

# **Vulnerability Scan Service**

## **Product Introduction**

### **Product Documentation**



## Copyright Notice

©2013-2022 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

## Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

## Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

# Contents

## Product Introduction

Overview

Features

Strengths

Use Cases

# Product Introduction

## Overview

Last updated : 2022-02-16 16:56:49

## Web Security Status Quo

With the rapid development of internet technologies, the key business activities of many government agencies, institutions, and enterprises rely more on web applications. While such applications provide users with web-based information management systems, the risks faced by users are also increasing, mainly in the following two aspects:

- More and more security vulnerabilities are brought by the widespread use of web application systems.
- As internet technologies evolve, hacking has become increasingly rampant, and more and more hacking application tools have been used for attacks.

75% of information security attacks on the internet come from web applications, 2/3 of which are vulnerable.

However, security investments for web applications only account for 10% of all information security investments.

Web security protection is becoming growingly important.

## Product Overview

VSS is a security service designed to monitor website vulnerabilities. It provides 24/7 comprehensive and accurate vulnerability monitoring service and professional repair suggestions to help you prevent vulnerabilities from being exploited by hackers and thus affecting website security.

## Deployment Mode

VSS is a pure SaaS service, which means that you can use it with no need to install any hardware or software or change your current network deployment status. Its powerful concurrent scanning capabilities can check thousands of websites simultaneously, which greatly reduces your security OPS costs.

## Customer Benefits

As an enterprise-grade security monitoring system, VSS brings you the following benefits:

- It helps you fully understand your network security risk situation and ensure business security.

- It helps you promptly deal with new types of hacking techniques and vulnerabilities.
- It complements your proprietary or purchased security products to fully guarantee network security.
- It reduces your security OPS costs.
- It provides you with professional security consulting and technical cooperation services.

## Use Cases

Based on its robust security detection capabilities, VSS can improve network and data security for enterprises in many different industries, including but not limited to:

- IT companies and large enterprises.
- Finance and telecommunications industries.
- Security companies and regulatory authorities.

# Features

Last updated : 2022-02-16 16:56:49

## Automatic Asset Discovery

VSS efficiently identifies device operating systems, ports, services, and components, so that you can better discover unknown assets as well as manage and control existing ones. It also visualizes asset risk data to help you gain clearer insights into the changes in asset risk trends.

## In-depth Vulnerability Scan

- Web vulnerability detection  
VSS protects websites from dozens of common vulnerabilities, such as SQL injection, command injection, code injection, file inclusion, XSS attack, and CSRF attack.
- 0/1/N-Day vulnerability detection  
VSS is preconfigured with thousands of harmless proof of concepts (POCs) tested and audited by Tencent Security engineers to verify vulnerabilities in web applications, web middleware, databases, operating systems, software services, IoT devices, routers, cameras, and industrial control devices.

## Weak Password Detection

VSS scans dozens of asset components for weak passwords, including FTP, SSH, RDP, MySQL, Oracle, IMAP, Memcached, and Redis.

## Risk Evaluation Report

VSS can generate comprehensive multidimensional risk scan reports based on scan results, which cover vulnerability detection and content risks and offer professional repair suggestions.

# Strengths

Last updated : 2022-09-22 11:48:09

VSS is a powerful enterprise-grade security monitoring system launched by Tencent Cloud, with the following strengths:

## Comprehensive Asset Risk Monitoring

VSS is built on the basis of Tencent Security's 20 years of experience in combating cybercrimes and accumulation of massive threat intelligence. It comprehensively monitors various risks in enterprise websites and assets, including weak passwords, web vulnerabilities, sensitive and non-compliant content, website tampering, trojans, and cryptomining.

## In-depth Risk Detection

- Adopting Tencent's web 2.0 threat detection engine and two decades of experience in combating cybercrimes, VSS carefully orchestrates attack policies to simulate real-world hacking attacks and intuitively present the vulnerability situation from the perspective of hackers.
- Preconfigured with thousands of harmless proof of concepts (POCs) and based on the strong 0-day vulnerability mining and sensing capabilities of Tencent's seven security labs (Yunding, Cohen, etc.), VSS can effectively detect 0/1/N-day vulnerabilities in asset components, such as operating systems, databases, web middleware, and CMS applications, to fully protect the asset security.
- Relying on the smart content security detection engine created from Tencent's many years of development in the field of social networking information security moderation, VSS further uses big data and AI technologies to quickly and accurately detect website tampering, sensitive words, phishing, trojans, private links, and pornographic and terrorism information.

## Precise Asset Detection

- VSS supports not only the assets of Linux and Windows servers but also common IoT devices such as cameras, routers, and industrial control devices.
- VSS has a vast built-in protocol and fingerprint library, through which it can quickly and accurately identify assets' operating systems, open ports, and service components.

## Integrated Monitoring-Defense Collaboration

Once VSS finds a security risk, it can collaborate with [CWPP](#) and [WAF](#) in the cloud to form a closed loop from risk monitoring to risk handling.

## Professional Security Team

- Tencent Security's expert team can provide professional repair suggestions for discovered security risks and regularly detect known threats to ensure that they have been eliminated.
- Tencent Security experts come from top-notch security labs and teams, including Cohen, Xuanwu, and Zhanlu labs that have won the titles of "Master of Pwn" and "Pwn2Own World Championship" and received many thanks from Microsoft, Adobe, and other tech giants, as well as the eee team that has won the championship in many Chinese and international cybersecurity challenges.

Note :

If you need to protect your websites or API services from vulnerabilities, you can purchase [WAF](#). It protects websites and applications from the top 10 OWASP vulnerabilities and combats web vulnerability exploitation, malicious crawlers, and CC attacks.

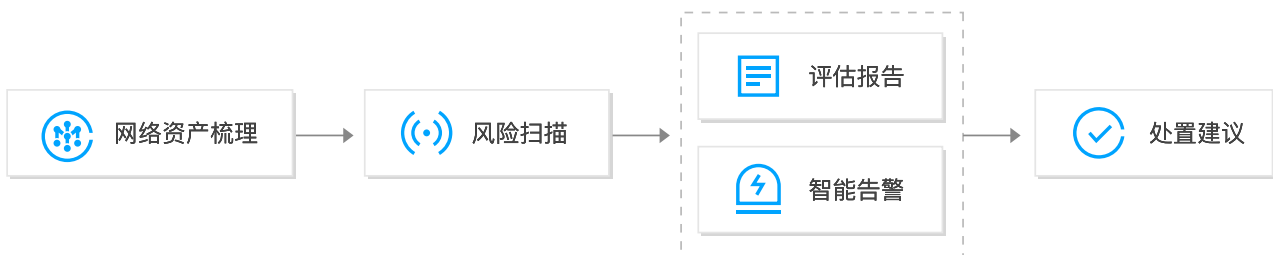


# Use Cases

Last updated : 2022-02-16 16:56:49

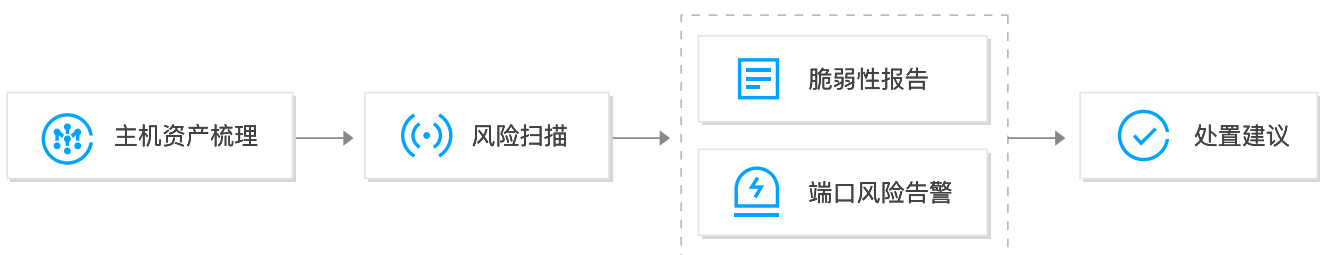
## Website Risk Scan

VSS scans your websites comprehensively to protect them from web vulnerabilities, 0/1/N-day vulnerabilities, availability threats, weak passwords, content security issues, trojans, and tampering.



## Server Risk Scan

VSS can sort out your servers in and off the cloud and scan them for vulnerabilities, service availability issues, and port risks, helping you discover shadow assets and ports. The scan results will be further presented in asset analysis reports and vulnerability reports, together with professional repair suggestions.



## API Security

VSS checks APIs for web-layer vulnerabilities, configuration compliance, data leakage, and feature availability, which facilitates your creation of proactive security models based on industry specifications such as OpenAPI as well as a

unified API security solution.



## IoT Security

VSS comes with many types of fingerprints and PoCs for IoT device discovery, vulnerability detection, and firmware security scan. It also provides code obfuscation and instruction-level binary obfuscation schemes based on a diversity of platforms such as ARM.

