MENU

PENTEST COLLABORATION FRAMEWORK

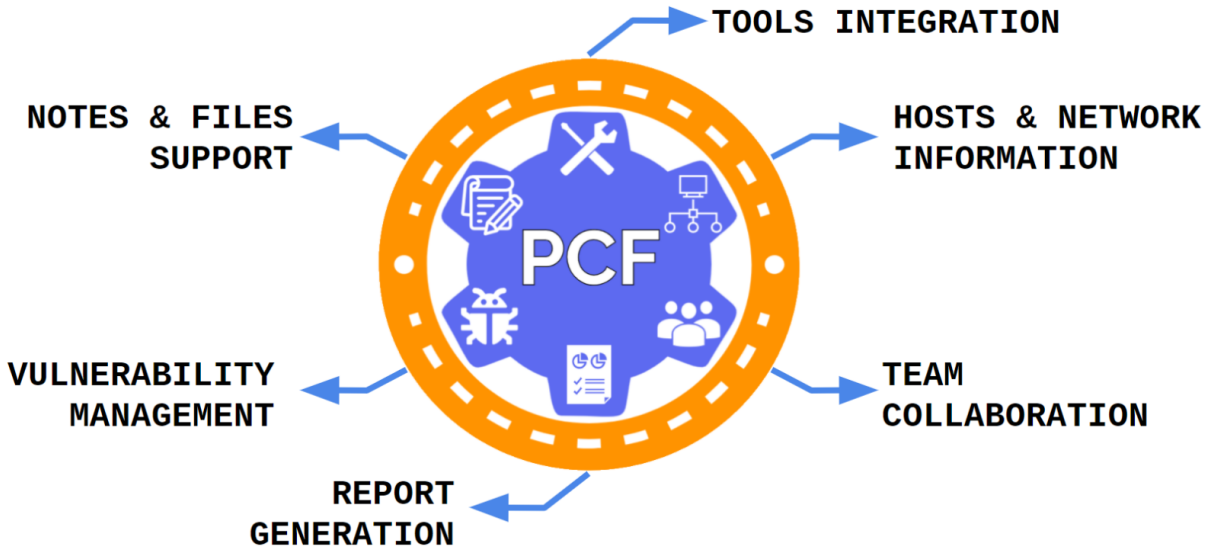
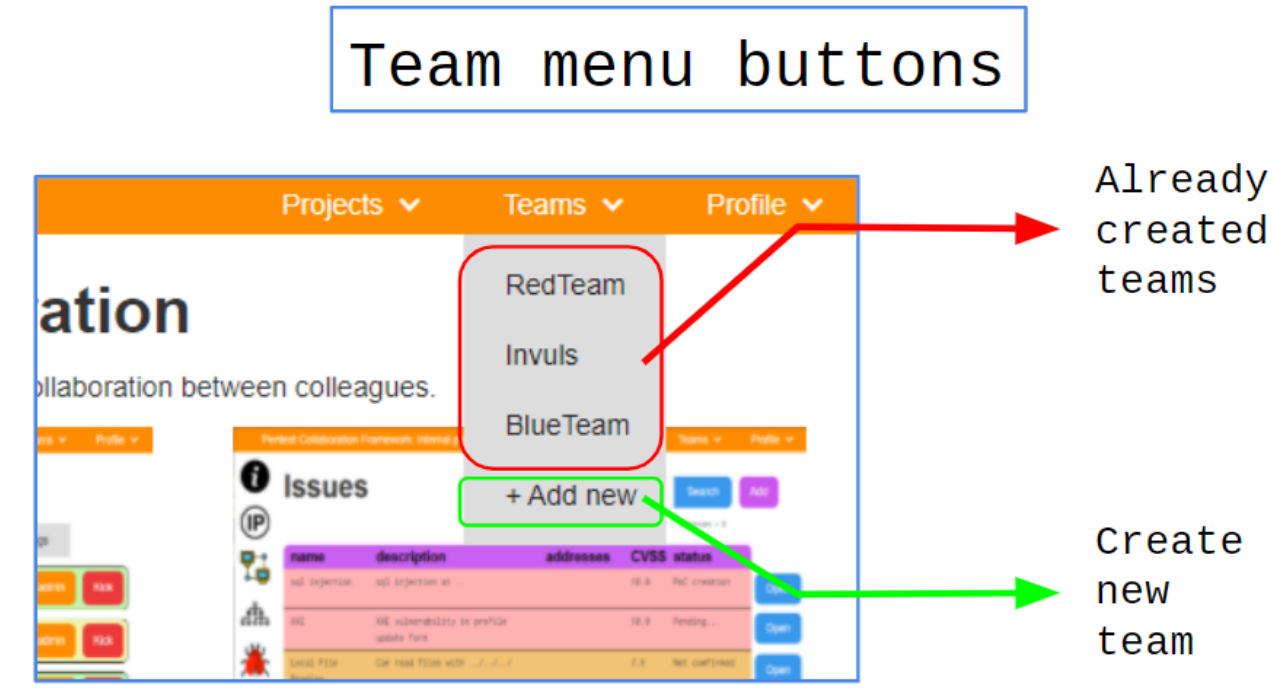


Table of Contents

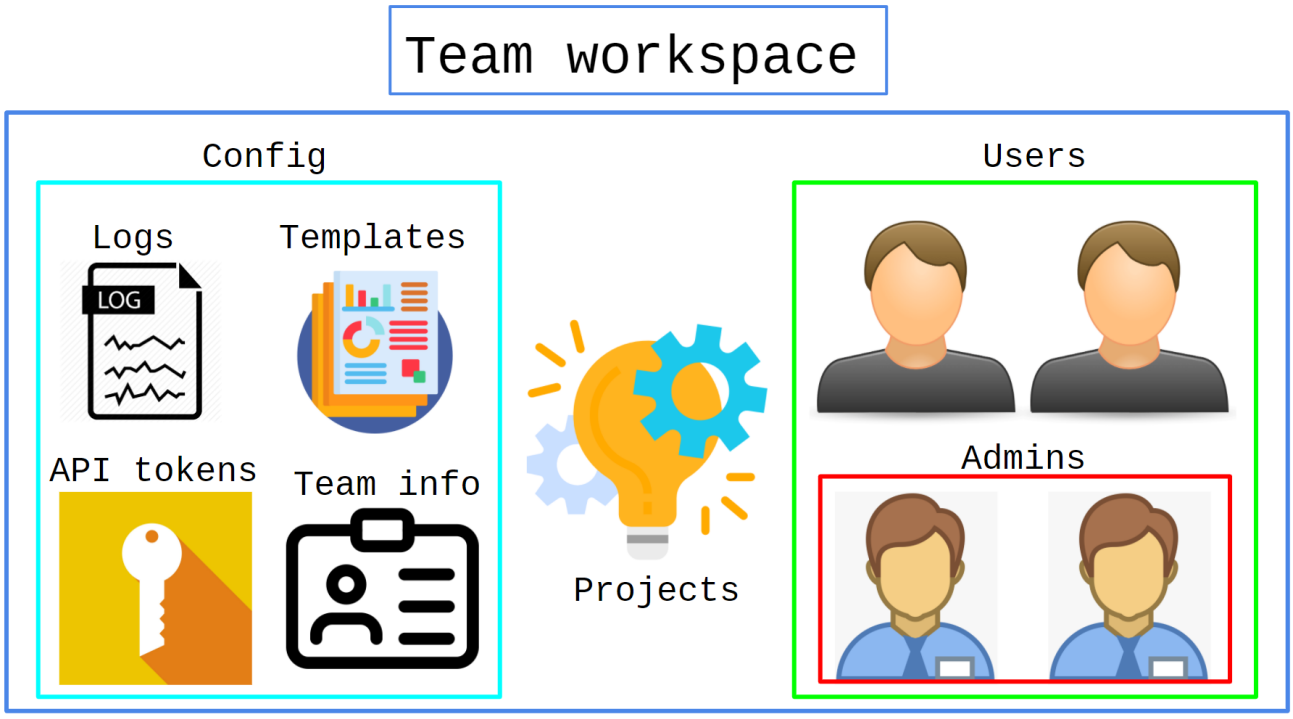
Usage

Teams



Sequencing

№	Action
1	Go to new team page
2	Create new team
3	Set team options
4	Add users to created team
5	Make some of them administrators
6	Go to Projects page!

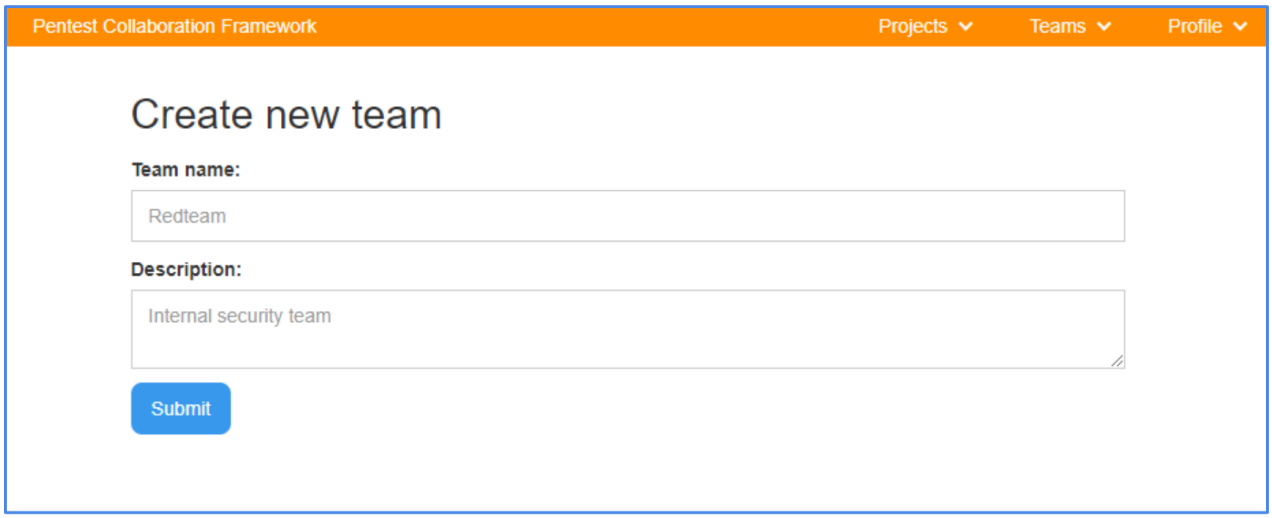


Endpoints

New Team Page

Name	Value
URL	/create_team
URL Example	-
Description	Create New Team
Capabilities	Create new team with description
Comments	Do not create teams with same name

New team page

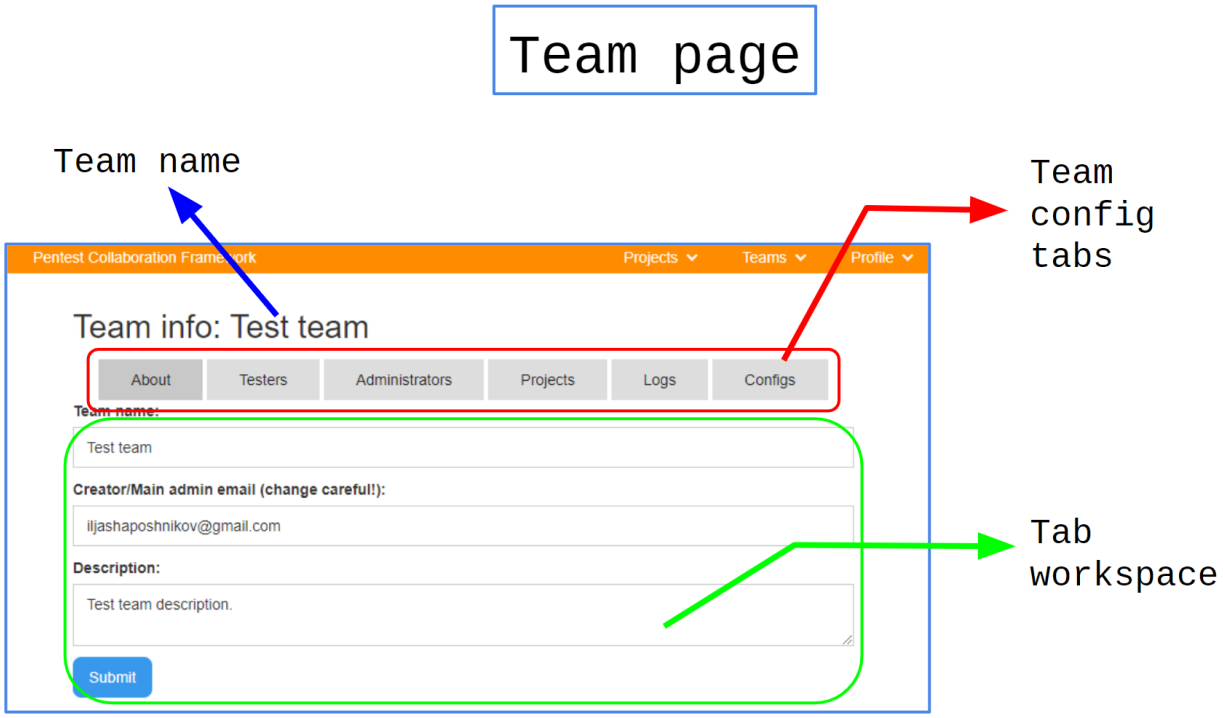


Team information

Name	Value
URL	/team/{{team_UUID}}
URL example	/team/760a3c76-2b65-4558-9f66-876a5c772c8e/
Description	Get team information
Capabilities	1. Edit team information 2. Edit team users 3. Get team projects 4. Get team logs 5. Edit team configs.
Comments	-

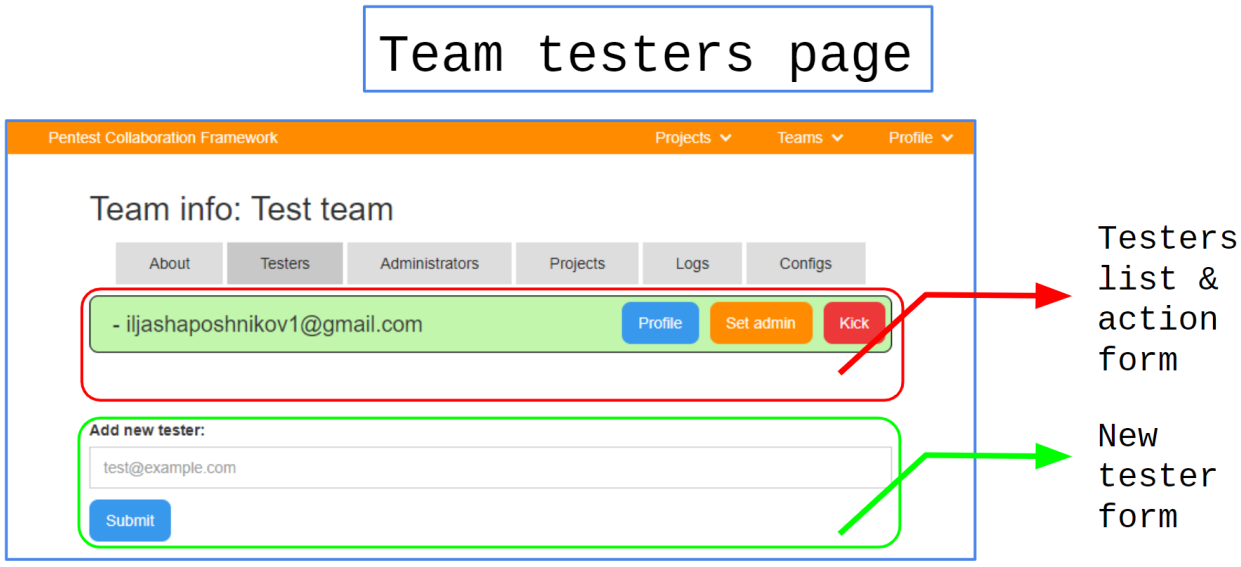
Team information: edit info

At this page you can edit team name, description and admin email.



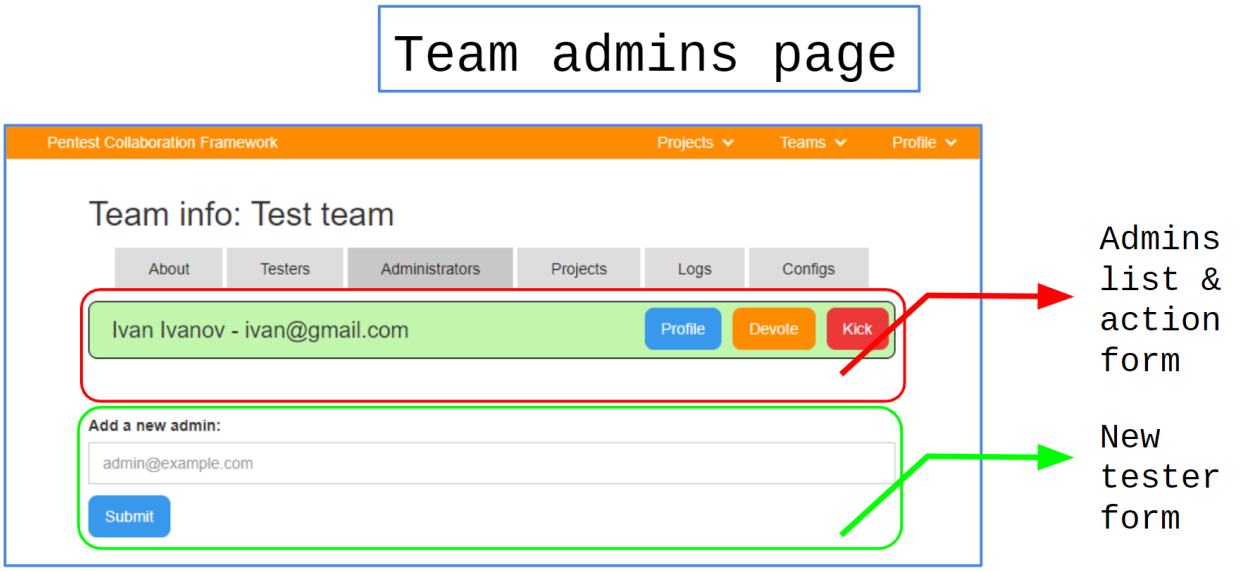
Team information: testers list

At this page you can add new testers or moderate existed.



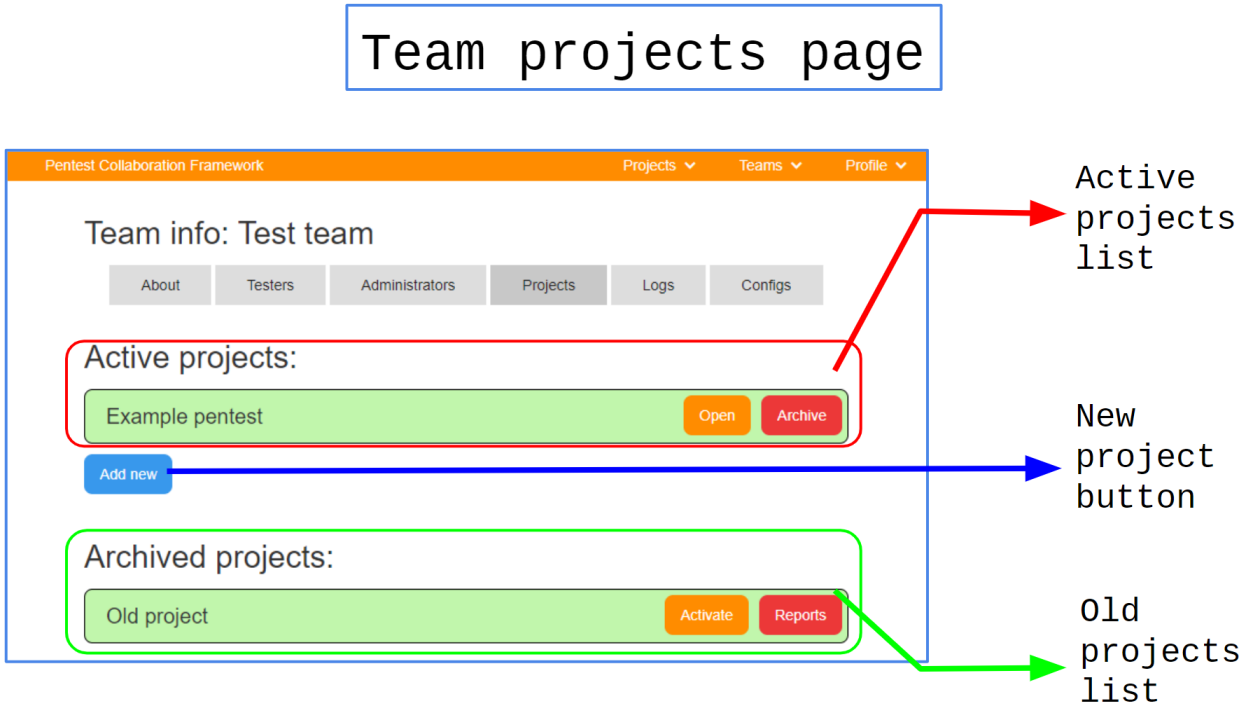
Team information: admins list

At this page you can add new administrators or moderate existed.



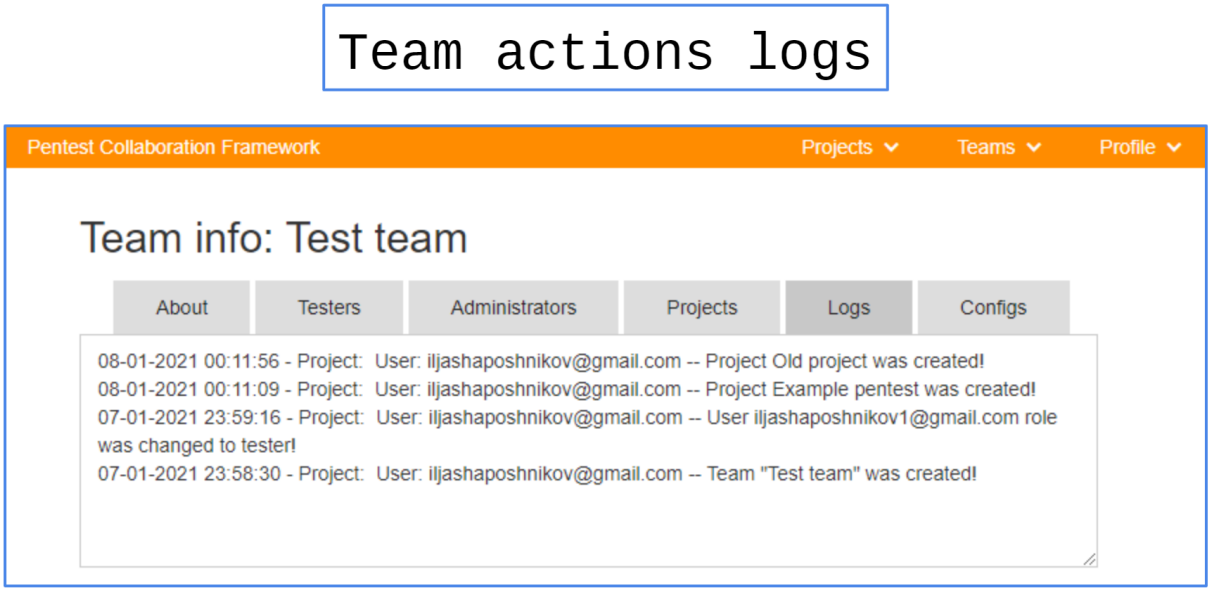
Team Information: Projects list

At this page you can add new projects or moderate existed.



Team Information: log file

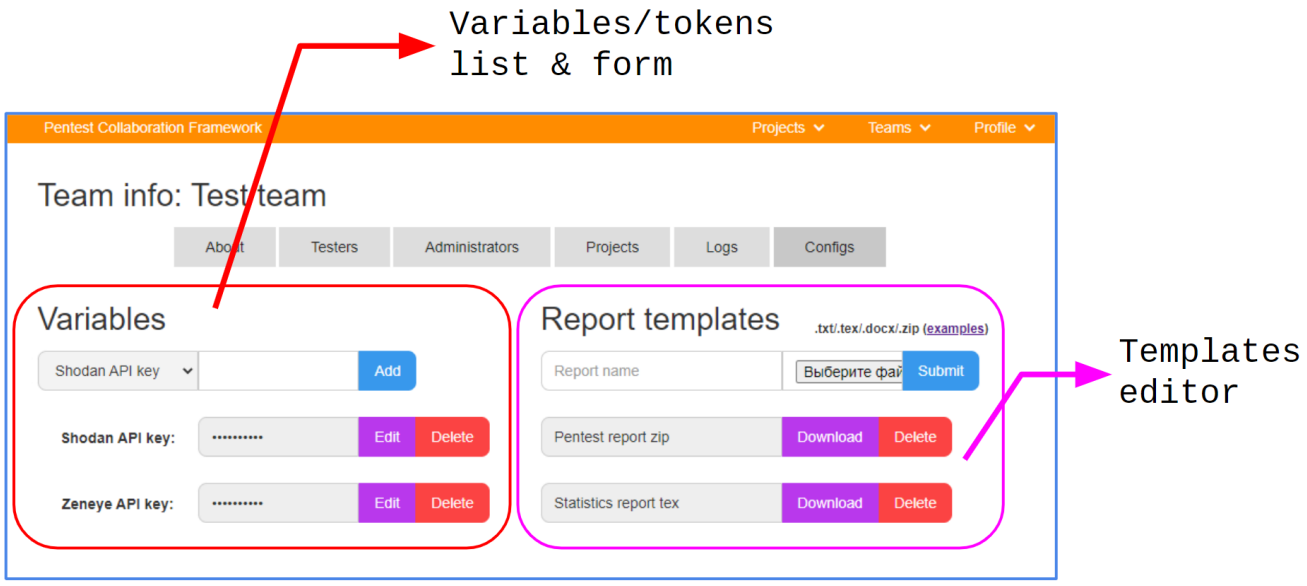
At this page you can get log of current team actions. There you can find any action of team or project teams even if initiator is not in team.



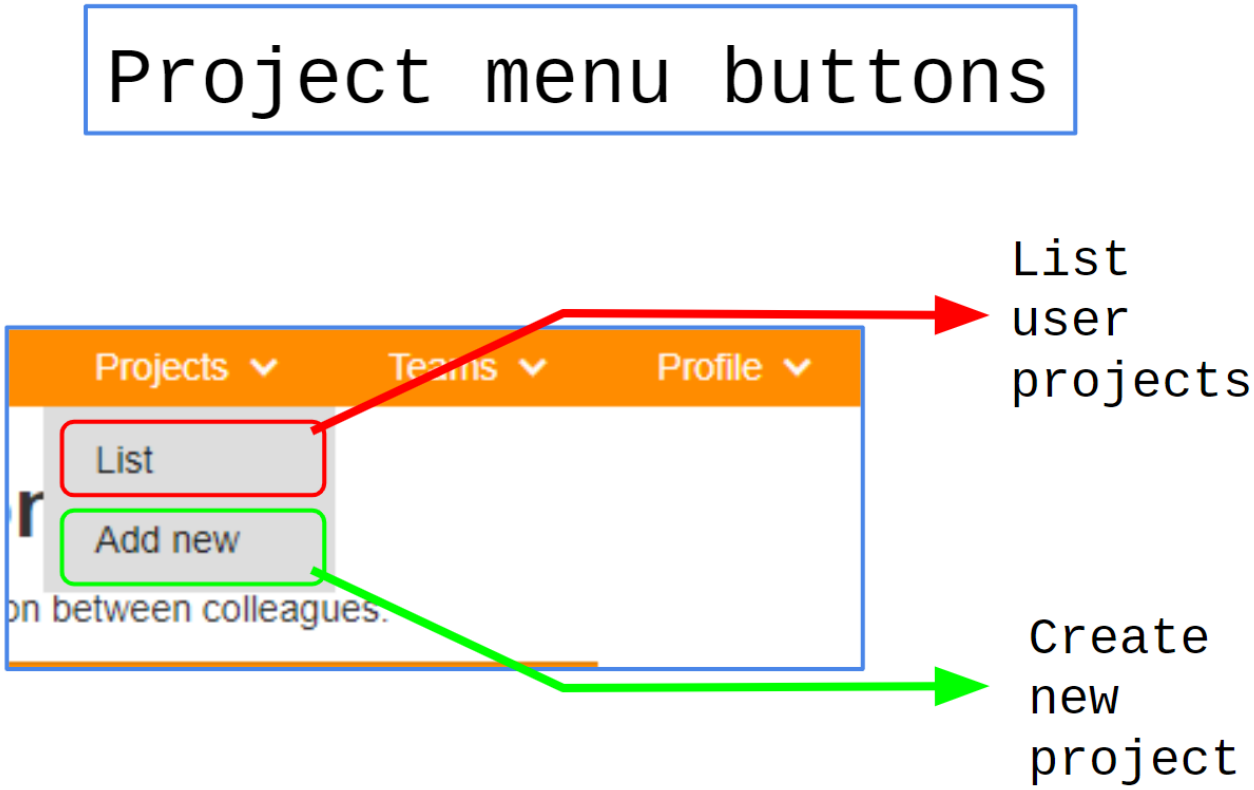
Team Information: Variables & Templates

At this page you can moderate team variables (usually API-tokens) and team report templates.

Team configs



Projects



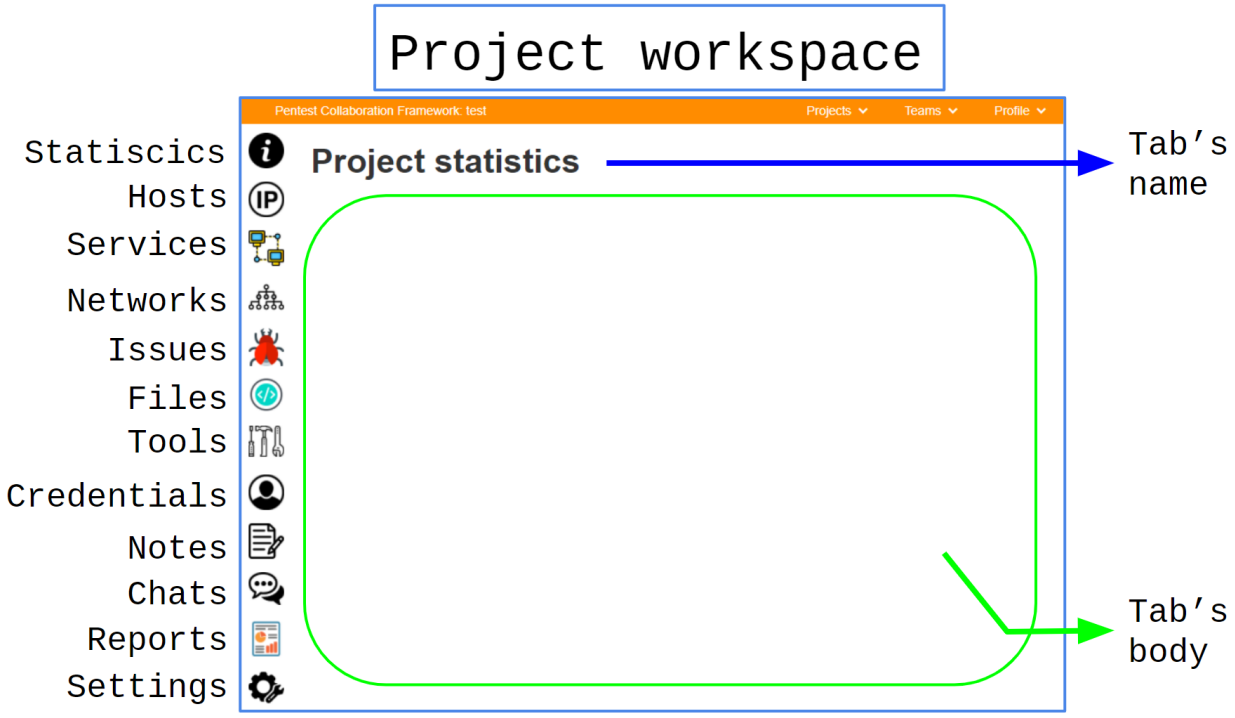
Sequencing

You need just open new project page, set project settings and press "Create" button :)

There are two types of project:

- Active - you can change them.
- Archived - you can only read them.

Project can't be removed due to security reasons, so be careful

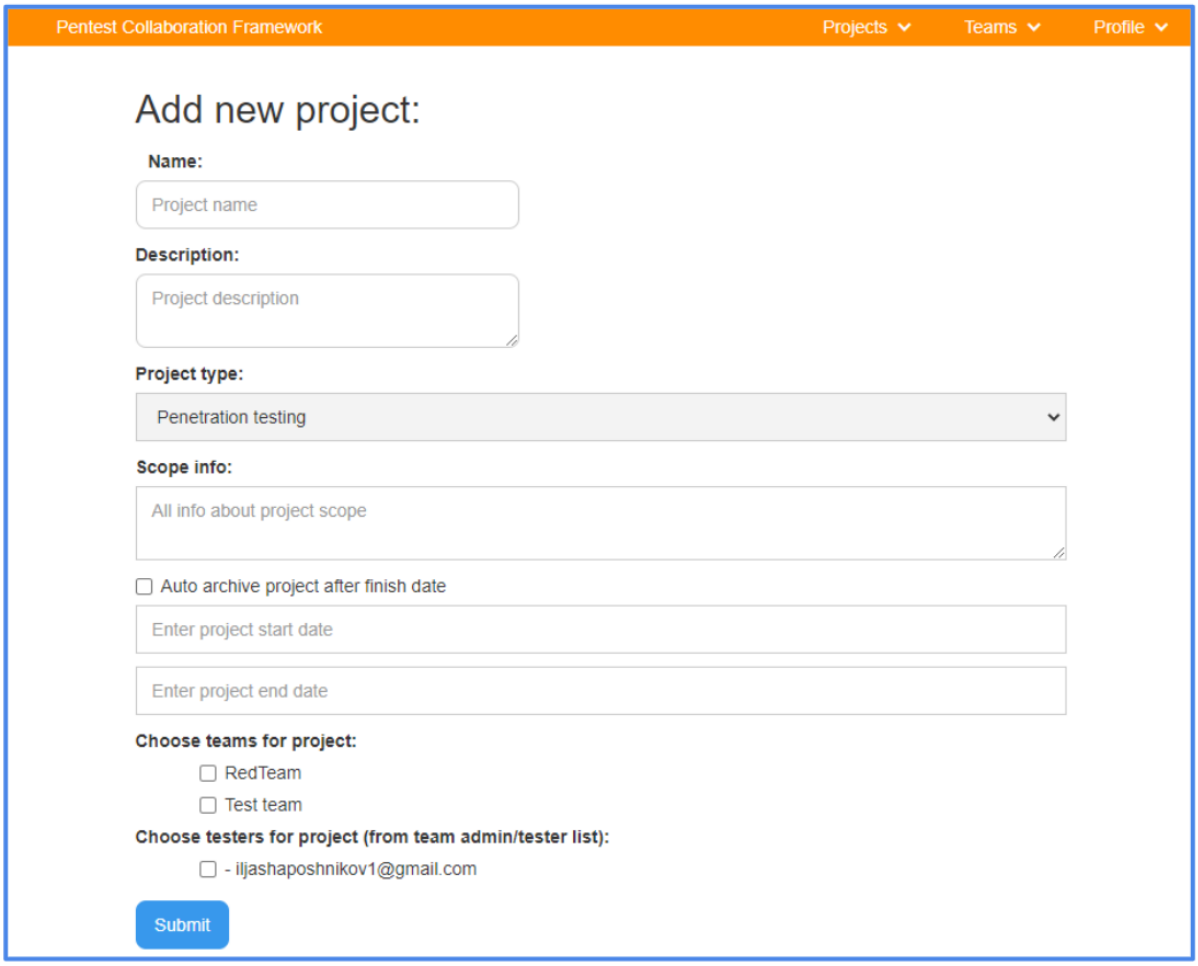


Endpoints

Project creation

Name	Value
URL	/new_project
URL Example	-
Description	Create new project
Capabilities	Create new project with name, scope, classification, level, and team lead
Comments	-

Project creation



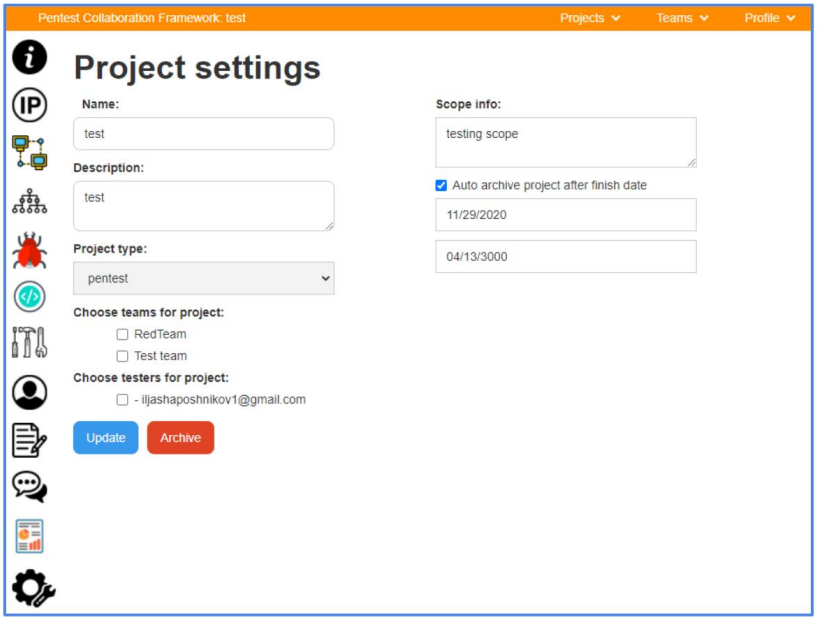
Project stats

Name	Value
URL	/project/{{project_uuid}}
URL example	/project/c7ff16f8-2dc8-4d70-b784-0a1d210ed784/
Description	Project index page
Capabilities	-
Comments	-

Project settings

Name	Value
URL	/project/{{project_uuid}}/settings
URL example	/project/c7ff16f8-2dc8-4d70-b784-0a1d210ed784/
Description	Project settings with edit form
Capabilities	Project settings with start/finish date, autoarchive, scope, description, team lead, teams, testers, classification, level, rating and more.
Comments	-

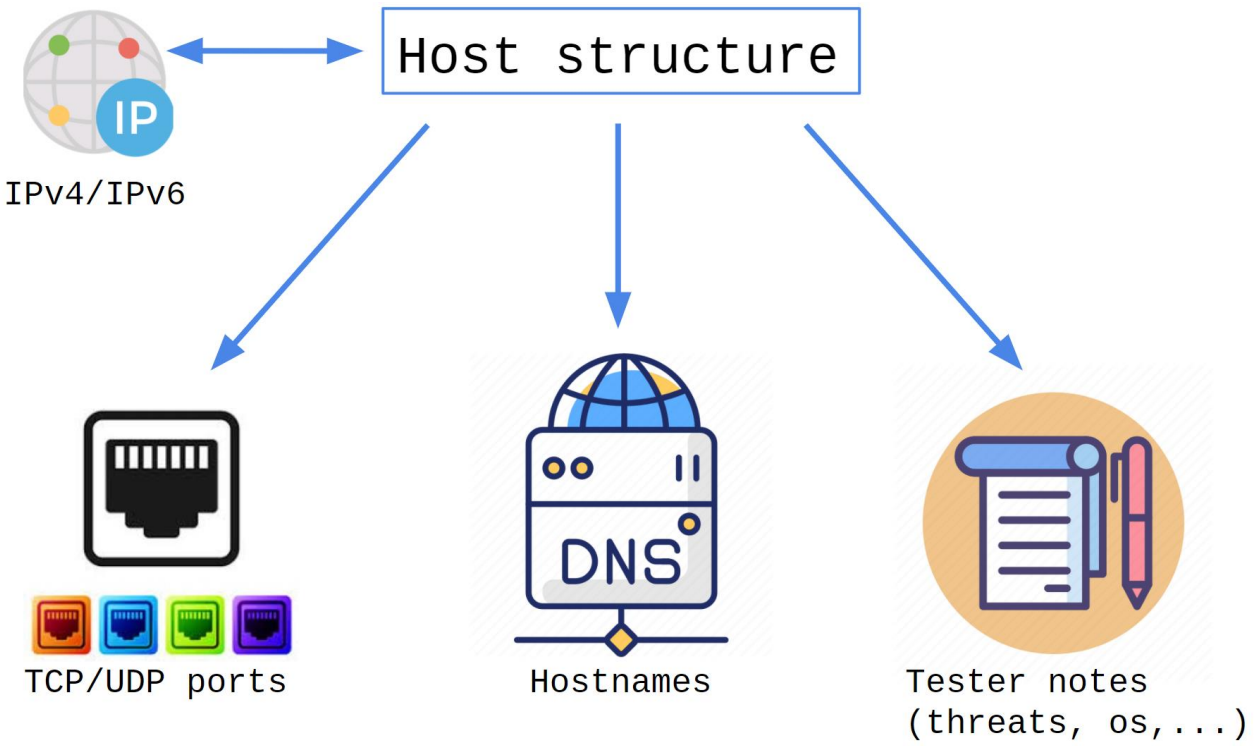
Project settings



Hosts

Sequencing

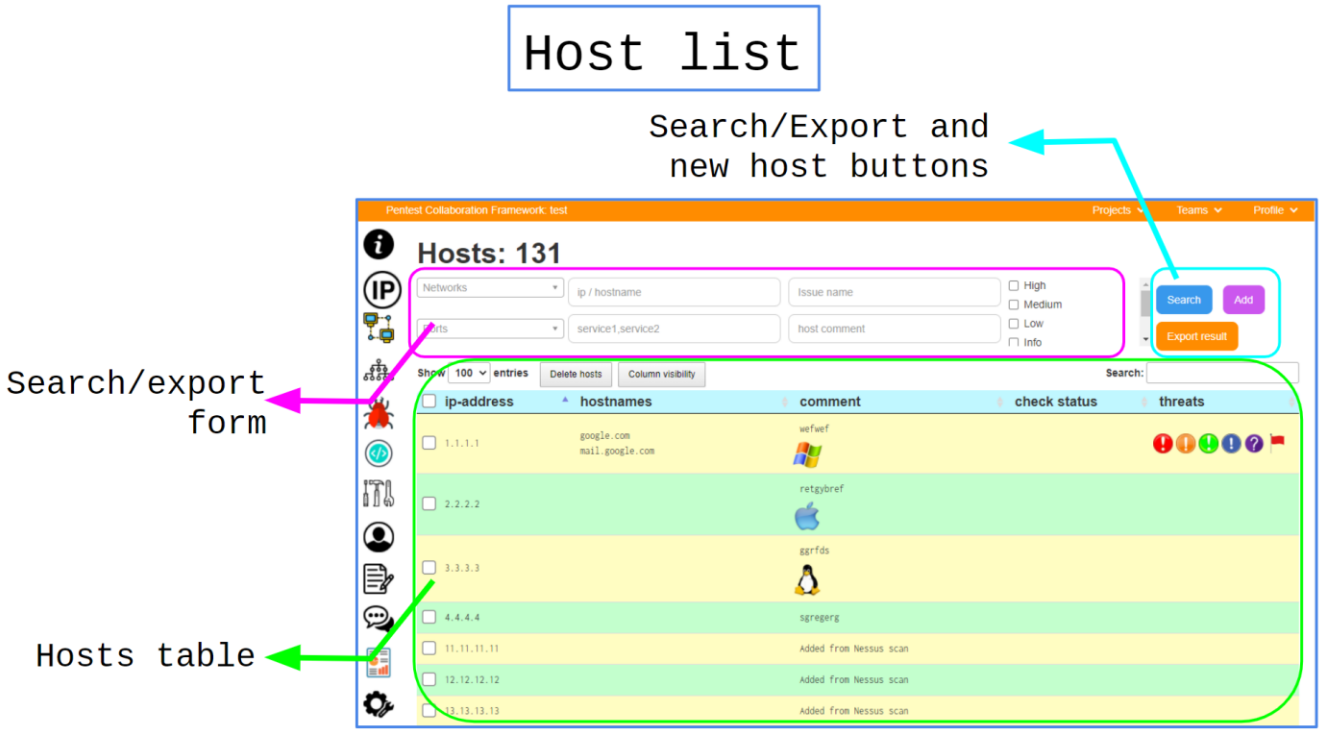
No	Action
1	Open project hosts page
2	Open new host form
3	Create new host
4	Open created host page
5	Add ports to host
6	Add hostnames
7	(optional) Add host issues, credentials
8	Change host information



Endpoints

Hosts list

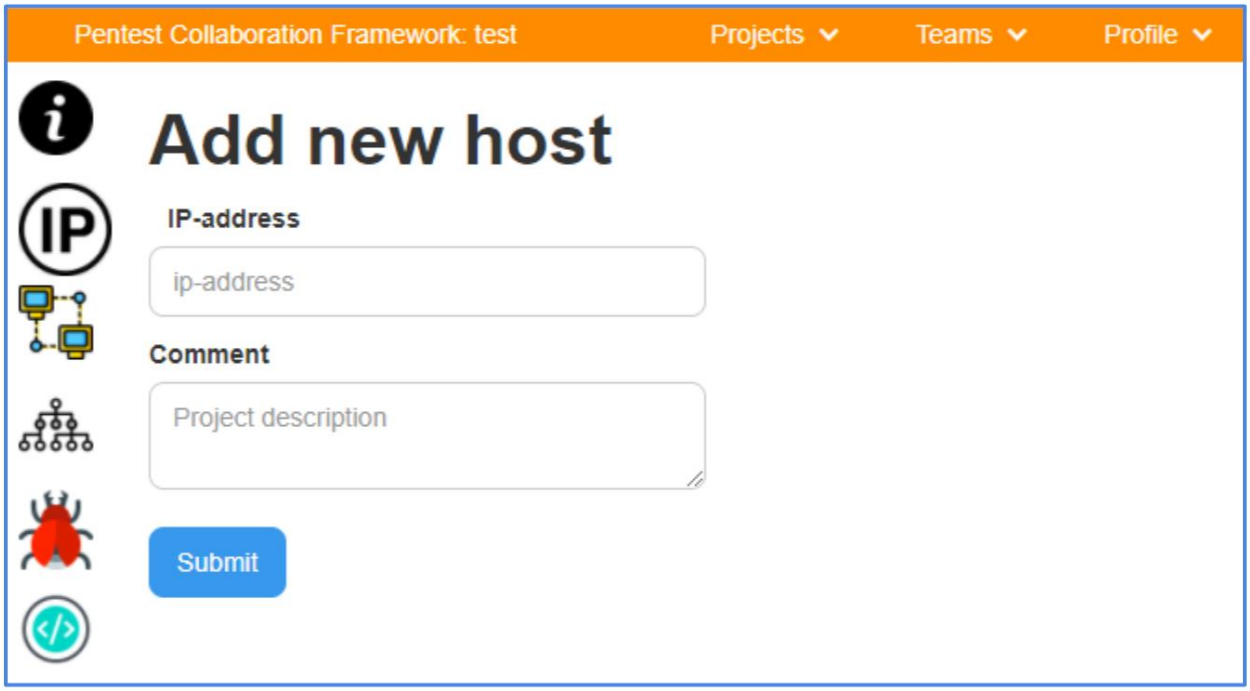
Name	Value
URL	/project/{{project_uuid}}/hosts/
URL example	/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/hosts/
Description	Project hosts list
Capabilities	Search for hosts, filter them or go to "Create Host" or "Export hosts" forms.
Comments	-



Host creation

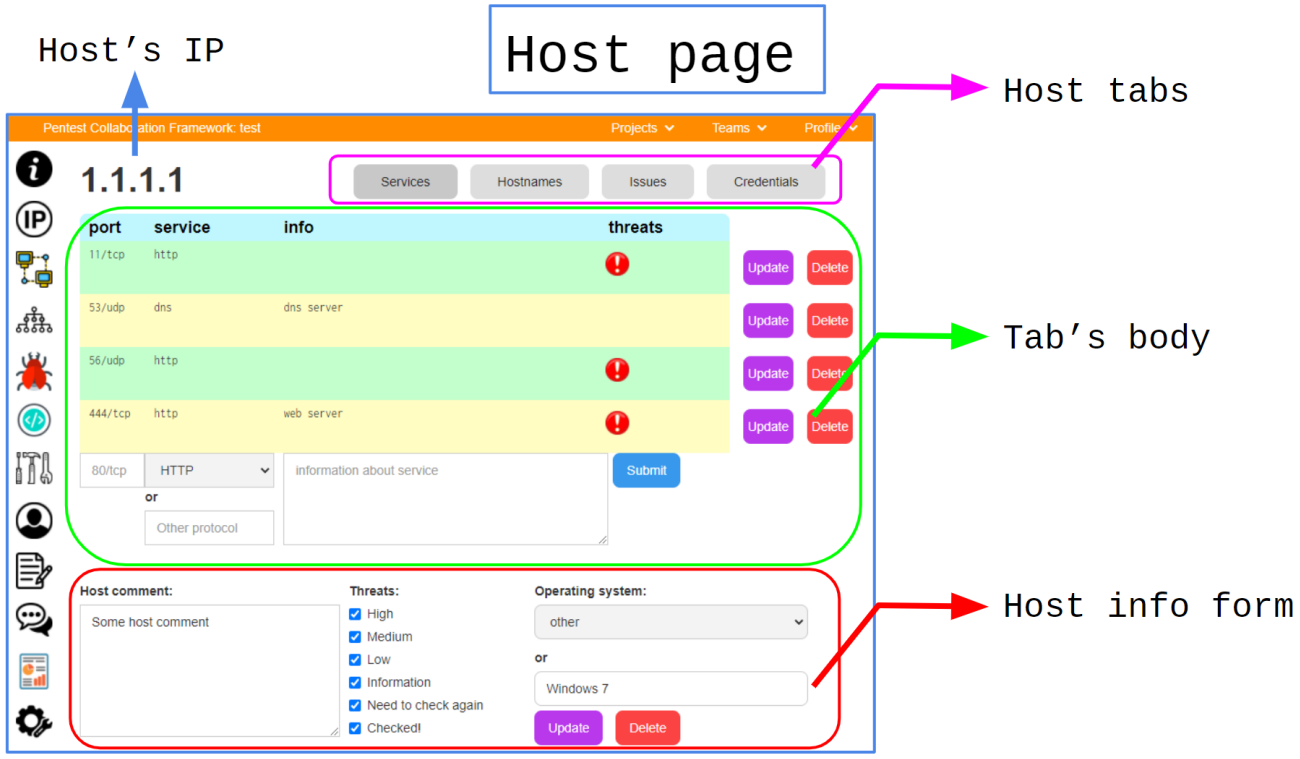
Name	Value
URL	`/project/{{project_uuid}}/`
URL example	/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/hosts/new_host
Description	Project host creation page.
Capabilities	Create a new host with unique IP and add a comment to it.
Comments	It can be IPv4 or IPv6.

New host



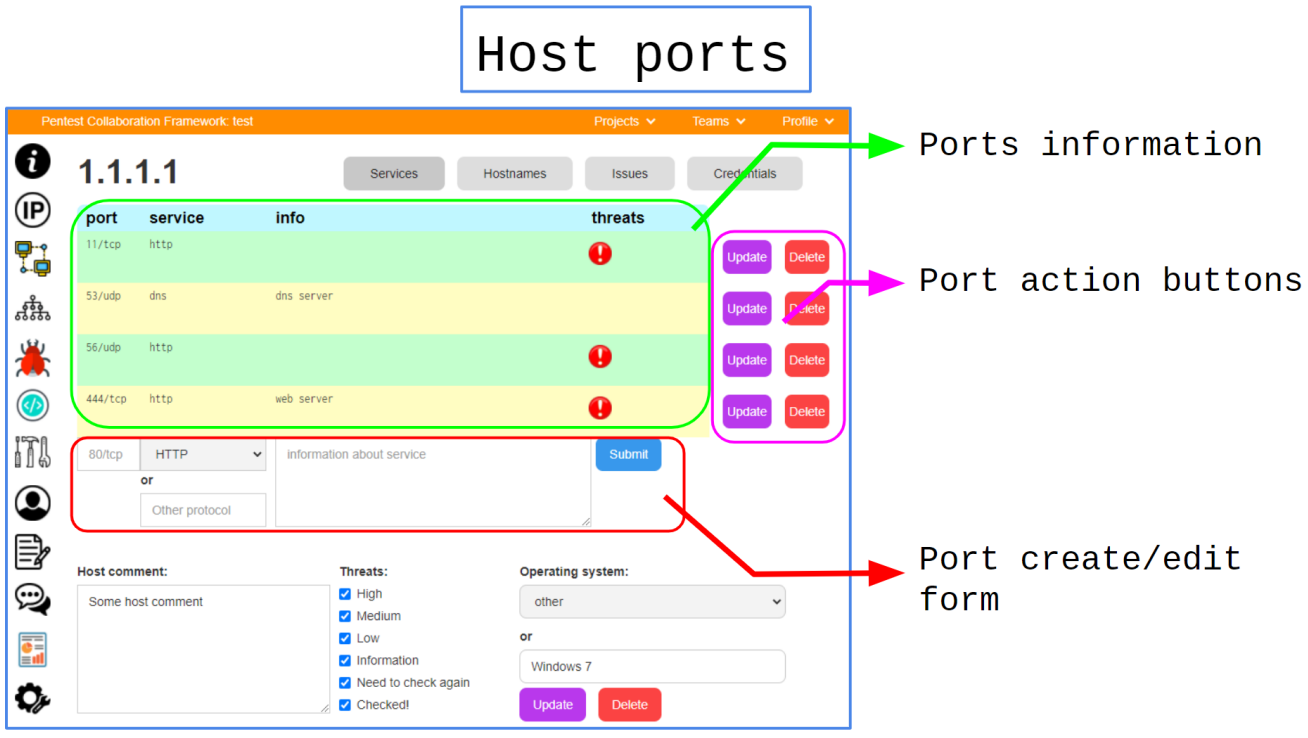
Host information

Name	Value
URL	/project/{{project_uuid}}/host/{{host_uuid}}/
URL example	/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/host/0c338176-42f0-4786-a3d8-bebd233faafc/
Description	Project host information page.
Capabilities	1. Edit host info 2. Modify ports 3. Modify hostnames 4. Modify issues 5. Modify credentials
Comments	4. More about Issues 5. More about Credentials



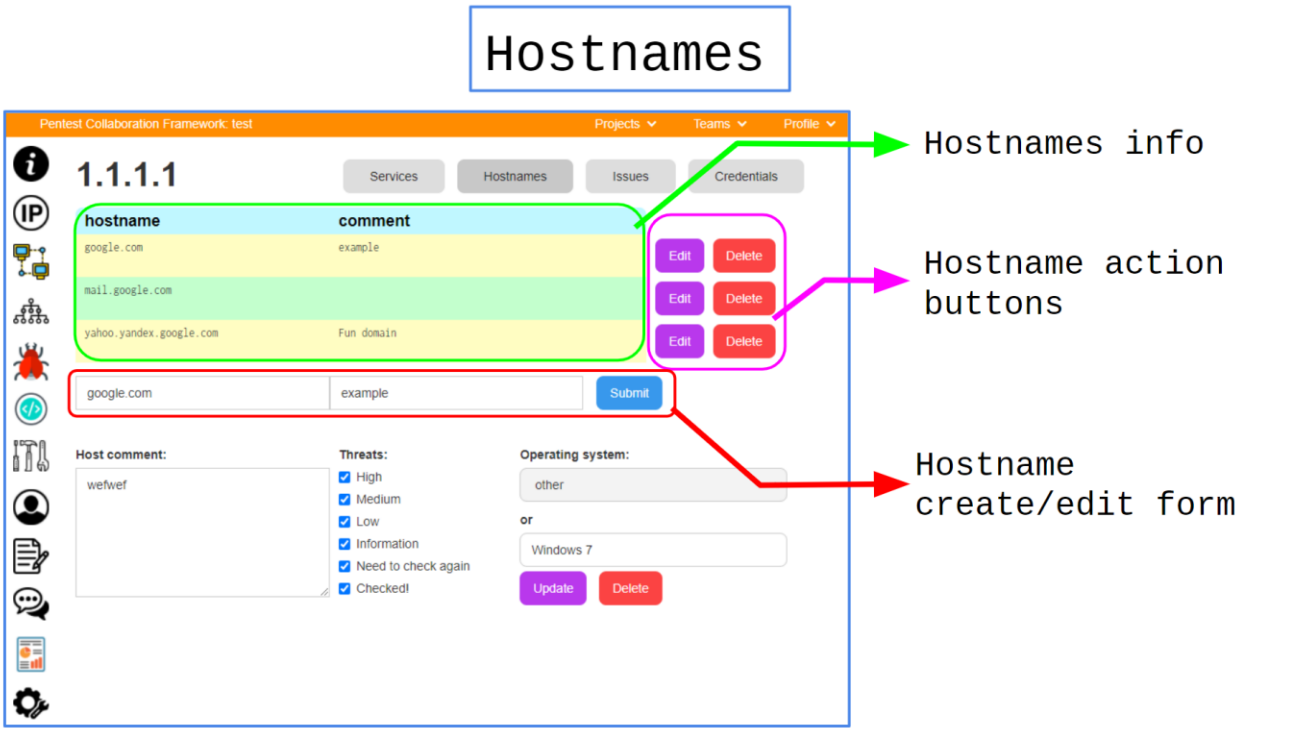
Host information: ports

Ports must be unique for one host!

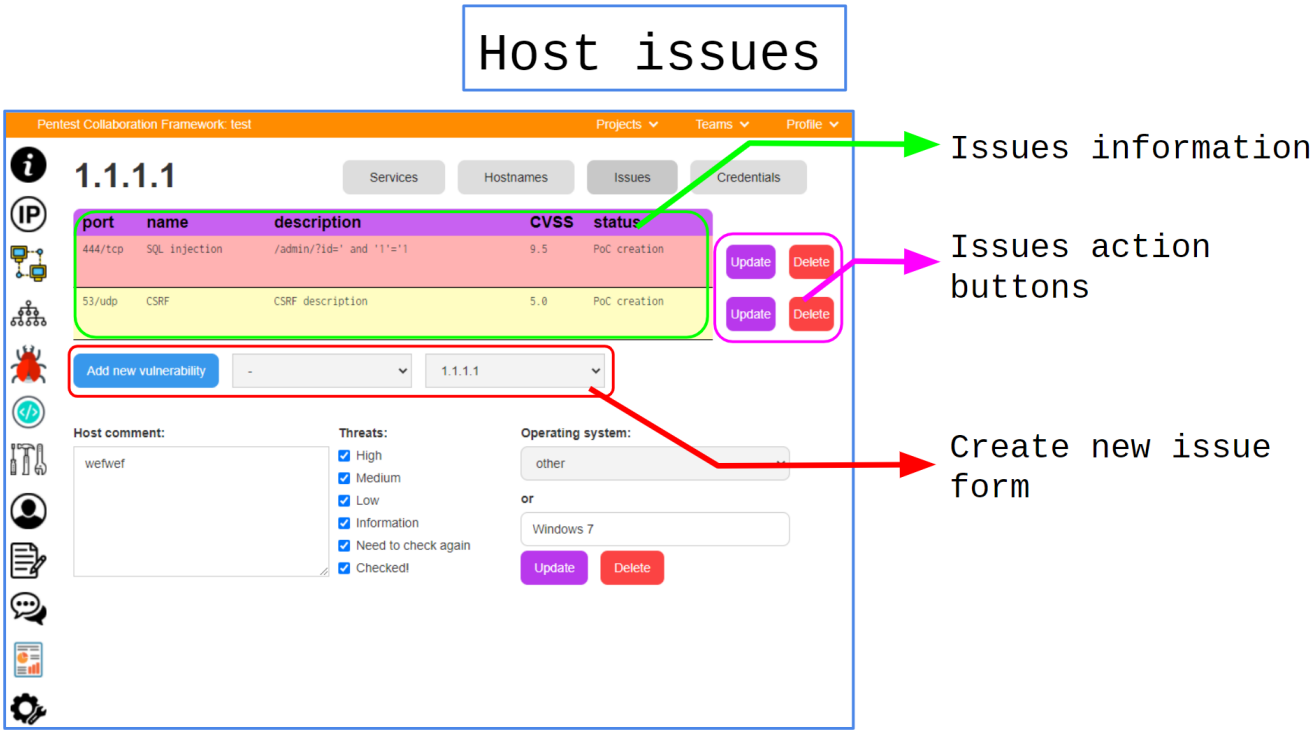


Host information: hostnames

Hostnames must be unique for one host!

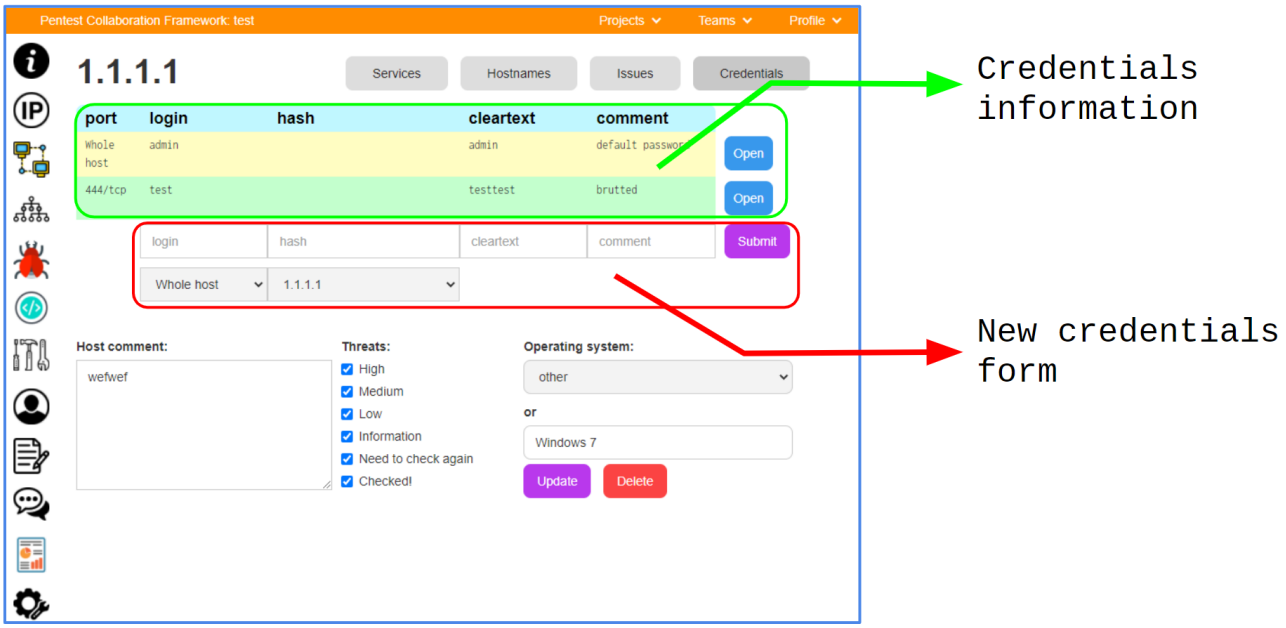


Host information: issues
More info here: Issues



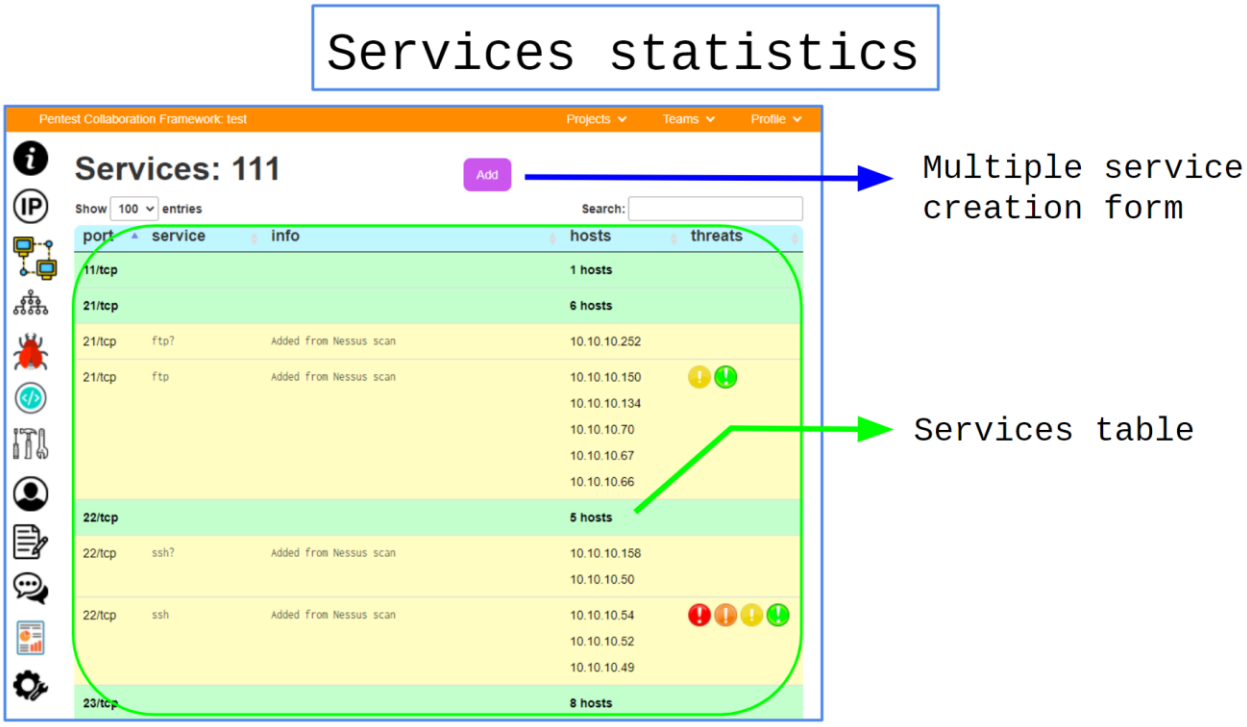
Host information: credentials
More info here: Credentials

Host credentials



Project services

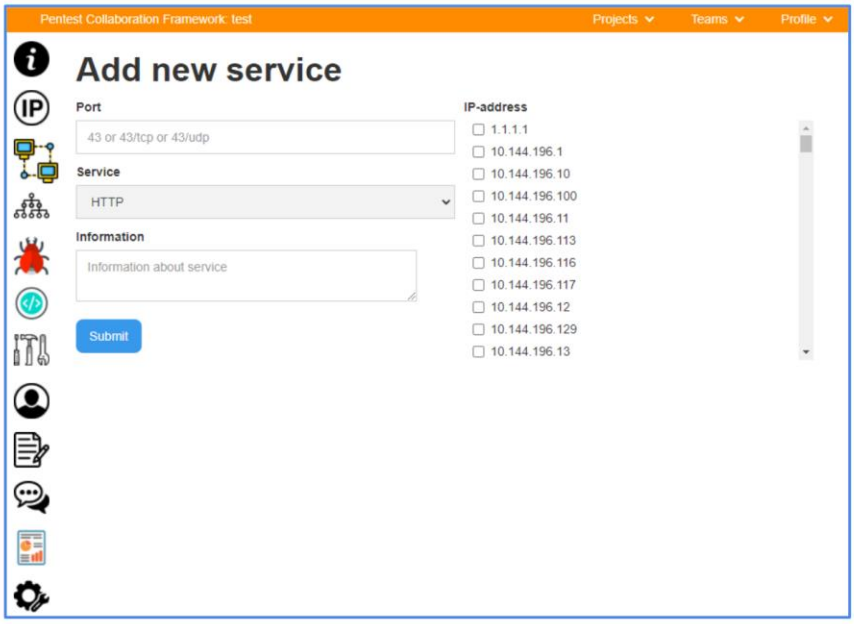
Name	Value
URL	/project/{{project_uuid}}/services/
URL example	/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/services/
Description	Project services list
Capabilities	Statistics with project services.
Comments	This page just combines information from hosts pages.



Multiple service creation

Name	Value
URL	/project/{{project_uuid}}/services/new_service
URL example	/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/services/new_service
Description	Project multiple services creation form.
Capabilities	Create service for several hosts in one form.
Comments	-

Multiple services creation



Networks Moderation

Sequencing

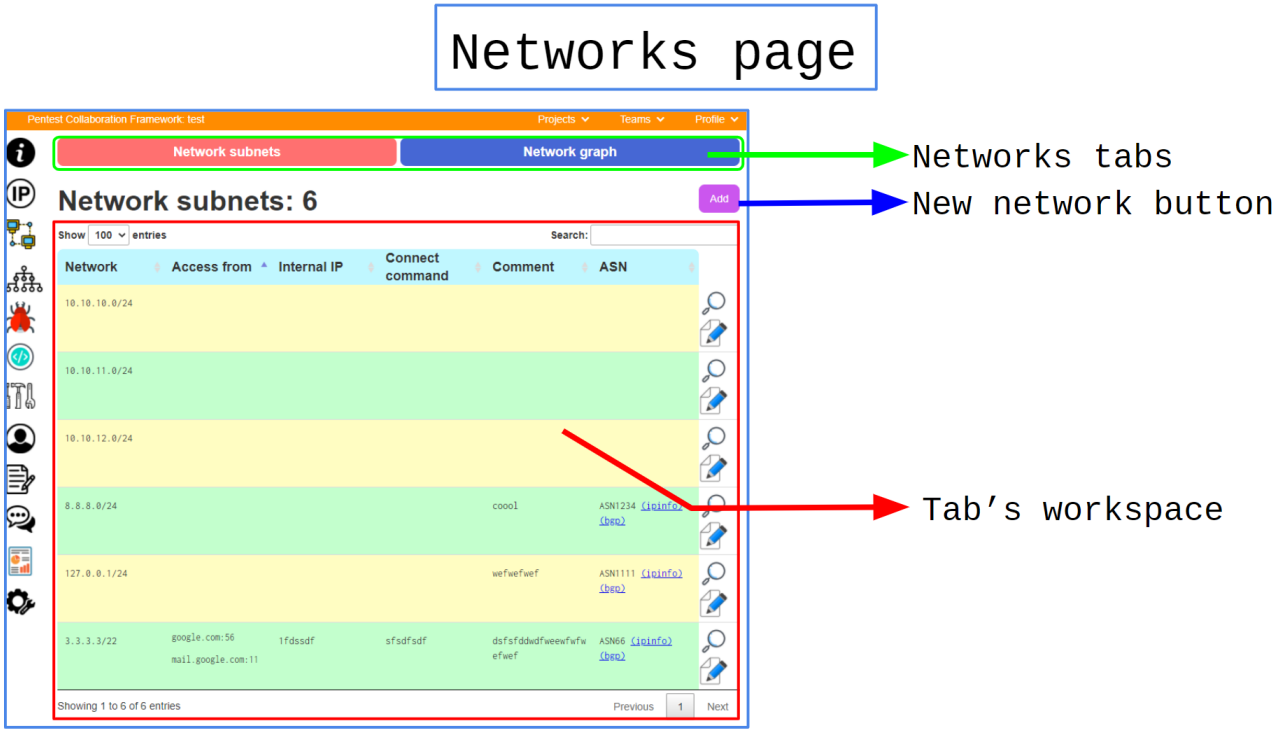
№	Action
1	Open new network form
2	Add new project network
3	Check it at networks list page
4	Get visualized network at networks list page

Endpoints

Project networks

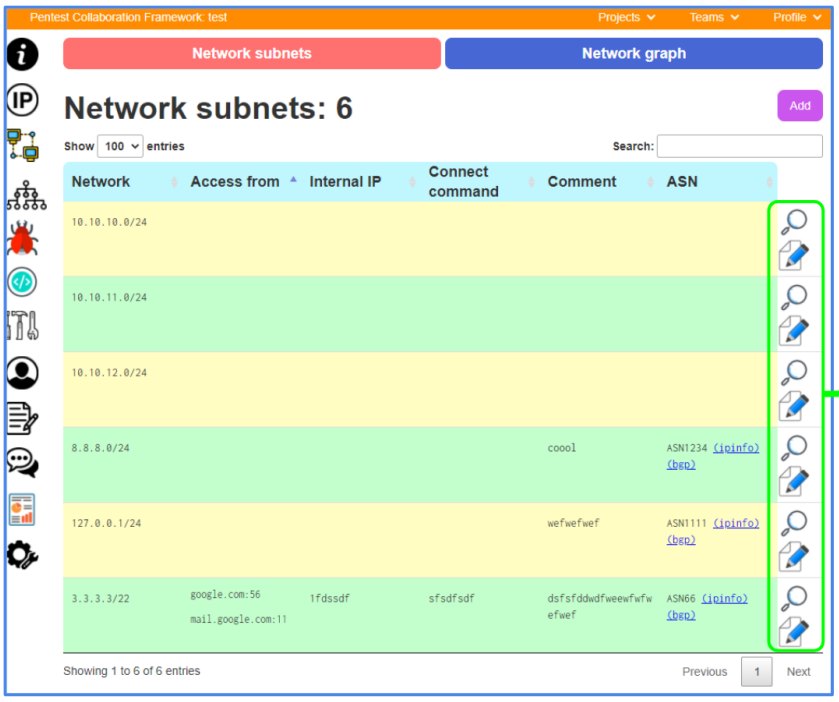
Name	Value
URL	`/project/{{project_uuid}}/networks/`
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/networks/`
Description	Project networks list and visualization.
Capabilities	1. List of project networks

Name	Value
	2. New network button 3. Network info/filter buttons 4. Network graph
Comments	Network traffic rules in development.



Networks list

Networks list



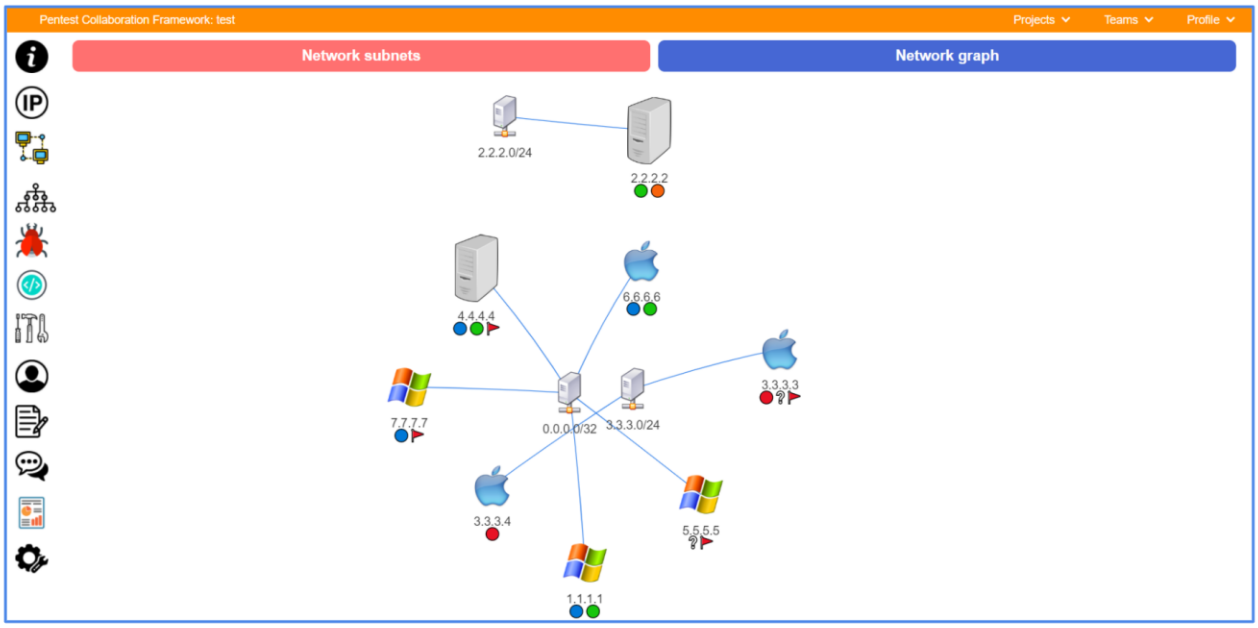
Filter and edit buttons

Networks graph

These variable are used for generating graph:

1. Host IPs
2. Host OS
3. Networks

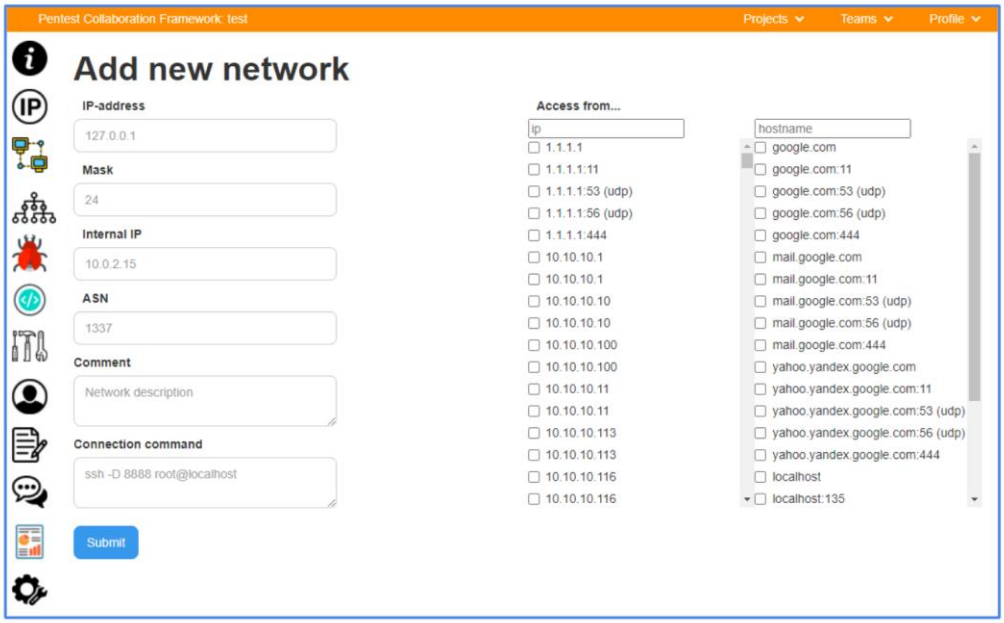
Networks graph



New network

Name	Value
URL	`/project/{{project_uuid}}/networks/new_network`
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/networks/new_network`
Description	Project network creation form.
Capabilities	Create a new network with some information.
Comments	-

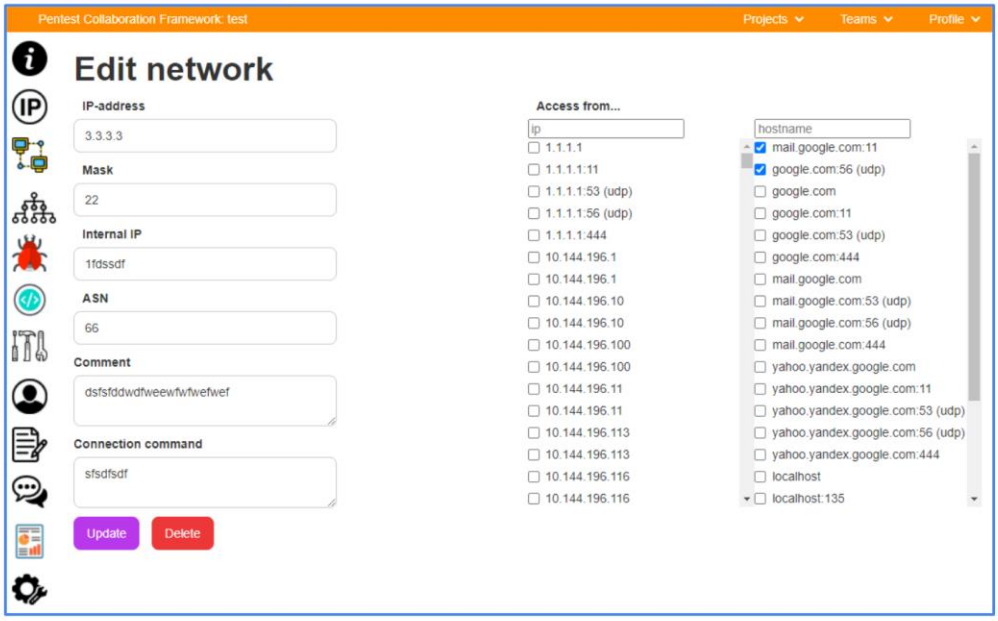
New network



Network page

Name	Value
URL	`/project/{{project_uuid}}/networks/{{network_uuid}}/`
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/networks/a8bd03fe-cd9b-4f22-bb08-e8ad6a161ae2/`
Description	Network information and edit form.
Capabilities	View, modify and delete network.
Comments	-

Edit network



Issues moderation

Sequencing

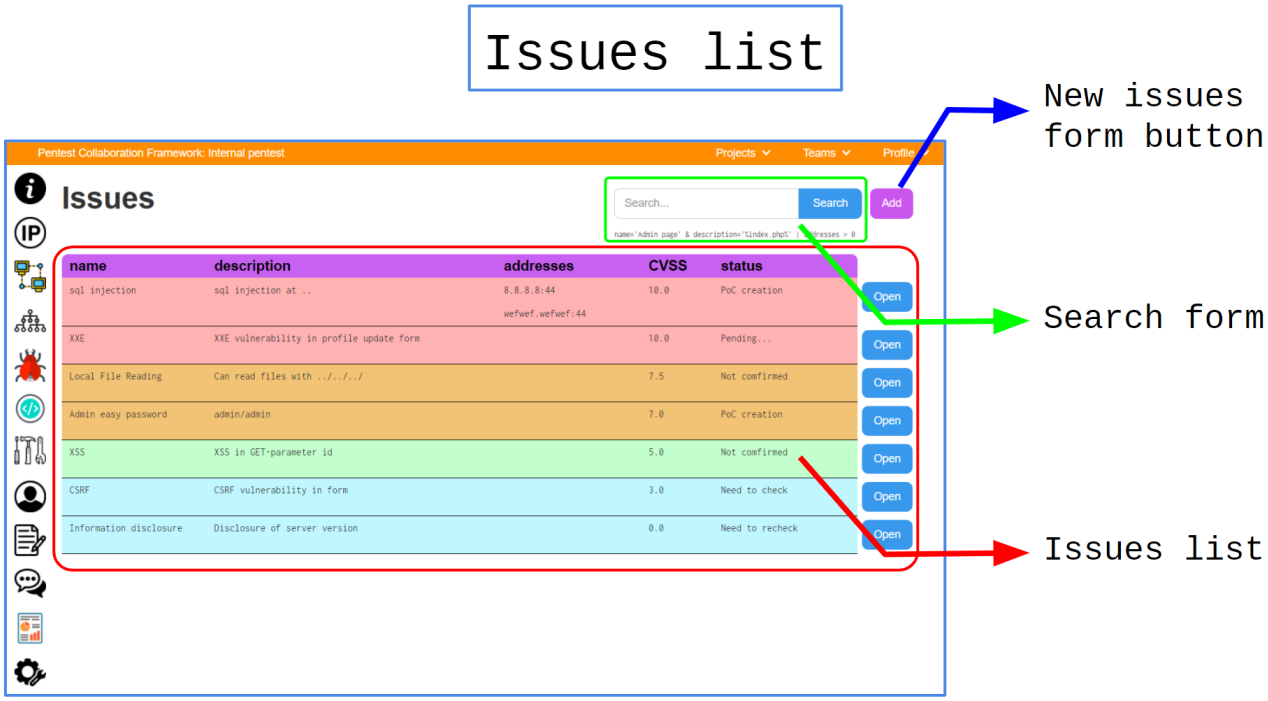
№	Action
1	Open new network form
2	Add new project network
3	Check it at networks list page
4	Get visualized network at networks list page

Endpoints

Issues list

Name	Value
URL	`/project/{{project_uuid}}/issues/`
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/issues/`
Description	Project issues list.

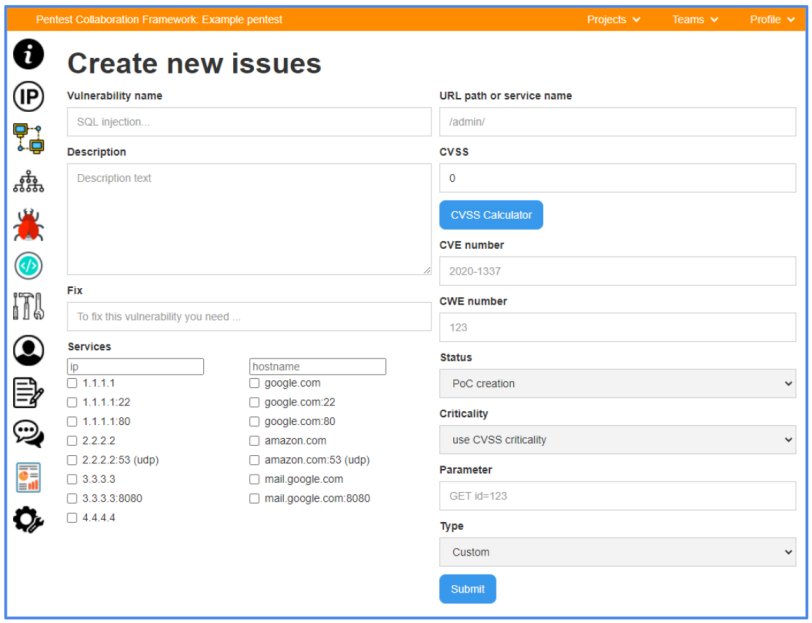
Name	Value
Capabilities	1. List of project issues 2. Issues search form 3. New issue button
Comments	Different colors - different issues criticality (CVSSv3)



New Issue

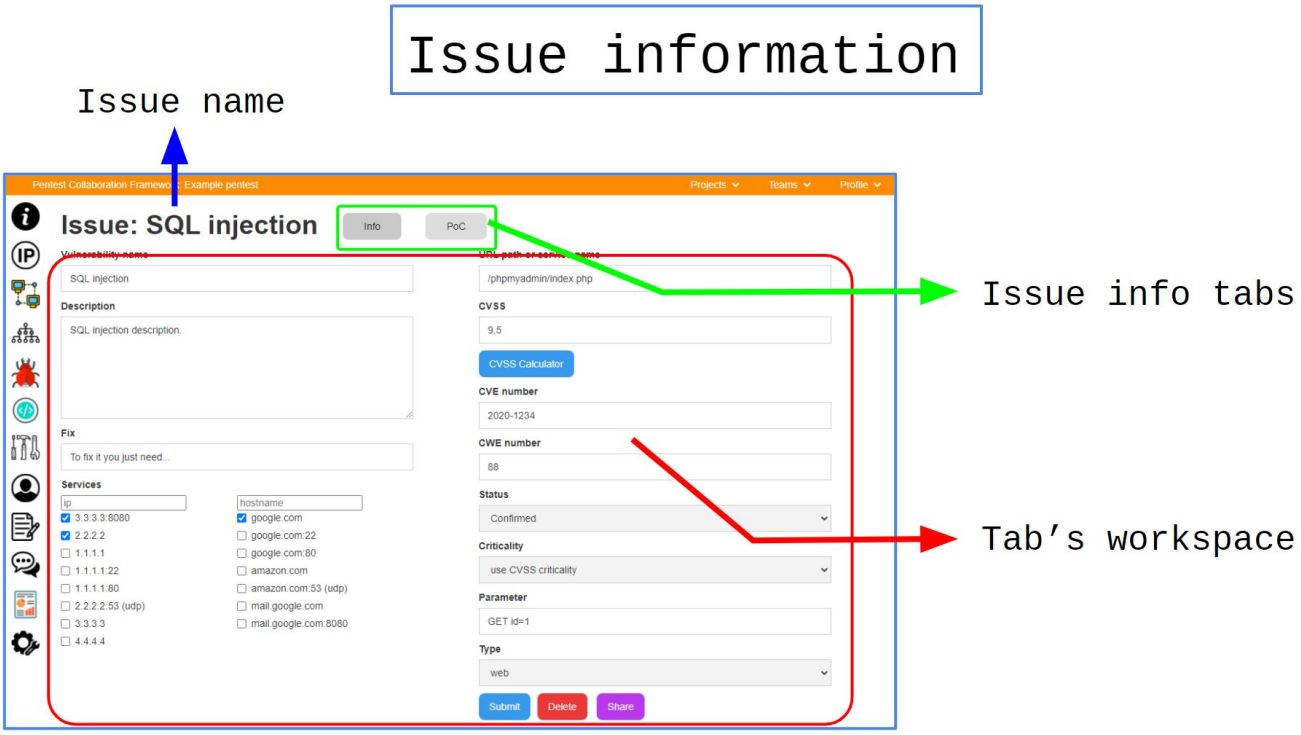
Name	Value
URL	`/project/{{project_uuid}}/new_issue`
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/new_issue`
Description	New issue form.
Capabilities	Create new issue in current project.
Comments	Some of additional fields will be available only after issue creation.

New issue

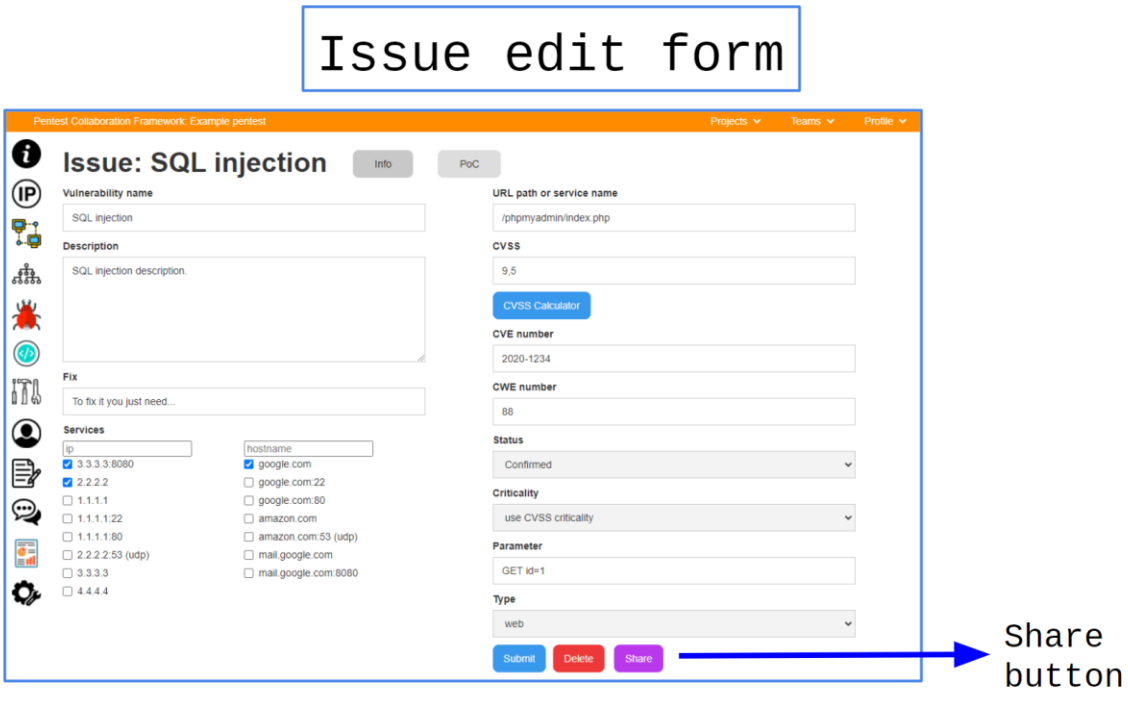


Issue information

Name	Value
URL	`/project/{{project_uuid}}/issue/{{issue_uuid}}/`
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/issue/3037349b-0111-4a62-a92d-4d10c5337daf/`
Description	Issue information and edit forms.
Capabilities	1. View/Edit issue information 2. Delete vulnerability 3. Moderate issue's Proof-of-Concepts
Comments	-



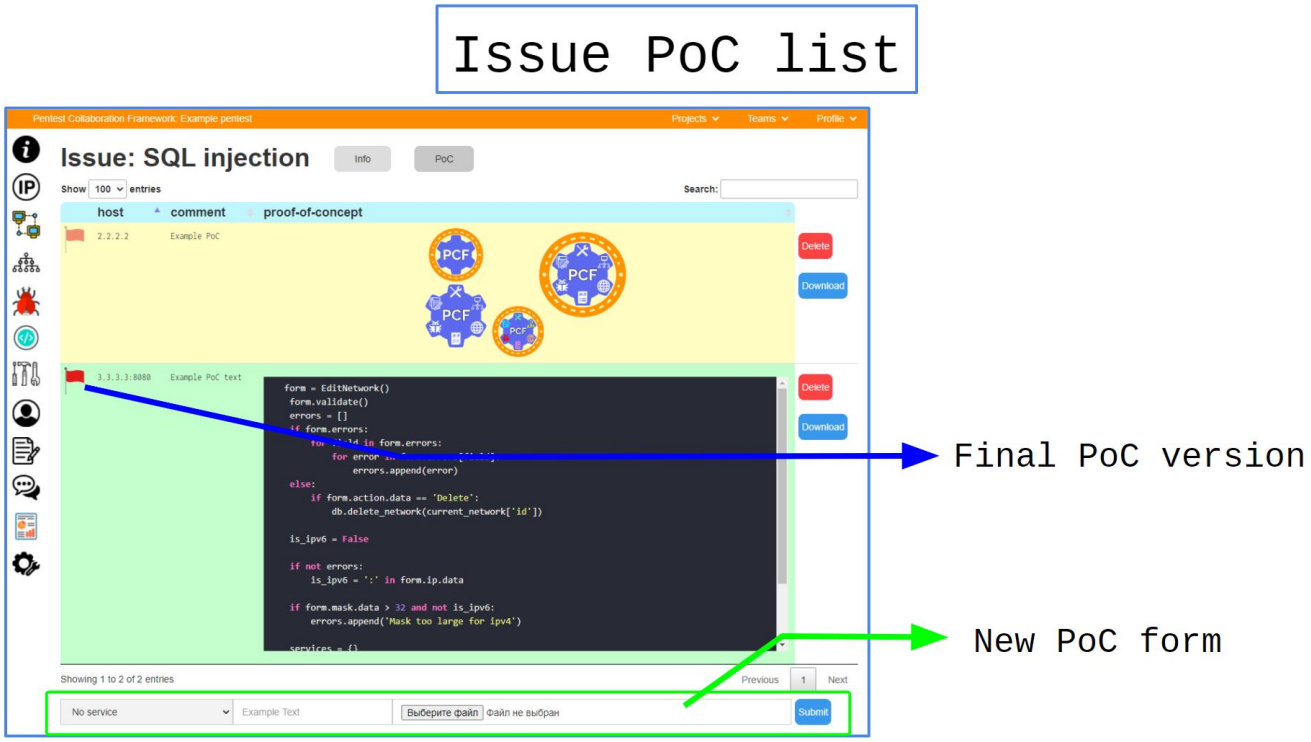
Issue information: edit form



Issue information: PoC form

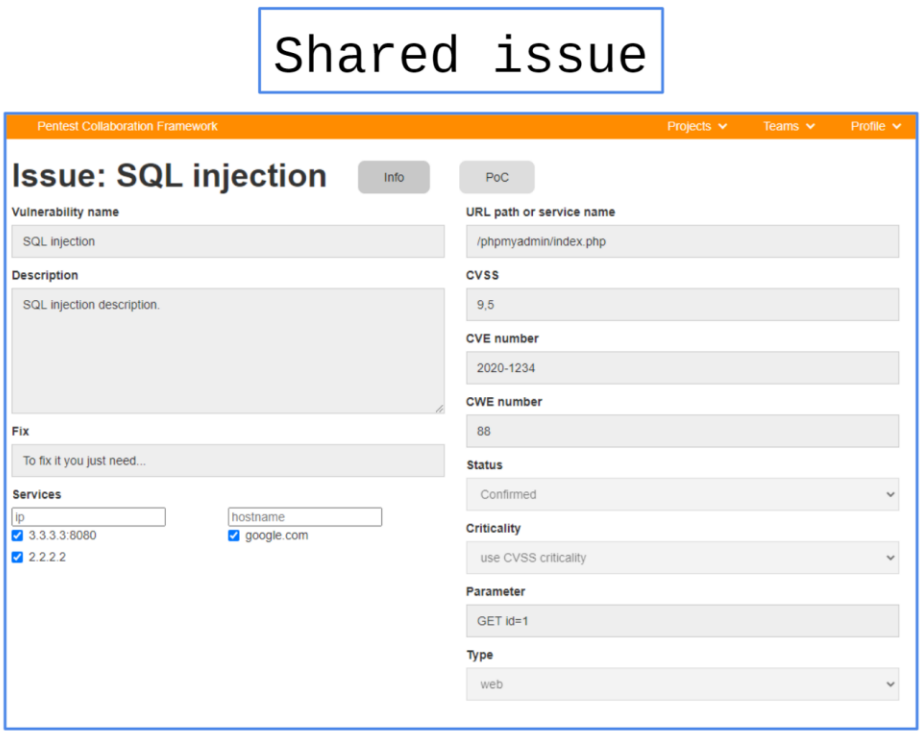
Proof-of-Concept can be a text file or image.

Symbol (near PoC) - final version of PoCs (for Reports).



Shared issue info

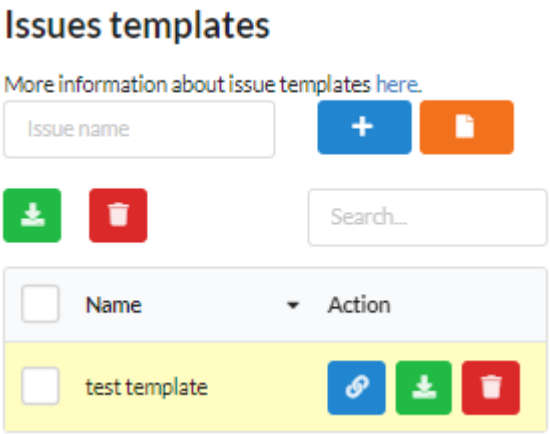
Name	Value
URL	`/share/issue/{{issue_uuid}}/`
URL example	`/share/issue/3037349b-0111-4a62-a92d-4d10c5337daf/`
Description	Share issue information.
Capabilities	Share issue information with unauthorized users.
Comments	You can just send this link to system administrators. The page is the same, as issue information link.



Issue Templates

Templates list

You can find templates list at /profile or team page:

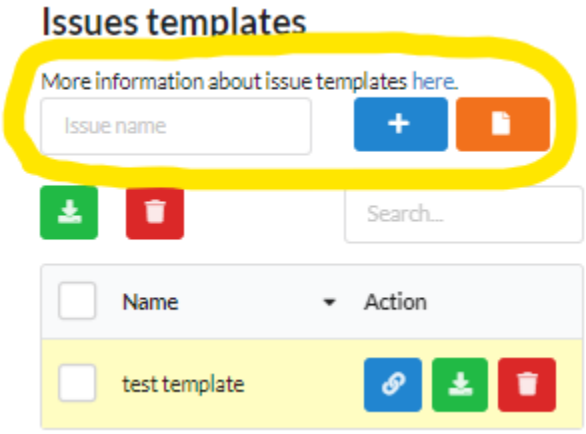


Here you can:

- Download (JSON)
- View/Edit
- Create a new template

Template creation

To create an issue template, you need to open configuration tab at /profile or team page:

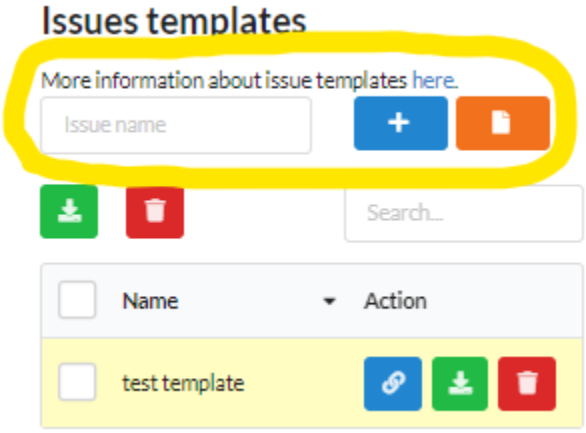


There are two variants of template creation:

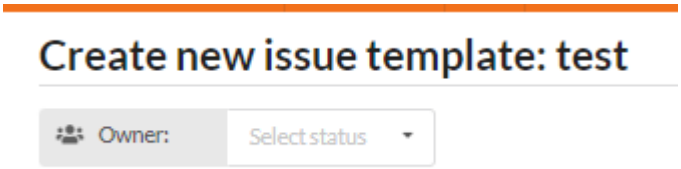
- Create a new template
- Create a new template from existed issue.
- Import templates JSON.

New Template Creation

1. Set a template name



2. Select owner of template

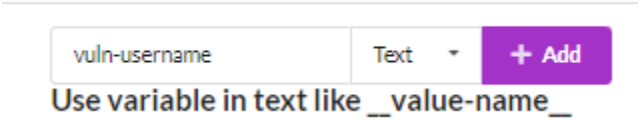


3. Create required variables

There are four types of required variables:

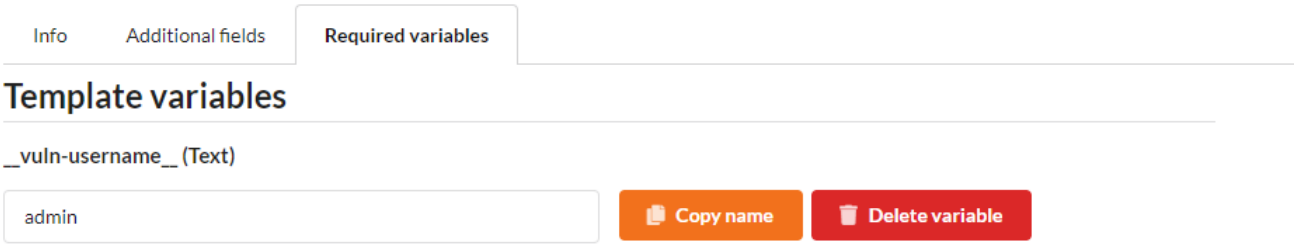
- Text
- Number
- Float
- Boolean

For example, create a text-variable vuln-username:



This variable will be automatically saved into clipboard as "__vuln-username__", so you can use it at next steps:

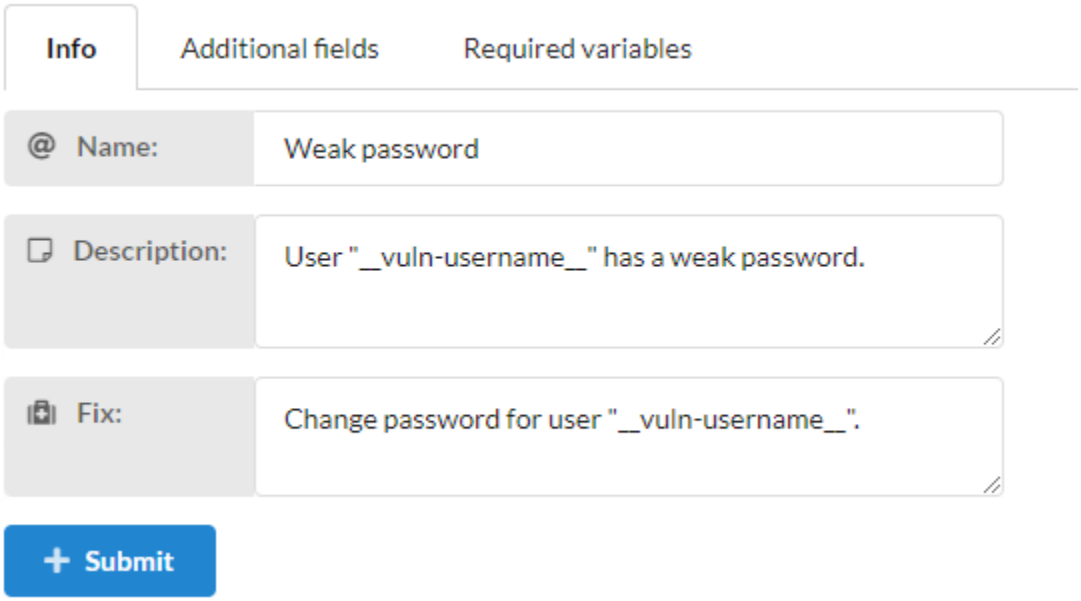
Also you can edit created variables at "Required variables" tab:



So, it's better to set a default variable value not to forget what this variable means in the future. At previous screenshot we set default value "admin" for variable "__vuln-username__".

4. Fulfill issue fields

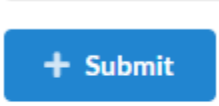
You must fullfill main issue fields. For example, you can fullfiil issue description and fix fields and insert into them required variable "__vuln-username__":



So, when you use this issue template, variable name will be replaced with variable value (by default, variable "__vuln-username__" will be replaced with string "admin").

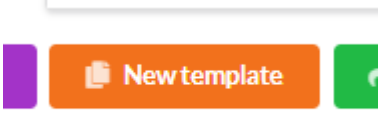
5. Save template

To save a template, you must click at submit button:



Create a template from an existing template

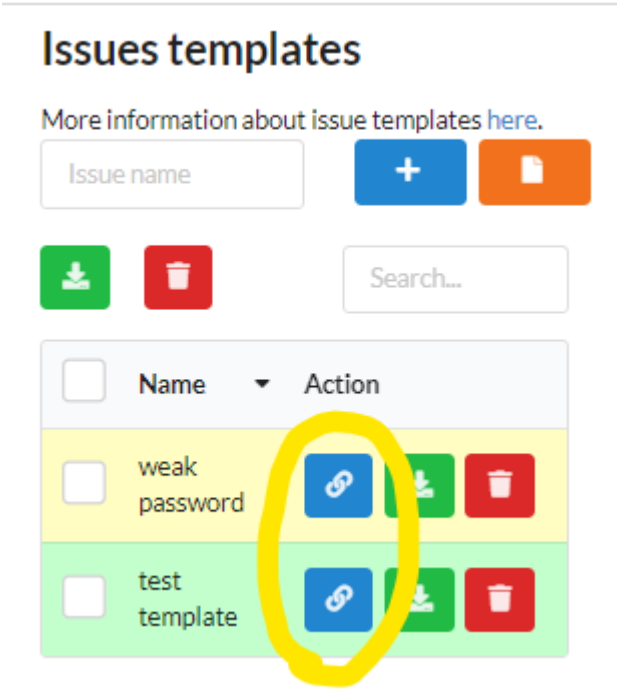
To create an issue template from an existing issue, you must click at “New template” button at issue page:



And next you will be redirected at fulfilled form from previous paragraph.

Template edit

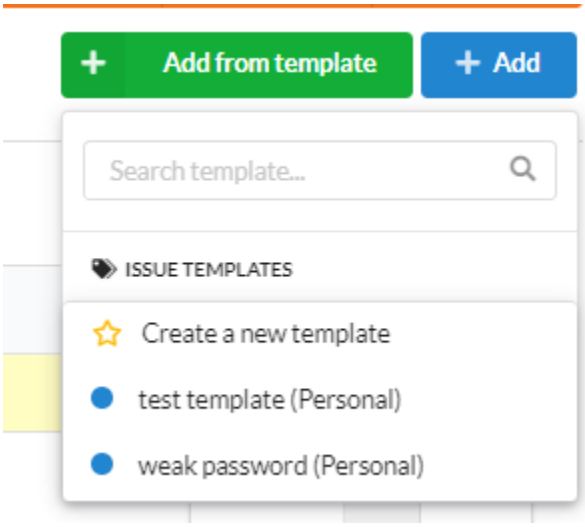
To edit template, you must open a configuration tab at /profile or team page and click at blue button:



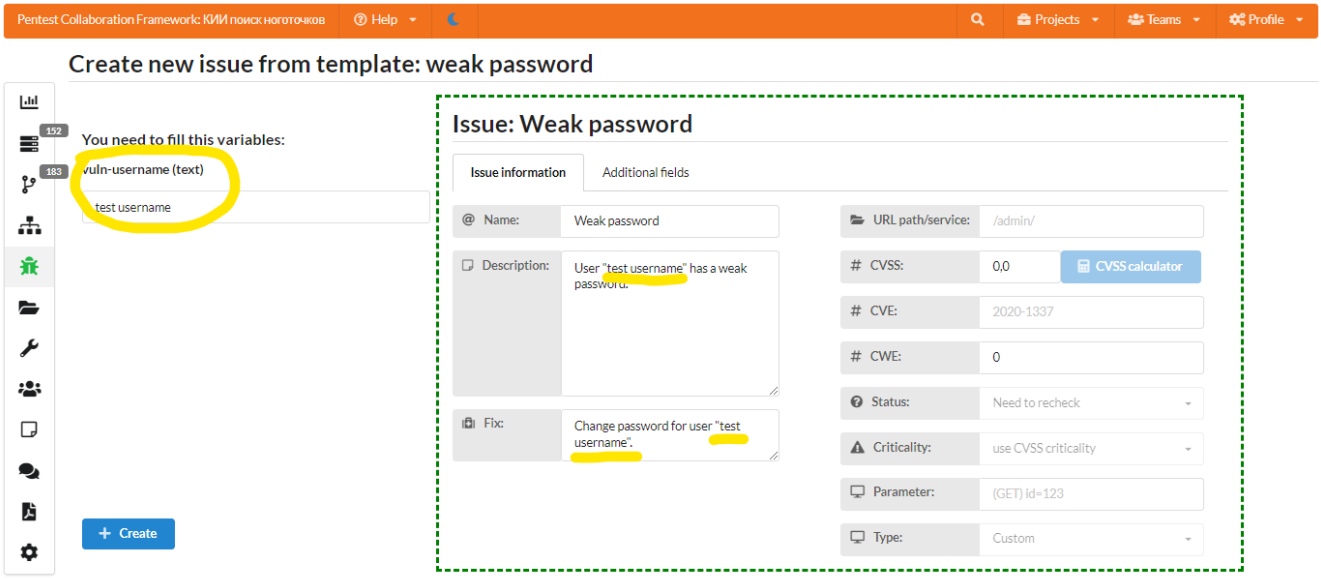
All next steps of template edition are the same as the new template creation steps.

Template usage

To use a template, you must click at "Add from template" green button at top right corner of issues list page and select needed template:



After this you will be redirected at new page where you need to insert required variables at left and see a result of new issue:



And next click at blue button "Create":

And next you will be redirected at new created issue.

Issue templates JSON

To export and import template issues, you can use JSON-format.

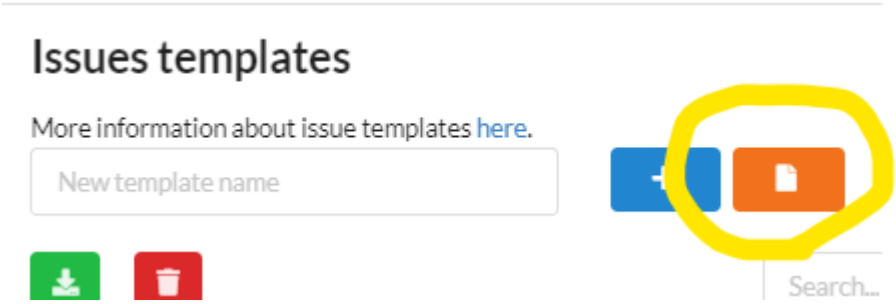
Example of JSON-file

```
[
  {
    "cve": "",
    "cvss": 0.0,
    "cwe": 0,
    "description": "User \"__vuln-username__\" has a weak password.",
    "fields": {},
    "fix": "Change password for user \"__vuln-username__\".",
    "name": "Weak password",
    "param": "",
    "status": "Need to recheck",
    "tpl_name": "weak password",
    "type": "custom",
    "url_path": "",
    "variables": {
      "vuln-username": {
        "type": "text",
        "value": "admin"
```

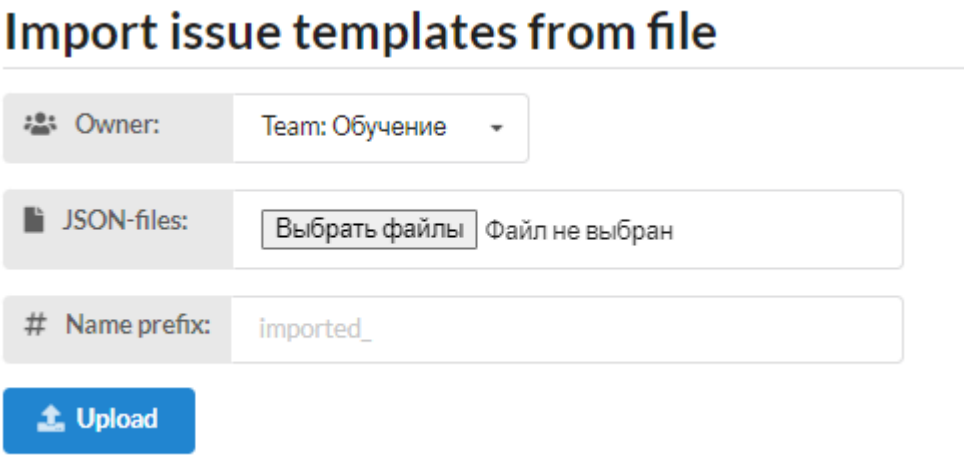
```
        }
      }
    }
]
```

Import

To import templates, you must use this link:



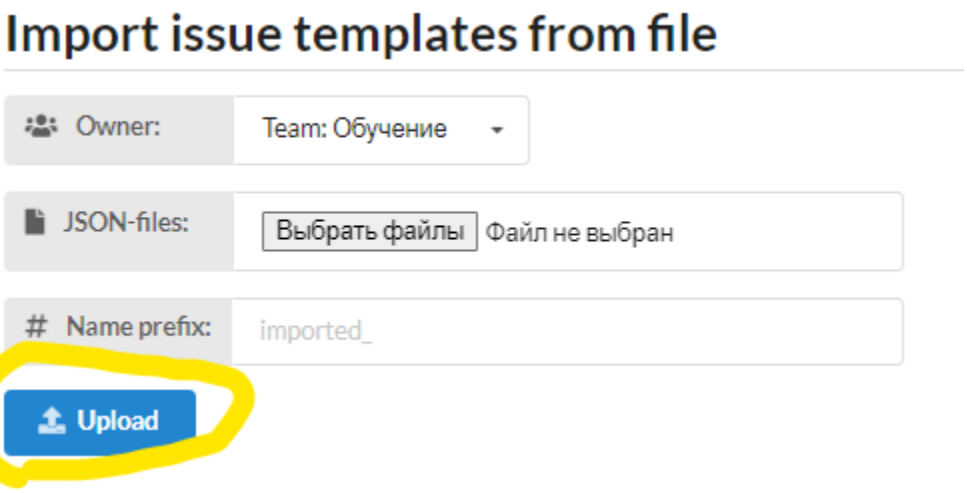
Then you will be redirected at /import_issue_templates page, which you must to fullfill:



There are three parameters:

- Owner - personal or team
- JSON-files - one or multiple json files
- Name prefix - prefix of imported issue templates.

After that click on the Upload button:

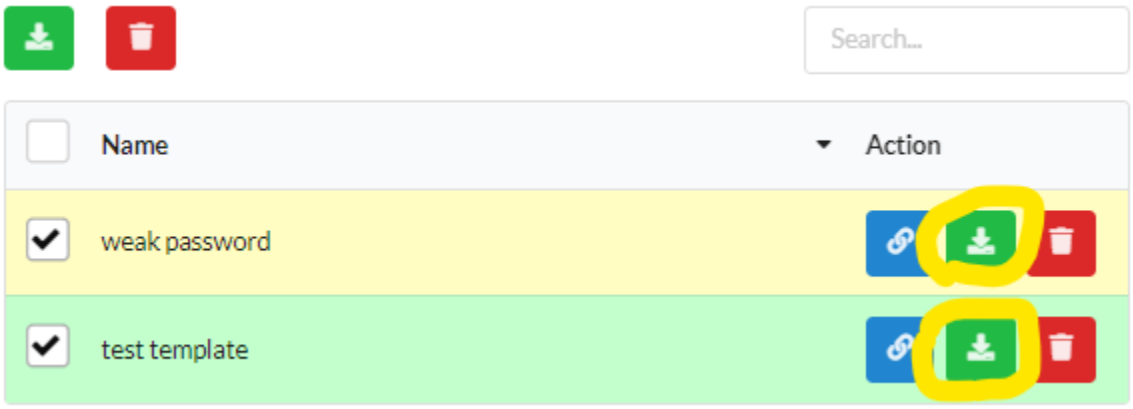


Export

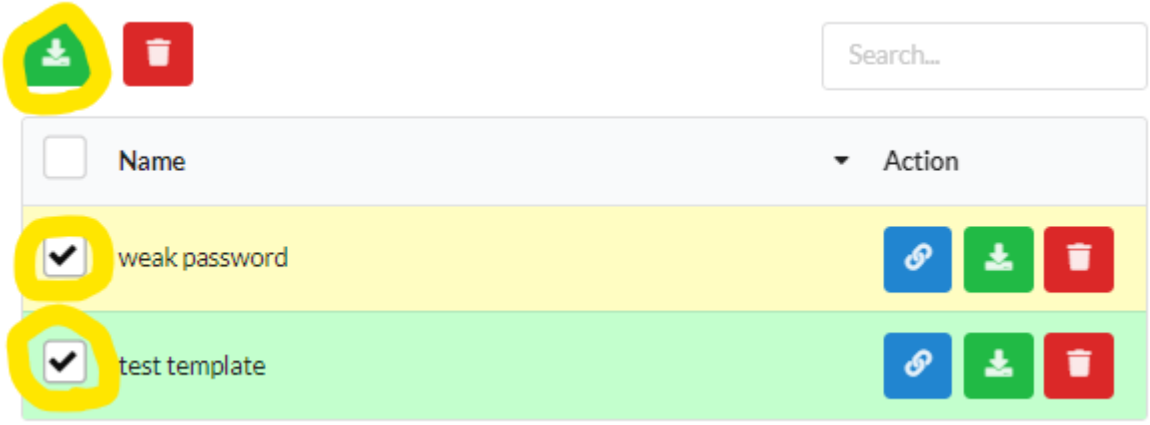
To export issue templates, you can:

- export one issue template
- export multiple issue templates

To export one issue template, you just need to click at green download button:



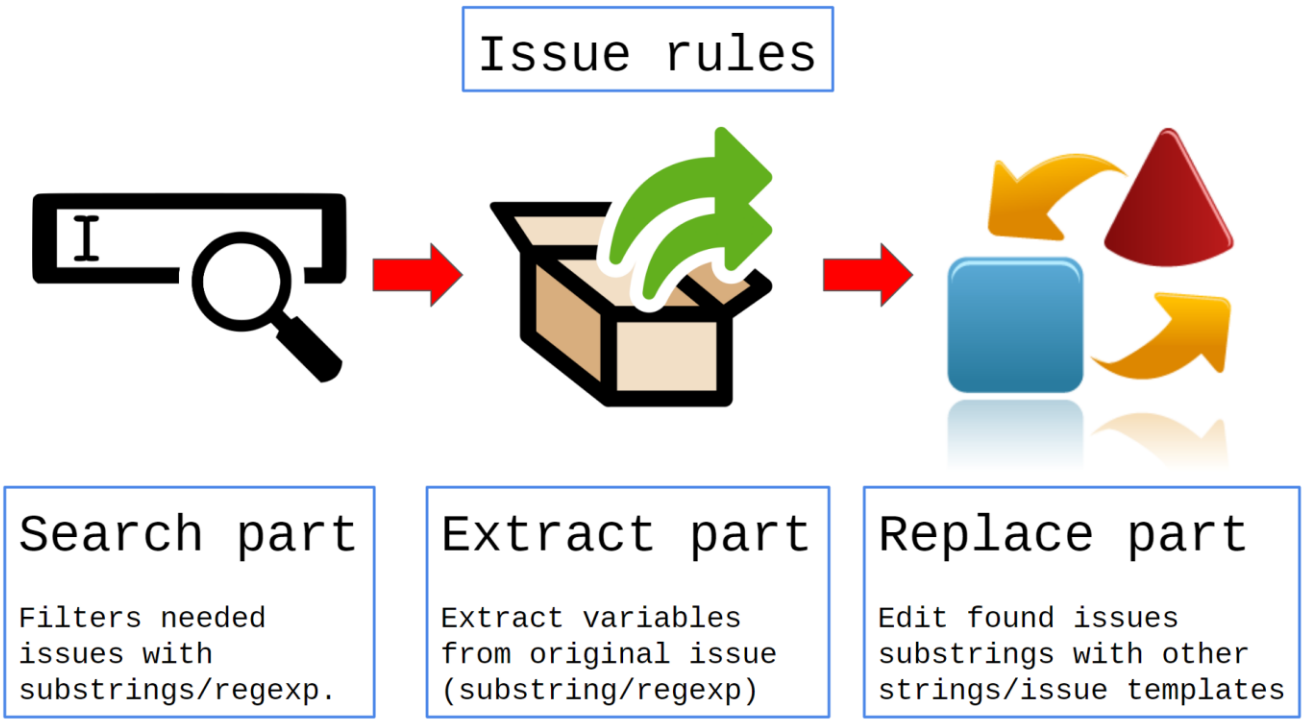
To export multiple issue templates, you must select them using first column checkboxes and click green download button at top of table:



After that, your browser will download issue template .json file.

Issue rules

Rules logics



Issue rule - an object which consists of three parts:

1. Search rules - rules which filters needed issues
2. Extract rules - rules to extract variables(substrings) from issue
3. Replace rules - rules to replace issue content with strings/issue templates.

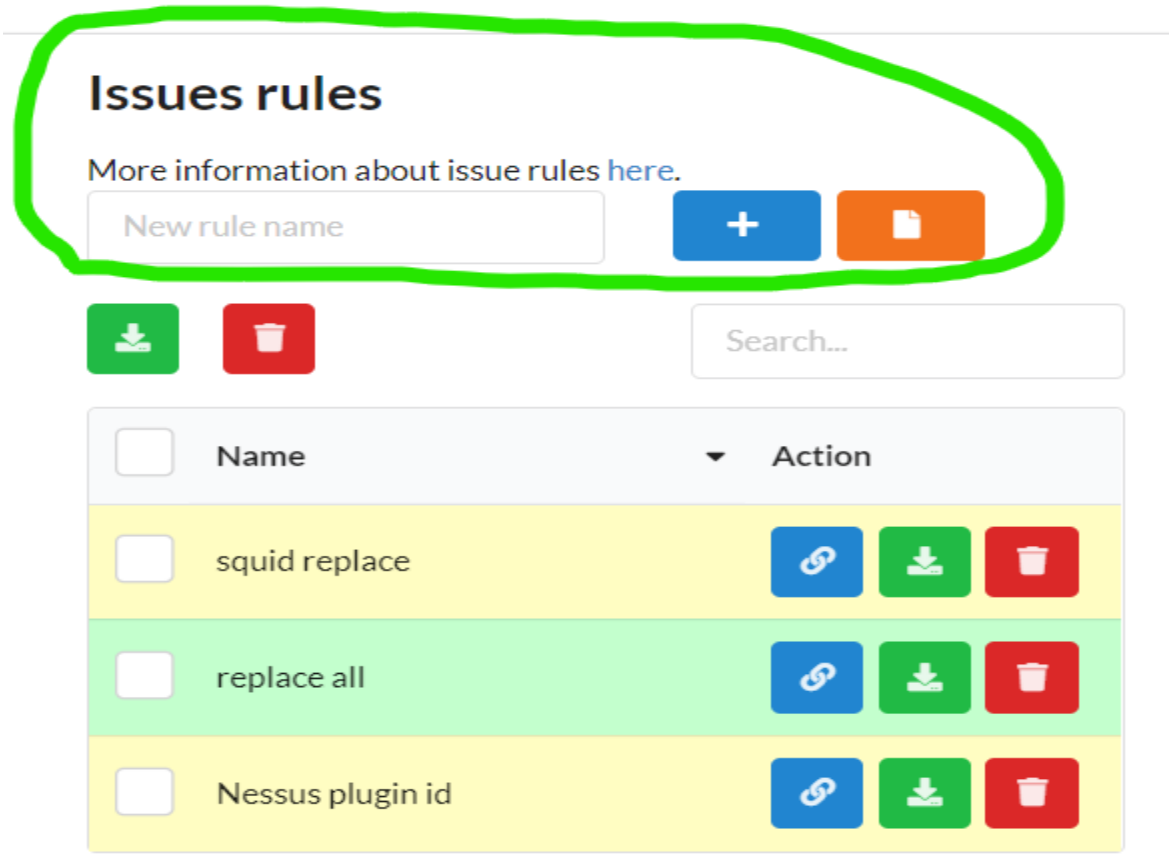
It can be used for massive edition of imported scanner results (1 rule == 1 scanner result) or other automated actions.

Search rules

Search rules - rules which filters needed issues.

It can be:

- Substring rule - you just must set field name and substring to search for.
- RegExp rule - same, but, instead of substring, it uses python regular expressions to search issues.



Extract rules

Extract rules - rules to extract variables(substrings) from issue.

Same as "Search rules" uses "Substring" or "RegExp" methods. This part extracts some special strings from original Issue, which can be used at next part.

Replace rules

Replace rules - rules to replace issue content with strings/issue templates.

Replace rules can be two types:

- Template rule - you must set template and it's fields (you can use variables from "Extract rules" inside fields).
- String rule - replace part of issue with string. It can also be "Substring" or "RegExp".

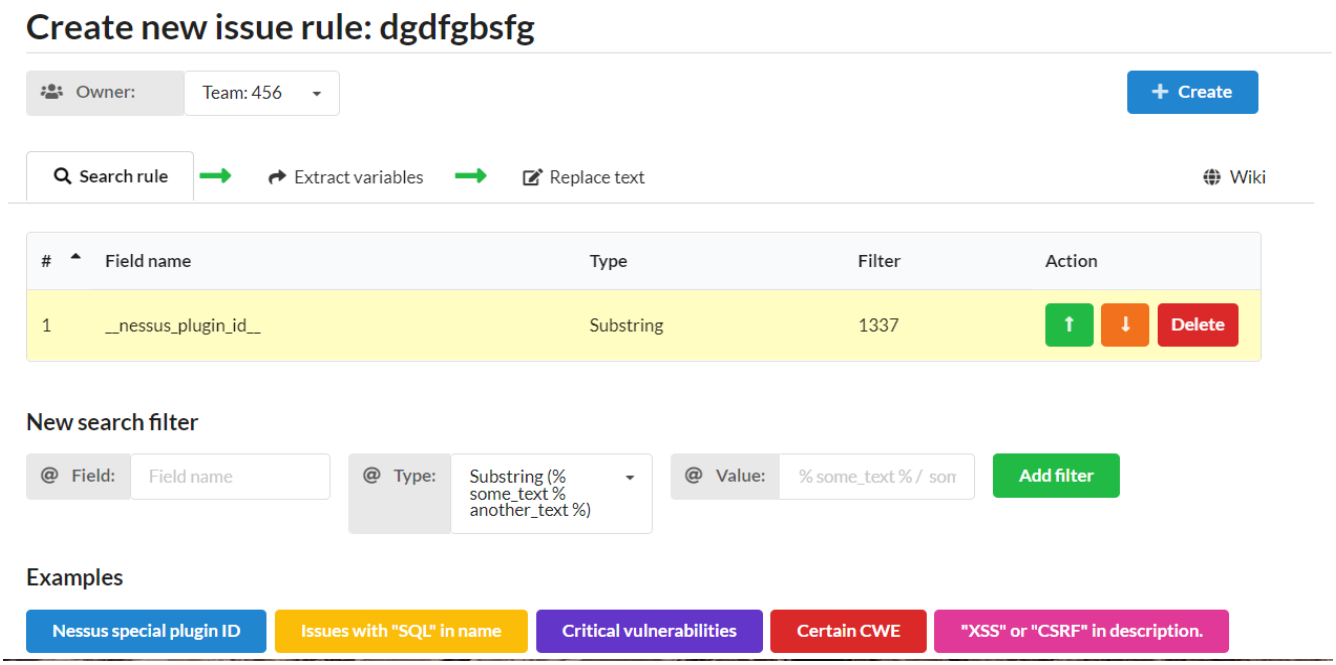
Create a rule

Find create button

It can be found at Profile -> Config or Team -> Config.

Set search rule

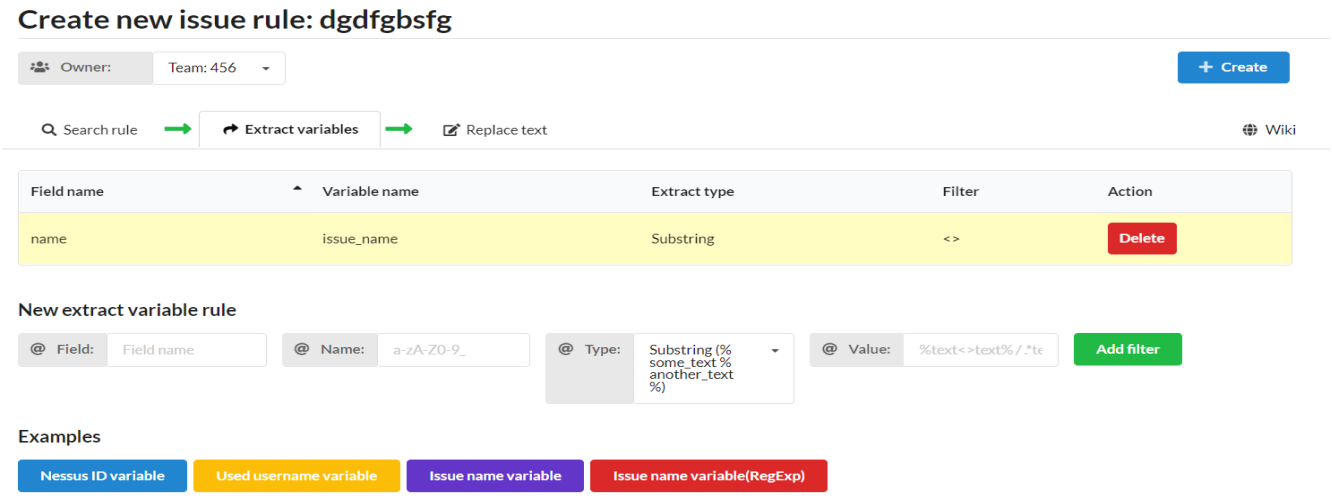
Set search rule - rule, which will filter issues.



Set extract rule

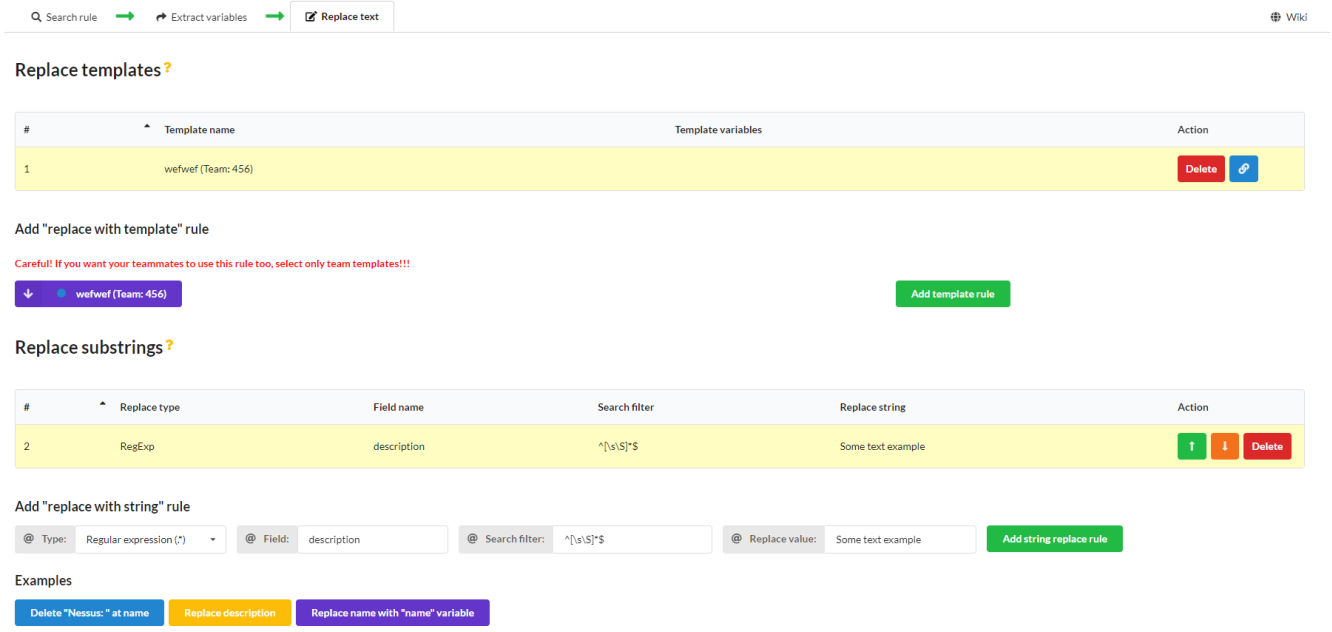
It's not necessary if you will not use variables at "Replace rules" part.
This rule will create variable names from issue fields substrings.

For example, you can create variable "name" and use it with "{{name}}" (without spaces!!!).



Set Replace Rules

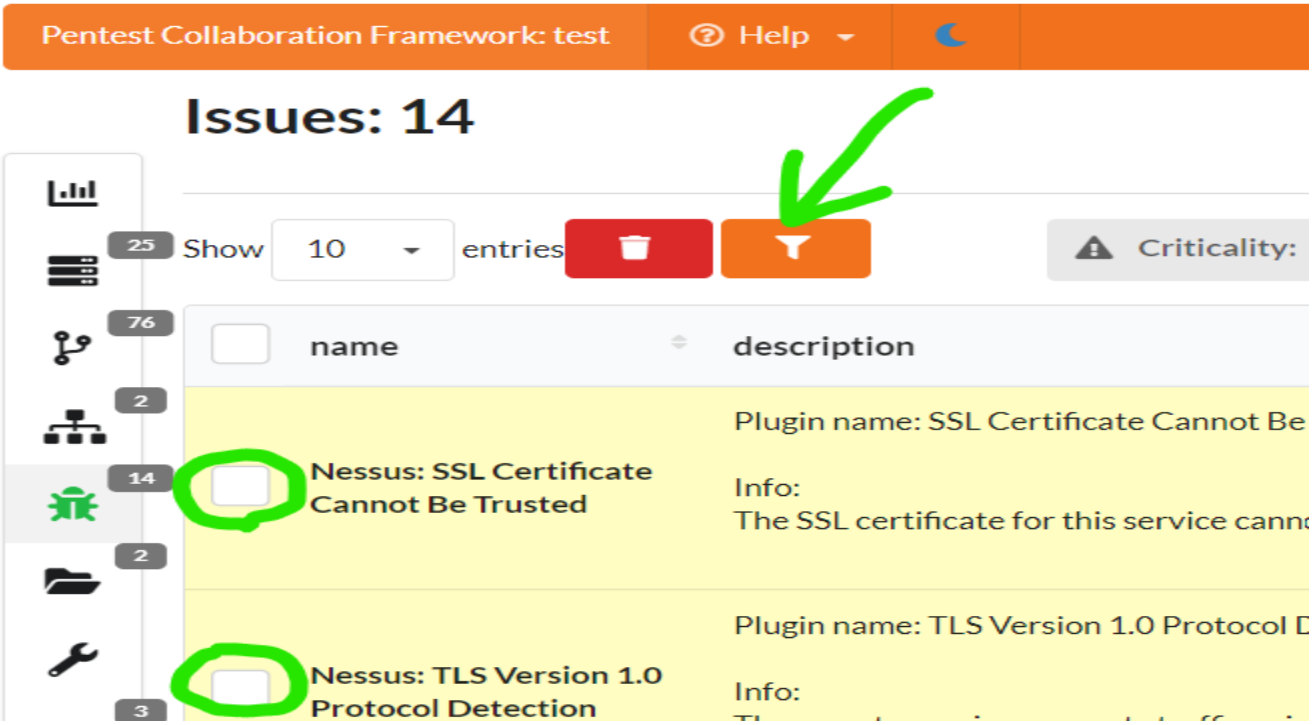
You can set two replace rule types: template and strings. Template rules always will be in priority (due to this replaces all issue fields):



Use rules

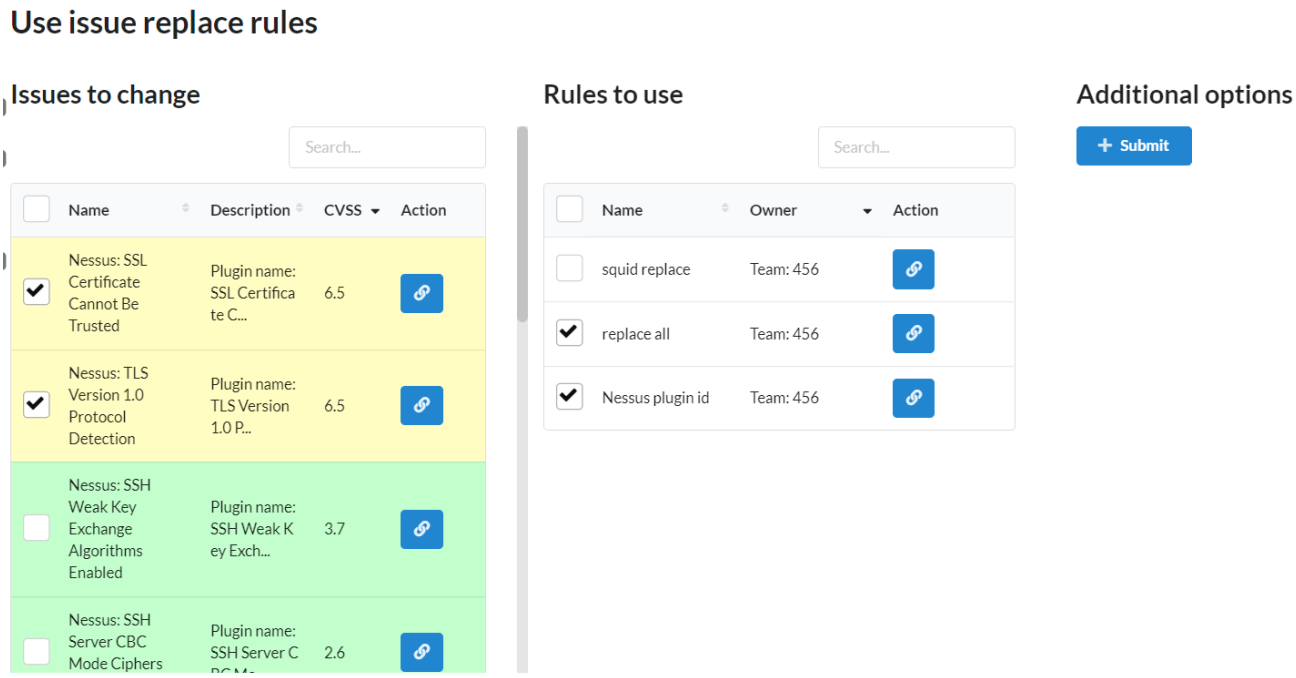
Open project issues

Open project issues, select needed issues and click at this button at the top of the page:



Select issues and rules

Select issues(first column) and rules(second column) and press "Submit" button:



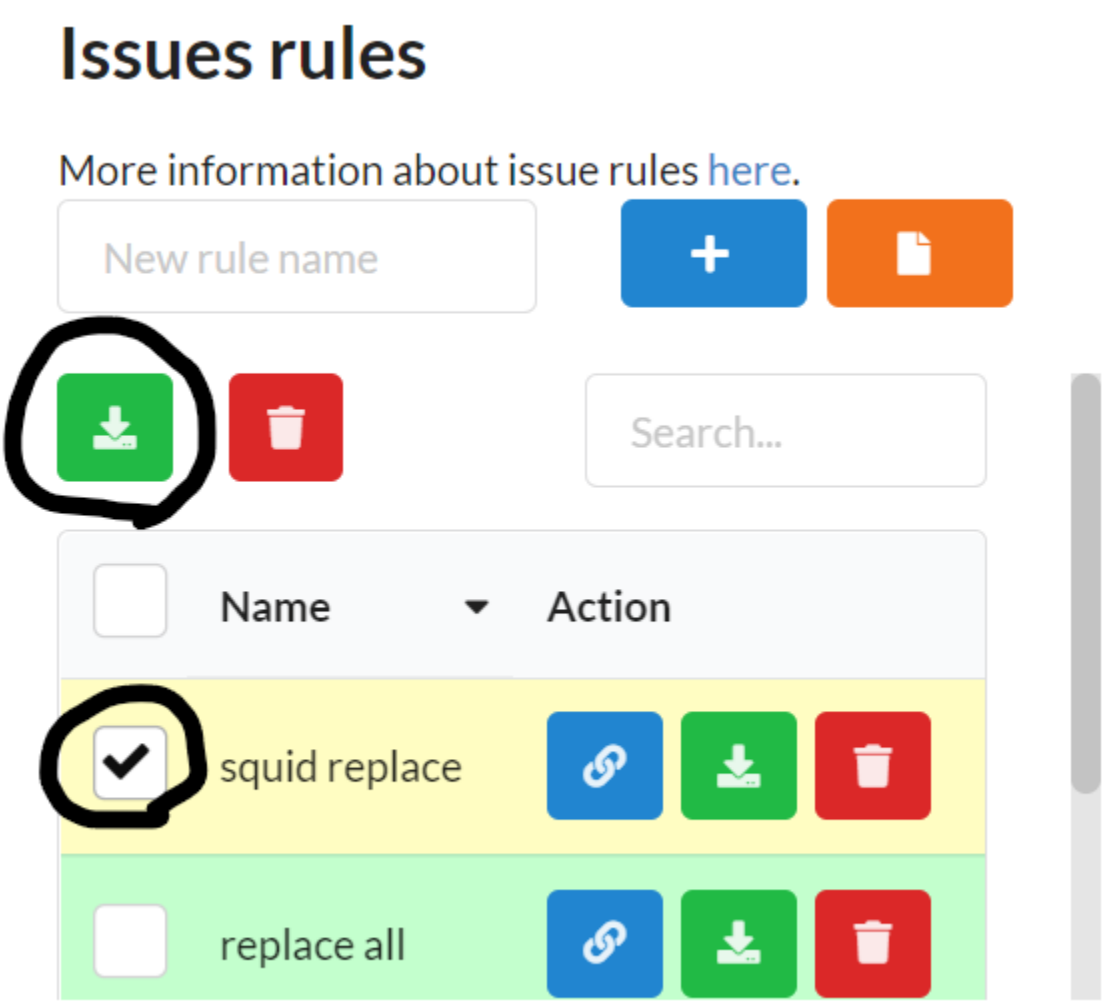
It will use selected rules at selected issues.

JSON features

You can also download/upload issue rules using JSON-files.

Download

Select rules at Profile -> Configs or Team -> Configs pages:



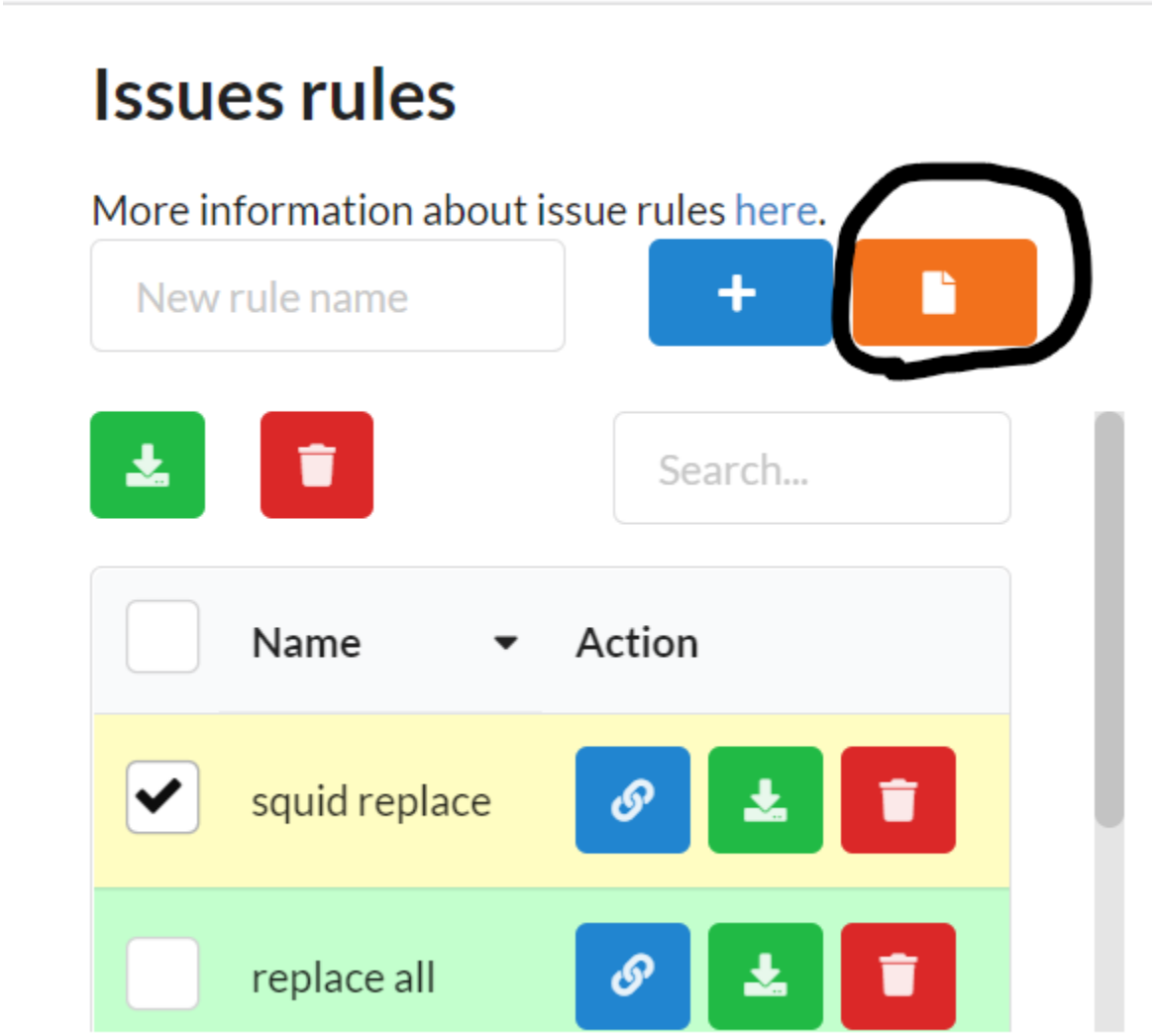
Example of JSON:


```
[
  {
    "extract_vars": [
      {
        "field_name": "name",
        "name": "test_name",
        "type": "regexp",
        "value": "^([\\s\\S]*)$"
      }
    ],
    "name": "Nessus plugin id",
    "replace_rules": [
      {
        "id": "cc7ebb3f-64eb-41a2-81a9-7b30ba04dffb",
        "md5": "3c82edeeb913f84a2b81b9a027b5db3a",
        "type": "template",
        "vars": {
          "service-name": "text {{test_name}} text"
        }
```

```
      },
      {
        "field_name": "fix",
        "replace_string": "New{{test_name}} string",
        "search_filter": "^[\\s\\S]*$",
        "type": "regexp"
      }
    ],
    "search_rules": [
      {
        "field_name": "__nessus_plugin_id__",
        "type": "substring",
        "value": "150154"
      }
    ]
  }
]
```

Upload

You just need to press this button:



If you use issue templates inside rules, it will try:

1. Search for issue template by its ID and check if owner of template is this team/profile.
2. Search for issue template by its MD5-checksum and check if owner of template is this team/profile.

If it doesn't find template, it will not be added to new created rule.

Restrictions

- If you want others to use created rule, check that they have access to used issue templates
- There are some time limits for operations due to fix ReDOS attack (2 sec for any RegExp operation)

Reports moderation

Sequencing

№	Action
1	Open new network form
2	Add new project network
3	Check it at networks list page
4	Get visualized network at networks list page

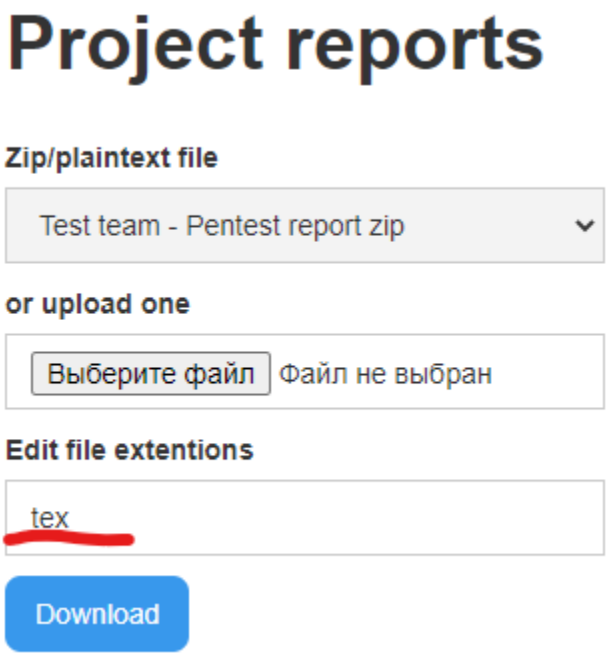
Tutorial

Next steps will help you to generate report with template. If you want to get just JSON project file - go to Endpoints part.

Step no 1: choose template type

There are three types of templates:

1. **Plaintext files** - just file with template fields. It can be any type: .txt, .html, .tex and so on. There is an example of Latex .tex template inside /report/examples folder.
2. **ZIP archive** - zip archive with plaintext/docx files. Any time you use this type of template - you need to set plaintext file extention or "docx" (inside .zip) to report creation form:



3**. docx files** - Best way! It uses crossplatform [docxtpl](#) library to parse .docx template and generate a report!

Step №2: examining the template engine

All three types uses [JINJA](#) template engine!

(.docx template also have some additional jinja tags)

Example report.txt file:

```
{% for i in example_array %}
    {{index.loop}}
{% endfor %}
```

Step №3: creating template

You must learn how to insert project variables inside template, so we created variable name map, which you can find at [/documentation/report/report_fields.txt](#)

Fragment of file:

```
. . .
2. issues {issue_id}
```

```
        2.1 name
        2.2 cve
        2.3 cwe
        2.4 cvss
        2.5 criticality [critical, high, medium, low, info]
        2.6 services {port_id}
                2.6.1 ip
                2.6.2 is_ip   # True/False
                2.6.3 hostnames [hostname_id,...]

. . .

5. ports {port_id}
        5.1 port
        5.2 is_tcp  # True / False
        5.3 comment
        5.4 service

. . .
```

.. and the example of creating list of issues:

```
{% for issue_id in issues %}
        Name - {{issues[issue_id]['name']}}
        {% if criticality=='critical' %}
                !!!RED ALERT!!!
        {% endif -%}
        {% set services = issues[issue_id]['services'] -%}
        {% for port_id in services -%}
                {% if ports[port_id]['port']== 0 %}
                        WHOLE HOST!
                {% else %}
                        JUST {{ports[port_id]['port']}} port :)
                {% endif %}
        {% endfor -%}
{% endfor -%}
```

Example output:

```
        Name - SQL injection

                        WHOLE HOST!


                        JUST 8080 port :)


                        WHOLE HOST!


        Name - XXE

        Name - CSRF
```

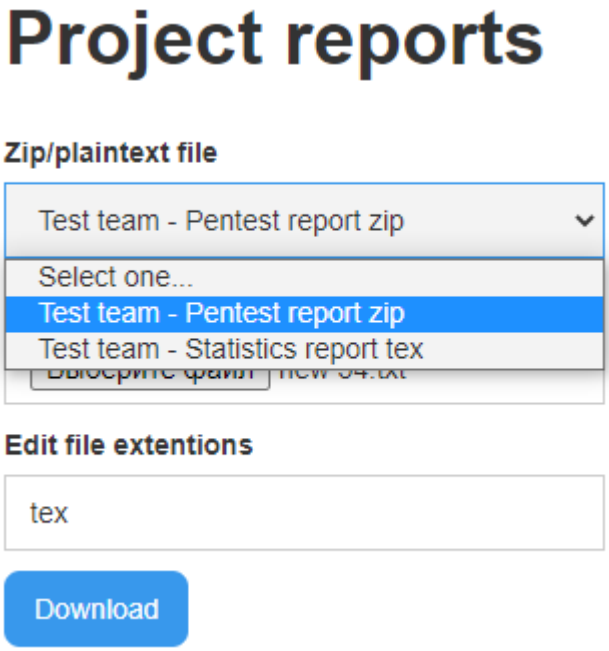
```
Name - PHP version disclosure
```

Step №4: save template (optional)

You can save team template at Teams page or personal templates at Personal page.

Step №5: use template

If you saved it before - you just need to select it from drop-down menu:



or upload it with file upload form and press **Download** button!

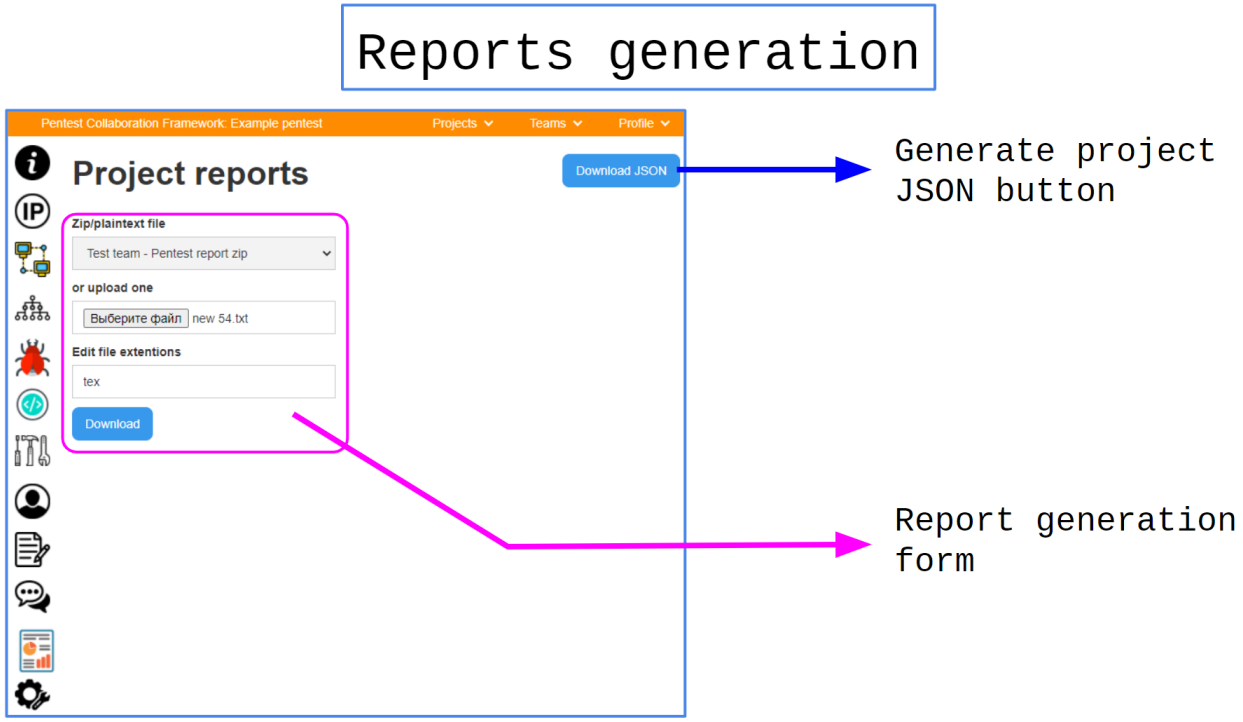
Don't forget to set plaintext/docx filetypes (saved in .zip) even if you saved .zip template before!

Endpoints

Reports page

Name	Value
URL	`/project/{{project_uuid}}/reports/`
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/reports/`
Description	Project report generation page.
Capabilities	1. Generate report from template

Name	Value
	2. Get JSON of project.
Comments	-



JSON Project download

Name	Value
URL	`/project/{{project_uuid}}/reports/export/json`
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/reports/export/json`
Description	Project JSON generation page.
Capabilities	Generated JSON file of project.
Comments	-

Project JSON generation


```
[{"cve":"2020-1234","cvss":9.5,"cwe":88,"description":"SQL injection description.","fix":"To fix it you
just need...","id":"3037349b-0111-4a62-a92d-4d10c5337daf","name":"SQL injection","param":"GET
id=1","project_id":"dfe91b40-1854-48ad-a127-01ff201f2884","services":[{"hostnames":
[],"ip":"2.2.2.2","pocs":[{"filename":"LogoMakr-71wG4m
(1).png","type":"image","url":"/static/files/poc/1069ce03-185e-4861-8e2c-c32dd667ae44"},{"filename":"new
54.txt","type":"text","url":"/static/files/poc/9a215828-fa20-4e09-8713-f66625d067b8"}],"port":0},
{"hostnames":[],"ip":"3.3.3.3","pocs":[{"filename":"LogoMakr-71wG4m
(1).png","type":"image","url":"/static/files/poc/1069ce03-185e-4861-8e2c-c32dd667ae44"},{"filename":"new
54.txt","type":"text","url":"/static/files/poc/9a215828-fa20-4e09-8713-f66625d067b8"}],"port":8080},
{"hostnames":["google.com"],"ip":"1.1.1.1","pocs":[{"filename":"LogoMakr-71wG4m
(1).png","type":"image","url":"/static/files/poc/1069ce03-185e-4861-8e2c-c32dd667ae44"},{"filename":"new
54.txt","type":"text","url":"/static/files/poc/9a215828-fa20-4e09-8713-
f66625d067b8"}],"port":0}],"status":"Confirmed","type":"web","url_path":"/phpmyadmin/index.php","user_id":"
c94ff3d3-8217-4242-914a-052ac29dde22"},{"cve":"","cvss":8.0,"cwe":0,"description":"XXE
example\r\nmultiline\r\ndescription","fix":"","id":"9fefbbc3-27c8-4499-b09c-
e4f774e02e7b","name":"XXE","param":"","project_id":"dfe91b40-1854-48ad-a127-01ff201f2884","services":
[],"status":"Not comfirmed","type":"custom","url_path":"","user_id":"c94ff3d3-8217-4242-914a-
052ac29dde22"},{"cve":"","cvss":2.0,"cwe":0,"description":"CSRF example
description","fix":"","id":"c055de07-6977-43e5-872b-
a87ea005172c","name":"CSRF","param":"","project_id":"dfe91b40-1854-48ad-a127-01ff201f2884","services":
[],"status":"Pending...","type":"custom","url_path":"","user_id":"c94ff3d3-8217-4242-914a-052ac29dde22"},
{"cve":"","cvss":0.0,"cwe":0,"description":"PHP version disclosure from headers","fix":"","id":"0ee6aad7-
50e2-486d-a9b0-24940d5b8282","name":"PHP version disclosure","param":"","project_id":"dfe91b40-1854-48ad-
a127-01ff201f2884","services":[],"status":"Need to
recheck","type":"custom","url_path":"","user_id":"c94ff3d3-8217-4242-914a-052ac29dde22"}]
```


Files moderation

Sequencing

№	Action
1	Open project files list
2	Add a new text/image/binary file
3	View it

You can change some file options at Settings page!

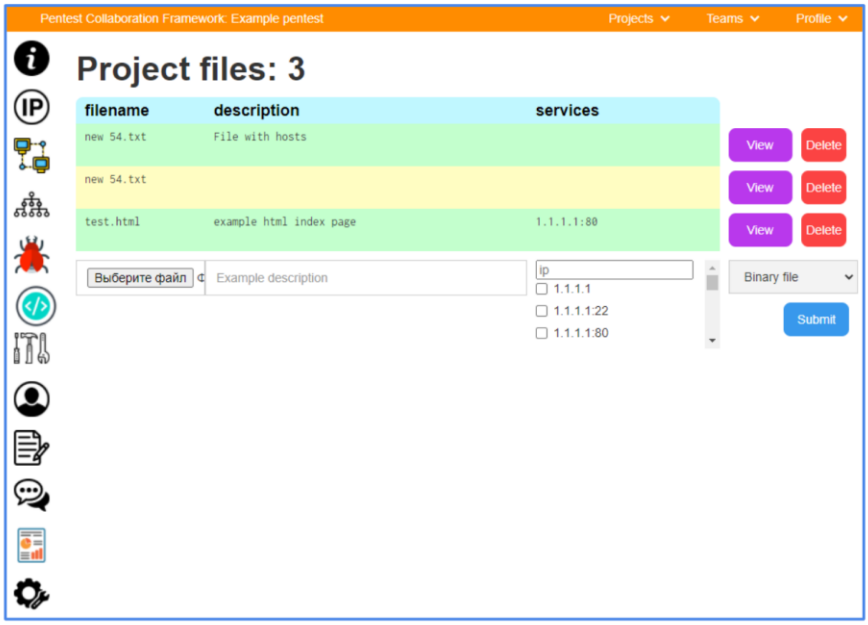
Endpoints

Files list

Name	Value
URL	`/project/{{project_uuid}}/files/`

Name	Value
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/files/`
Description	Project files list.
Capabilities	1. View/modify project files 2. Upload file form
Comments	-

Files list



File viewer

Name	Value
URL	`/project/{{project_uuid}}/files/{{file_uuid}}/`
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/files/a87172bf-b226-43d9-92fd-ef16672a8d22/`
Description	Project file viewer.
Capabilities	View/Download/Remove files
Comments	-

File viewer

File download

Name	Value
URL	`/static/files/code/{{file_uuid}}`
URL example	`/static/files/code/a87172bf-b226-43d9-92fd-ef16672a8d22`
Description	Project file downloader.
Capabilities	Download file by uuid
Comments	-

Credentials moderation

Sequencing

№	Action
1	Open project credentials

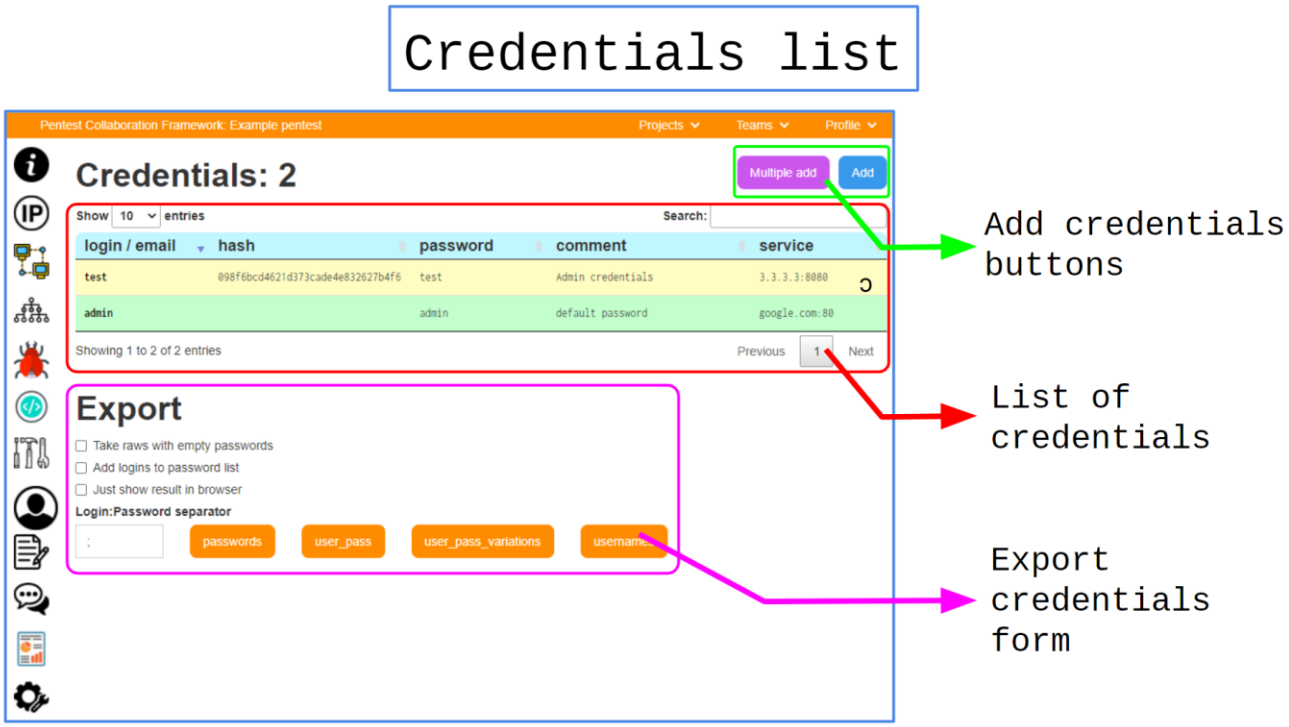
№	Action
	list
2	Add new found credentials
3	Check their information
4	Export credentials

You can change some credentials options at Settings page!

Endpoints

Credentials list

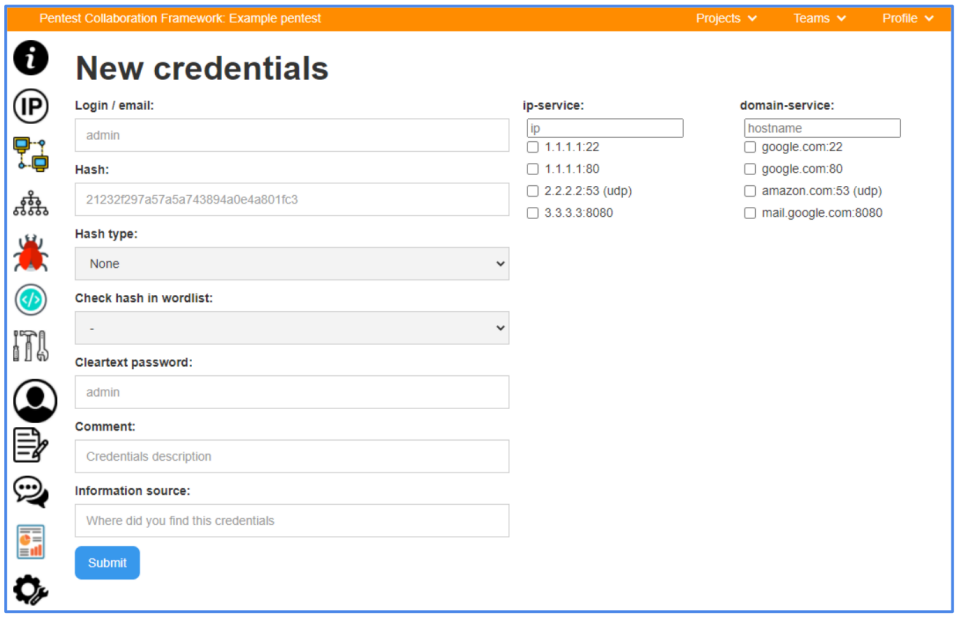
Name	Value
URL	`/project/{{project_uuid}}/credentials/`
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/credentials/`
Description	Project credentials list.
Capabilities	List of credentials.
Comments	-



Add single credentials

Name	Value
URL	`/project/{{project_uuid}}/credentials/new_creds`
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/credentials/new_creds`
Description	Add new single credentials.
Capabilities	Add new project single credentials form.
Comments	-

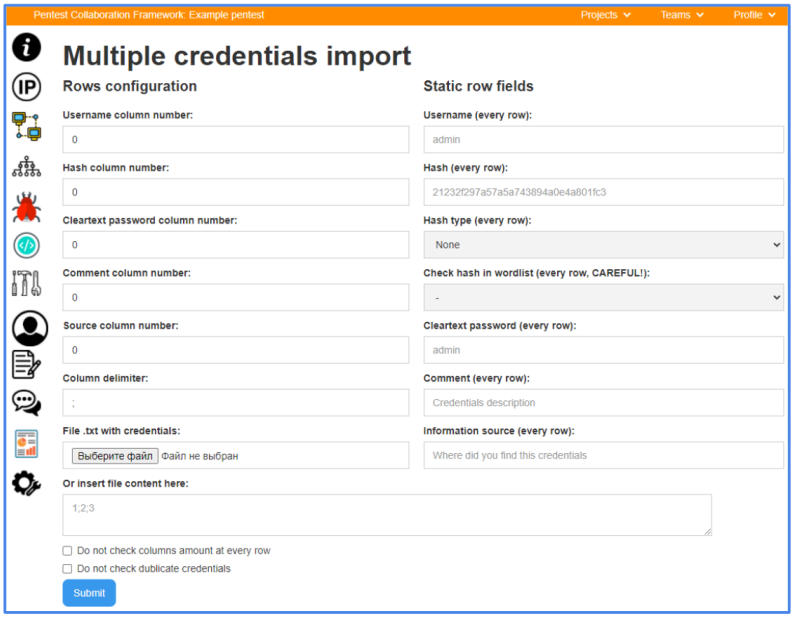
Add single credentials form



Add multiple credentials

Name	Value
URL	`/project/{{project_uuid}}/credentials/import_creds`
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/credentials/import_creds`
Description	Add multiple credentials.
Capabilities	Add new project multiple credentials form.
Comments	-

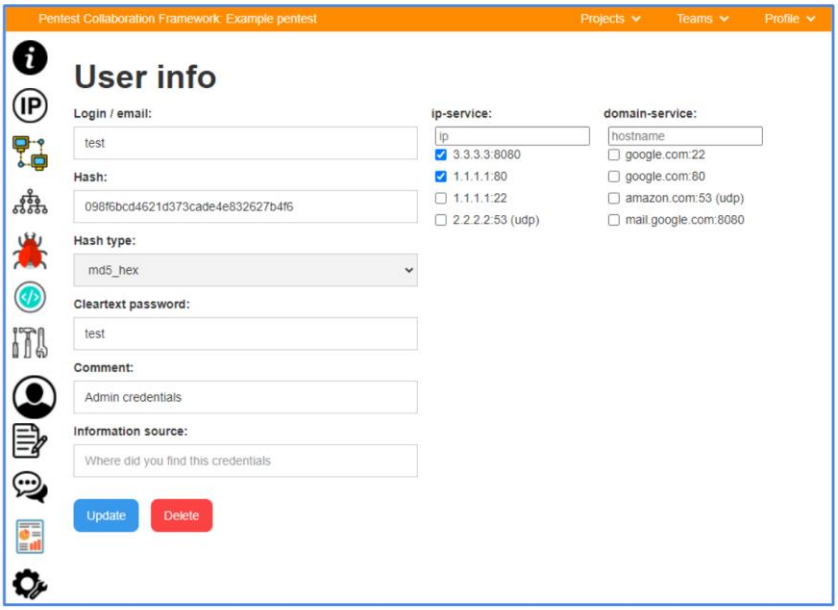
Add multiple credentials form



Credentials Information

Name	Value
URL	`/project/{{project_uuid}}/credentials/{{credentials_uuid}}`
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/credentials/6f81a2bf-4767-41e1-a7f3-e8ce0f3318a6/`
Description	Credentials information page.
Capabilities	View/edit credentials information.
Comments	-

Credentials editing form



Notes moderation

Sequencing

№	Action
1	Open project notes page
2	Create new note
3	Update note text

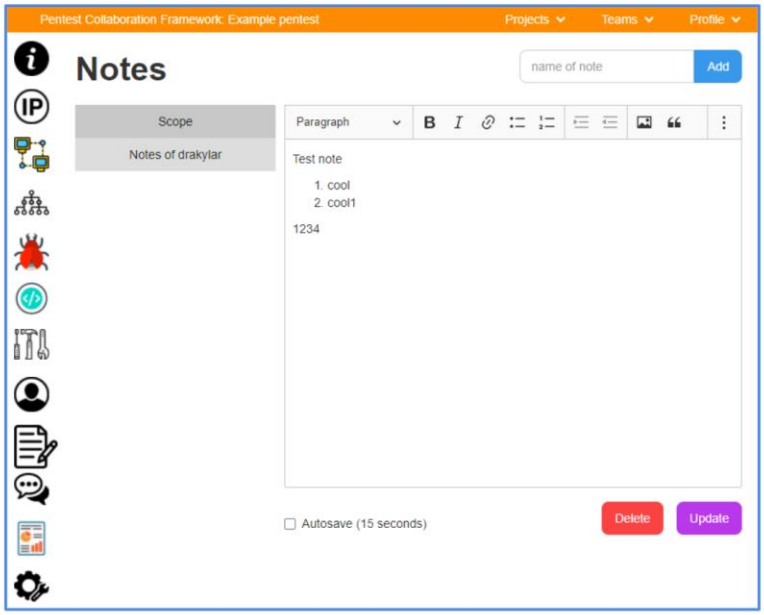
Endpoints

Notes Page

Name	Value
URL	`/project/{{project_uuid}}/notes/`
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/notes/`

Name	Value
Description	Project notes page.
Capabilities	1. View/edit existed notes 2. Create new notes.
Comments	-

Notes page



Chats moderation

Sequencing

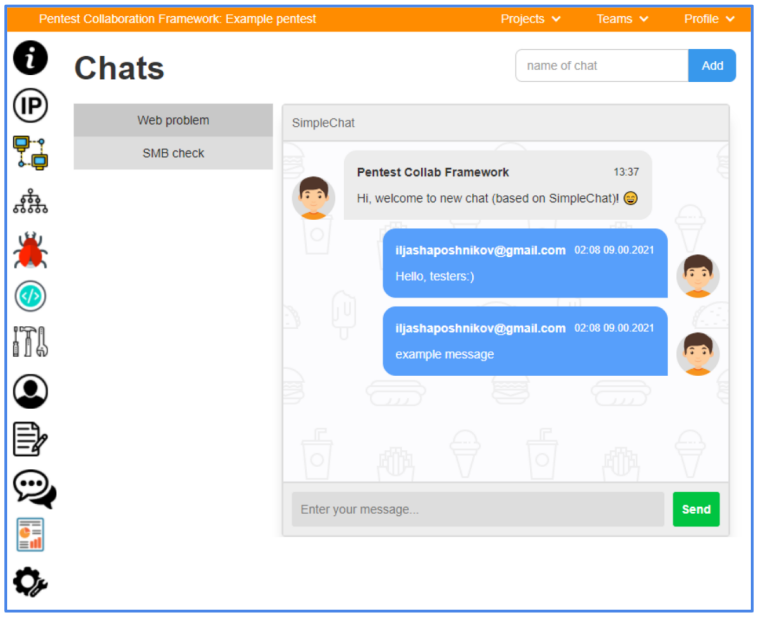
№	Action
1	Open project chats page
2	Create a new chat
3	Start chatting

Endpoints

Chats Page

Name	Value
URL	`/project/{{project_uuid}}/chats/`
URL example	`/project/53ade0ed-ea2d-4812-9676-8bdcf5b7412c/chats/`
Description	Project chats list.
Capabilities	Create chats, send messages.
Comments	-

Chats page



Tools Usage

Supported tools

Tool name	Integration type	Description
Nmap	Import	Import XML results (ip, port, service type, service version, hostnames, os). Supported plugins: vulners
Nessus	Import	Import .nessus results (ip, port, service type, security issues, os)
Qualys	Import	Import .xml results (ip, port, service type, security issues)

Tool name	Integration type	Description
Masscan	Import	Import XML results (ip, port)
Nikto	Import	Import XML, CSV, JSON results (issue, ip, port)
Acunetix	Import	Import XML results (ip, port, issue)
Burp Suite Enterprise	Import	Import HTML results (ip, port, hostname, issue, poc)
kube-hunter	Import	Import JSON result (ip, port, service, issue)
Checkmarx SAST	Import	Import XML/CSV results (code info, issue)
Dependency-check	Import	Import XML results (code issues)
OpenVAS/GVM	Import	Import XML results (ip, port, hostname, issue)
NetSparker	Import	Import XML results (ip, port, hostname, issue)
BurpSuite	Import/Extention	Extention for fast issue send from burpsuite.
WPScan	Import	Import JSON results (ip, port, hostname, issue)
DNSrecon	Import	Import JSON/CSV/XML results (ip, port, hostname)
theHarvester	Import	Import XML results (ip, hostname)
Metasploit	Import	Import XML project (ip, port, hostname, issue)
Nuclei	Import	Import JSON results (ip, hostname, port, issue)
PingCastle	Import	Import XML results (ip, issue)
MaxPatrol	Import	Import XML results (ip, port, issue)
Scanvus	Import	Import JSON report (issue)