Web Service Validation

https://campus.barracuda.com/doc/24215943/

XML Validation Settings

The XML Validation Settings allows you to set custom validation rules for XML requests or responses. For example, a rule that aborts request processing if there are more than 50 total elements in the XML or limit the message size or total number of bytes, minimizing the chance of an unknown attacker flooding the service with too much data.

SOAP Validations and the **WS-I Basic Profile** tests (described in the next sections) determine whether a SOAP message is valid, identifying invalid messages as intrusions. Blocking the invalid messages is enabled through **XML Validation Settings**.

The XML validation parameters are set to default values which can be modified.

The XML requests which violates the XML validation rules are listed under the attack group xmlfwdos-violations on the **SECURITY > Action Policy** page. Action policy specifies the action to be taken when a violation occurs. You can edit the default attack action settings for a policy.

WS-I Basic Profile Assertions

The Web Services Interoperability Organization (WS-I) Basic Profile Version 1.0 contains implementation guidelines for the core web services specifications: XML 1.0, XML Schema 1.0, SOAP 1.1, and WSDL 1.1. These guidelines define how the specifications should be used to develop inter-operable web services. The WS-I test tools Basic Profile Test Assertions can be used to verify that a web service conforms to these requirements. The Barracuda Web Application Firewall performs these tests during run time to validate SOAP messages.

There are forty two test case parameters, all set to *Yes* by default, meaning the test is applied; a *No* setting would cause that test to be ignored. You can modify existing settings.

XML requests violating the WS-I Basic Profile Assertions are listed under the attack group **xmlfwwsi-assertion-failures** on the **SECURITY > Action Policy** page. Action policy specifies the action to be taken when a violation occurs. You can edit the default attack action settings to implement the desired attack response.

SOAP Validations

SOAP is the transfer mechanism protocol for sending web service descriptions in an HTTP message. The SOAP validation parameters set the SOAP validation checks to apply. (These checks verify the message adheres to SOAP standards.)

SOAP is a lightweight communication protocol for exchanging data using XML over HTTP. SOAP is a mechanism that provides communication between web applications. SOAP is both platform independent and language independent. SOAP was developed as a W3C standard protocol. SOAP is a call-response mechanism that operates in a client-server paradigm. The client application makes a call to the server, passing in parameters, and the server provides a response. Both call and response are transported in the form of XML documents.

SOAP messages are susceptible to a number of potential attacks. Unintentionally exposing SOAP services could make the back-end server or application vulnerable to attacks. These attacks include the same attacks as in HTTP, such as SQL injection, and buffer overflow attacks. SOAP makes the back-end server more vulnerable because it allows actions to be invoked remotely on the back-end server.

There are four SOAP validation parameters, which are all set to *No* by default. You can edit the existing values setting them to *Yes* to validate these SOAP standards.

The XML requests which violate the SOAP Validations are listed under the attack group **xmlfw-soapviolations** on the **SECURITY > Action Policy** page. Action policy specifies the action to be taken when a violation occurs. You can edit the default attack action settings to implement the desired attack response.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.