WisQuas™

Digital Footprint Discovery
& Inventory Asset Analysis

Lost Rabbit Labs™

https://lostrabbitlabs.com
info@lostrabbitlabs.com   (904) 513-1337

What is WisQuas?

The WisQuas engine attempts to reveal that which may be hidden, through slight fuzzing, enumeration, and fingerprinting around your entire domain and its web services ('Digital Footprint Discovery and Inventory'). Using a small number of web requests, WisQuas attempts to identify areas of weakness around Information Disclosures, Security and Service Misconfigurations, Default Installations, Missing Input Sanitization, and more. Hidden web containers granting access to Shadow VHosts and localhost data, are detected along with WAF bypassing payloads, Host Header Manipulations, successful VERB Tampering, and User Agent redirection. DNS anomalies and Domain Shadowing may also be detected across a domain.

How Does WisQuas Work?

When a domain name is submitted to WisQuas, an initial Whois Lookup on the domain is performed, and all associated domain names are collected for further inspection and analysis. All subdomains will be collected for scanning on discovered web services, using custom HTTP request settings and payloads. Once all crawls have completed you may now search all saved data using our custom **Rabbit Query Language (RQL)**. **RQL** is Lucene based, with some additional custom search parameters and scoring methods to increase likelihood of retrieving legitimate findings versus false positive findings. Our goal is to decrease noise-to-signal ratio, and increase the amount of actionable intelligence provided by WisQuas.

What makes WisQuas unique?

WisQuas allows an analyst to quickly gather incredible amounts of information about a domain's digital web assets and search through that data found in our **Report View** and **Query View**. Our custom **Rabbit Query Language (RQL)** and enriched user interfaces allows an analyst to effectively find multiple needles amongst the haystack of data to look for any misconfigurations, anomalys, and potential security vulnerabilities. Our tool allows you, the security researcher/analyst/executive, to learn about what your domain really looks like under the hood and how the overall health appears at that moment in time.

Where Can I Sign Up?

wisquas.lostrabbitlabs.com/signup

Is There A Manual?

lostrabbitlabs.com/manual-how-to

Where Can I Learn More?

lostrabbitlabs.com/wisquas

Join Our Discord!

discord.gg/YYRvxnCGFk

Follow Us On Twitter!

twitter.com/lostrabbitlabs

Follow Us On LinkedIn!

linkedin.com/company/lost-rabbit-labs/

Rabbit Query Language (RQL) & Data Structures

WISQUAS SEARCH DATA	*PARAMETERS*	*RQL EXAMPLES*
Baseline Request Data This is the original request to a domain name or host. You can search this request based on status, title, server name.	**baseline.status:** **baseline.title:** **baseline.server:**	You MUST use the ***payload*** parameter to start a baseline query and optionally use ***url*** to search baseline requests (due to how WisQuas currently stores data). **payload:. url:login baseline.title:login** **payload:. url:. baseline.title:”IIS Windows Server”** **payload:. baseline.title:tomcat**
Payload Request Data After the baseline request, 88 more requests are performed using a predefined list of files, dictionaries, and non-standard characters.	**payload:** **ps:**min_val,max_val (values must be between 0 and 83)	*Payload value may be a period (.) for a wildcard or one of the predefined payloads (full list below).* **payload:. status:200 ps:1,15** **payload:server-status url:. title:$”Apache Stat”** **payload:”/” status:500 baseline.status:!200** **payload:phpinfo.php title:”phpinfo()”**
HTTP Verb Request Data Additionally, several HTTP verbs are enumerated and results are stored here.	**verb:**	*Verb value may be a period (.) for wildcard or one of the predefined HTTP Verbs.* **verb:trace status:200 length:99,999999** **verb:post status:200 title:content** **verb:. title:error** **verb:connect title:”Index of /”**
Host Header Request Data Also enumerated are 9 host headers that commonly reveal available Shadow VHosts and default web containers.	**host:**	*Host value may be a period (.) for wildcard or one of the predefined Host Header values.* **host: 127.0.0.1 status:200 title:welcome** **host:127.0.0.1 status:200 title:upload** **host:localhost status:200 baseline.status:!200** **host:. status:200 title:login baseline.status:!200**
User-Agent Request Data Additionally, 12 other user-agents are enumerated and results are stored here.	**ua:**	*User-Agent value may be a period (.) for a wildcard or one of the predefined User-Agent values.* **ua:Mozilla status:!200** **ua:Wget status:500** **ua:curl status:500** **ua:Googlebot status:500**
HTTP Header Request Data HTTP Headers are found and stored here once a scan has completed.	**header:** **header.*name*:**	*Header value may be a period (.) for a wildcard or any header you can think of finding.* **header:"x-pingback"** **header:set-cookie** **header:”x-ms-server-fqdn”** **header:”x-powered-by”** **header.set-cookie:ASP** **header.x-powered-by:”ASP.NET”** **header.x-xss-protection:0**

Parameter values listed below are based on the default WisQuas fuzzing list and configuration.
If a custom fuzz list was used for the scan, those values can be used instead along with the corresponding parameters.

RQL - Default Payload Queries

payload:/
payload://
payload:robots.txt
payload:index.html
payload:index.htm
payload:index.shtml
payload:index.php
payload:index.jsp
payload:index.asp
payload:index.aspx
payload:default.asp
payload:default.aspx
payload:home.asp
payload:home.aspx
payload:aspnet_files/
payload:aspnet_client/
payload:web.config
payload:trace.axd
payload:xyz/abc
payload:test/
payload:code/
payload:admin/
payload:temp/
payload:tmp/
payload:uploads/
payload:bin/
payload:files/
payload:webdav/
payload:manager/
payload:logs/
payload:ghost/
payload:jmx-console
payload:phpMyAdmin/
payload:INSTALL.mysql.txt
payload:INSTALL.txt
payload:UPGRADE.txt
payload:LICENSE.txt
payload:LICENSE
payload:wp-login.php
payload:README
payload:WEB-INF/
payload:server-status
payload:server-info
payload:config.php
payload:xmlrpc.php
payload:sitemap.xml
payload:login.php
payload:console
payload:status
payload:error
payload:phpinfo.php
payload:info.php
payload:access_log
payload:php.ini
payload:.git
payload:.git/
payload:.git/HEAD
payload:.htaccess
payload:.htpasswd
payload:mysql_history
payload:.bashrc
payload:.ssh
payload:.history
payload:.passwd
payload:.hta
payload:?id=0
payload:api/
payload:%
payload:%%
payload:&
payload:script
payload:cgi-bin
payload:webmail
payload:nginx_status
payload:?url=
payload:redirect
payload:{
payload:}
payload:%2f
payload:%7b
payload:`
payload:1’=1
payload:~
payload:Flood
payload:%00
payload:package.json
payload:elmah.axd
payload:public/

RQL - Default HTTP Verb Queries

verb:OPTIONS
verb:GET
verb:TEST
verb:POST
verb:PUT
verb:TRACK
verb:PATCH
verb:HEAD
verb:TRACE
verb:DELETE
verb:CONNECT

RQL - Default Host Header Queries

host:localhost
host:127.0.0.1
host:root
host:127.0.1.1
host:null
host:test
host:0
host:-1
host:admin

RQL - Default User-Agent Queries

ua:Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/79.0.3945.0 Safari/537.36
ua:Mozilla/5.0 (Linux; U; Android 4.4.2; en-us; SCH-I535 Build/KOT49H) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30
ua:Mozilla/5.0 (Linux; Android 9; SM-G955U) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.93 Mobile Safari/537.36
ua:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.1439
ua:Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)
ua:Mozilla/5.0 (compatible, MSIE 11, Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
ua:Mozilla/5.0 (iPad; CPU OS 8_4_1 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12H321 Safari/600.1.4
ua:Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_1 like Mac OS X) AppleWebKit/603.1.30 (KHTML, like Gecko) Version/10.0 Mobile/14E304 S
ua:Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
ua:Mozilla/5.0 (Linux; Android 7.0; HTC 10 Build/NRD90M) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.83 Mobile Safari
ua:curl/7.35.0
ua:Wget/1.15 (linux-gnu)

RQL - Typical HTTP Header Queries

header:content-encoding
header:x-content-type
header:set-cookie
header:etag
header:x-xss-protection
header:strict-transport-security

WisQuas Arcade

The WisQuas Arcade aims at providing an entertaining arcade gaming experience to the user by scoring successful findings based on the scan the user ran and awards them points based on those successful findings. Everytime you run a scan, you will consume one of your credits. The ‘My Account’ section in your WisQuas account shows exactly what findings you have found and how many points have been earned in that category. The breakdown of the categories and the points associated with those categories can be found below.

FINDING CATEGORY	*POINTS GIVEN*
Directory Listings	+ 1000
Docker Containers	+ 500
Bypasses - 2f 7b //	+ 700
IOC - Hacked/Breached/Compromised	+ 2500
Web Config/Status Disclosure	+ 800
Titles of Interest	+ 800
Apache Sling	+ 800
API & Endpoints	+ 500
FTP & Files	+ 500
GIT Disclosures	+ 350
Wordpress	+ 500
LINUX/UNIX Disclosures	+ 800
Default Install	+ 500
Python SimpleHTTP/Console	+ 750
PHP	+ 500
Errors from Bypass	+ 700
Errors & Exceptions	+ 100
Frameworks & Software	+ 100
Admin & Login	+ 500