Checks made by QRadar Vulnerability Manager

QRadar® Vulnerability Manager uses a combination of active checks that involves sending packets and remote probes, and passive correlation checks. The QRadar Vulnerability Manager database covers approximately 70,000 Network, OS, and Application layer vulnerabilities.
You can search the complete scanning library by CVE, date range, vendor name, product name, product version, and exposure name from the Research window on the **Vulnerabilities** tab.

QRadar Vulnerability Manager tests

The following examples are some of the categories that QRadar Vulnerability Manager tests:

- Router checks
- Firewall checks
- Database checks
- Web server checks
- Web application server checks
- Common web scripts checks
- Custom web application checks
- DNS server checks
- Mail server checks
- Application server checks
- Wireless access point checks
- Common service checks
- Obsolete software and systems

The following table describes some checks that are made by QRadar Vulnerability Manager.

Table 1. Types of QRadar Vulnerability Manager checks

Type of Check	Description

Type of Check	Description
Port scan	Scans for active hosts and the ports and services that are open on each active host Returns MAC if the host is on the same subnet as the scanner Returns OS information
Web application scanning	Checks each web application and web page on a web server by using the following checks: File upload HTTP directory browsing CWE-22 - Improper limitation of a path name to a restricted directory (path traversal) Interesting file / seen in logs Auto complete password in Browser Misconfiguration in default files Information disclosure Unencrypted login form Directory index-able: checks if the server directories can be browsed HTTP PUT allowed: checks if the PUT option is enabled on server directories Existence of obsolete files CGI scanning: common web page checks Injection (XSS/script/HTML) Remote file retrieval (server wide) Command execution from remote shell SQL injection, including authentication bypass, software identification, and remote source

Type of Check	Description
	Reverse tuning options, except for specified options **Note** Authenticated web app scanning is not supported. For example, if authentication is required to access the site, you can't run web app tests.
Router	Known vulnerabilities and configuration issues in the firmware. Weak and default passwords Default community strings Denial of service Retrieval of sensitive account information
Firewall	Denial of service Firewall bypassing techniques Bypassing TCP filtering Reveal IP addresses of protected assets Insert Trojan horses Access sensitive data (firewall rules, user name, and passwords) Cross site scripting User name and password weakness

Type of Check	Description
OS	User name and password disclosure Access to file systems Default user names and passwords Privilege escalation Denial of service Remote command execution Cross site scripting (Microsoft)
Database	Exploits and open access to databases. Default passwords Compromised user names and passwords Denial of service Admin rights
Web server	Known vulnerabilities, exploits, and configuration issues on web servers. Denial of service Default admin passwords File system view ability Cross site scripting
Common web scripts	Commonly found web scripts such as CGI E-commerce related scripts ASP PHP

Type of Check	Description
DNS server	Weak password encryption Denial of service Determine account names Send emails Read arbitrary emails and sensitive account information Get admin access
Wireless access point	Default admin account passwords Default SNMP community names Plain text password storage Denial of service
Common services	Domain name system (DNS) File transfer protocol (FTP) Simple mail transfer protocol (SMTP)
Application server	Authentication bypass Denial of service Information disclosure Default user names and passwords Weak file permissions Cross site scripting
Oval	Client-side vulnerabilities on IE, Chrome, Skype, and others.
Password testing	Default password testing
Windows patch scanning	Collects registry key entries, windows services, installed windows applications, and patched Microsoft bugs.
Unix patch scanning	Collects details of installed RPMs

Web application scanning

QRadar Vulnerability Manager uses unauthenticated scanning for core web application scanning. The following list describes QRadar Vulnerability Manager web vulnerability checks:

- SQL Injection Vulnerabilities
  SQL injection vulnerabilities occur when poorly written programs accept user-provided data in a database query without validating the input, which is found on web pages that have dynamic content. By testing for SQL injection vulnerabilities, QRadar Vulnerability Manager assures that the required authorization is in place to prevent these exploits from occurring.

- Cross-Site Scripting (XSS) Vulnerabilities
  Cross-Site Scripting vulnerabilities can allow malicious users to inject code into web pages that are viewed by other users. HTML and client-side scripts are examples of code that might be injected into web pages. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy. QRadar Vulnerability Manager tests for varieties of persistent and non-persistent cross-site scripting vulnerabilities to ensure that the web application is not susceptible to this threat.

- Web Application Infrastructure
  QRadar Vulnerability Manager includes thousands of checks that check default configurations, cgi scripts, installed and supporting application, underlying operating systems and devices.

- Web page errors

For in-depth web application scanning, QRadar Vulnerability Manager integrates with IBM® Security AppScan® to provide greater web application visibility to your vulnerabilities.

Network device scanning

QRadar Vulnerability Manager includes the following plug-ins that support scanning of network devices:

- SNMP
  QRadar Vulnerability Manager uses a dictionary of known community defaults for various SNMP-enabled devices. You can customize the dictionary.

- OVAL scanning

QRadar Vulnerability Manager uses OVAL to detect and report known vulnerabilities. The QRadar Vulnerability Manager OVAL scanning plug-in currently works only with Cisco devices.

External scanner checks

The external scanner scans the following OWASP (Open Web Application Security Project) CWEs (Common Weakness Enumerations):

- Directory Listing
- Path Traversal, Windows File Parameter Alteration, Unix File Parameter Alteration, Poison Null Byte Windows Files Retrieval, Poison Null Byte Unix Files Retrieval
- Cross-Site Scripting, DOM Based Cross-Site Scripting
- SQL Injection, Blind SQL Injection, Blind SQL Injection (Time Based)
- Autocomplete HTML Attribute Not Disabled for Password Field
- Unencrypted Login Request, Unencrypted Password Parameter
- Remote Code Execution, Parameter System Call Code Injection, File Parameter Shell Command Injection, Format String Remote Command Execution

Database scanning

QRadar Vulnerability Manager detects vulnerabilities on major databases by using authenticated scanning of target hosts. In addition, QRadar Vulnerability Manager targets several databases by using plug-ins.

Operating system checks

Table 2. Operating system checks

Operating system	Vulnerability scanning	Patch scanning	Configuration
Windows	Yes	Yes	Yes
AIX® Unix	Yes	Yes	No
CentOS Linux	Yes	Yes	No
Debian Linux	Yes	Yes	No

Operating system	Vulnerability scanning	Patch scanning	Configuration
Fedora Linux	Yes	Yes	No
RedHat Linux	Yes	Yes	No
Sun Solaris	Yes	Yes	No
HP-UX	Yes	Yes	No
Suse Linux	Yes	Yes	No
Ubuntu Linux	Yes	Yes	No
CISCO	Yes	Yes	No
AS/400® / iSeries	No	No	No

OVALs and operating systems

OVAL definitions are supported on the following operating systems:

- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003
- CentOS versions 3 - 7
- IBM AIX versions 4-7
- RHEL versions 3 - 7
- SUSE versions 10 - 11

- Ubuntu versions 6-14
- Red Hat 9
- Solaris versions 2.6, 7 - 10

Parent topic:

→ Overview of QRadar Vulnerability Manager