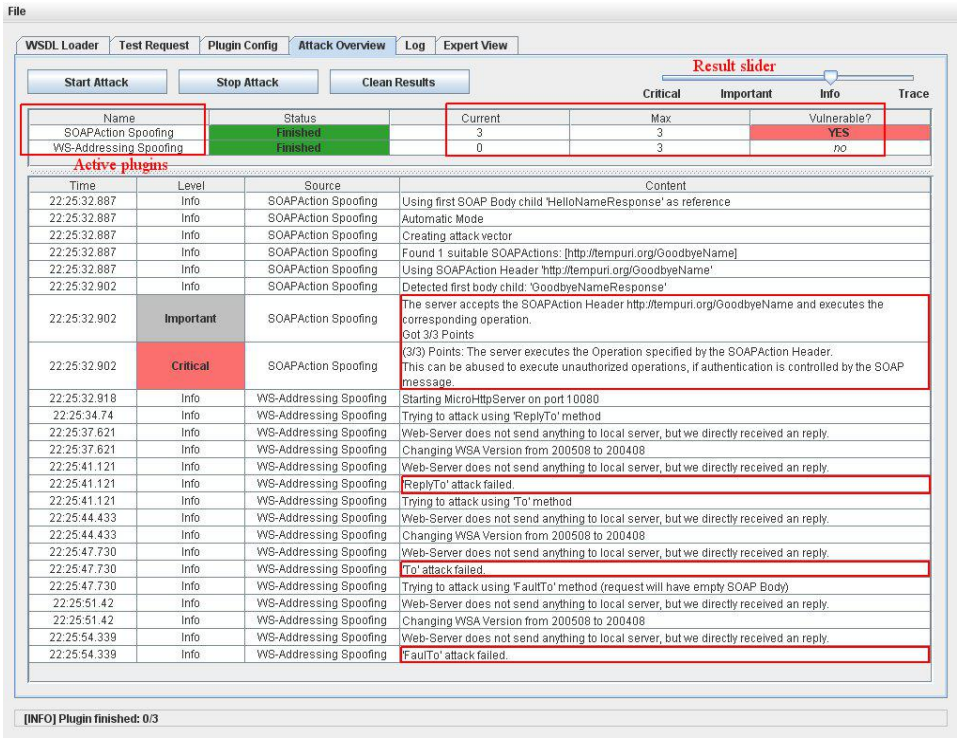

Figure 5: Penetration test finished.

The web service is vulnerable to SOAPAction Spoofing but resistant to WS-Addressing Spoofing. This is indicated different aspects:

1. The *vulnerable* column values show **YES** for SOAPAction Spoofing and *no* for WS-Addressing Spoofing.
2. The SOAPAction Spoofing plugin got the maximum rating – three of three points in this case – and WS-Addressing Spoofing got zero points.
3. The results show, that the server has executed the operation defined in the SOAP-Action Header, which is the most critical security issue.