# Sneakprobe scanner

#### 0x01 Sneakprobe scanner introduction:

Sneakprobe's Scan official website <https://scan.bwwteam.com/#/>

Sneakprobe adopts the form of B/C architecture. The client can easily access the scanner through a WEB browser and transmit the data directly to the Web server. In addition, Sneakprobe can also realize cross-platform and cross-device scanning and management, and users can access the scan results through the web anytime and anywhere.

Sneakprobe uses front-end and back-end technologies for development, and uses redis for data caching to reduce the performance and response speed of the web service system. Front-end and back-end technologies can achieve better user experience and interaction and meet user needs for functions.

Sneakprobe uses a plug-in to perform vulnerability scanning. Its main functions are:

Port scanning: Port scanning using TCP, SYN, ICMP, UDP and other protocols

Subdomain name scanning: Dictionary scanning for status codes

Directory scanning: Dictionary scanning for status codes

Weak password blasting: Weak password blasting verification for some commonly used ports

Plug-in scan: Determine the fingerprint and perform a specified POC scan. When the fingerprint scan cannot be performed, a complete POC scan is performed.

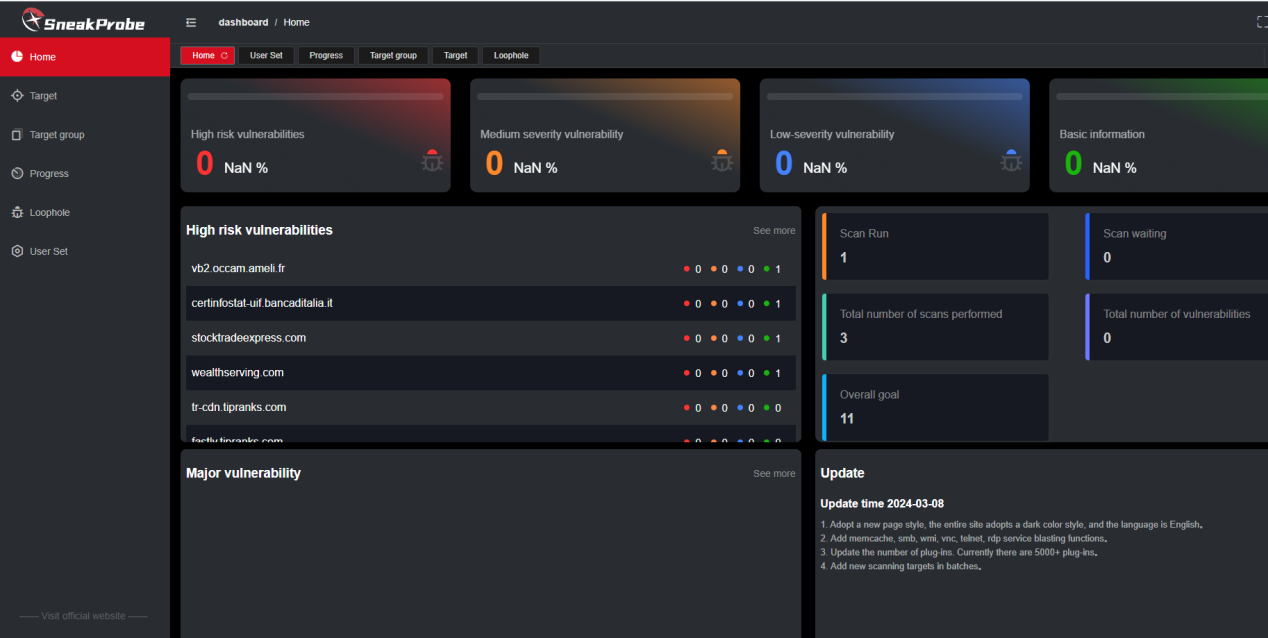
#### 0x02 Sneakprobe scanner features:

1. Adopt a new page style, the entire site adopts a dark color style, and the language is English
2. Has memcache, smb, wmi, vnc, telnet, rdp service blasting functions
3. Number of plug-ins, currently there are 5,000+ plug-ins
4. Add scan targets in batches
5. Customize what to scan
6. Database blasting, including MSSQL, ftp, orcale, postgresql

#### 0x03 User Manual:

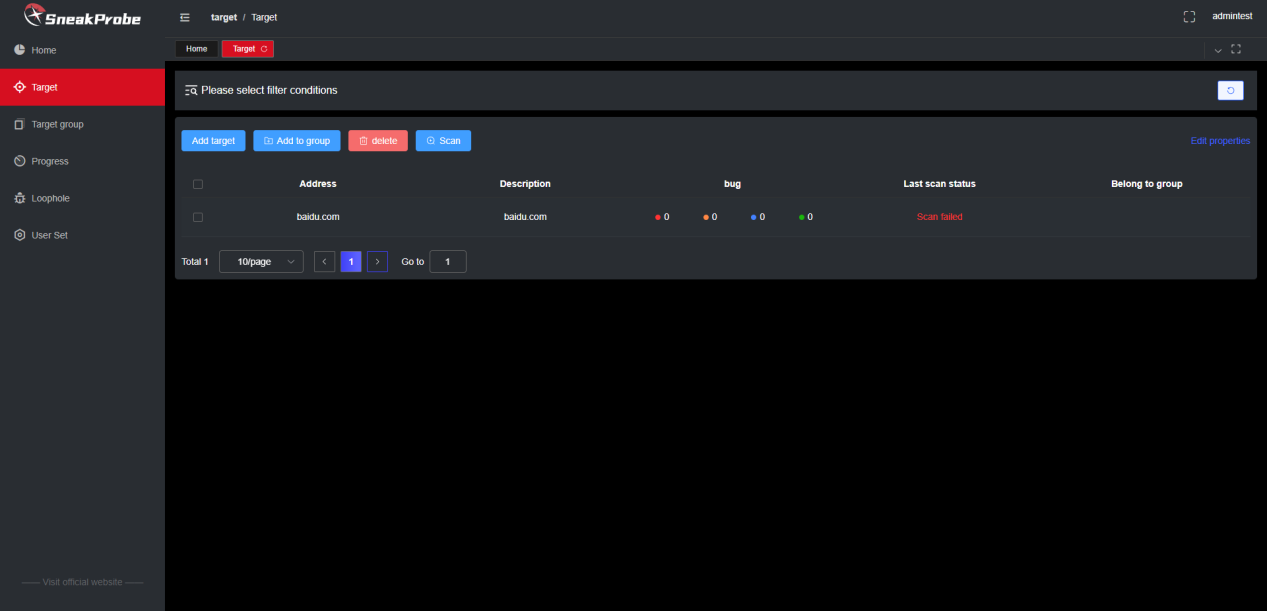
If you do not have an account, please click " Register " to register as a user. Registration is currently open and there is no invitation code, email or mobile phone verification.

1. Home



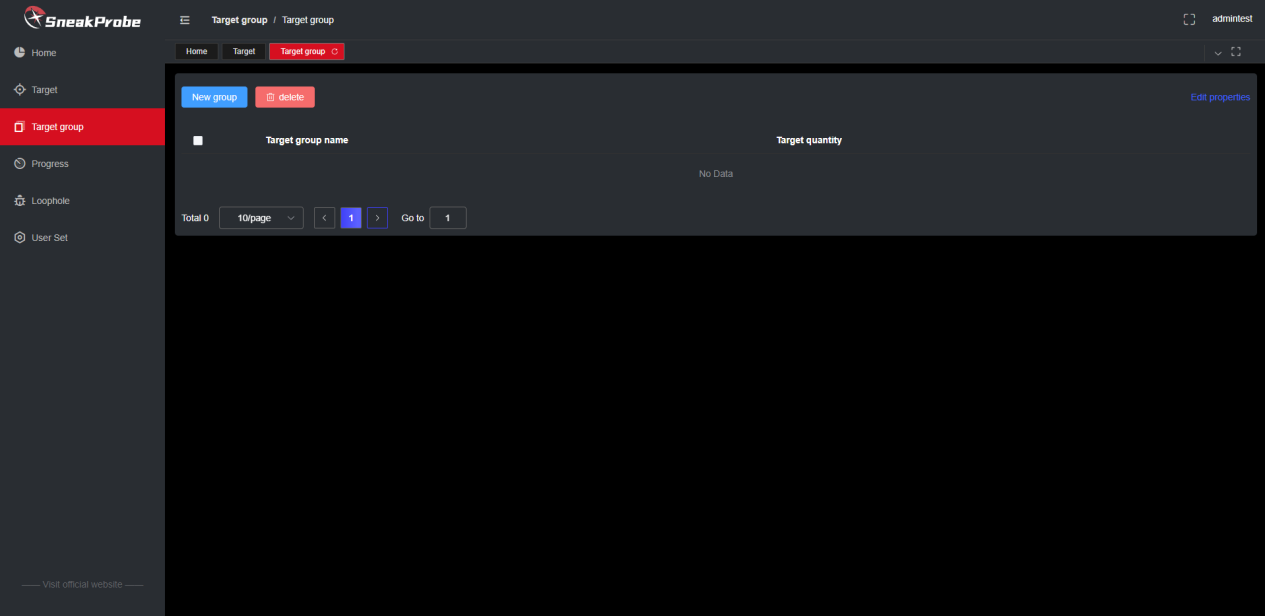
After logging in, there is a menu bar on the left, including Home , Target , Target group , Progress , Loophole , and User Set . On the right is the approximate number of vulnerability data, etc., which can be clearly seen visually.

1. Target



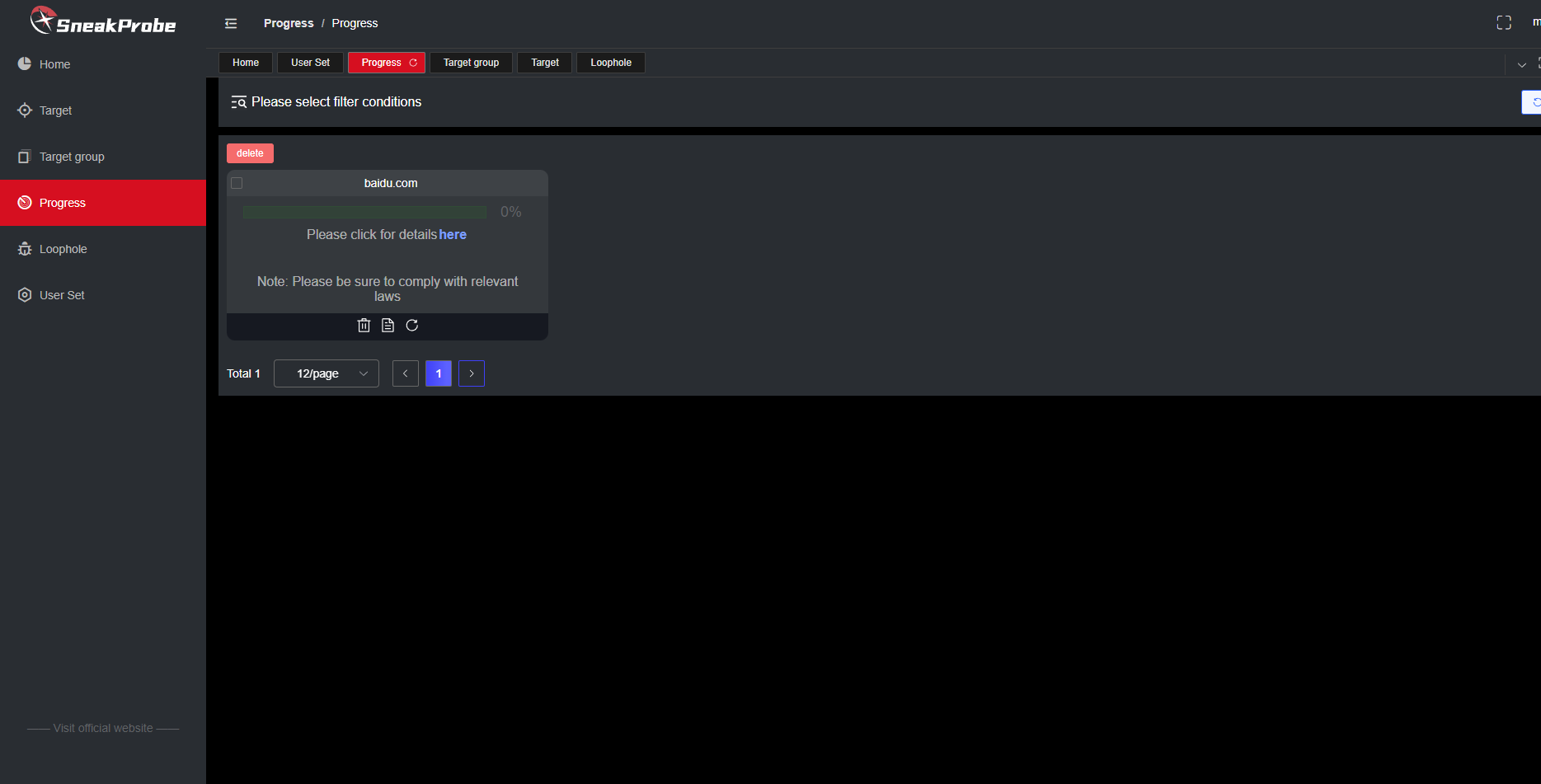
The right side of the target column is mainly used to add targets, start scanning, etc. Easy to operate

1. Target group

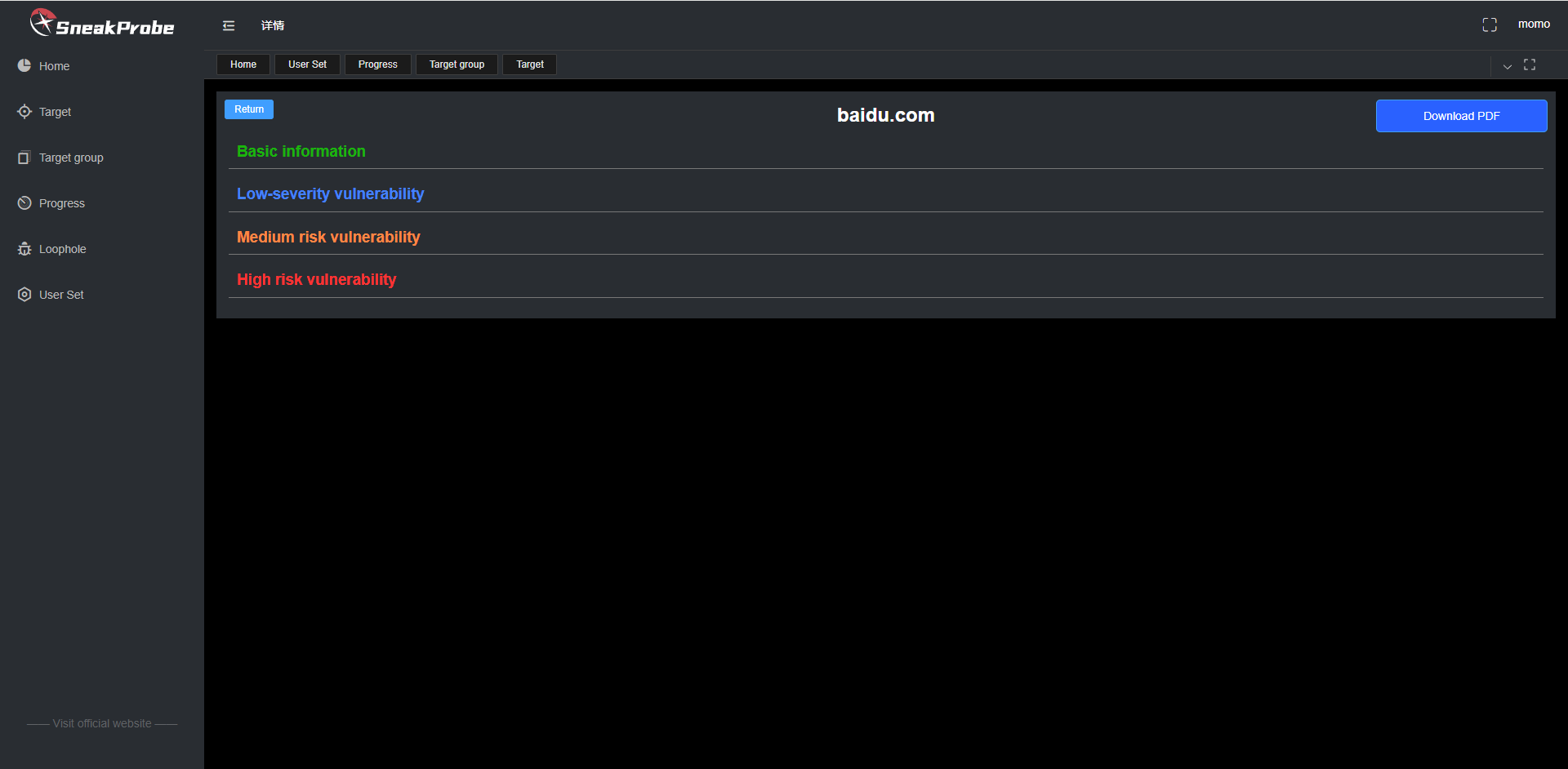


In the target group, you can classify your targets and then scan this category.

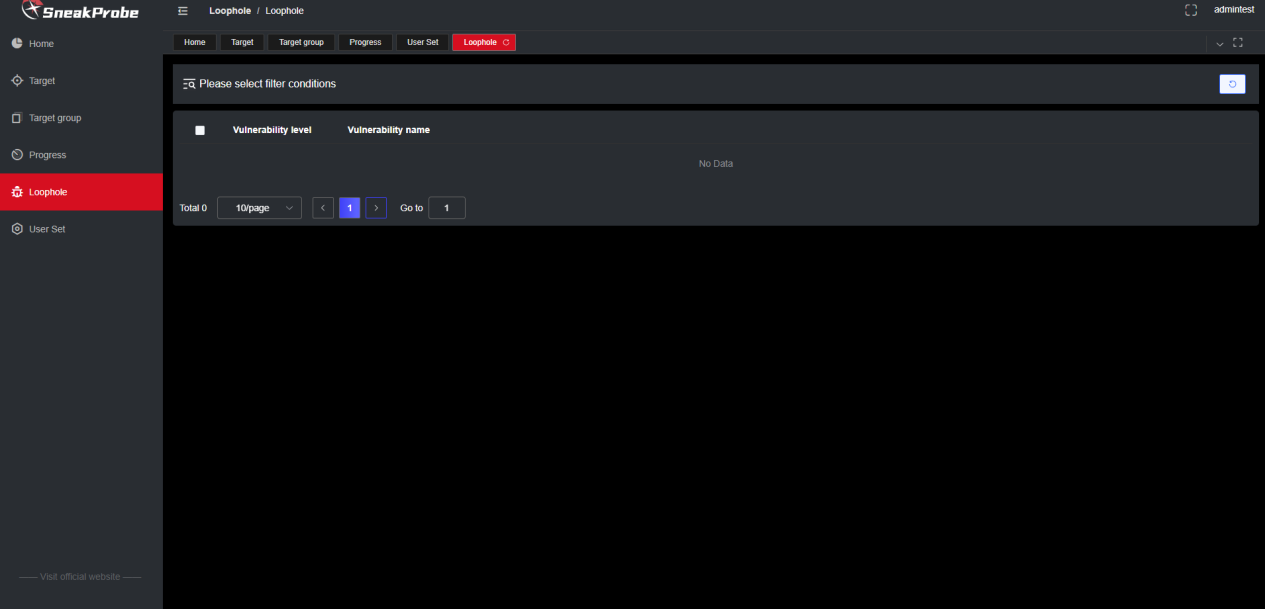
1. Progress



On the right side of the progress, you can see some progress in vulnerability scanning of the target, so you can know whether you are still in the scanning stage. When you click on the report icon or details, you can see some details of the vulnerability.

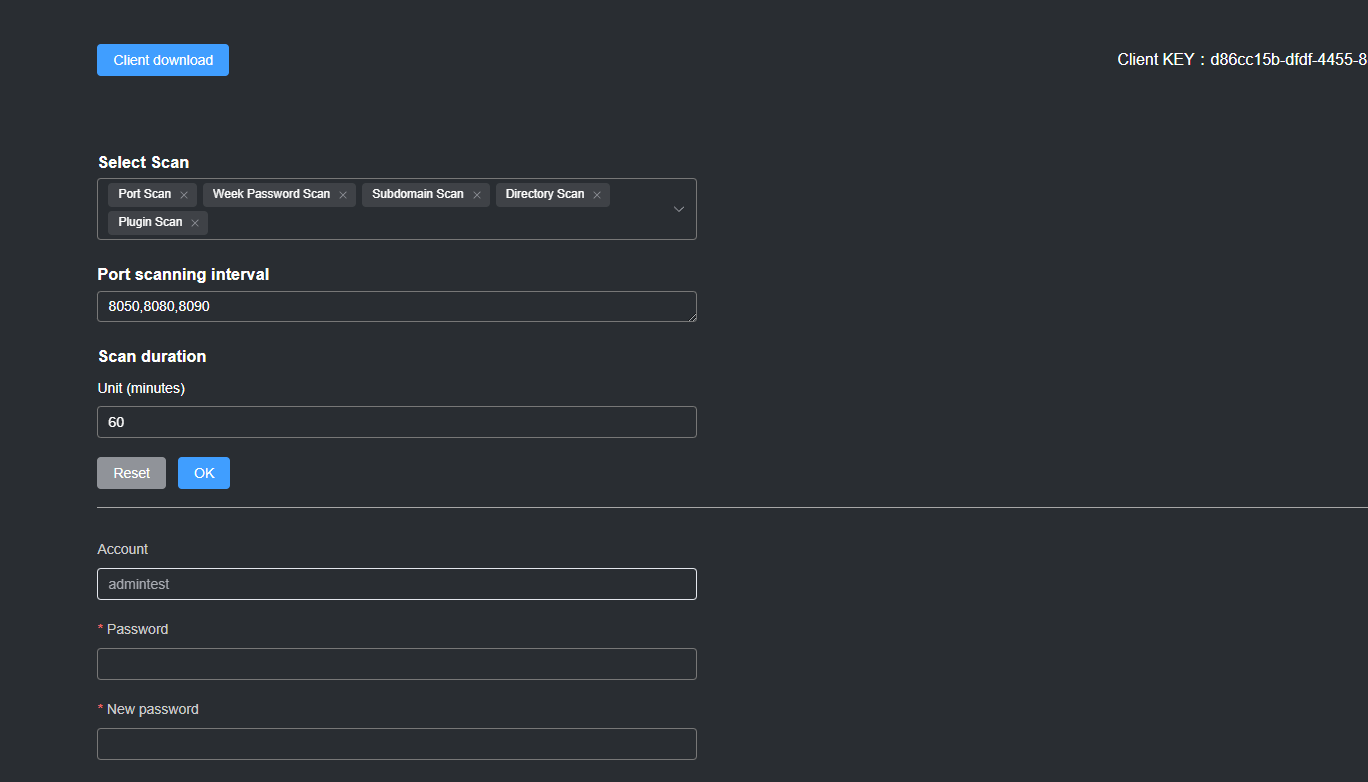


1. Loophole



Here is a rough classification of vulnerabilities, the level and quantity of vulnerabilities.

1. User Set



User settings are mainly the selection of these scans. For example, if you only want to select port scan, then select port scan. The port range is also chosen by you. The scanning time is mainly used for some network problems. When the scanning time of a target exceeds the set default 60 minutes, the scanning of this target will be ended directly, reducing the need for the client to Some consumption of the machine, etc.

Below is the user's password reset

There is a client at the top, currently only compiled for Linux and Windows. On the right are some service keys of the web side that the client connects to.

Next is a demonstration. After downloading the client, you can directly unzip it and see the two clients for win and linux.



Copy your unique key from the web



When the connection is returned successfully, it means that vulnerability scanning and detection can be performed. Be careful not to close the client! Once closed, all targets that are being scanned, or targets that are queued to be scanned, are deemed to have ended or failed!

#### 0x04 Technical exchange:

Our Telegram group is, welcome all newbies to join us to make progress and communicate together

Technical exchange group <https://t.me/+ctCCdrBrB_0wZjQy>

bww technology sharing channel : https://t.me/bwwtechnology