

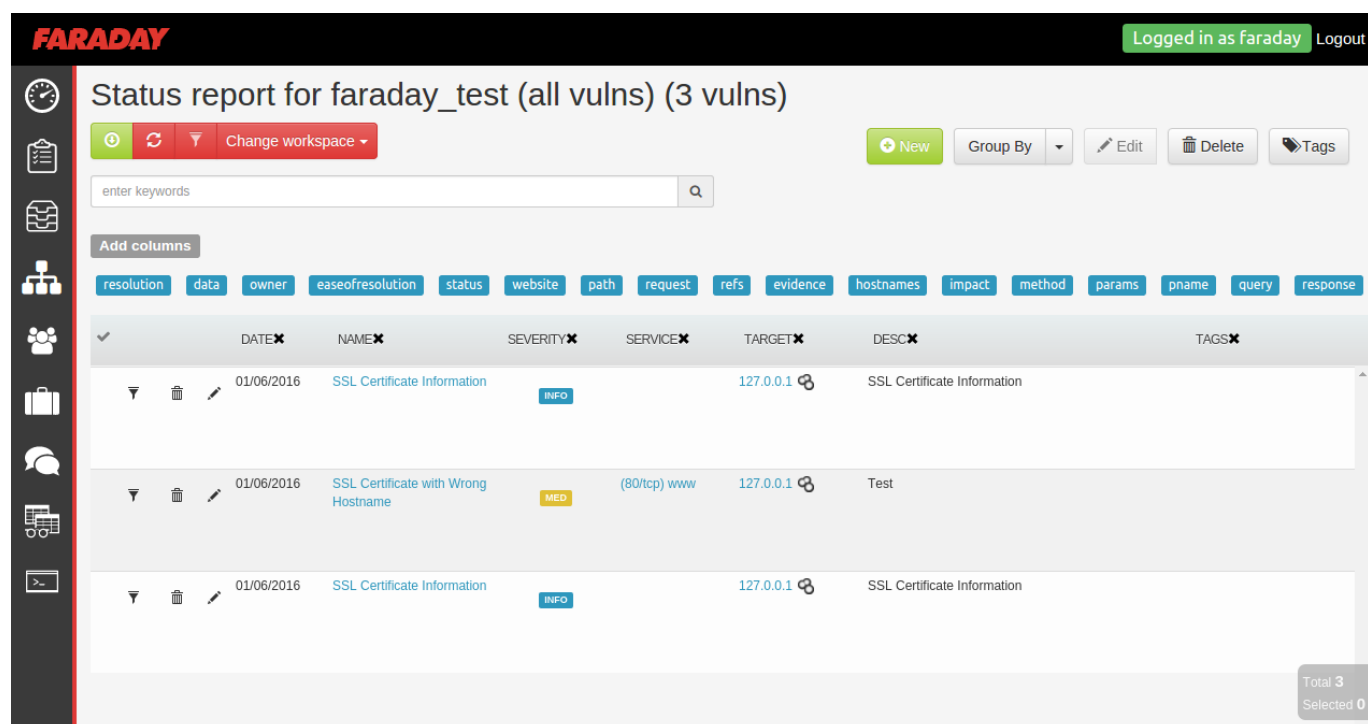
- Commercial version -

Tags allow you to organize your vulnerabilities. by letting you make and edit categories: environment, technology, state, language, projects, whatever. The team can then see the tagged vulnerabilities and lets you organize the security evaluation.

The tags are assigned to the team's workspace letting you use different tags for different projects.

How to tag vulnerabilities

Using the specified credentials during the configuration, from the Navigator start the session in Faraday's GUI. Once you have obtained the authentication and you are in, click on the "Status Report" icon.



The screenshot displays the Faraday GUI interface. At the top, the 'FARADAY' logo is on the left, and a green bar on the right indicates 'Logged in as faraday' with a 'Logout' link. A sidebar on the left contains various navigation icons. The main content area is titled 'Status report for faraday_test (all vulns) (3 vulns)'. Below the title, there are buttons for 'New', 'Group By', 'Edit', 'Delete', and 'Tags'. A search bar with the placeholder 'enter keywords' is also present. A section labeled 'Add columns' shows a list of available columns: resolution, data, owner, easeofresolution, status, website, path, request, refs, evidence, hostnames, impact, method, params, pname, query, and response. Below this, a table lists the vulnerabilities. The table has columns for DATE, NAME, SEVERITY, SERVICE, TARGET, DESC, and TAGS. Three vulnerabilities are listed, all dated 01/06/2016. The first two are 'SSL Certificate Information' (INFO severity) and 'SSL Certificate with Wrong Hostname' (MED severity). The third is 'SSL Certificate Information' (INFO severity). The table also includes icons for expand, delete, and edit for each row. At the bottom right, a summary box shows 'Total 3' and 'Selected 0'.

DATE	NAME	SEVERITY	SERVICE	TARGET	DESC	TAGS
01/06/2016	SSL Certificate Information	INFO		127.0.0.1	SSL Certificate Information	
01/06/2016	SSL Certificate with Wrong Hostname	MED	(80/tcp) www	127.0.0.1	Test	
01/06/2016	SSL Certificate Information	INFO		127.0.0.1	SSL Certificate Information	

Select the vulnerabilities that you want to tag (for example those that have to do with SSL protocol)

FARADAY Logged in as faraday Logout










Status report for faraday_test (all vulns) (3 vulns)

Change workspace New Group By Edit Delete Tags

enter keywords

Add columns

resolution data owner easeofresolution status website path request refs evidence hostnames impact method params pname query response

	DATE	NAME	SEVERITY	SERVICE	TARGET	DESC	TAGS
  	01/06/2016	SSL Certificate Information	INFO		127.0.0.1	SSL Certificate Information	
  	01/06/2016	SSL Certificate with Wrong Hostname	MED	(80/tcp) www	127.0.0.1	Test	
  	01/06/2016	SSL Certificate Information	INFO		127.0.0.1	SSL Certificate Information	

Total 3
Selected 2

After picking one of the vulnerabilities click on the "Tags" button

FARADAY Logged in as faraday Logout










Status report for faraday_test (all vulns) (3 vulns)

Change workspace New Group By Edit Delete Tags

enter keywords

Add columns

resolution data owner easeofresolution status website path request refs evidence hostnames impact method params pname query response

	DATE	NAME	SEVERITY	SERVICE	TARGET	DESC	TAGS
  	01/06/2016	SSL Certificate Information	INFO		127.0.0.1	SSL Certificate Information	
  	01/06/2016	SSL Certificate with Wrong Hostname	MED	(80/tcp) www	127.0.0.1	Test	
  	01/06/2016	SSL Certificate Information	INFO		127.0.0.1	SSL Certificate Information	

Total 3
Selected 2

Vulnerability TAGs

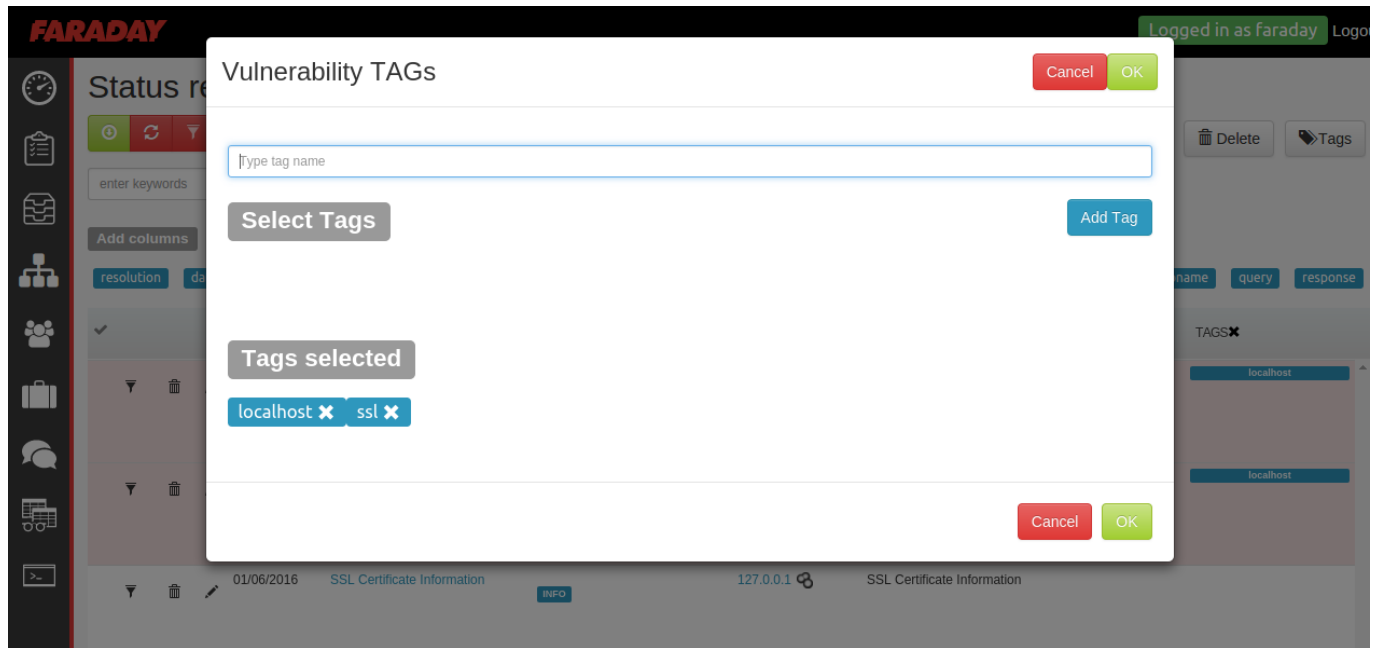
Select Tags Add Tag

Tags selected

localhost ✕

Cancel OK

Create the tag that you want (in our case SSL) and click OK



Search tagged vulnerabilities

From the Status Report you will be able to find the information using the `tags` parameter. For example: "tags:ssl" as shown in the image below.

