SANGFOR

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 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

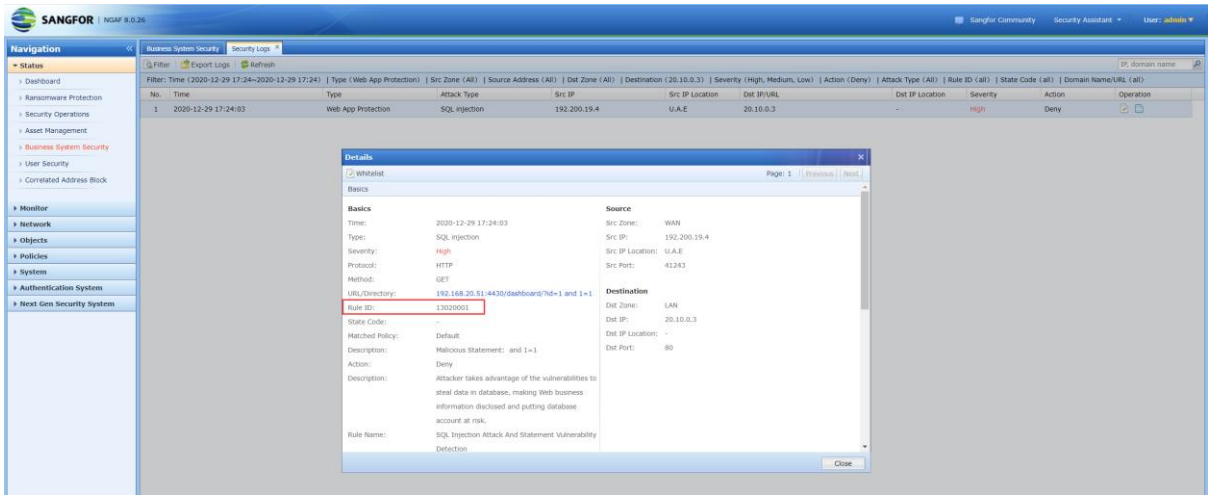
2.1 SQL Injection

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:



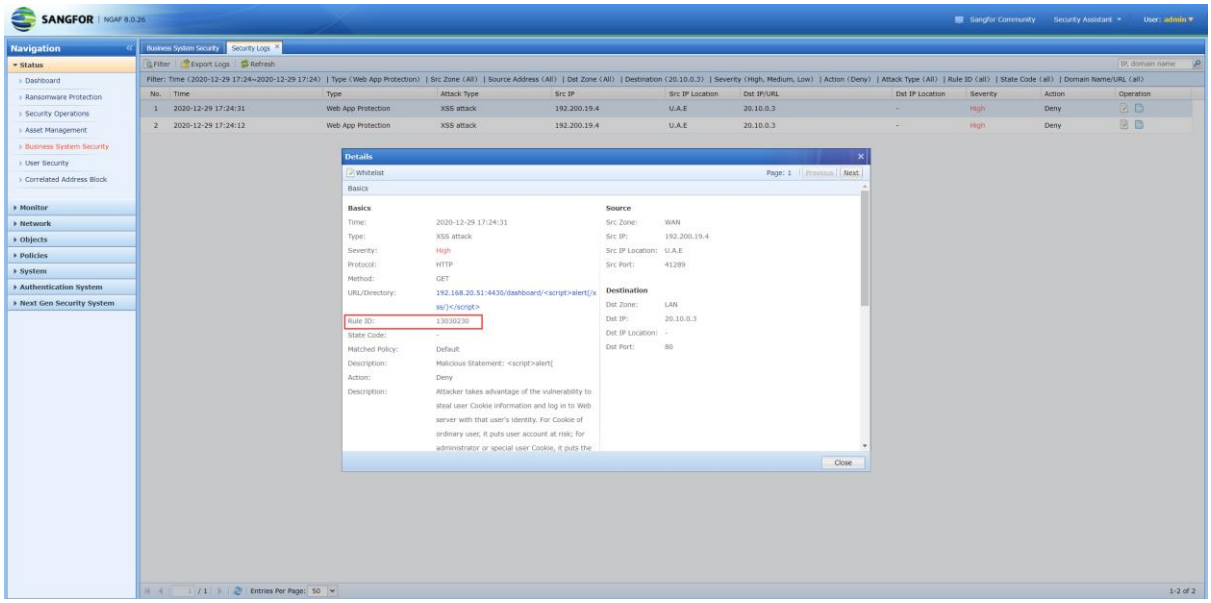
2.2 XSS Injection

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>, enter the browser to access

XSS logs will appear in the data center at this time, as shown below:

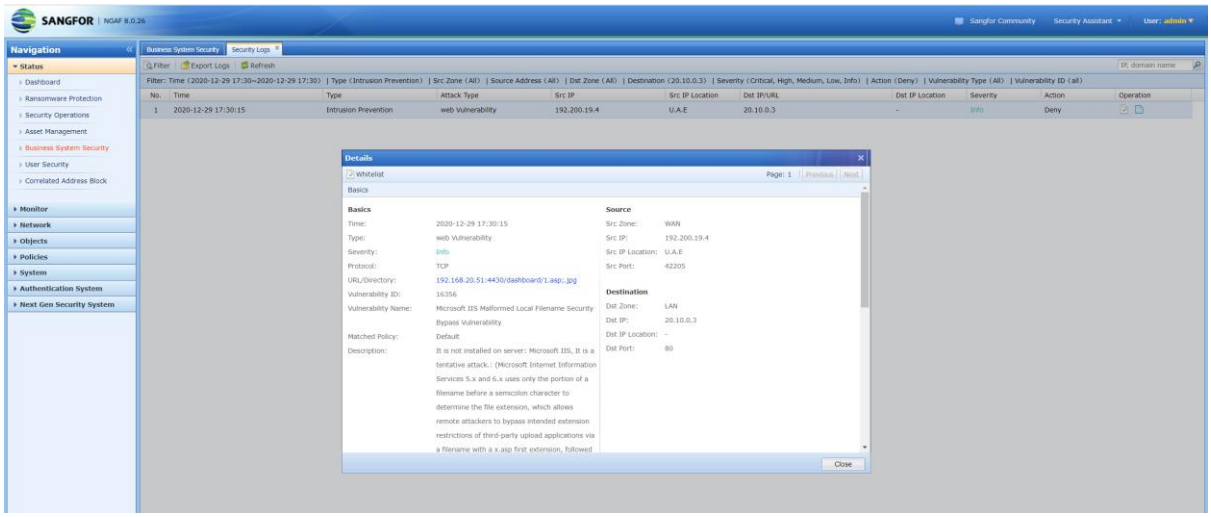


Chapter 3 IPS Effectiveness Test

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

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

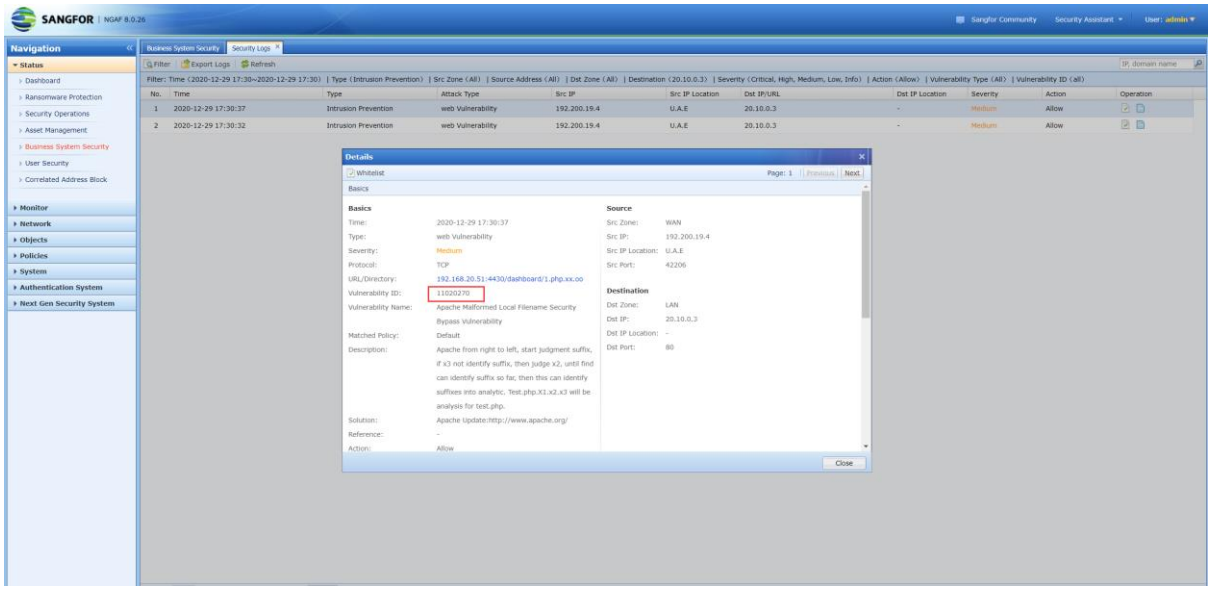
When accessing the above URL, a log with IPS rule id 16356 will appear, as shown in the figure below:



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:


SANGFOR
Navigation
Status
Dashboard
Ransomware Protection
Security Operations
Asset Management
Business System Security
User Security
Correlated Address Block
Monitor
Network
Objects
Policies
System
Authentication System
Next Gen Security System
Business System Security
Security Logs
Filter
Export Logs
Refresh
No.
Time
Type
Attack Type
Src IP
Src IP Location
Dst IP/URL
Dst 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
Whitelist
Page: 1
Previous
Next
Basics
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.xx.oo
Vulnerability ID:
11020270
Vulnerability Name:
Apache Malformed Local Filename Security Bypass Vulnerability
Matched Policy:
Default
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
Dst Zone:
LAN
Dst IP:
20.10.0.3
Dst IP Location:
Dst Port:
80
Close