



NGAF

Best Practices for Scenarios_Security Policy Availability Check

Version 8.0.17



Change Log

Date	Change Description
Nov 2, 2020	Document release.
May 17, 2021	Document update.

CONTENT

Chapter 1 Backgroud.....	1
Chapter 2 WAF Policy Effectiveness Test	1
2.1 SQL Injection	1
2.2 XSS Injection.....	1
Chapter 3 IPS Effectiveness Test	2
3.1 Test web Server Parsing Vulnerability Rules 1. IIS Parsing Vulnerability.....	2
3.2 apache parsing vulnerability.....	2

Chapter 1 Background

Usually, after configuring the WAF and IPS policies, we cannot verify whether the policies are correctly configured, and we only discover that the policy configuration errors are only after being attacked. Therefore, the following test methods are provided to quickly and easily test whether the WAF and IPS policies are effective.

Chapter 2 WAF Policy Effectiveness Test

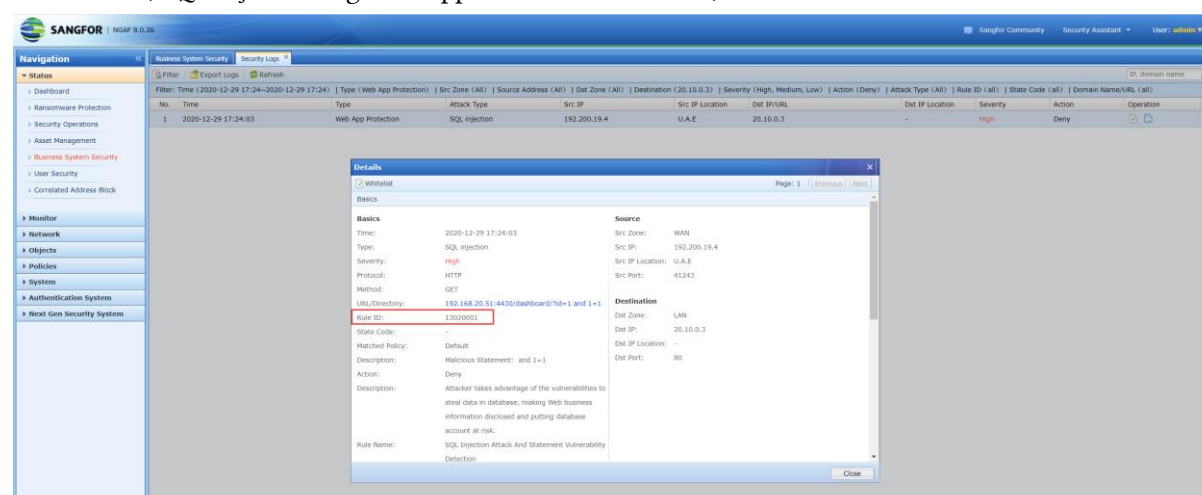
2.1 SQL Injection

For the web server deployed in the intranet, just find a page and add ?id=1 and 1=1 after the URL to see the SQL injection log. If there is no log, the WAF is not effective.

For example, find a url: <http://192.200.200.134/>

Add **?id=1 and 1=1** after the url to become <http://192.200.200.134/?id=1 and 1=1>, enter the browser to visit

At this time, SQL injection logs will appear in the data center, as shown below:

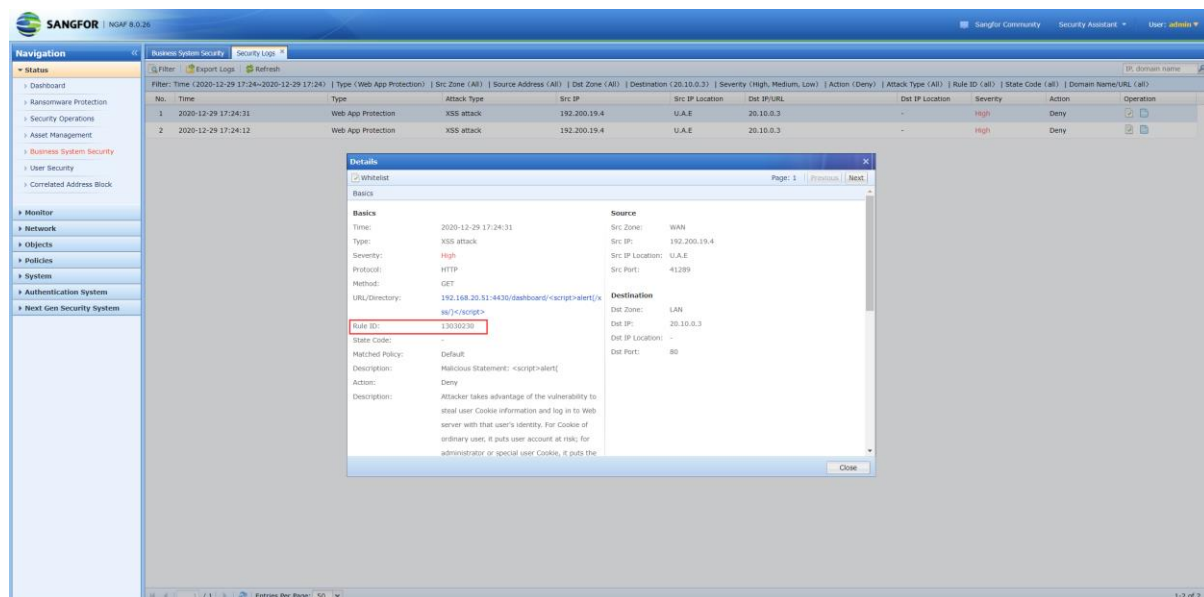


2.2 XSS Injection

For the web server in the intranet, find any URL and add <script>alert(/xss/)</script> after the URL to see the XSS log. If there is no log, the WAF is not effective

For example, find a url: <http://192.200.200.134/>

Add **<script>alert(/xss/)</script>** after the url to become [http://192.200.200.134/<script>alert\(/xss/\)</script>](http://192.200.200.134/<script>alert(/xss/)</script>), enter the browser to access
XSS logs will appear in the data center at this time, as shown below:

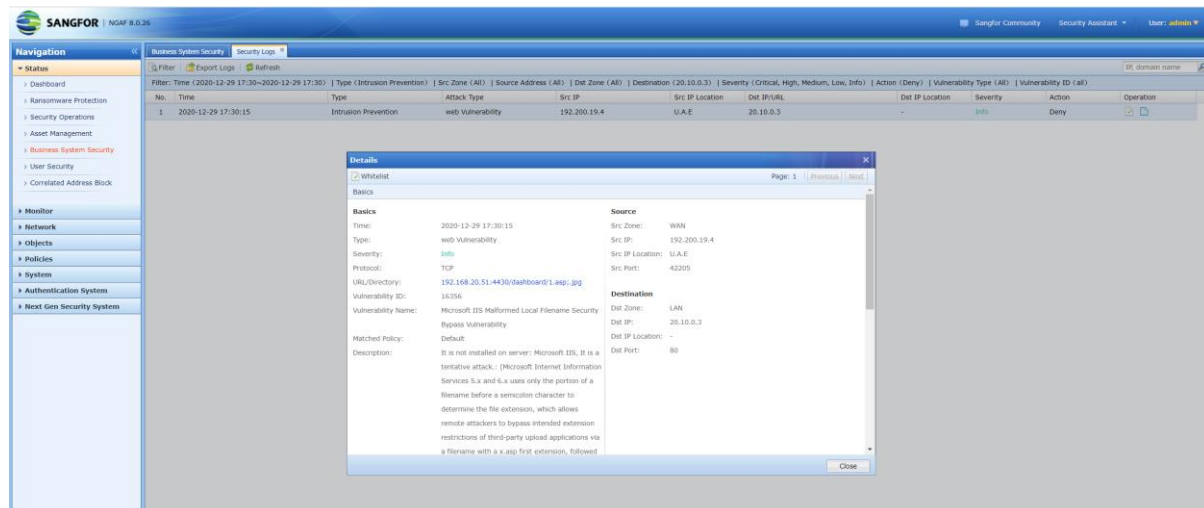


Chapter 3 IPS Effectiveness Test

3.1 Test web Server Parsing Vulnerability Rules 1. IIS Parsing Vulnerability

<http://server/1.asp;.jpg>

When accessing the above URL, a log with IPS rule id 16356 will appear, as shown in the figure below:



3.2 apache parsing vulnerability

<http://server/1.php.xx.oo>

When accessing the above URL, a log with IPS rule id 11020270 will appear, as shown in the figure below:

Best Practice_Security Policy Availability Check

The screenshot displays the Sangfor NGAF 8.0.26 Security Log interface. The main window shows a list of security events. A 'Details' dialog box is open, providing a comprehensive view of a specific event.

Security Log Table:

No.	Time	Type	Attack Type	Src IP	Src IP Location	Dest IP/URL	Dest IP Location	Severity	Action	Operation
1	2020-12-29 17:30:37	Intrusion Prevention	web Vulnerability	192.200.19.4	U.A.E	20.10.0.3	-	Medium	Allow	
2	2020-12-29 17:30:32	Intrusion Prevention	web Vulnerability	192.200.19.4	U.A.E	20.10.0.3	-	Medium	Allow	

Details Dialog Box:

Basics

- Time: 2020-12-29 17:30:37
- Type: web Vulnerability
- Severity: Medium
- Protocol: TCP
- URL/Directory: 192.168.20.51:4430/dashboard/1.php.xxoo
- Vulnerability ID: **17203279**
- Vulnerability Name: Apache Misformed Local Filename Security
- Matched Policy: Bypass Vulnerability
- Description: Apache from right to left, start judgment suffix, if x3 not identify suffix, then judge x2, until find can identify suffix so far, then this can identify suffixes into analytic. Test.php.x1.x2.x3 will be analysis for test.php.
- Solution: Apache Update: <http://www.apache.org/>
- Reference: -
- Action: Allow

Source

- Src Zone: WAN
- Src IP: 192.200.19.4
- Src IP Location: U.A.E
- Src Port: 42206

Destination

- Dest Zone: LAN
- Dest IP: 20.10.0.3
- Dest IP Location: -
- Dest Port: 80



SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc