



**WisQuas™**

Digital Footprint Discovery  
& Inventory Asset Analysis

**Lost Rabbit Labs™**

<https://lostrabbitlabs.com>  
[info@lostrabbitlabs.com](mailto: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, anomalies, 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](https://wisquas.lostrabbitlabs.com/signup)

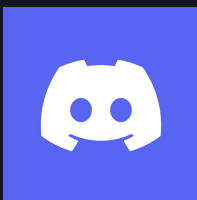
### Is There A Manual?

[lostrabbitlabs.com/manual-how-to](https://lostrabbitlabs.com/manual-how-to)

### Where Can I Learn More?

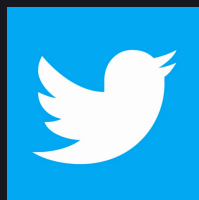
[lostrabbitlabs.com/wisquas](https://lostrabbitlabs.com/wisquas)

### Join Our Discord!



[discord.gg/YVRvxnCGFk](https://discord.gg/YVRvxnCGFk)

### Follow Us On Twitter!



[twitter.com/lostrabbitlabs](https://twitter.com/lostrabbitlabs)

### Follow Us On LinkedIn!



[linkedin.com/company/lost-rabbit-labs/](https://linkedin.com/company/lost-rabbit-labs/)

# Rabbit Query Language (RQL) & Data Structures

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

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

## RQL - Default HTTP Verb Queries

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

## RQL - Default Host Header Queries

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

## 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/14.14393

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 Safari/602.1

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/537.36

ua:curl/7.35.0

ua:Wget/1.15 (linux-gnu)

## RQL - Typical HTTP Header Queries

header:content-encoding	header:set-cookie	header:x-xss-protection
header:x-content-type	header:etag	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.

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