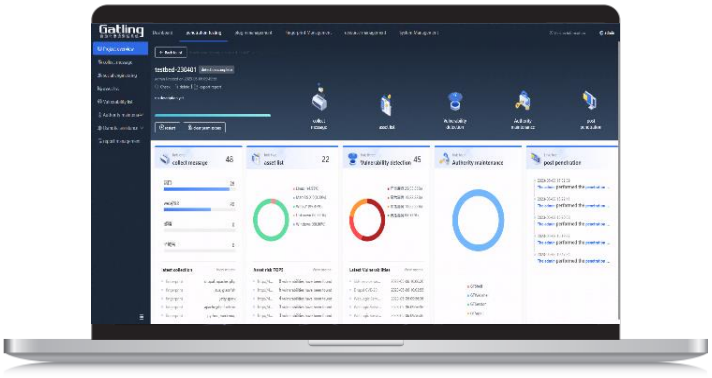
Auto-Penetration Test (Gatling)

Product Overview

Gatling is a leading automated penetration testing tool, and QAX is a leader in network security in the Asia-Pacific region. Relying on years of accumulated practical attack and defense experience, it has accumulated leading 1-day vulnerabilities and advanced attack methods, and independently developed Gatling intended to improve penetration testing results through tools and empower penetration testers to: Attack surface collection, Vulnerability validation, Red team simulation, etc.



System Components

Components	User scenario
Portable TSS10000-PT-5000(Laptop)	Site security evaluation，Individual Combat，intranet patrol
Rack type TSS10000-PT-9600(Server)	Data center deployment，teamwork, SecDevOps integration

Function Architecture

Attack Surface Collection

Collect the available information of the target from the perspective of the attacker, and summarize the information into the attack surface, so that you can understand its vulnerability and reduce the security risk

Support the collection of attack target related information through port scanning, crawler, dictionary blasting and other ways, including but not limited to:

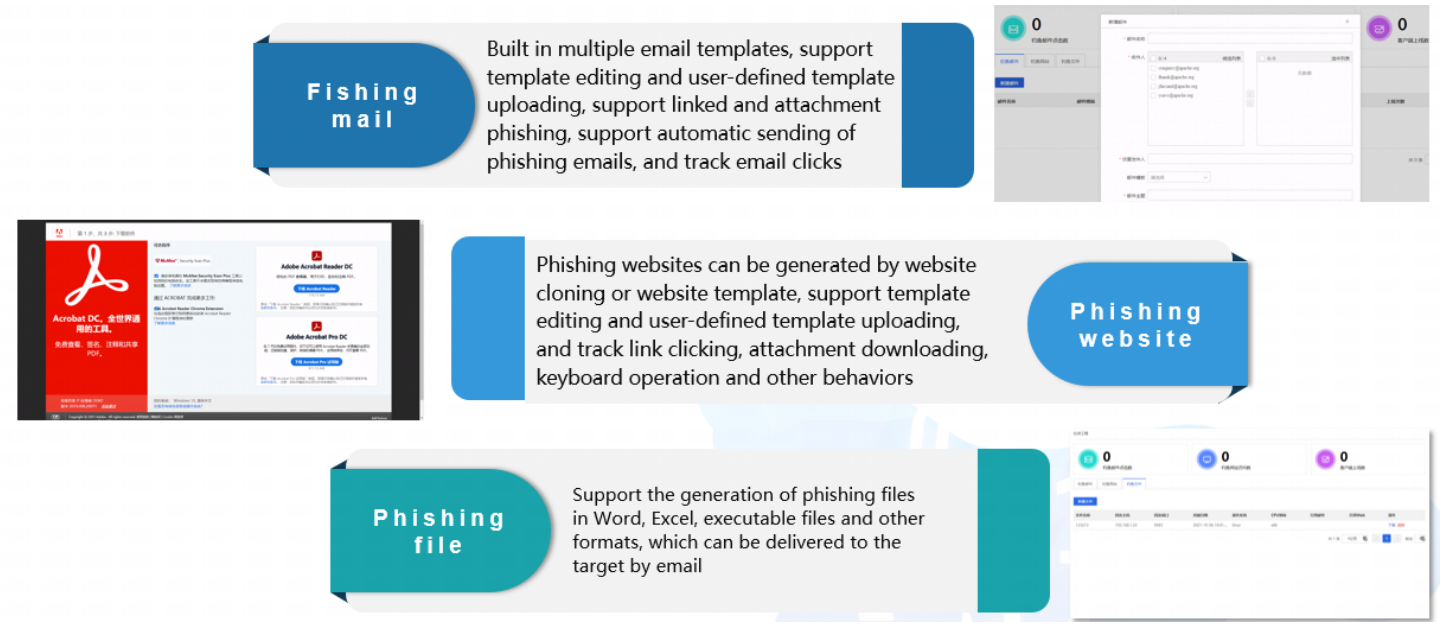
IP. domain name. port. WEB information. Mailbox. Assets and application fingerprint. Backup files

Support through zoomeye, fofa, Hunter, Shodan, etc.

Cloud interface accesses asset information to supplement attack surface

Social engineering attack

Check and cultivate users' security awareness through social engineering phishing attacks



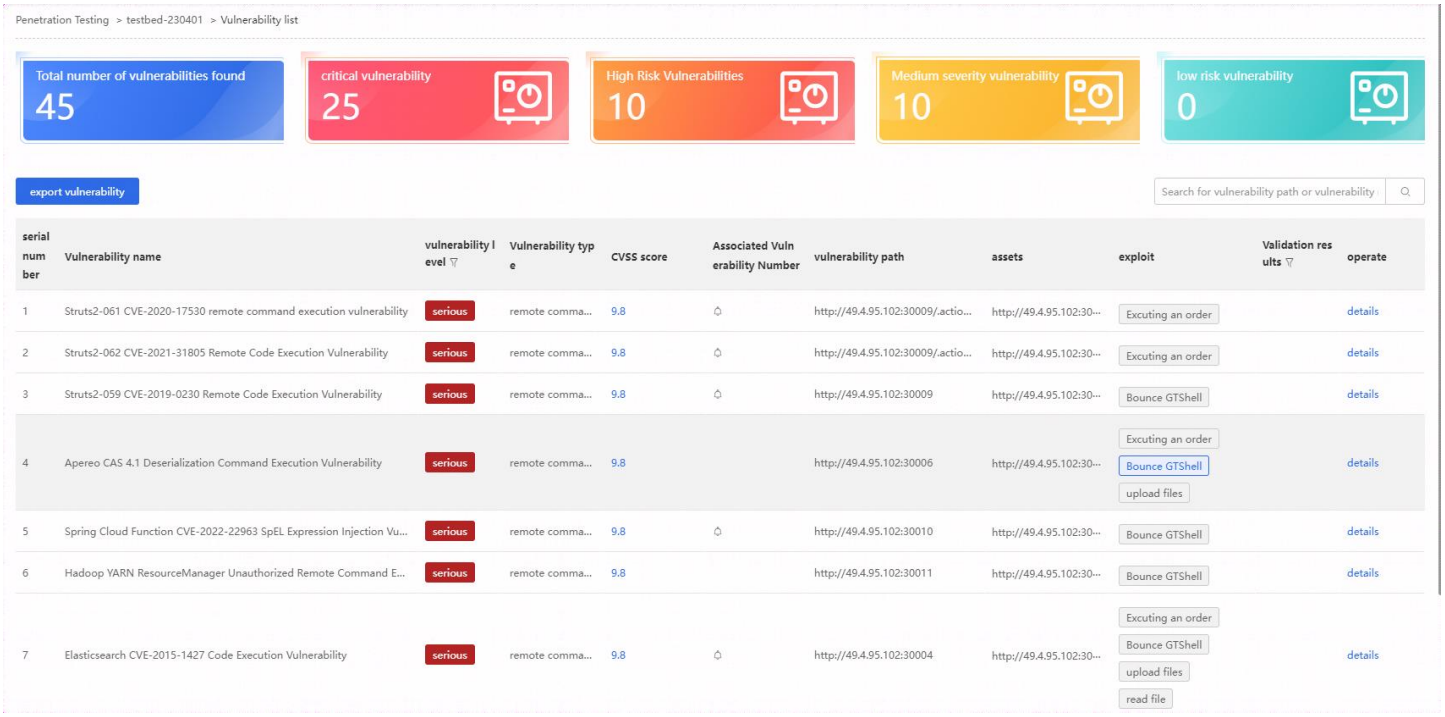
Vulnerability validation and utilization

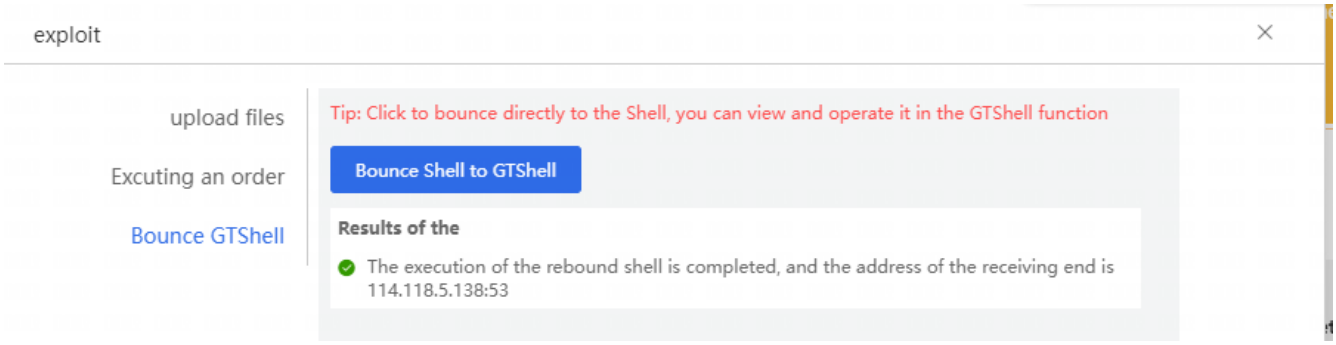
Validate and utilize the vulnerability, provide basis for the priority of vulnerability repair

It contains more than 4000 vulnerability plug-ins, covering Web, middleware, database, big data, network equipment, operating system, intelligent device, mobile terminal, industrial control equipment and other systems, and can find vulnerabilities not limited to SQL injection, XXE, XSS, arbitrary file upload, arbitrary file download, arbitrary file operation, information disclosure, weak password, local file inclusion, directory traversal, command execution, error configuration and other types of vulnerabilities

Provide detailed request/response messages, support rapid verification, filter false positives, and output verification results to the report

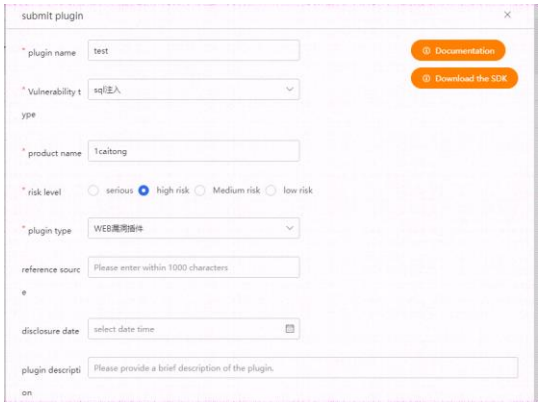
Support one click vulnerability exploitation

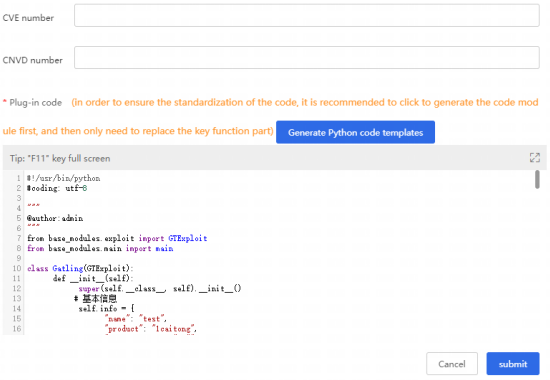




Strong scalability

Gatling provides rich SDK and API interfaces, Enhanced the scalability of the attack, especially for private 0day vulnerabilities and fingerprint, and reserves Plug-in cold template for advanced users like: Custom vulnerability and fingerprint plug-in



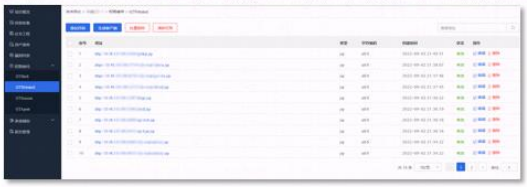


Automatic authority maintenance

Reduce user operation steps and automate authority maintenance

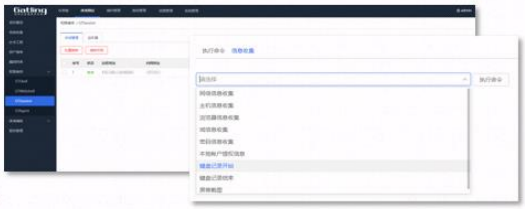
➢ **GTShell - Automatic rebound shell**

- Provide an interactive shell management platform. execute vim, interactive execution operations and other functions
- All Unix operating systems are supported for remote control. Python, JAVA



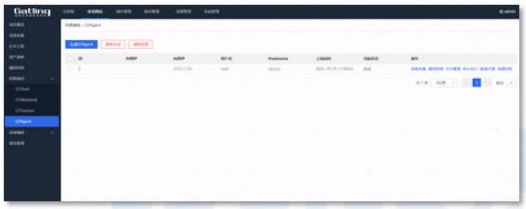
➢ **GTWebshell - Get webshell automatically**

- Encrypt the transmitted data with encryption algorithm, It can bypass the detection of the static Web shell killing tool



➢ **GTSession - Get Session Automatically**

- Connect with third-party tools such as Metasploit and CobaltStrike through GTSession module, provide intranet horizontal functions,



➢ **GTAgent - Automatically deploy agent for remote control**

- Support generate agents, and support plug-in remote calls
- It also has built-in proxy springboards for asset detection and vulnerability utilization to assist in further intranet horizontal and post penetration

Advantages

Extensive Data Collection

Gatling has a huge asset fingerprint database leading traditional network security vendors, which can not only identify basic asset information (device type, vendor, domain name, IP, port, etc.), but also accurately identify application information running on assets (including middleware, application services,

technical architecture, etc.), and achieve extremely high accuracy.

Full & Fast Update of Plug-ins and Vulnerabilities

We submitted to the "National Information Security Vulnerability Sharing Platform" (CNVD) has ranked first for consecutive years

We has one of the most comprehensive and timely vulnerability databases in China, "Butian Vulnerability Database", which contains many 0day and 1day vulnerabilities

Based on the independent vulnerability mining capability and the vulnerability database

Fast update, provide verification plug-ins within 72 hours for major vulnerabilities

Regularly update the latest fingerprint library and plug-in library every week

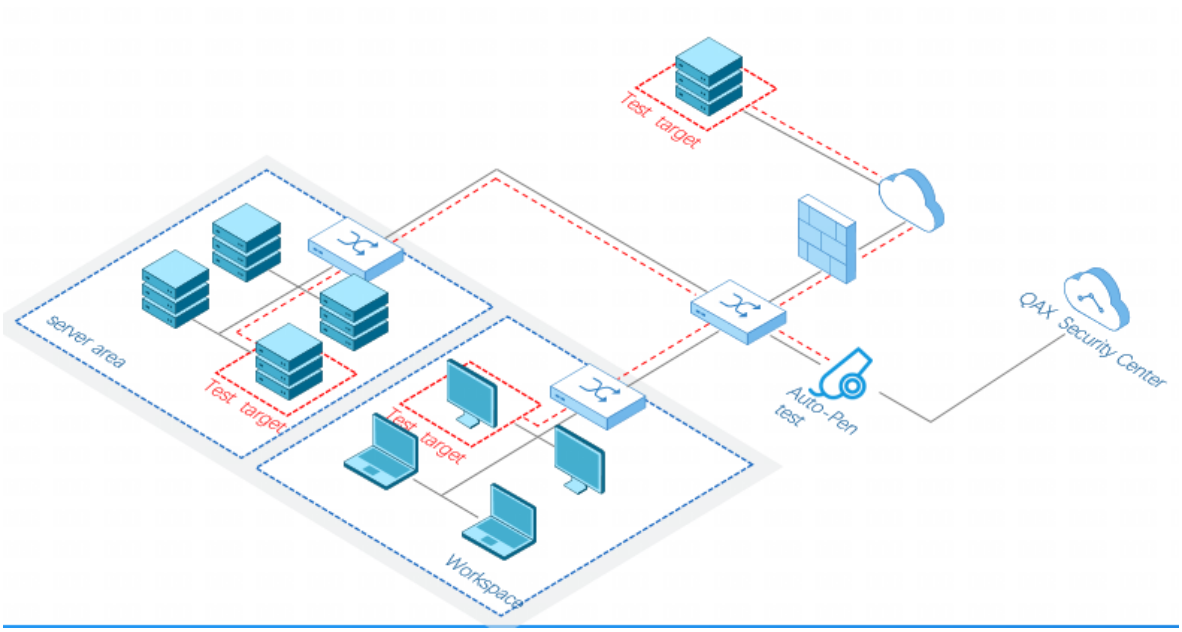
Automation and Ease of Use

Focus on ease of use, flexibility, and humanized designs to started quickly and adapt to different use scenarios.

Leading APT Detection and Tracking Ability

More than 50 domestic and global APT organization have been detected by QI-ANXIN Threat Intelligence Center.

Typical Deployment



Customer case

Gatling has been used in the company for a long time, with customers all over military, police, Confidentiality, finance, energy, operators and so on

Internal case

Gatling was used in the actual offensive and defensive exercises of 19 industries and many large enterprises, such as tax, power, telecommunications, banking, and railway

- GABHW (2016-2021)
- China Electronic Attack and Defense Exercise (2020-2021)
- State Administration of Taxation (2018-2021)
- Attack and Defense Exercise of the Ministry of Finance (2018-2021)
- Attack and Defense Exercise of the Ministry of Water Resources (2018-2020)
- Belt and Road Offensive and Defensive Exercise (2017)
- Offensive and defensive drills of Liaoning Provincial Public Security Department (2017, 2018)
- Attack and Defense Exercise of Sichuan Provincial Public Security Department (2017)

Commercial bank

- Support the internal vulnerability verification of the Security Department and the effectiveness verification of security devices
- Support attack teams to participate in national and industrial attack and defense exercises

Middle East Gov

- Site Risk Assessment
- Regular penetration testing

Southeast Asia military

- Application System Risk Mining
- Key department vulnerability management

Energy Industry Leader

- SaaS deployment
- Open to secondary enterprises

North African Military

- Offensive and defensive exercises
- Isolate network vulnerabilities and harden