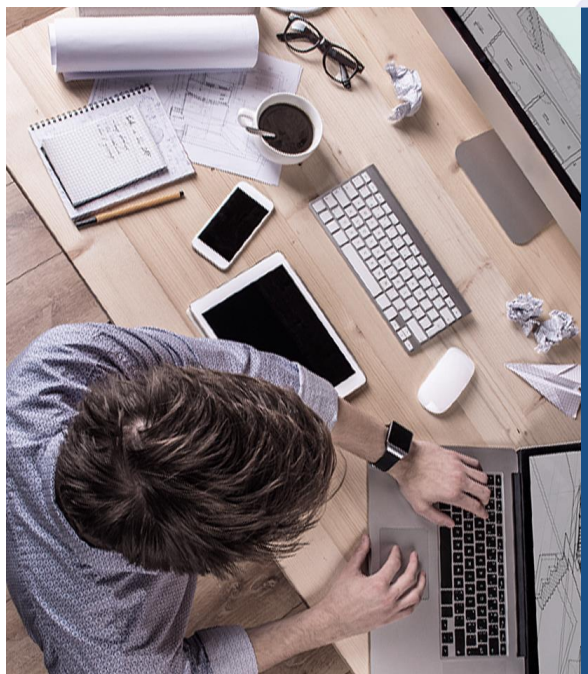




# SANGFOR\_NGAF\_V8.0.6\_Professional

Security Assistant





1 Analisis Kerentanan RT

2 Peringatan Ancaman

3 Analisis Resiko

4 Web Scanner

# 1. Analisis Kerentanan RT

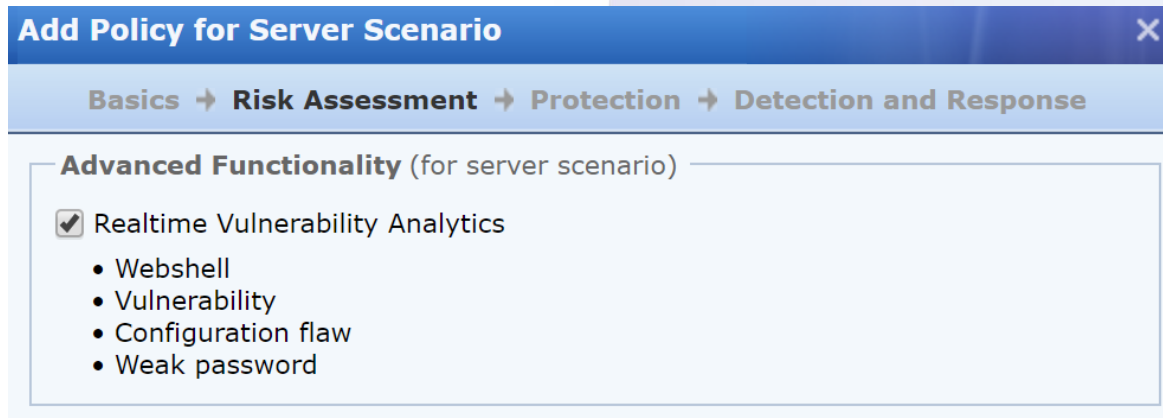
---



# Analisis Kerentanan RT

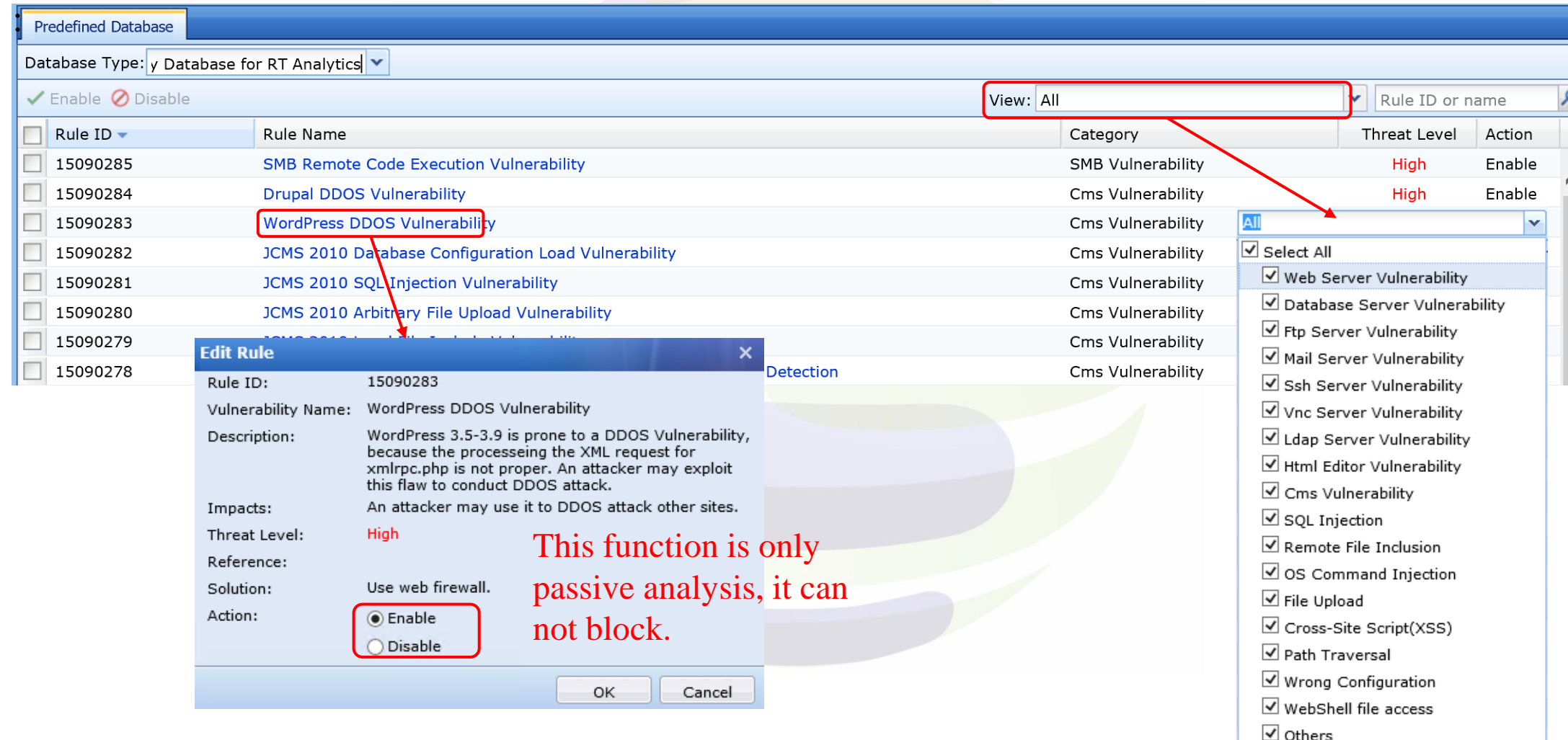
RT Vulnerability Analytics adalah pemindai kerentanan pasif. Data yang melalui perangkat atau bypass akan dicerminkan untuk menganalisis deteksi real-time masalah security di jaringan pelanggan. Proses ini tidak akan mengganggu proses penerusan data di perangkat, tidak akan mengirim paket reset, dan tidak akan mempengaruhi kinerja. Laporan informasi kerentanan akan diproduksi setelah pemindaian selesai.

Ini mendeteksi hal-hal berikut:



# Analisis Kerentanan RT

Screenshot di bawah ini menunjukkan database Analisis Kerentanan RT



Predefined Database

Database Type: y Database for RT Analytics

Enable Disable

View: All

Rule ID	Rule Name	Category	Threat Level	Action
15090285	SMB Remote Code Execution Vulnerability	SMB Vulnerability	High	Enable
15090284	Drupal DDOS Vulnerability	Cms Vulnerability	High	Enable
15090283	WordPress DDOS Vulnerability	Cms Vulnerability		
15090282	JCMS 2010 Database Configuration Load Vulnerability	Cms Vulnerability		
15090281	JCMS 2010 SQL Injection Vulnerability	Cms Vulnerability		
15090280	JCMS 2010 Arbitrary File Upload Vulnerability	Cms Vulnerability		
15090279		Cms Vulnerability		
15090278		Cms Vulnerability		

**Edit Rule**

Rule ID: 15090283

Vulnerability Name: WordPress DDOS Vulnerability

Description: WordPress 3.5-3.9 is prone to a DDOS Vulnerability, because the processeing the XML request for xmlrpc.php is not proper. An attacker may exploit this flaw to conduct DDOS attack.

Impacts: An attacker may use it to DDOS attack other sites.

Threat Level: High

Reference:

Solution: Use web firewall.

Action: ☒ Enable ☐ Disable

OK Cancel

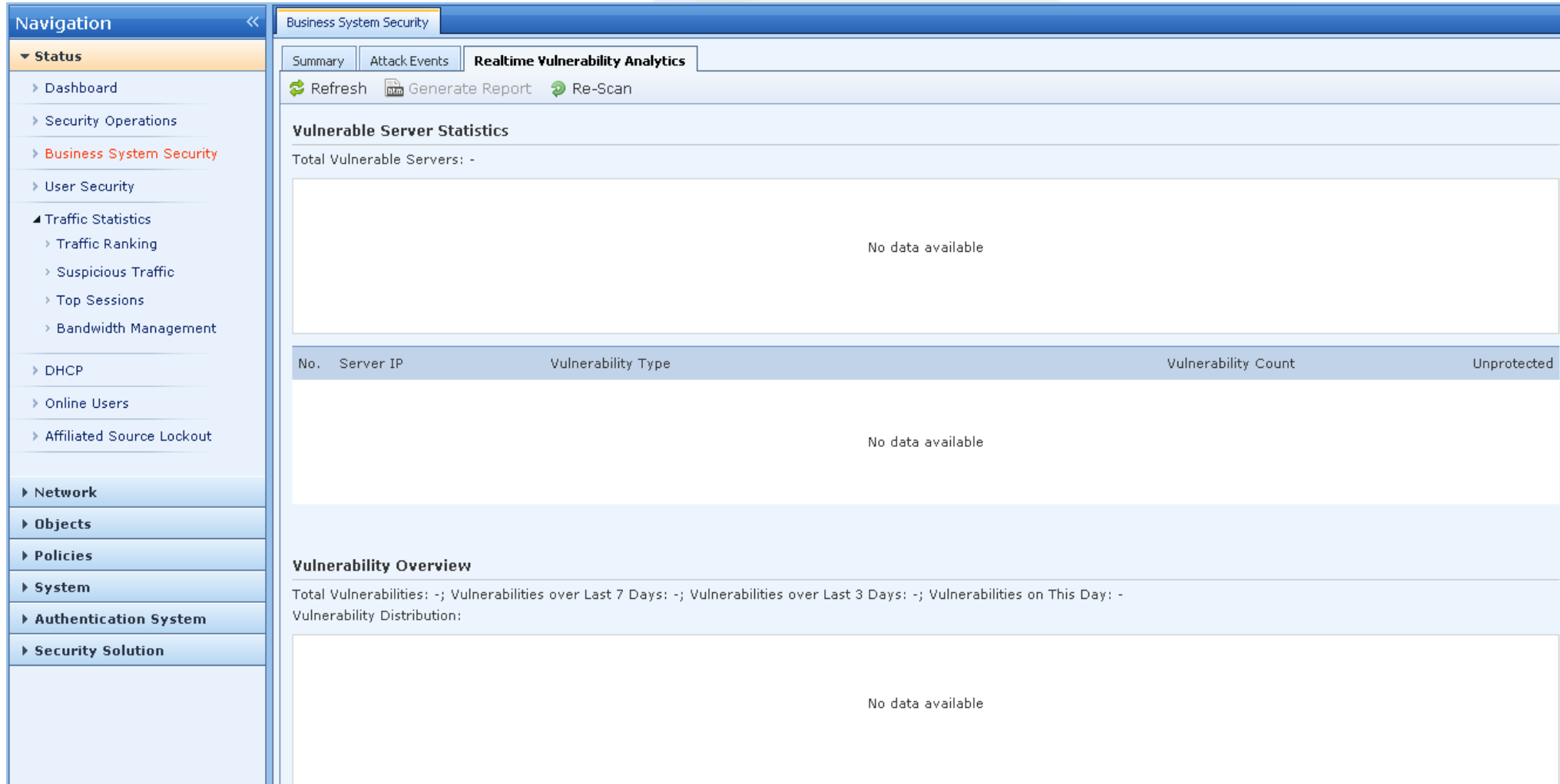
**This function is only passive analysis, it can not block.**

**All**

- ☒ Select All
- ☒ Web Server Vulnerability
- ☒ Database Server Vulnerability
- ☒ Ftp Server Vulnerability
- ☒ Mail Server Vulnerability
- ☒ Ssh Server Vulnerability
- ☒ Vnc Server Vulnerability
- ☒ Ldap Server Vulnerability
- ☒ Html Editor Vulnerability
- ☒ Cms Vulnerability
- ☒ SQL Injection
- ☒ Remote File Inclusion
- ☒ OS Command Injection
- ☒ File Upload
- ☒ Cross-Site Script(XSS)
- ☒ Path Traversal
- ☒ Wrong Configuration
- ☒ WebShell file access
- ☒ Others

# Analisis Kerentanan RT

Screenshot memperlihatkan contoh Laporan Analisis Kerentanan RT:



The screenshot displays the 'Business System Security' dashboard with the 'Realtime Vulnerability Analytics' tab selected. The left sidebar shows a navigation menu with categories like Status, Network, Objects, Policies, System, Authentication System, and Security Solution. The main content area includes a 'Vulnerable Server Statistics' section with a table that is currently empty, displaying 'No data available'. Below this is a 'Vulnerability Overview' section, also displaying 'No data available'.

**Navigation**

- ▼ Status
  - Dashboard
  - Security Operations
  - Business System Security
  - User Security
  - ▲ Traffic Statistics
    - Traffic Ranking
    - Suspicious Traffic
    - Top Sessions
    - Bandwidth Management
  - DHCP
  - Online Users
  - Affiliated Source Lockout
- ▶ Network
- ▶ Objects
- ▶ Policies
- ▶ System
- ▶ Authentication System
- ▶ Security Solution

**Business System Security**

Summary | Attack Events | **Realtime Vulnerability Analytics**

Refresh | Generate Report | Re-Scan

**Vulnerable Server Statistics**

Total Vulnerable Servers: -

No data available

No.	Server IP	Vulnerability Type	Vulnerability Count	Unprotected
No data available				

**Vulnerability Overview**

Total Vulnerabilities: -; Vulnerabilities over Last 7 Days: -; Vulnerabilities over Last 3 Days: -; Vulnerabilities on This Day: -

Vulnerability Distribution:

No data available



# Analisis Kerentanan RT

## Laporan Analisis Kerentanan RT

RT Vulnerability Analytics akan membandingkan konfigurasi IPS / WAF saat ini dan menunjukkan bahwa kerentanan telah dilindungi, atau potensi risiko yang terdeteksi AF sebagai tidak terlindungi.

No.	Vulnerability Type	Threat Level	Server Domain/IP	Total Vulnerabilities	Protection State
1	Wrong Configuration	Medium	192.200.19.200(69) 192.200.19.201(4) 192.200.19.231(1)	74	unprotected
2	Weak Password	High	192.200.19.200(32) 192.200.19.221(1) 192.200.19.199(1) 192.200.19.201(1) 192.200.19.220(1)	36	unprotected
3	Apache Httpd Vulnerability	High	192.200.19.200(16) 192.200.19.199(12)	28	unprotected
4	SQL Injection	High	192.200.19.200(15)	15	unprotected
5	Sendmail Vulnerability	High	192.200.19.200(12)	12	unprotected

# Analisis Kerentanan RT

## RT Vulnerability Analytics Report

Laporan akan memberikan rincian untuk setiap kerentanan yang terdeteksi, termasuk solusi dan proses deteksi. Laporan tidak termasuk kerentanan angka yang ditemukan. Hanya waktu terakhir ditemukan akan diperbarui.

**Potential Risk** Vulnerability (6/12): Apache HTTP Server Vulnerability In The Mod\_Session\_Dbd Module

Application Details	Apache Httpd 2.2.15
Protocol	TCP
Port	80
Service Type	HTTP
Vulnerability Analysis Rule ID	15010045
Threat Level	High
Protection State	Potential Risk
CVE	CVE-2013-2249
Time Last Found	2015-12-09 18:35:38

**Details**  
mod\_session\_dbd.c in the mod\_session\_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.

**Solution**  
Method 1: Upgrade to Apache HTTP Server 2.4.5 or later.

**Detection Process**

RESPONSE:  
HTTP/1.1 302 Found  
Date: Wed, 09 Dec 2015 10:35:40 GMT  
Server: Apache/2.2.15 (CentOS)



# Analisis Kerentanan RT

## Catatan:

1. RT Vulnerability Scanner bergantung pada hasil identifikasi aplikasi. Oleh karena itu, disarankan untuk memiliki lisensi database identifikasi aplikasi yang valid.
2. RT Vulnerability Scanner hanya mendukung protokol TCP dan tidak mendukung analisis protokol UDP, seperti DNS dan layanan lainnya.

Identifikasi dukungan FTP dan HTTP untuk port apa pun namun layanan lain hanya mendukung port standar, seperti SSH, MySQL, dan layanan lainnya.

4. Setiap policy independen satu sama lain. Jika grup IP server tumpang tindih, kerentanan identik akan ditemukan berulang dalam daftar.

## 2. Peringatan Ancaman

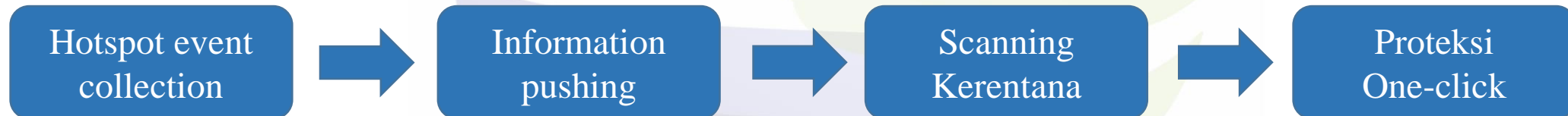
---



# Threat Alerts

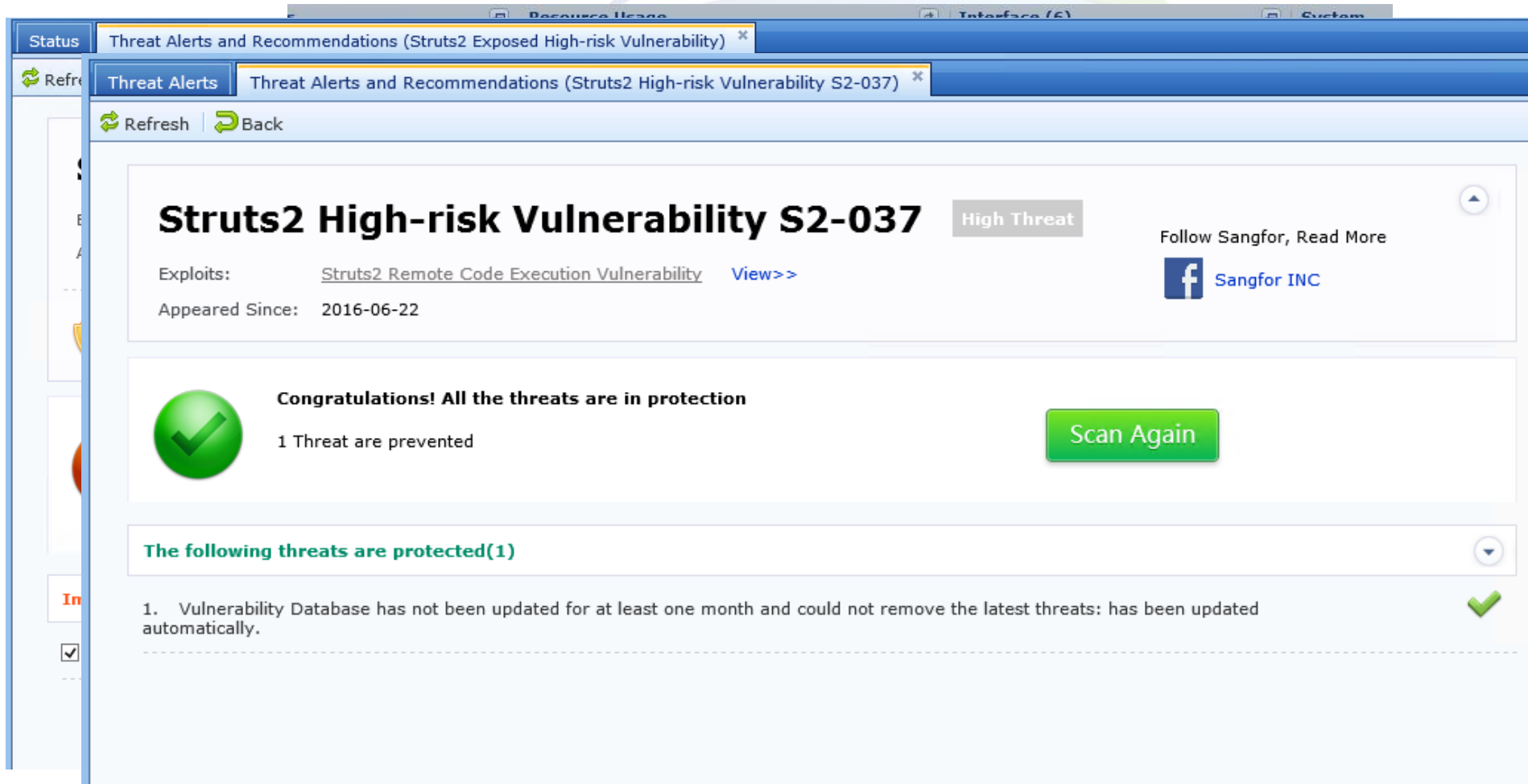
Peringatan Ancaman akan memberi tahu tentang peristiwa security yang mengkhawatirkan dalam setiap insiden security yang terjadi di industri dalam waktu 48 jam setelah wabah untuk memberikan deteksi kerentanan 0 Hari lengkap dan memberikan program proteksi yang memungkinkan pengguna untuk fokus pada bisnis mereka, tanpa mengenai ancaman dan kerentanan setiap saat. Pengguna juga dapat belajar tentang situasi security baru-baru ini melalui Threat Intelligence Center.

Peringatan Ancaman mencakup langkah-langkah berikut:



# Threat Alerts

Ketika Sangfor mendeteksi peristiwa yang mengkhawatirkan, itu akan muncul informasi security dalam login pertama hari itu.



The screenshot shows the Sangfor Threat Alerts interface. At the top, there's a navigation bar with tabs for 'Status', 'Threat Alerts and Recommendations (Struts2 Exposed High-risk Vulnerability)', and 'Interface (6)'. Below this, a sub-header reads 'Threat Alerts and Recommendations (Struts2 High-risk Vulnerability S2-037)'. A 'Refresh' button and a 'Back' button are visible. The main content area features a large heading 'Struts2 High-risk Vulnerability S2-037' with a 'High Threat' badge. Below the heading, it lists 'Exploits: Struts2 Remote Code Execution Vulnerability' with a 'View >>' link, and 'Appeared Since: 2016-06-22'. To the right, there's a social media link 'Follow Sangfor, Read More' with a Facebook icon and 'Sangfor INC'. A green checkmark icon is followed by the text 'Congratulations! All the threats are in protection' and '1 Threat are prevented'. A green 'Scan Again' button is also present. Below this, a section titled 'The following threats are protected(1)' shows a single entry: '1. Vulnerability Database has not been updated for at least one month and could not remove the latest threats: has been updated automatically.' with a green checkmark icon.

# Threat Alerts

## Pengaturan

Support Community Security Assistant Internal Report Center User: admin

Risk Analytics

Security Dashboard Threat Alerts

Refresh: 10 seconds Refresh Settings Latest Threats

No.	Appeared Since	Description	Threat Level	Protection	Operation
1	2017-09-05	Remote Code Execution Vulnerability in Struts 2(S2-052)	High Threat	Unprotected	Protect
2	2017-07-07	Remote Code Execution Vulnerability in Struts 2(S2-048)	High Threat	In protection	Details
3	2017-06-27	Petya Ransomware Attack	High Threat	In protection	Details
4	2017-05-12	WannaCry Ransomware Attack	High Threat	In protection	Details
5	2017-04-10	PHPCMS Arbitrary File Upload Vulnerability	High Threat	In protection	Details
6	2017-03-07	Remote Code Execution Vulnerability in Struts 2(S2-052)	High Threat	In protection	Details
7	2017-02-03	Content Injection Vulnerability in Struts 2(S2-052)	High Threat	In protection	Details
8	2016-11-15	Nginx Privilege Escalation Vulnerability	High Threat	In protection	Details
9	2016-10-20	Joomla Component Vulnerability	High Threat	In protection	Details
10	2016-08-15	Java Unserialize Vulnerability	High Threat	Unprotected	Protect
11	2016-08-12	Zabbix High Risk SQL Injection Vulnerability	High Threat	In protection	Details
12	2016-07-12	Struts2 devMode High-risk Vulnerability	High Threat	In protection	Details

### Settings

Network Object:

Protection Options:

- ☒ Trigger automatic scan when new event occurs
- ☐ Enable high protection

OK Cancel

1. IPv4 address only, no more than 20 network objects are allowed

2. Number of IP addresses is no more than 1024

3. If no network object is specified, it scans associated internal servers only.

Once it is enabled, the scans and protections performed in Status > Security Operations will be based on all the associated rules and policies.

# Threat Alerts

Satu klik me-generate policy secara otomatis .

Dashboard

Threat Alerts

Threat Alerts and Recommendations (Bash shellshock vulnerability)

Refresh

Back

Bash shellshock vulnerability

High Threat

Follow Sangfor to Learn More

Dashboard

Threat Alerts

Threat Alerts and Recommendations (Bash shellshock vulnerability)

Policies

+ Add

✕ Delete

✓ Enable

✗ Disable

↑ Move Up

↓ Move Down

↔ Move


↻ Refresh

⚙ Advanced

⌕ Filter

Search

<input type="checkbox"/>	Priority	Name	Type	Source	Destination	Risk Assessment	Protection	Detection and Response	Status
<input type="checkbox"/>	1	OneClickProtection_...	Server	Zone: WAN,LAN Network Objects: All	Zone: WAN,LAN Network Objects: OneCli	-	<a href="#">Exploit Protection</a>	-	✓



1 threats need

1 IP addresses hav

Network Objects

OneClickProtection\_Bash\_shellshock\_vulnerability

Policies

OneClickProtection\_Bash\_shellshock\_vulnerability

Protect Now

Re-Scan

Immediate protection is requi

OK

Cancel

- ☒
Server 172.17.1.10 2 vulnerabilities are not well protected: GNU Bash remote code execution vulnerability, GNU Bash remote code execution vulnerability due to incomplete repairment

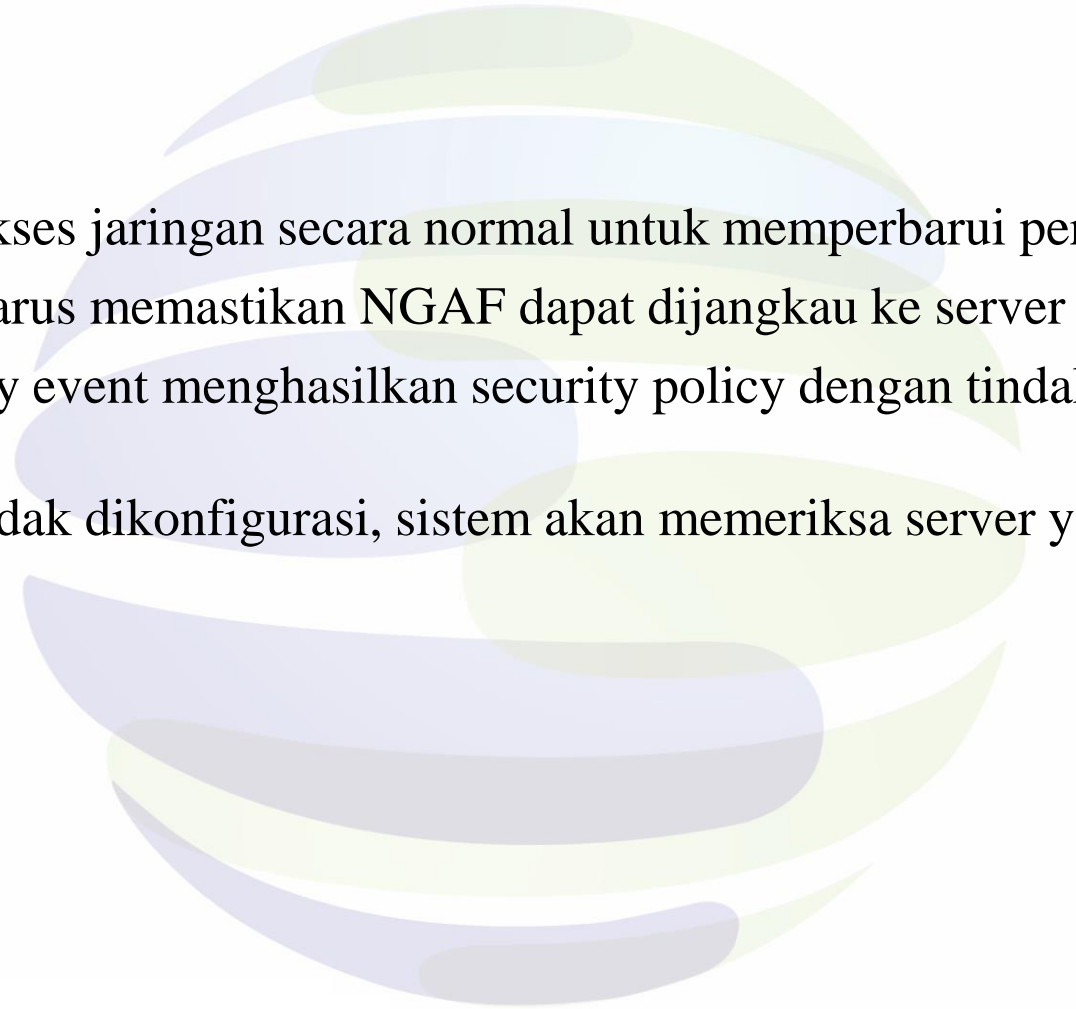
Details



# Threat Alerts

## Catatan:

- Perangkat perlu mengakses jaringan secara normal untuk memperbarui peristiwa security.
- Pemindaian ancaman harus memastikan NGAF dapat dijangkau ke server intranet.
- Proteksi hotspot security event menghasilkan security policy dengan tindakan sebagai penolakan.
- Jika [Objek Jaringan] tidak dikonfigurasi, sistem akan memeriksa server yang ditemukan secara otomatis.

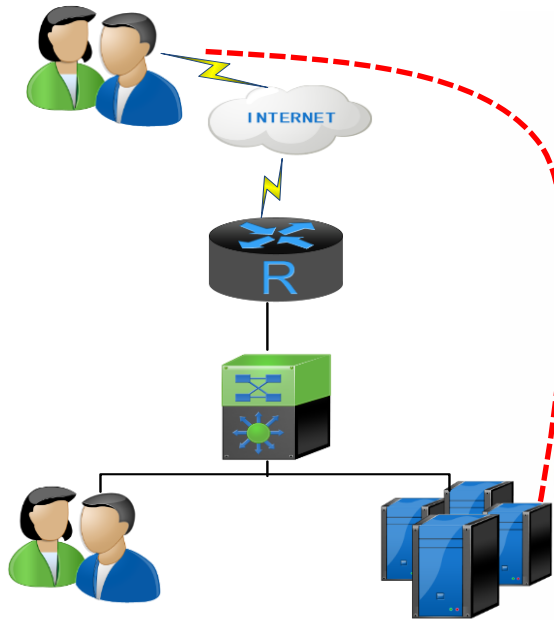


# 3. Risk Analytics

---



# Risk Analytics



Server mungkin memiliki masalah berikut:

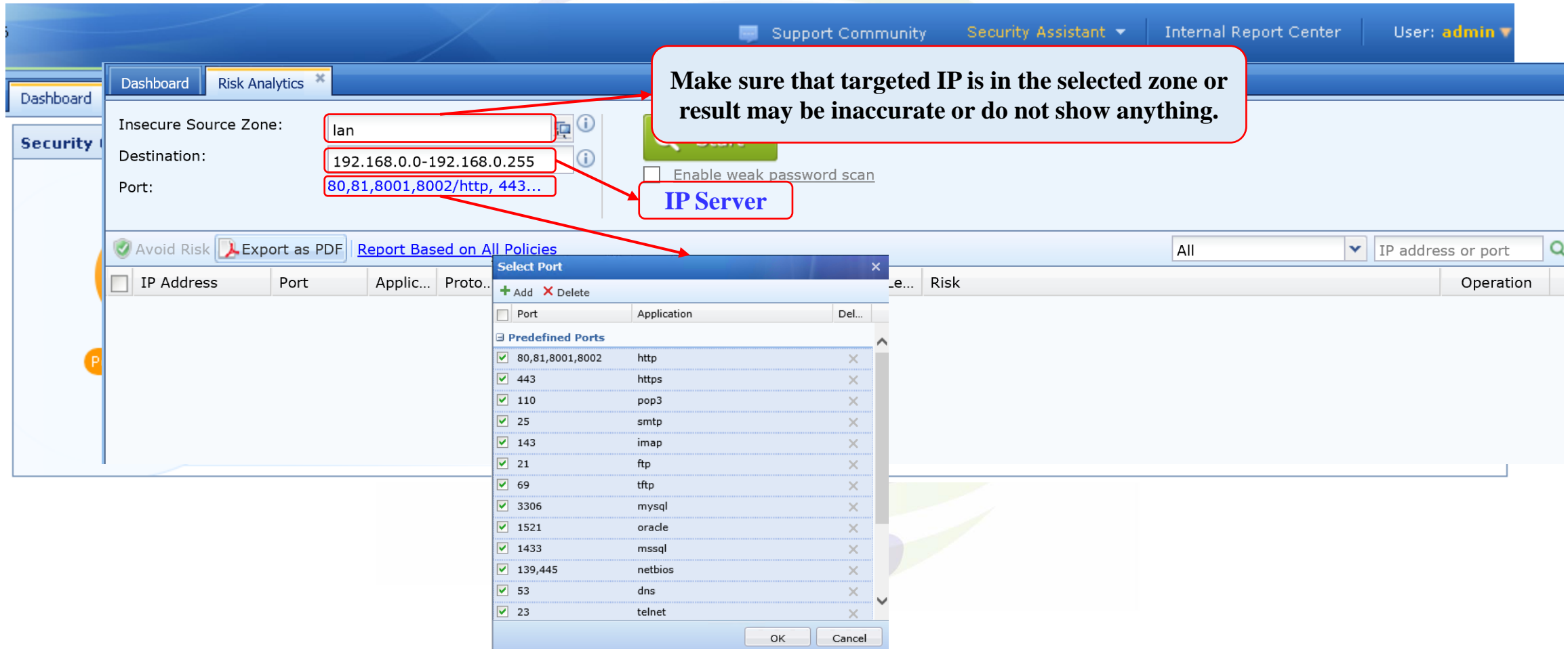
- (1) Port terbuka yang tidak perlu
- (2) Kerentanan dari server itu sendiri (untuk sistem operasi server)
- (3) Kerentanan dalam software server
- (4) Password lemah yang digunakan dalam login situs web

Analisis risiko mencakup dua aspek:

1. Port scan pada IP yang ditargetkan memungkinkan administrator server untuk memiliki pemahaman yang jelas tentang port terbuka server, layanan, dan kerentanan yang mungkin ada di server, yang memungkinkan administrator untuk menutup port terbuka yang tidak perlu, memblokir kerentanan parah dan meningkatkan security server.
2. Pemindaian password yang lemah pada situs yang ditargetkan digunakan untuk mengatasi ketidakamanan password yang lemah yang diterapkan sebelum akses ke database penting dan rahasia. Pada saat yang sama, analisis risiko dapat dilakukan secara cerdas untuk menghasilkan aturan yang sesuai berdasarkan hasil pemindaian bagi pelanggan untuk menjaga security perangkat.

# Risk Analytics

Menetapkan kondisi penilaian risiko.



The screenshot shows the Sangfor Risk Analytics web interface. The top navigation bar includes links for Support Community, Security Assistant, Internal Report Center, and a user profile for 'admin'. The main content area has a 'Risk Analytics' tab selected. Below the tab, there are input fields for 'Insecure Source Zone' (set to 'lan'), 'Destination' (set to '192.168.0.0-192.168.0.255'), and 'Port' (set to '80,81,8001,8002/http, 443...'). A red box highlights the 'Port' field with the text 'Make sure that targeted IP is in the selected zone or result may be inaccurate or do not show anything.' Below the input fields, there is a checkbox for 'Enable weak password scan'. A red box labeled 'IP Server' points to the 'Port' field. At the bottom, there is a 'Select Port' dialog box with a table of predefined ports. The table has columns for 'Port', 'Application', and 'Del...'. The ports listed are 80,81,8001,8002 (http), 443 (https), 110 (pop3), 25 (smtp), 143 (imap), 21 (ftp), 69 (tftp), 3306 (mysql), 1521 (oracle), 1433 (mssql), 139,445 (netbios), 53 (dns), and 23 (telnet). All ports are checked. The dialog box also has 'OK' and 'Cancel' buttons.

Support Community Security Assistant Internal Report Center User: admin

Dashboard Risk Analytics

Insecure Source Zone: lan

Destination: 192.168.0.0-192.168.0.255

Port: 80,81,8001,8002/http, 443...

Enable weak password scan

Make sure that targeted IP is in the selected zone or result may be inaccurate or do not show anything.

IP Server

Avoid Risk Export as PDF Report Based on All Policies

Select Port

Port	Application	Del...
80,81,8001,8002	http	X
443	https	X
110	pop3	X
25	smtp	X
143	imap	X
21	ftp	X
69	tftp	X
3306	mysql	X
1521	oracle	X
1433	mssql	X
139,445	netbios	X
53	dns	X
23	telnet	X

OK Cancel

# Risk Analytics

## Weak password scan setting

**Select service/application**

Service Application
<input checked="" type="checkbox"/> ftp
<input checked="" type="checkbox"/> mysql
<input type="checkbox"/> oracle
<input checked="" type="checkbox"/> mssql
<input checked="" type="checkbox"/> netbios
<input type="checkbox"/> ssh
<input type="checkbox"/> rdp
<input type="checkbox"/> vnc

**Enable weak password scan**

Range: ftp, mysql, mssql, netbio...

Method: Full password dict (takes longer time)

**Advanced Settings**

**RDP/VNC Service**

RDP/VNC scan and full scan take longer time. By default, it implements general scan.

☒ Implement full scan

**Username/Password Dictionaries**

Username Dictionary:

Password Dictionary:

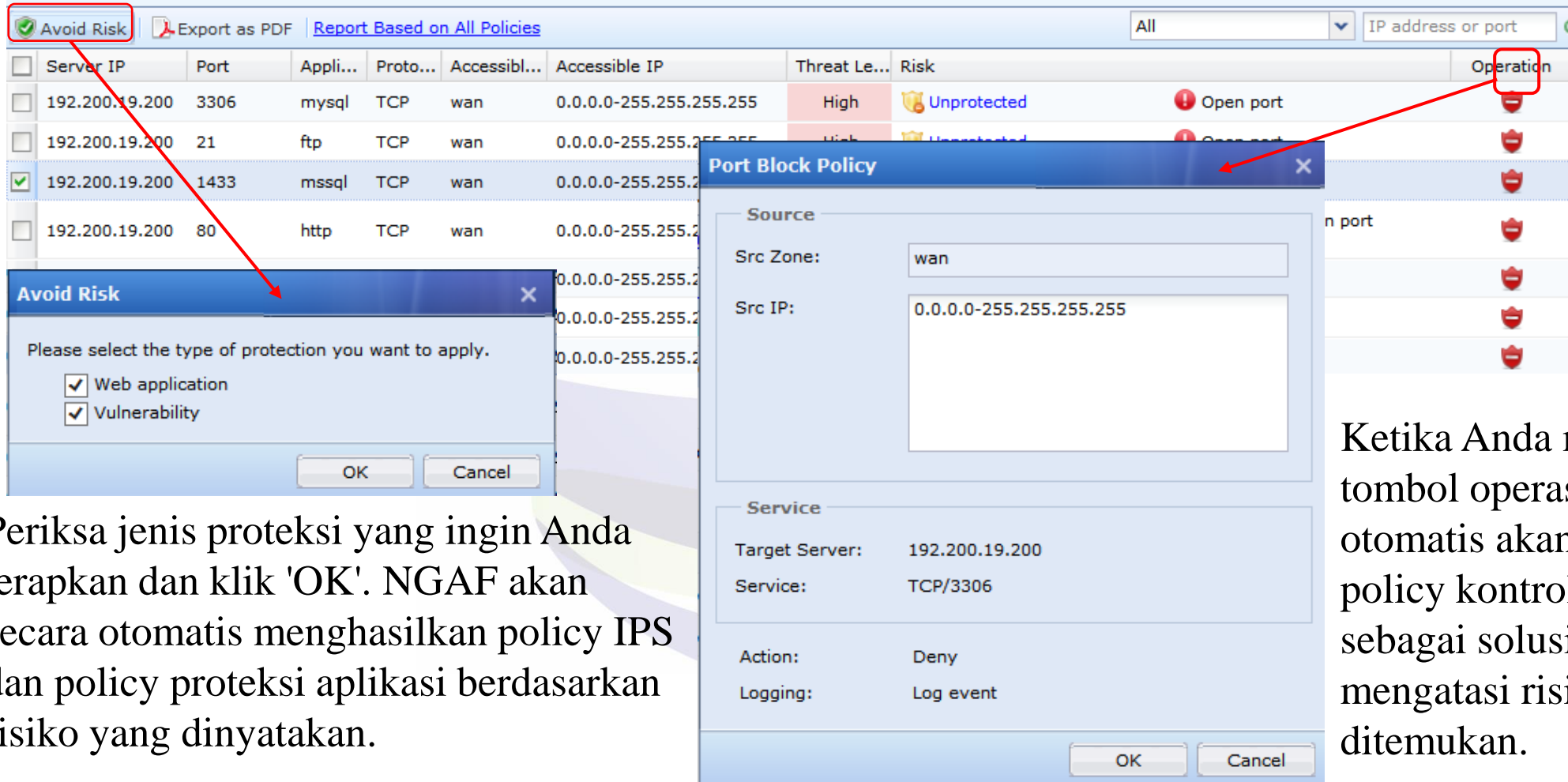
**Pilih layanan/aplikasi untuk pemindaian password yang lemah**

**Kamus password konvensional hanya berisi password default sistem.**

1. Kamus password konvensional hanya berisi password default sistem.
2. Tambahkan nama pengguna sebagai Sangfor, pemindaian NGAF akan menyertakan nama pengguna default dan nama pengguna yang disesuaikan 'Sangfor'.
3. Tambahkan password sebagai Sangfor, pemindaian NGAF akan menyertakan password default dan password yang disesuaikan 'Sangfor'.

# Risk Analytics

Atur pemindaian port dan pemindaian password yang lemah, klik mulai pindai, dan itu akan menunjukkan risiko di setiap server



The screenshot displays the Sangfor Risk Analytics interface. At the top, there's a navigation bar with 'Avoid Risk' (highlighted with a red box), 'Export as PDF', and 'Report Based on All Policies'. Below this is a table of risks. The table has columns: Server IP, Port, Appli..., Proto..., Accessibl..., Accessible IP, Threat Le..., Risk, and Operation. The 'Operation' column is highlighted with a red box. Two modal windows are open: 'Avoid Risk' and 'Port Block Policy'.

**Avoid Risk Modal:**

Please select the type of protection you want to apply.

- ☒ Web application
- ☒ Vulnerability

Buttons: OK, Cancel

**Port Block Policy Modal:**

**Source**

Src Zone: wan

Src IP: 0.0.0.0-255.255.255.255

**Service**

Target Server: 192.200.19.200

Service: TCP/3306

Action: Deny

Logging: Log event

Buttons: OK, Cancel

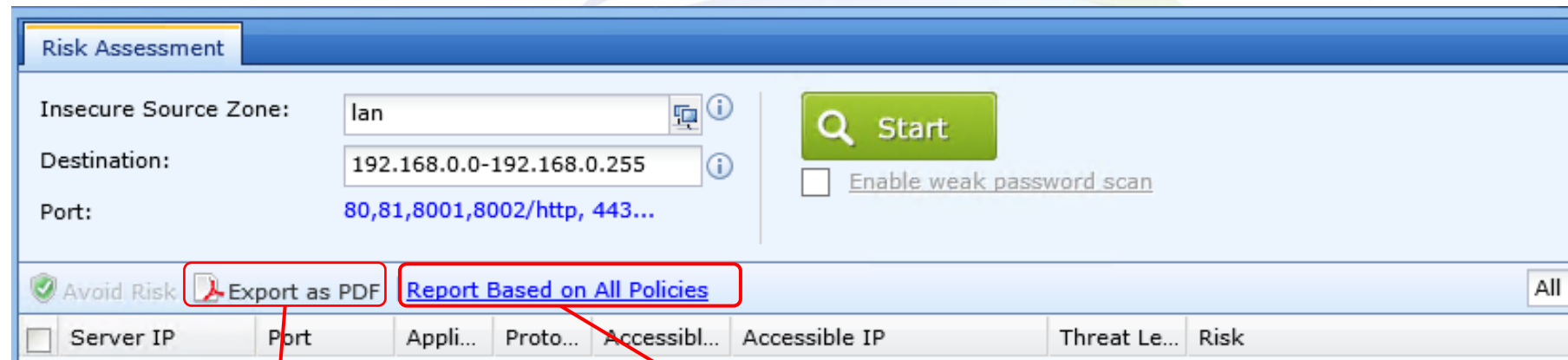
Periksa jenis proteksi yang ingin Anda terapkan dan klik 'OK'. NGAF akan secara otomatis menghasilkan policy IPS dan policy proteksi aplikasi berdasarkan risiko yang dinyatakan.

Ketika Anda mengklik tombol operasi, secara otomatis akan menghasilkan policy kontrol aplikasi deny sebagai solusi untuk mengatasi risiko yang ditemukan.



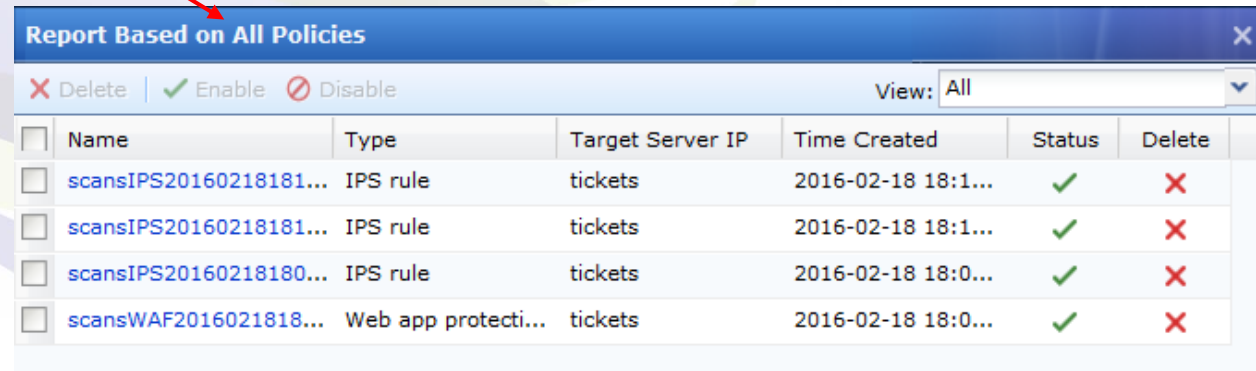
# Risk Analytics

Ekspor laporan penilaian risiko, dan melihat aturan yang ditambahkan secara otomatis.



The Risk Assessment interface includes fields for Insecure Source Zone (lan), Destination (192.168.0.0-192.168.0.255), and Port (80,81,8001,8002/http, 443...). It features a Start button and an option to Enable weak password scan. Below these fields, there are buttons for Avoid Risk, Export as PDF, and Report Based on All Policies. A table header is visible at the bottom with columns: Server IP, Port, Appli..., Proto..., Accessibl..., Accessible IP, Threat Le..., and Risk.

Menghasilkan laporan analisis pemindaian proaktif dalam format PDF



The Report Based on All Policies window displays a table of security rules. It includes a View dropdown set to 'All' and a table with columns: Name, Type, Target Server IP, Time Created, Status, and Delete. The table contains four entries, all with a Status of '✓' and a Delete button (✗).

Name	Type	Target Server IP	Time Created	Status	Delete
scansIPS20160218181...	IPS rule	tickets	2016-02-18 18:1...	✓	✗
scansIPS20160218181...	IPS rule	tickets	2016-02-18 18:1...	✓	✗
scansIPS20160218180...	IPS rule	tickets	2016-02-18 18:0...	✓	✗
scansWAF2016021818...	Web app protecti...	tickets	2016-02-18 18:0...	✓	✗

## 4. Web Scanner

---



# Web Scanner

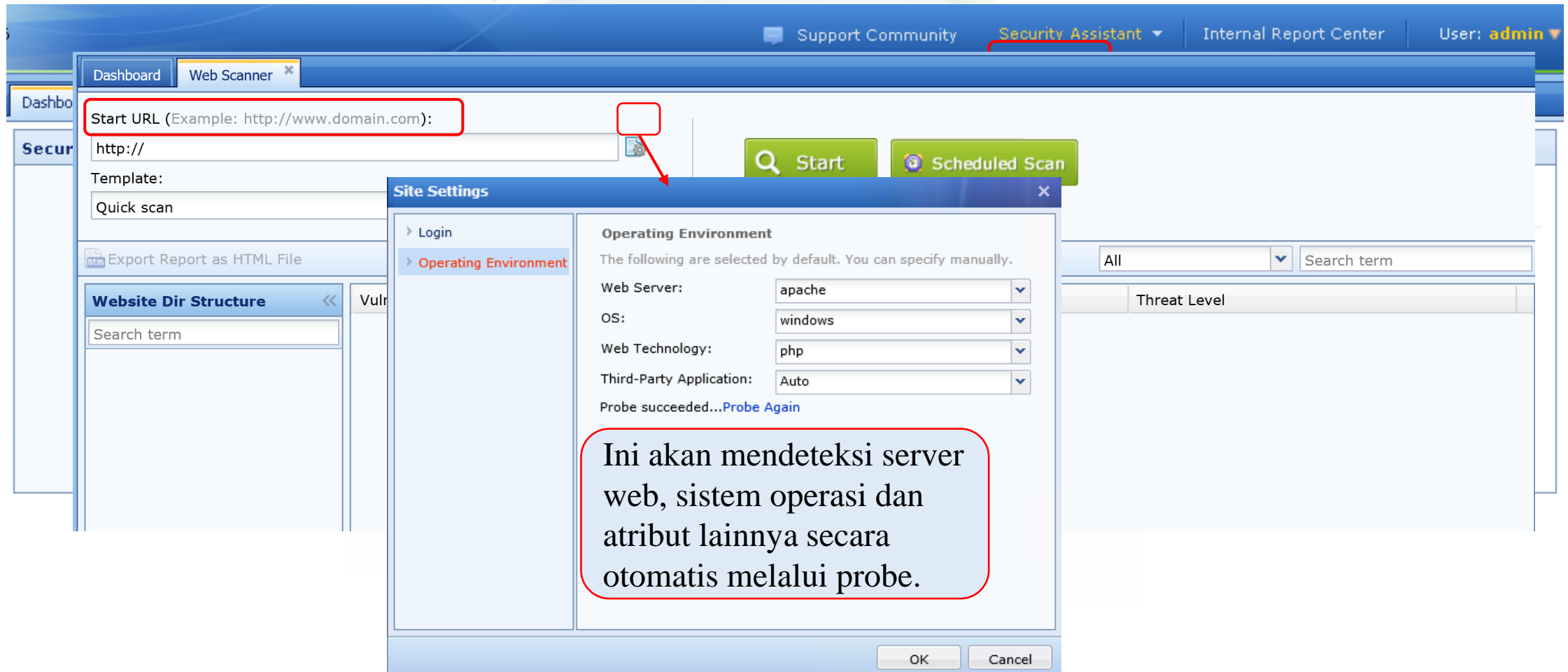
Pemindai web mendukung pemindaian kerentanan berikut:

Injeksi SQL, mengikat injeksi SQL, serangan scripting lintas situs (XSS), serangan skrip lintas situs yang disimpan, injeksi perintah OS, inklusi file lokal, inklusi file jarak jauh, serangan brute force, password lemah, pemalsuan permintaan lintas situs (CSRF), injeksi XPATH, injeksi LDAP, divisi respons, sisi server Termasuk (SSI), pengalihan yang tidak aman, konfigurasi DAV yang tidak aman, metode HTTP yang tidak aman, mengaktifkan WebDAV, memancing iframe, pelacakan lintas situs (XST), pengungkapan informasi phpinfo, konfigurasi PHP yang tidak aman, temukan daftar direktori, temukan direktori tersembunyi.

1. Penting untuk memberi tahu pengguna sebelum memindai: Pemindai Web memiliki risiko merusak data situs, oleh karena itu pemindaian tidak dapat dilakukan secara langsung di server web produksi. Klien harus menyediakan server cermin untuk memindai kerentanan.
2. Jika Anda memindai server produksi secara langsung, Anda perlu mendapatkan persetujuan dan tekanan pelanggan tentang kemungkinan risiko terhadap pelanggan, dan mencadangkan data situs dan kode sumber sebelum melakukan pemindaian untuk memastikan bahwa jika ada masalah, data dapat dipulihkan dari cadangan.

# Web Scanner

Isi URL mulai serta templat pemindaian, klik ikon pena di sebelah kanan untuk memasukkan antarmuka pengeditan



The screenshot displays the Sangfor Web Scanner web interface. At the top, there's a navigation bar with links for 'Support Community', 'Security Assistant', 'Internal Report Center', and a user profile 'User: admin'. Below this, the 'Web Scanner' tab is active. The main area contains a 'Start URL (Example: http://www.domain.com):' field with 'http://' entered, a 'Template:' dropdown set to 'Quick scan', and two buttons: 'Start' and 'Scheduled Scan'. A 'Site Settings' dialog box is open, showing the 'Operating Environment' tab. This tab lists default settings: 'Web Server: apache', 'OS: windows', 'Web Technology: php', and 'Third-Party Application: Auto'. A message at the bottom of the dialog states 'Probe succeeded...Probe Again'. A red box highlights the 'Start URL' field, and a red arrow points from it to the 'Site Settings' dialog. Another red box highlights the 'Operating Environment' section of the dialog, with a text box overlaying it.

Start URL (Example: http://www.domain.com):

http://

Template: Quick scan

Start Scheduled Scan

Site Settings

Operating Environment

The following are selected by default. You can specify manually.

Web Server: apache

OS: windows

Web Technology: php

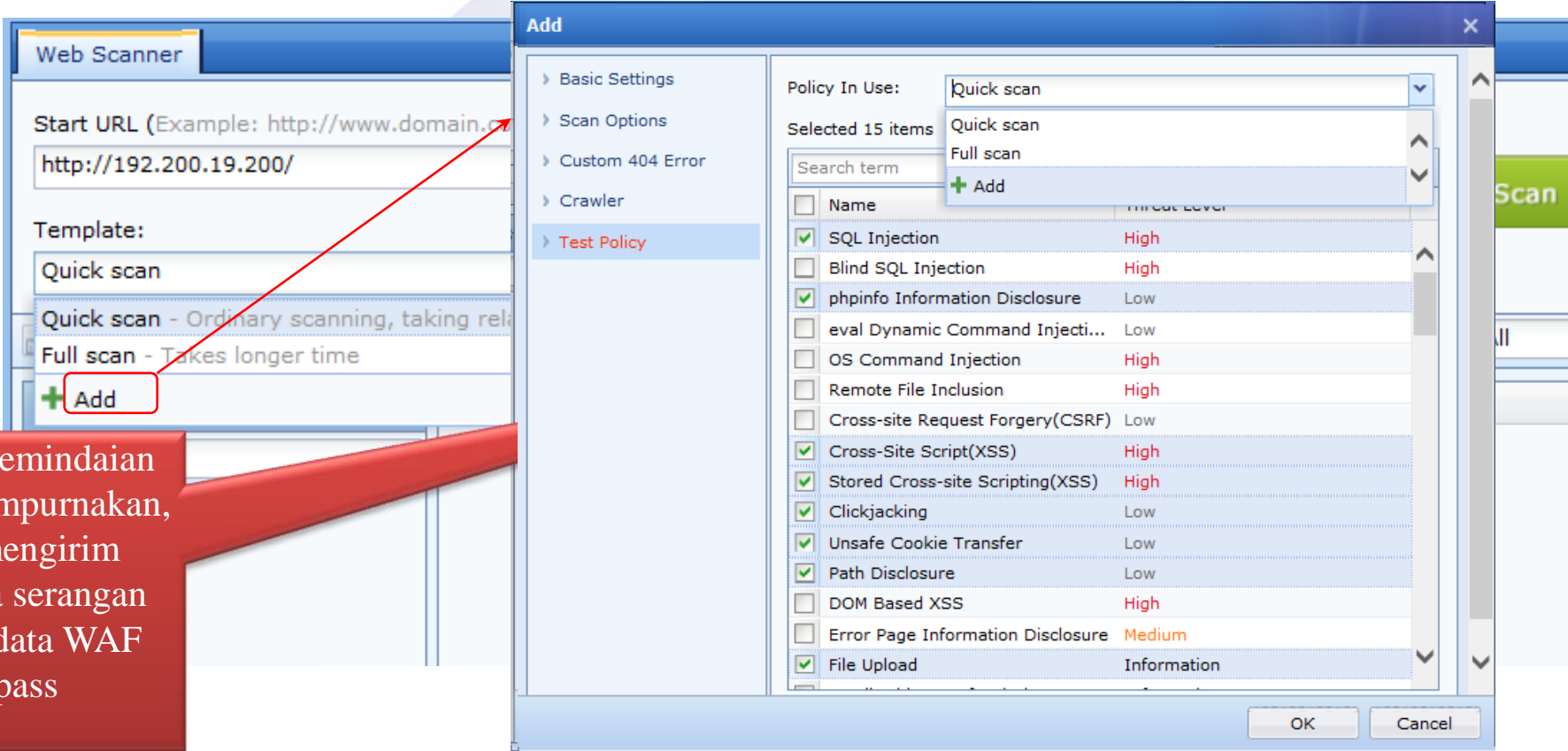
Third-Party Application: Auto

Probe succeeded...Probe Again

Ini akan mendeteksi server web, sistem operasi dan atribut lainnya secara otomatis melalui probe.

# Web Scanner

Template pemindai web bawaan (pemindaian cepat dan pemindaian penuh) tidak dapat diubah. Anda perlu mengklik menu drop-down untuk menambahkan template seperti yang ditunjukkan pada tangkapan layar di bawah ini:



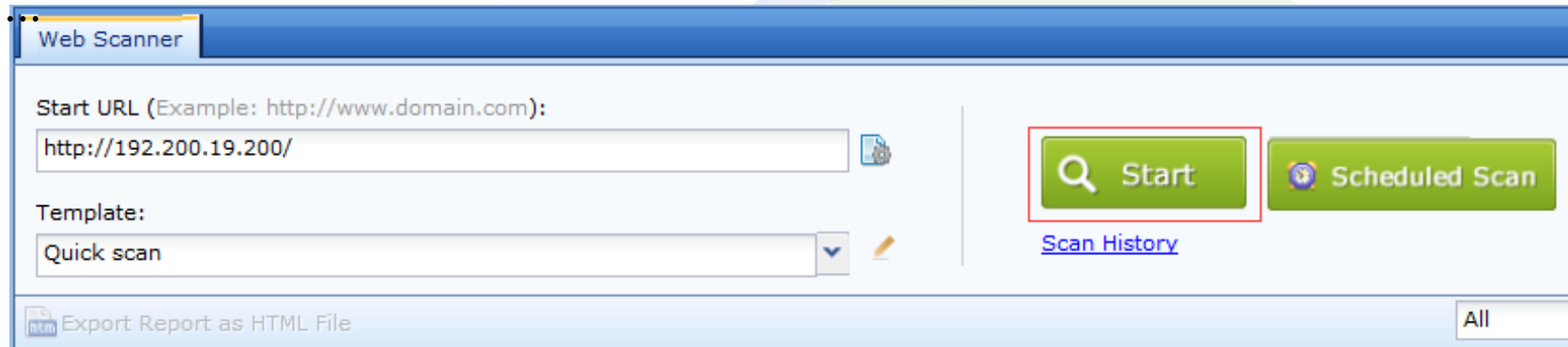
The screenshot shows the 'Web Scanner' application window. In the background, the 'Template' dropdown menu is open, showing 'Quick scan' and 'Full scan' options, with an 'Add' button at the bottom. A red arrow points from this 'Add' button to the 'Add' dialog box in the foreground. The 'Add' dialog box has a sidebar with 'Test Policy' selected. The main area shows a list of 15 items with checkboxes and threat levels. The 'Policy In Use' dropdown is set to 'Quick scan'.

Periksa pemindaian yang disempurnakan, akan mengirim beberapa serangan dengan data WAF bypass

Name	Threat Level
<input checked="" type="checkbox"/> SQL Injection	High
<input type="checkbox"/> Blind SQL Injection	High
<input checked="" type="checkbox"/> phpinfo Information Disclosure	Low
<input type="checkbox"/> eval Dynamic Command Injecti...	Low
<input type="checkbox"/> OS Command Injection	High
<input type="checkbox"/> Remote File Inclusion	High
<input type="checkbox"/> Cross-site Request Forgery(CSRF)	Low
<input checked="" type="checkbox"/> Cross-Site Script(XSS)	High
<input checked="" type="checkbox"/> Stored Cross-site Scripting(XSS)	High
<input checked="" type="checkbox"/> Clickjacking	Low
<input checked="" type="checkbox"/> Unsafe Cookie Transfer	Low
<input checked="" type="checkbox"/> Path Disclosure	Low
<input type="checkbox"/> DOM Based XSS	High
<input type="checkbox"/> Error Page Information Disclosure	Medium
<input checked="" type="checkbox"/> File Upload	Information

# Web Scanner

Periksa pemindaian yang disempurnakan, akan mengirim beberapa serangan dengan data WAF bypass



Web Scanner

Start URL (Example: http://www.domain.com):

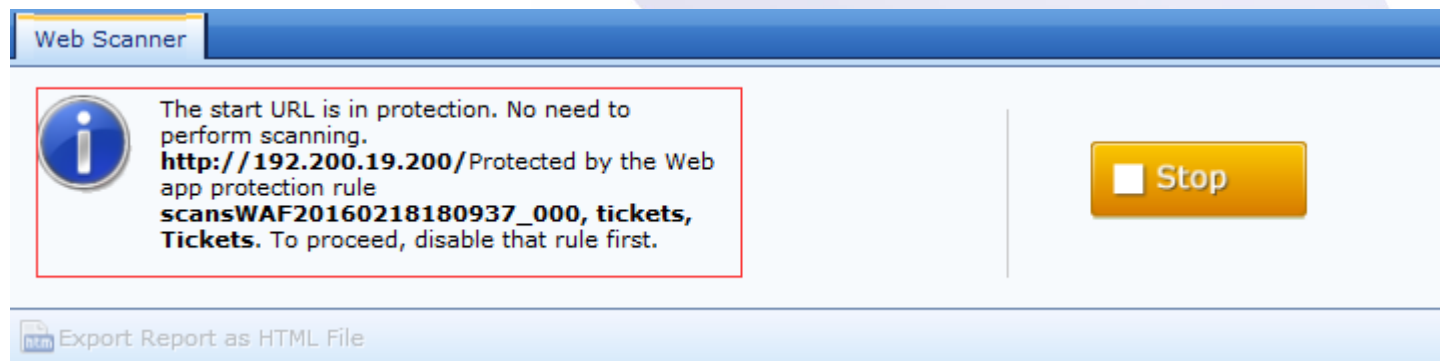
Template:

[Scan History](#)

[Export Report as HTML File](#) All

**Start** **Scheduled Scan**

•Catatan: Jika ada policy WAF untuk melindungi URL yang ditargetkan dan tindakan ditolak, itu akan mendorong "URL awal dalam proteksi. Tidak perlu melakukan pemindaian." Anda harus menonaktifkan atau mengubah tindakan policy WAF yang relevan untuk mengaktifkan pemindaian



Web Scanner

**The start URL is in protection. No need to perform scanning.**  
**http://192.200.19.200/Protected by the Web app protection rule**  
**scansWAF20160218180937\_000, tickets, Tickets.** To proceed, disable that rule first.

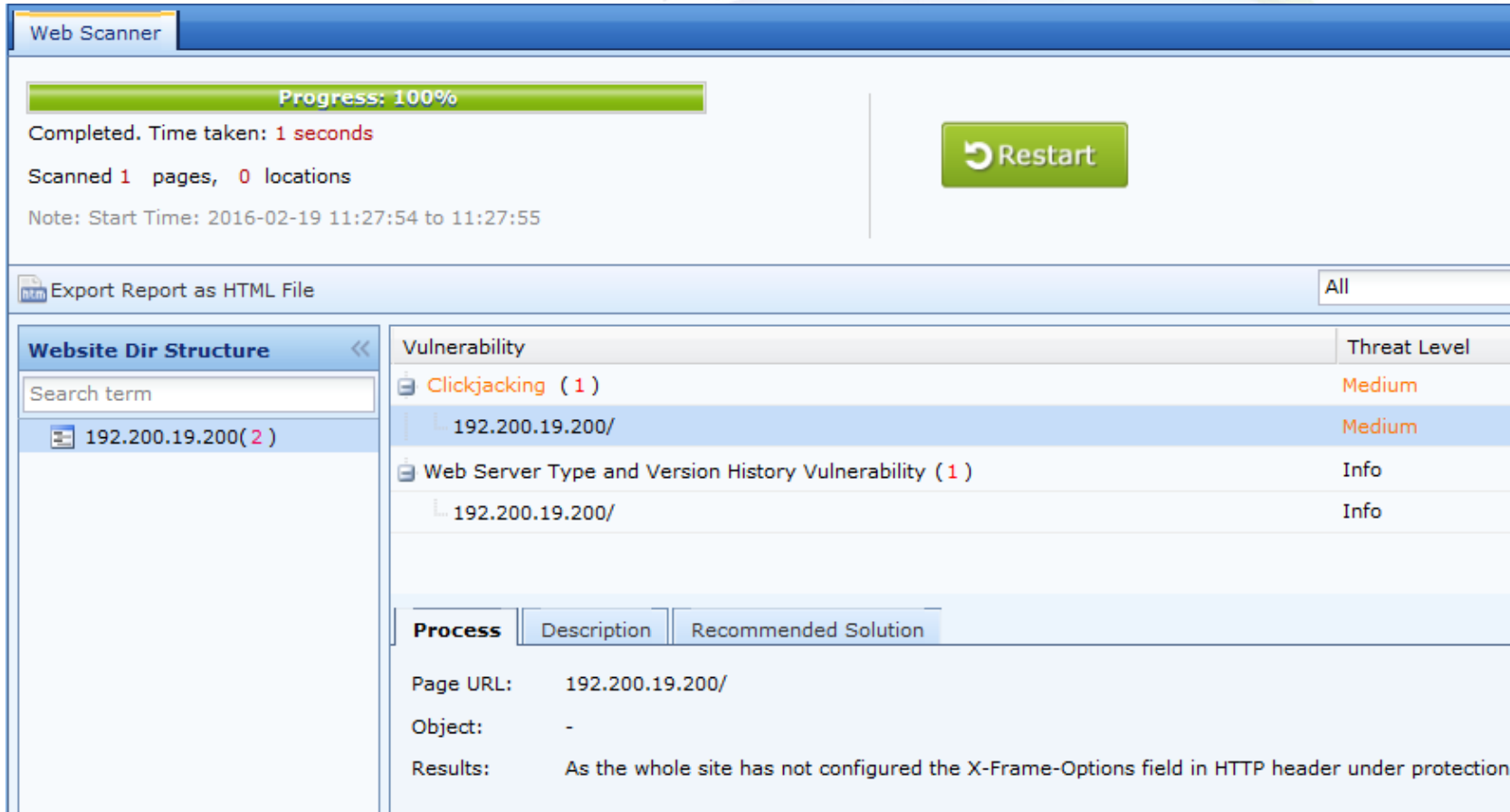
[Export Report as HTML File](#)

**Stop**



# Web Scanner

Setelah pemindaian selesai, Anda dapat melihat proses pemindaian, deskripsi, dan solusi kerentanan yang direkomendasikan.




**Web Scanner**

**Progress: 100%**

Completed. Time taken: 1 seconds

Scanned 1 pages, 0 locations

Note: Start Time: 2016-02-19 11:27:54 to 11:27:55



Export Report as HTML File All

**Website Dir Structure**

Search term

192.200.19.200(2)

Vulnerability	Threat Level
Clickjacking (1)	Medium
192.200.19.200/	Medium
Web Server Type and Version History Vulnerability (1)	Info
192.200.19.200/	Info

Process	Description	Recommended Solution
Page URL:	192.200.19.200/	
Object:	-	
Results:	As the whole site has not configured the X-Frame-Options field in HTTP header under protection,	

# Web Scanner

Setelah pemindaian selesai, Anda dapat mengekspor Laporan Kerentanan Web html.

## Web Vulnerability Report

Start Time:2016-02-19 11:27:54

Scanning Duration:1 seconds

[Target Site](#)  
[Overview](#)  
[Vulnerability Content](#)  
[\\*Clickjacking \(1\)](#)  
[Information Content](#)  
[\\*Web Server Type and Version History Vulnerability \(1\)](#)

### Target Site

Start URL: <http://192.200.19.200/>  
 Web Server: Apache/2.2.11 (Win32) PHP/5.2.8  
 OS: windows  
 Web Language: Unknown  
 Third-Party Application: unknown 0  
 Login Method: Not login  
 URLs Scanned: 0

### Overview



#### Possible Threats:

- Intercept session, get user login credential to get access to site.

#### Solution(s):

1. Check validity of data on client-side and server-side, and filter special characters.
2. Deploy security appliance that is able to perform Web application protection.

### No. Page

1 <http://192.200.19.200/>

Vulner

### Vulnerability Content Details

#### Clickjacking (1)

##### Description:

Clickjacking is a malicious technique that attacker uses multiple transparent or opaque layers to trick a user into clicking on something different from what the user p

##### Solution:

Increase or set value of HTTP header option X-Frame-Options to DENY or SAMEORIGIN

# Web Scanner

## Catatan:

1. Jika ada policy WAF yang dibuat untuk melindungi URL yang ditargetkan dan tindakannya ditolak, itu akan mendorong "URL awal dalam proteksi. Tidak perlu melakukan pemindaian." Anda harus menonaktifkan atau mengubah tindakan policy WAF yang relevan untuk memindai.
2. Ketersediaan tinggi tidak menyinkronkan konfigurasi dalam pemindai web.
3. Untuk memiliki hasil yang lebih akurat pada pemindaian password yang lemah, pengguna harus masuk ke URL yang ditargetkan. Ini tidak melibatkan penyertaan kode otentikasi, dll.
4. Setelah pemindaian selesai, Anda dapat segera mengeksport laporan pemindaian dalam format PDF. Perangkat tidak akan menyimpan laporan. Laporan akan dihapus lagi setiap kali pemindaian baru dimulai.

# Terimakasih!

tech.support@sangfor.com  
community.sangfor.com

**Sangfor Technologies (Kantor Pusat)**  
Blok A1, Nanshan iPark, No.1001  
Jl. Xueyuan, Distrik Nanshan,  
Shenzhen, Provinsi Guangdong,  
P. R. China (518055)

