SANGFOR

NGAF

Pedoman yang Direkomendasikan untuk Skenario Security Policy Availability Check

Versi 8.0.17

Data Perubahan

Tanggal	Keterangan Perubahan
Nov 2, 2020	Rilis dokumen.
May 17, 2021	Pembaruan dokumen.

DAFTAR ISI

BAB 1 Latar Belakang

Umumnya, setelah konfigurasi policy WAF dan IPS, kita tidak dapat memastikan apakah konfigurasi dari policy benar atau tidak, dan kita hanya menemukan konfigurasi terdapat kesalahan hanya setelah terjadinya penyerangan. Maka dari itu, diberikan metoda pengujian cepat dan mudah apakah policy dari WAF dan IPS telah efektif.

BAB 2 Pengujian Efektifitas Policy WAF

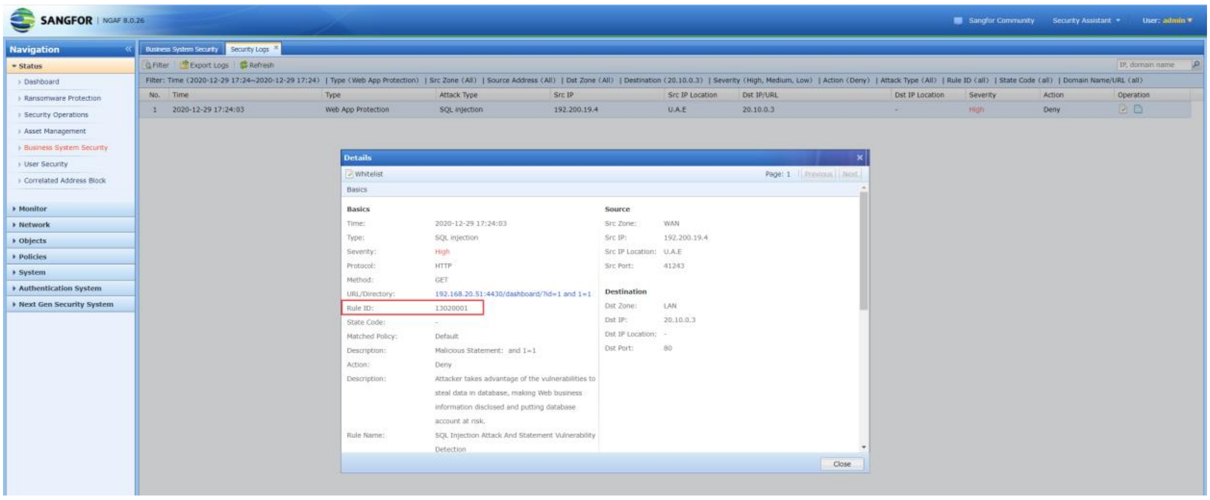
2.1 SQL Injection

Untuk web server yang digunakan dalam intranet, cukup cari halamannya dan tambahkan ?id=1 and 1=1 setelah itu lihat pencatatan SQL injection. Jika tidak terdapat pencatatan maka WAF yang dikonfigurasi tidak efektif.

Contohnya: cari url: http://192.200.200134/

Tambahkan **?id=1 and 1=1** sehingga url menjadi http://192.200.200.134/?id=1 and 1=1, masukan kedalam perambah/browser untuk mengunjunginya.

Saat ini, pencatatan SQL injection langsung akan muncul dengan tampilan sebagai berikut di bawah ini:



Filter: Time (2020-12-29 17:24~2020-12-29 17:24) | Type (Web App Protection) | Src Zone (All) | Source Address (All) | Dst Zone (All) | Destination (20.10.0.3) | Severity (High, Medium, Low) | Action (Deny) | Attack Type (All) | Rule ID (all) | State Code (all) | Domain Name/URL (all)

No.	Time	Type	Attack Type	Src IP	Src IP Location	Dst IP/URL	Dst IP Location	Severity	Action	Operation
1	2020-12-29 17:24:03	Web App Protection	SQL injection	192.200.19.4	U.A.E	20.10.0.3	-	High	Deny	

Details

Basics

Basics

Time: 2020-12-29 17:24:03
Type: SQL injection
Severity: High
Protocol: HTTP
Method: GET
URL/Directory: 192.168.20.51:4430/dashboard/?id=1 and 1=1
Rule ID: 13020001
State Code: -
Matched Policy: Default
Description: Malicious Statement: and 1=1
Action: Deny
Description: Attacker takes advantage of the vulnerabilities to steal data in database, making Web business information disclosed and putting database account at risk.
Rule Name: SQL Injection Attack And Statement Vulnerability Detection

Source

Src Zone: WAN
Src IP: 192.200.19.4
Src IP Location: U.A.E
Src Port: 41243

Destination

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

2.2 XSS Injection

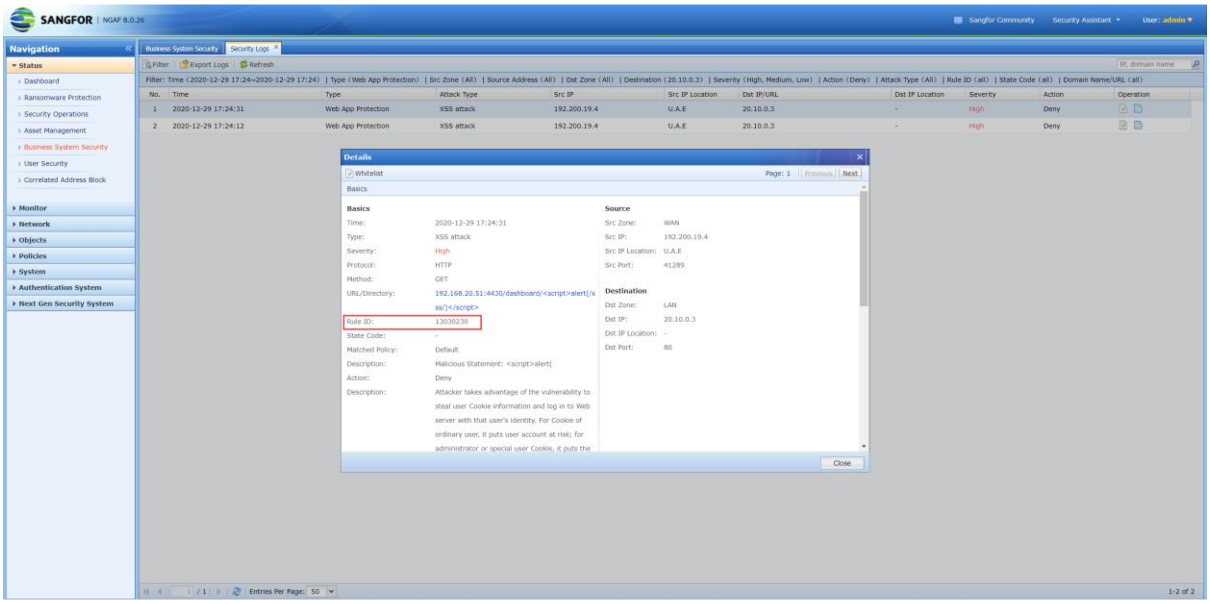
Untuk seb server yang digunakan dalam intranet, cari URL apapun dan tambahkan <script>alert(/xss/)</script> setetlah itu lihat pencatatan untuk XSS. Jika tidak terdapat pencatatan maka WAF yang dikonfigurasi tidak efektif.

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

Contohnya: cari url: http://192.200.200.134/

Tambahkan **<script>alert(/xss/)</script>** sehingga url menjadi http://192.200.200.134/<script>alert(/xss/)</script>, masukan kedalam perambah.browser untuk mengunjunginya.

Pencatatan XSS logs akan muncul dengan tampilah sebagai berikut di bawah ini:



Filter: Time (2020-12-29 17:24~2020-12-29 17:24) | Type (Web App Protection) | Src Zone (All) | Source Address (All) | Dst Zone (All) | Destination (20.10.0.3) | Severity (High, Medium, Low) | Action (Deny) | Attack Type (All) | Rule ID (all) | State Code (all) | Domain Name/URL (all)

No.	Time	Type	Attack Type	Src IP	Src IP Location	Dst IP/URL	Dst IP Location	Severity	Action	Operation
1	2020-12-29 17:24:31	Web App Protection	XSS attack	192.200.19.4	U.A.E	20.10.0.3	-	High	Deny	
2	2020-12-29 17:24:12	Web App Protection	XSS attack	192.200.19.4	U.A.E	20.10.0.3	-	High	Deny	

Details

Whitelist — Page: 1 — Previous — Next

Basics

Basics		Source	
Time:	2020-12-29 17:24:31	Src Zone:	WAN
Type:	XSS attack	Src IP:	192.200.19.4
Severity:	High	Src IP Location:	U.A.E
Protocol:	HTTP	Src Port:	41289
Method:	GET		
URL/Directory:	192.168.20.51:4430/dashboard/<script>alert(/xss/)</script>	**Destination**	
Rule ID:	13030230	Dst Zone:	LAN
State Code:	-	Dst IP:	20.10.0.3
Matched Policy:	Default	Dst IP Location:	-
Description:	Malicious Statement: <script>alert(	Dst Port:	80
Action:	Deny		
Description:	Attacker takes advantage of the vulnerability to steal user Cookie information and log in to Web server with that user's identity. For Cookie of ordinary user, it puts user account at risk; for administrator or special user Cookie, it puts the		

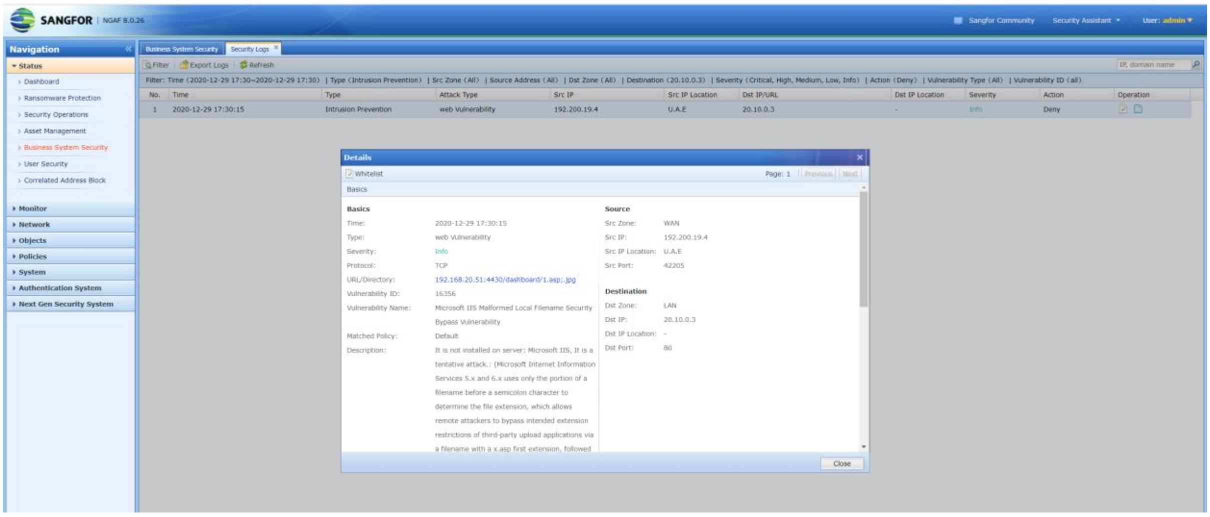
Close

BAB 3 Pengujian Efektifitas IPS

3.1 Pengujian Kerentanan Aturan Web Server 1. Kerentanan pada IIS

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

Ketika mengakses URL diata, pencatatan dengan id aturan 16356 akan muncul, gambar seperti dibawah ini:



Filter: Time（2020-12-29 17:30~2020-12-29 17:30）| Type（Intrusion Prevention）| Src Zone（All）| Source Address（All）| Dst Zone（All）| Destination（20.10.0.3）| Severity（Critical, High, Medium, Low, Info）| Action（Deny）| Vulnerability Type（All）| Vulnerability ID（all）

No.	Time	Type	Attack Type	Src IP	Src IP Location	Dst IP/URL	Dst IP Location	Severity	Action	Operation
1	2020-12-29 17:30:15	Intrusion Prevention	web Vulnerability	192.200.19.4	U.A.E	20.10.0.3	-	Info	Deny	

Details

Basics

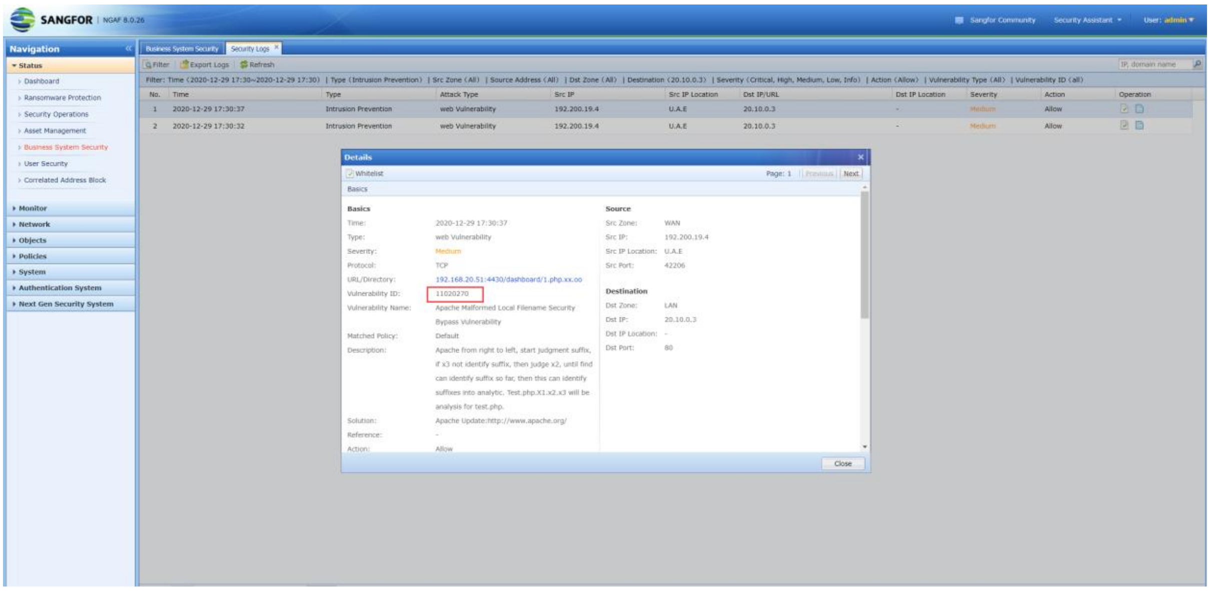
Basics	
Time:	2020-12-29 17:30:15
Type:	web Vulnerability
Severity:	Info
Protocol:	TCP
URL/Directory:	192.168.20.51:4430/dashboard/1.asp;.jpg
Vulnerability ID:	16356
Vulnerability Name:	Microsoft IIS Malformed Local Filename Security Bypass Vulnerability
Matched Policy:	Default
Description:	It is not installed on server: Microsoft IIS, It is a tentative attack.: (Microsoft Internet Information Services 5.x and 6.x uses only the portion of a filename before a semicolon character to determine the file extension, which allows remote attackers to bypass intended extension restrictions of third-party upload applications via a filename with a x.asp first extension, followed

Source	
Src Zone:	WAN
Src IP:	192.200.19.4
Src IP Location:	U.A.E
Src Port:	42205
Destination	
Dst Zone:	LAN
Dst IP:	20.10.0.3
Dst IP Location:	-
Dst Port:	80

3.2 Kerentanan pada Apache

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

Ketika mengakes URL diatas, pencatatan dengan id aturan 11020270 akan muncul, gambar seperti dibawah ini:



Filter: Time（2020-12-29 17:30~2020-12-29 17:30）| Type（Intrusion Prevention）| Src Zone（All）| Source Address（All）| Dst Zone（All）| Destination（20.10.0.3）| Severity（Critical, High, Medium, Low, Info）| Action（Allow）| Vulnerability Type（All）| Vulnerability ID（all）

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

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

SANGFOR

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