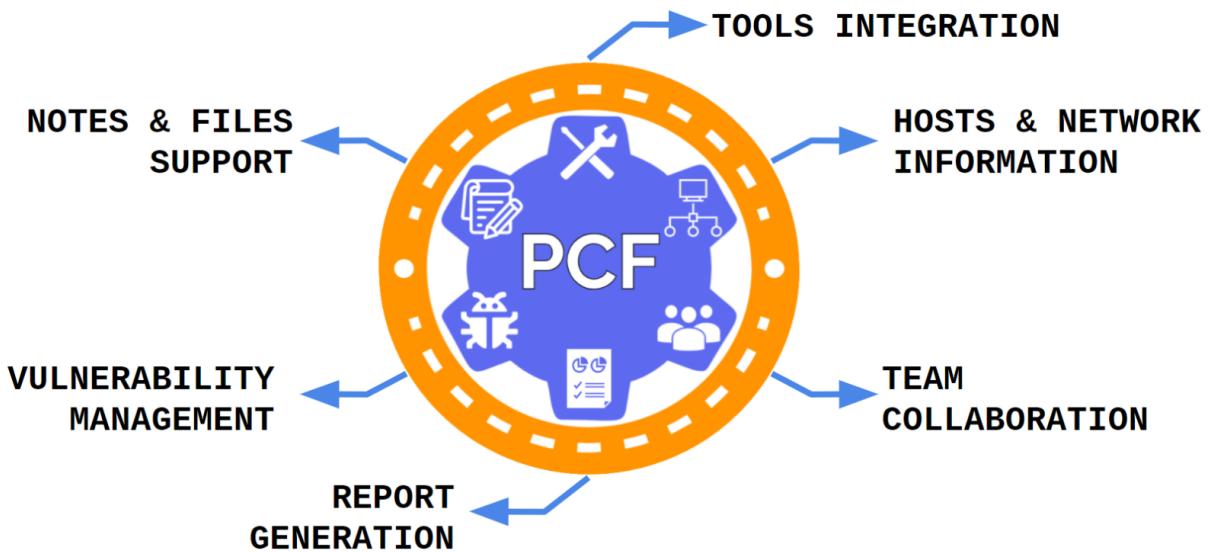


**MENU** 

## PENTEST COLLABORATION FRAMEWORK



## Table of Contents

Usage.....	4
Teams .....	4
Sequencing.....	4
Endpoints .....	5
Projects.....	11
Sequencing.....	11
Endpoints .....	12
Hosts.....	14
Sequencing.....	14
Endpoints .....	15
Networks Moderation .....	22
Sequencing.....	22
Endpoints .....	22
Issues moderation.....	27
Sequencing.....	27
Endpoints .....	27
Issue Templates .....	32
Issue rules.....	40
Reports moderation.....	49
Sequencing.....	49
Tutorial .....	49
Endpoints .....	52
Files moderation.....	54
Sequencing.....	54
Endpoints .....	54
Credentials moderation .....	56
Sequencing.....	56
Endpoints .....	57
Notes moderation .....	61
Sequencing.....	61
Endpoints .....	61
Chats moderation .....	62
Sequencing.....	62
Endpoints .....	62
Tools Usage.....	63

Supported tools .....	63
-----------------------	----

# Usage

## Teams

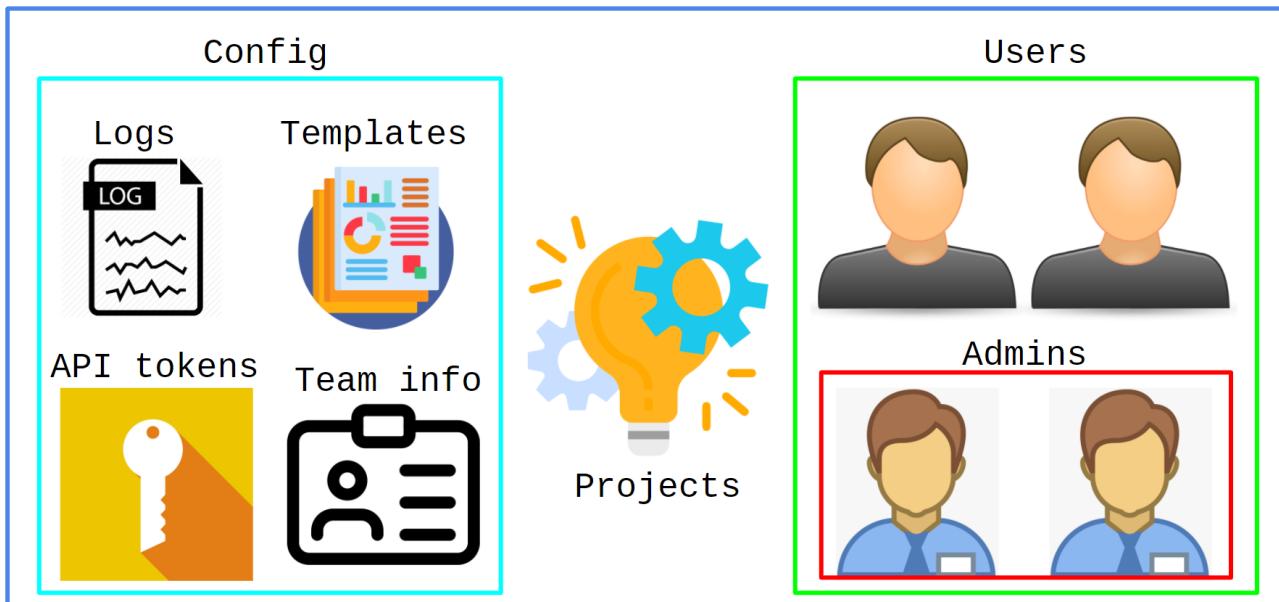
**Team menu buttons**

The screenshot shows a user interface with a top navigation bar containing 'Projects', 'Teams', and 'Profile' dropdowns. The 'Teams' dropdown is open, displaying three team names: 'RedTeam', 'Invuls', and 'BlueTeam', each enclosed in a rounded red box. Below the dropdown is a green rectangular button with white text that reads '+ Add new'. To the right of the screenshot, there are two annotations: a red arrow pointing to the 'RedTeam', 'Invuls', and 'BlueTeam' items with the text 'Already created teams'; and a green arrow pointing to the '+ Add new' button with the text 'Create new team'.

## Sequencing

Nº	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 <a href="#">Projects</a> page!

# Team workspace



## 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

Pentest Collaboration Framework

Projects ▾ Teams ▾ Profile ▾

## Create new team

Team name:

Description:

**Submit**

### Team information

Name	Value
URL	/team/{team_UUID}
URL example	/team/760a3c76-2b65-4558-9f66-876a5c772c8e/
Description	Get team information
Capabilities	<ol style="list-style-type: none"><li>1. Edit team information</li><li>2. Edit team users</li><li>3. Get team projects</li><li>4. Get team logs</li><li>5. Edit team configs.</li></ol>
Comments	-

### Team information: edit info

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

## Team page

Team name

Team config tabs

Tab workspace

The screenshot shows the 'Team info: Test team' section. At the top, there is a navigation bar with tabs: About, Testers, Administrators, Projects, Logs, and Configs. The 'Testers' tab is highlighted with a red border. Below the navigation bar, there is a form with fields for 'Team name' (containing 'Test team'), 'Creator/Main admin email (change careful!)' (containing 'iljashaposhnikov@gmail.com'), and 'Description' (containing 'Test team description'). A green arrow points from the 'Description' field to the text 'Tab workspace'.

## Team information: testers list

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

## Team testers page

Testers list & action form

New tester form

The screenshot shows the 'Team info: Test team' section. It displays a list of testers with one entry: '- iljashaposhnikov1@gmail.com'. To the right of this entry are three buttons: 'Profile' (blue), 'Set admin' (orange), and 'Kick' (red). A red arrow points from the 'Kick' button to the text 'Testers list & action form'. Below the tester list is a form titled 'Add new tester:' containing a single input field with the value 'test@example.com' and a 'Submit' button. A green arrow points from this form to the text 'New tester form'.

## Team information: admins list

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

### Team admins page

The screenshot shows a web interface titled "Team admins page". At the top, there's a navigation bar with "Pentest Collaboration Framework" and dropdown menus for "Projects", "Teams", and "Profile". Below the header, it says "Team info: Test team". A horizontal menu bar includes "About", "Testers", "Administrators" (which is highlighted), "Projects", "Logs", and "Configs". A red box highlights the "Administrators" section, which lists "Ivan Ivanov - ivan@gmail.com" with buttons for "Profile", "Devote", and "Kick". Below this is a green box containing a form titled "Add a new admin:" with a text input field containing "admin@example.com" and a "Submit" button.

Red arrow: Admins list & action form

Green arrow: New tester form

## Team Information: Projects list

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

### Team projects page

The screenshot shows a web interface titled "Team projects page". At the top, there's a navigation bar with "Pentest Collaboration Framework" and dropdown menus for "Projects", "Teams", and "Profile". Below the header, it says "Team info: Test team". A horizontal menu bar includes "About", "Testers", "Administrators", "Projects" (which is highlighted), "Logs", and "Configs". A red box highlights the "Active projects:" section, which lists "Example pentest" with buttons for "Open" and "Archive". A blue arrow points from this section to a blue button labeled "Add new". Below this is a green box containing the "Archived projects:" section, which lists "Old project" with buttons for "Activate" and "Reports".

Red arrow: Active projects list

Blue arrow: New project button

Green arrow: Old projects list

## 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 actions logs

The screenshot shows a web application interface for 'Ppentest Collaboration Framework'. At the top, there's a navigation bar with links for 'Projects', 'Teams', and 'Profile'. Below the navigation, the title 'Team info: Test team' is displayed. Underneath the title is a horizontal menu bar with tabs: 'About', 'Testers', 'Administrators', 'Projects', 'Logs', and 'Configs'. The 'Logs' tab is currently selected. A large text area contains a log of team actions:

```
08-01-2021 00:11:56 - Project: User: iljashaposhnikov@gmail.com -- Project Old project was created!
08-01-2021 00:11:09 - Project: User: iljashaposhnikov@gmail.com -- Project Example pentest was created!
07-01-2021 23:59:16 - Project: User: iljashaposhnikov@gmail.com -- User iljashaposhnikov1@gmail.com role
was changed to tester!
07-01-2021 23:58:30 - Project: User: iljashaposhnikov@gmail.com -- Team "Test team" was created!
```

## Team Information: Variables & Templates

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

# Team configs

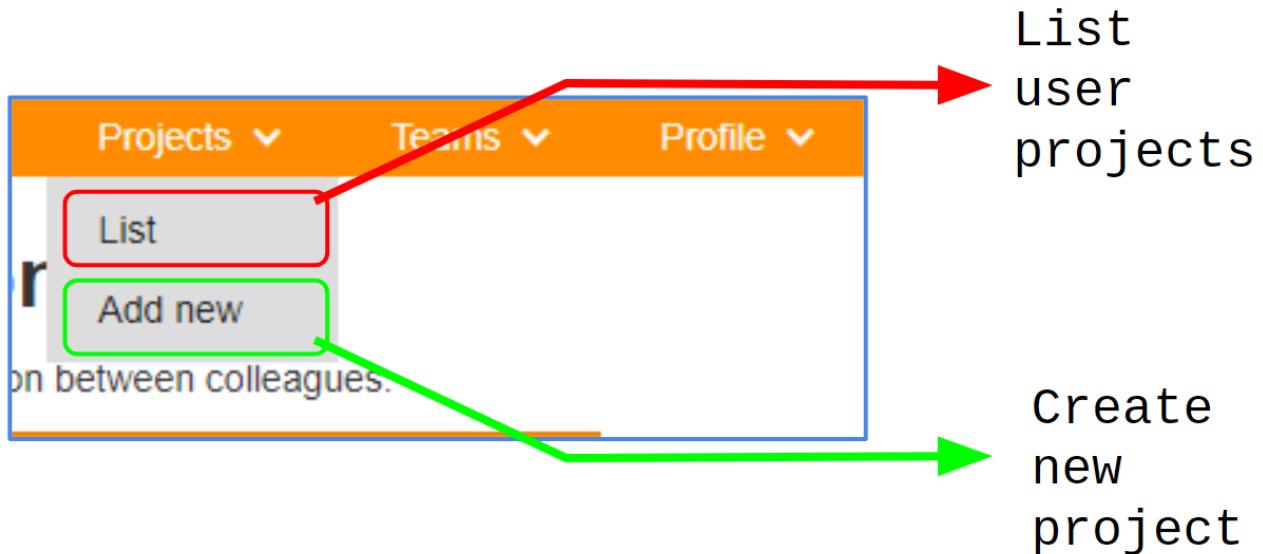
Variables/tokens  
list & form

Templates  
editor

The screenshot shows the 'Team info: Test team' page. At the top, there are navigation tabs: Projects, Teams, and Profile. Below the tabs, there are buttons for About, Testers, Administrators, Projects, Logs, and Configs. The main content area has two sections: 'Variables' and 'Report templates'. The 'Variables' section contains fields for Shodan API key and Zeneye API key, each with an 'Edit' and 'Delete' button. The 'Report templates' section has a 'Report name' field with a file upload button ('Выберите файл') and a 'Submit' button. It also includes download and delete buttons for 'Pentest report zip' and 'Statistics report tex'.

## Projects

### Project menu buttons



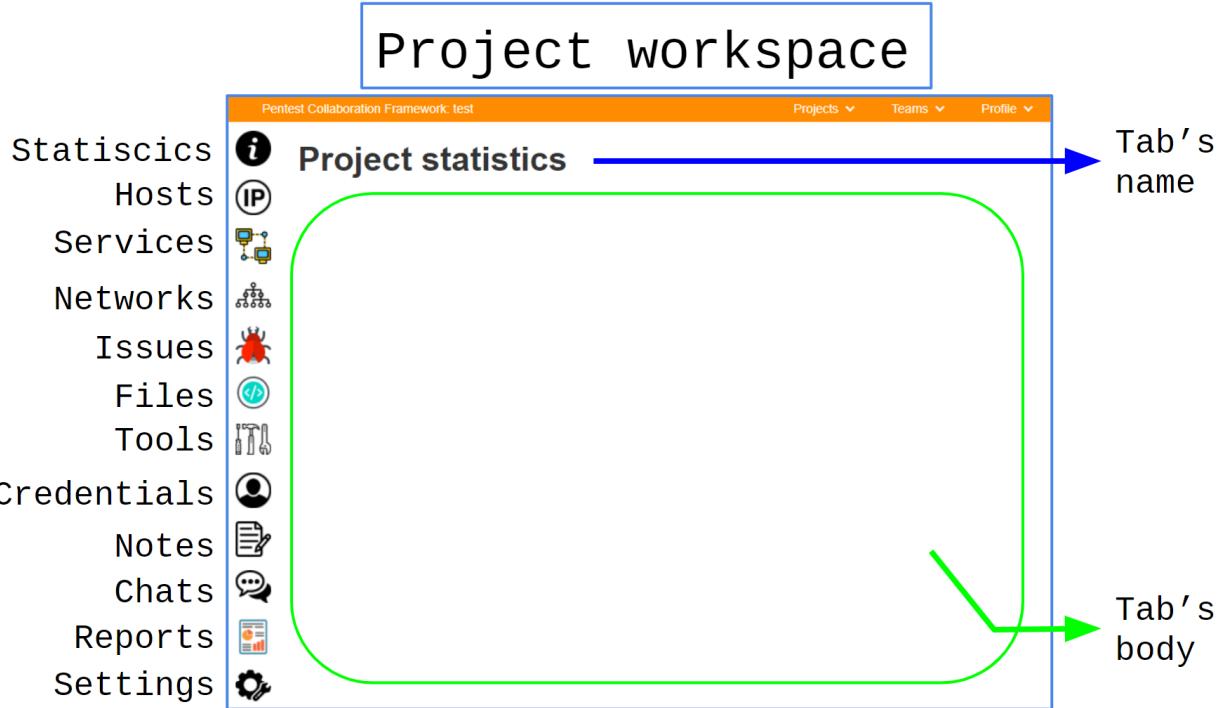
## Sequencing

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

Pentest Collaboration Framework

Projects ▾ Teams ▾ Profile ▾

Add new project:

**Name:**

**Description:**

**Project type:**

**Scope info:**

Auto archive project after finish date

**Choose teams for project:**  
 RedTeam  
 Test team

**Choose testers for project (from team admin/tester list):**  
 - iljashaposhnikov1@gmail.com

**Submit**

## 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**

Pentest Collaboration Framework: test

Project settings

Name: test

Description: test

Project type: pentest

Scope info: testing scope

Auto archive project after finish date:

11/29/2020

04/13/3000

Choose teams for project:

- RedTeam
- Test team

Choose testers for project:

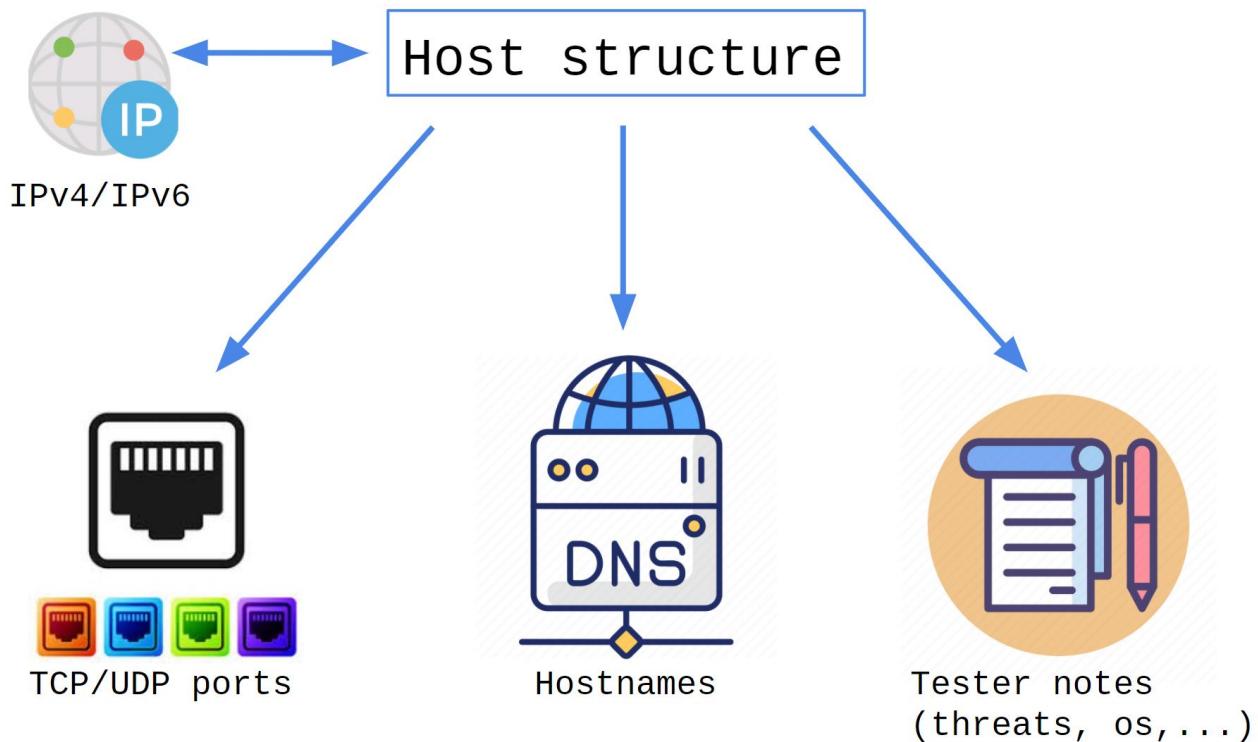
- iljashaposhnikov1@gmail.com

Update Archive

## 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-4812-9676-8bd5b7412c/hosts/
Description	Project hosts list
Capabilities	Search for hosts, filter them or go to "Create Host" or "Export hosts" forms.
Comments	-

**Host list**

Search/Export and new host buttons

Search/export form

Hosts table

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.

## 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

Pentest Collaboration Framework: test      Projects ▾      Teams ▾      Profile ▾

## Add new host

**IP**

IP-address

Comment

**Submit**

### 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	<ol style="list-style-type: none"><li>1. Edit host info</li><li>2. Modify ports</li><li>3. Modify hostnames</li><li>4. Modify issues</li><li>5. Modify credentials</li></ol>
Comments	<ol style="list-style-type: none"><li>4. More about <a href="#">Issues</a></li><li>5. More about <a href="#">Credentials</a></li></ol>

**Host page**

The Host page displays host details for IP 1.1.1.1. It includes sections for Services, Hostnames, Issues, and Credentials. A green box highlights the Services section, which lists ports, services, and threats. A red box highlights the Host info form at the bottom right.

**Host's IP:** 1.1.1.1

**Host tabs:** Services, Hostnames, Issues, Credentials

**Tab's body:** Services section (highlighted by a green box)

**Host info form:** Host comment, Threats (High, Medium, Low, Information, Need to check again, Checked), Operating system (other or Windows 7) (highlighted by a red box)

Host information: ports  
**Ports must be unique for one host!**

**Host ports**

The Host ports interface shows the same host information as the Host page, but with a focus on port details. A green box highlights the Services section, and a pink box highlights the port action buttons (Update, Delete) for each row. A red box highlights the Port create/edit form at the bottom right.

**Ports information:** Services section (highlighted by a green box)

**Port action buttons:** Update, Delete buttons for each port entry (highlighted by a pink box)

**Port create/edit form:** Port comment, Threats (High, Medium, Low, Information, Need to check again, Checked), Operating system (other or Windows 7) (highlighted by a red box)

Host information: hostnames  
**Hostnames must be unique for one host!**

## Hostnames

The screenshot shows the 'Hostnames' section of the Pentest Collaboration Framework. At the top, there are navigation tabs: Services, Hostnames (which is selected), Issues, and Credentials. Below the tabs, there's a table with columns for 'hostname' and 'comment'. A green box highlights the first row ('google.com', 'example'). To the right of the table is a form for creating or editing a hostname, with fields for 'Host comment:' (containing 'wefwef'), 'Threats:' (checkboxes for High, Medium, Low, Information, Need to check again, Checked!), and 'Operating system:' (dropdowns for 'other' and 'Windows 7'). Below the form are 'Update' and 'Delete' buttons. A red box highlights the 'Submit' button. A pink box highlights the 'Edit' and 'Delete' buttons for the first row in the table. A green arrow points from the text 'Hostnames info' to the table. A pink arrow points from the text 'Hostname action buttons' to the 'Edit' and 'Delete' buttons. A red arrow points from the text 'Hostname create/edit form' to the 'Submit' button.

## Host information: issues

More info here: [Issues](#)

## Host issues

The screenshot shows the 'Host issues' section of the Pentest Collaboration Framework. At the top, there are navigation tabs: Services, Hostnames, Issues (selected), and Credentials. Below the tabs, there's a table with columns for 'port', 'name', 'description', 'CVSS', and 'status'. A green box highlights the first row ('444/tcp', 'SQL injection', '/admin/?id=' and ''1'='1', '9.5', 'PoC creation'). To the right of the table is a form for creating a new vulnerability, with fields for 'Host comment:' (containing 'wefwef'), 'Threats:' (checkboxes for High, Medium, Low, Information, Need to check again, Checked!), and 'Operating system:' (dropdowns for 'other' and 'Windows 7'). Below the form are 'Update' and 'Delete' buttons. A red box highlights the 'Add new vulnerability' button. A pink box highlights the 'Edit' and 'Delete' buttons for the first row in the table. A green arrow points from the text 'Issues information' to the table. A pink arrow points from the text 'Issues action buttons' to the 'Edit' and 'Delete' buttons. A red arrow points from the text 'Create new issue form' to the 'Add new vulnerability' button.

## Host information: credentials

More info here: [Credentials](#)

# Host credentials

Pentest Collaboration Framework: test

1.1.1.1

port	login	hash	cleartext	comment
Whole host	admin		admin	default password
444/tcp	test		testtest	brutted

New credentials form

Host comment: wefwef

Threats:  High  Medium  Low  Information  Need to check again  Checked!

Operating system: other or Windows 7

Submit

Whole host 1.1.1.1

## 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.

## Services statistics

Pentest Collaboration Framework: test

**Services: 111**

Add

Show 100 entries Search:

port	service	info	hosts	threats
11/tcp			1 hosts	
21/tcp			6 hosts	
21/tcp	ftp?	Added from Nessus scan	10.10.10.252	
21/tcp	ftp	Added from Nessus scan	10.10.10.150 10.10.10.134 10.10.10.70 10.10.10.67 10.10.10.66	!!
22/tcp			5 hosts	
22/tcp	ssh?	Added from Nessus scan	10.10.10.158 10.10.10.50	
22/tcp	ssh	Added from Nessus scan	10.10.10.54 10.10.10.52 10.10.10.49	!!!!!!
23/tcp			8 hosts	

### 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

Pentest Collaboration Framework: test

Projects ▾ Teams ▾ Profile ▾

### Add new service

**IP**

Port: 43 or 43/tcp or 43/udp

Service: HTTP

Information: Information about service

Submit

IP-address:

- 1.1.1.1
- 10.144.196.1
- 10.144.196.10
- 10.144.196.100
- 10.144.196.11
- 10.144.196.113
- 10.144.196.116
- 10.144.196.117
- 10.144.196.12
- 10.144.196.129
- 10.144.196.13

## Networks Moderation Sequencing

Nº	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

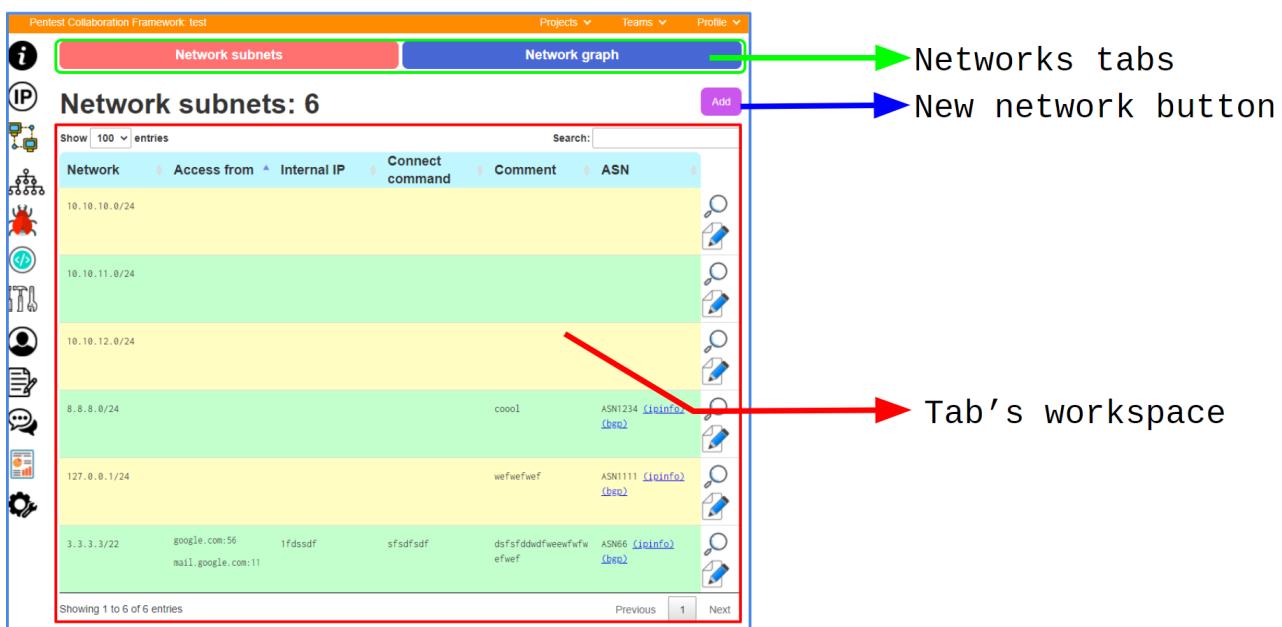
## Endpoints

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 page



The screenshot shows the 'Networks' page interface. At the top, there are three tabs: 'Network subnets' (highlighted in red), 'Network graph' (highlighted in blue), and 'Add'. A green arrow points from the 'Network subnets' tab to the text 'Networks tabs'. A blue arrow points from the 'Add' button to the text 'New network button'. Below the tabs is a section titled 'Network subnets: 6'. This section contains a table with the following data:

Network	Access from	Internal IP	Connect command	Comment	ASN
10.10.10.0/24					
10.10.11.0/24					
10.10.12.0/24					
8.8.8.0/24	coool			ASN1234 <a href="#">(ieinfo)</a> <a href="#">(beo)</a>	
127.0.0.1/24	wefwefwef			ASN1111 <a href="#">(ieinfo)</a> <a href="#">(beo)</a>	
3.3.3.3/22	google.com:56	fdssdf	sfsdfsdf	dsfsfddwdweewfwfw efwef	ASN66 <a href="#">(ieinfo)</a> <a href="#">(beo)</a>
mail.google.com:11					

A red arrow points from the table area to the text 'Tab's workspace'. At the bottom of the table, it says 'Showing 1 to 6 of 6 entries' and has navigation buttons for 'Previous', '1', and 'Next'.

## Networks list

# Networks list

The screenshot shows a web-based interface titled "Networks list". At the top, there are tabs for "Network subnets" (selected) and "Network graph". Below the tabs, the title "Network subnets: 6" is displayed. A search bar and a dropdown for "Show 100 entries" are present. The main area contains a table with the following data:

Network	Access from	Internal IP	Connect command	Comment	ASN
10.10.10.0/24					
10.10.11.0/24					
10.10.12.0/24					
8.8.8.0/24				coool	ASN1234 ( <a href="#">[info]</a> ) ( <a href="#">[bgp]</a> )
127.0.0.1/24				wefwefwef	ASN1111 ( <a href="#">[info]</a> ) ( <a href="#">[bgp]</a> )
3.3.3.3/22	google.com:56	1fdssdf	sfsdfsdf	dsfsfddwdfwewfwfw efwef	ASN66 ( <a href="#">[info]</a> ) ( <a href="#">[bgp]</a> )
mail.google.com:11					

On the right side of the table, there is a vertical column of icons representing filter and edit functions, each with a small green circle around it. A green arrow points from the text "Filter and edit buttons" to this column.

Showing 1 to 6 of 6 entries

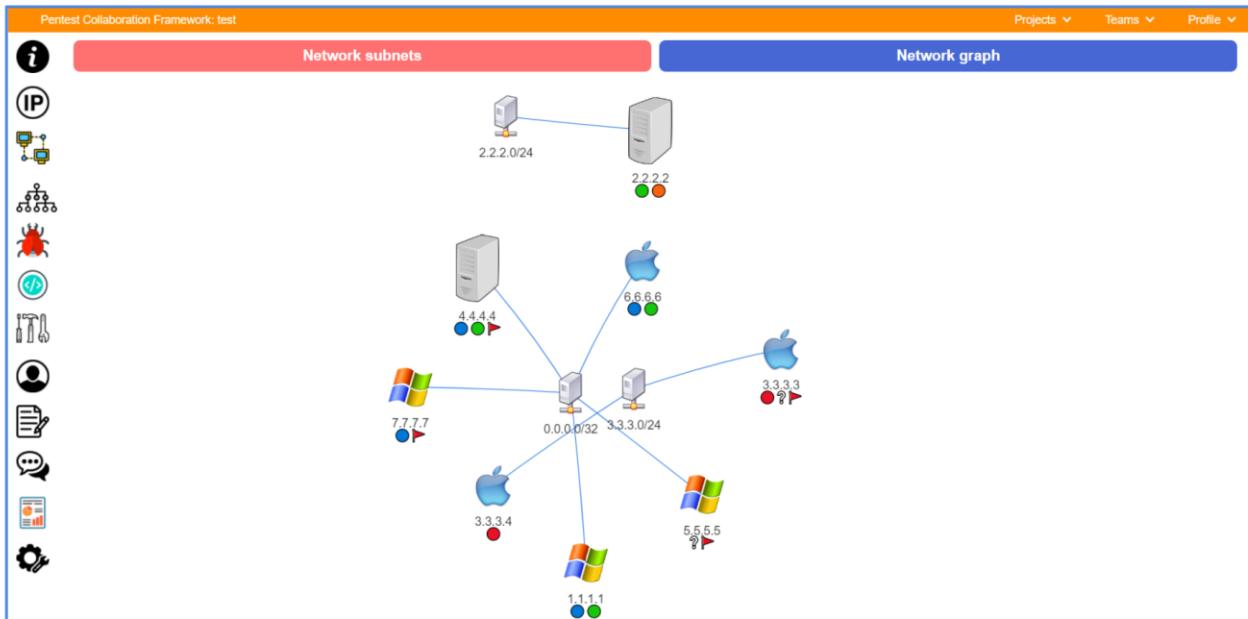
Filter and edit buttons

## 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

Pentest Collaboration Framework test

Projects ▾ Teams ▾ Profile ▾

## Add new network

**IP**

IP-address: 127.0.0.1  
Mask: 24  
Internal IP: 10.0.2.15  
ASN: 1337  
Comment: Network description  
Connection command: ssh -D 8888 root@localhost

**Access from...**

ip  
 1.1.1.1  
 1.1.1.1:11  
 1.1.1.1:53 (udp)  
 1.1.1.1:56 (udp)  
 1.1.1.1:444  
 10.10.10.1  
 10.10.10.10  
 10.10.10.100  
 10.10.10.1000  
 10.10.10.11  
 10.10.10.111  
 10.10.10.113  
 10.10.10.116  
 10.10.10.116  
hostname  
 google.com  
 google.com:11  
 google.com:53 (udp)  
 google.com:56 (udp)  
 google.com:444  
 mail.google.com  
 mail.google.com:11  
 mail.google.com:53 (udp)  
 mail.google.com:56 (udp)  
 mail.google.com:444  
 yahoo.yandex.google.com  
 yahoo.yandex.google.com:11  
 yahoo.yandex.google.com:53 (udp)  
 yahoo.yandex.google.com:56 (udp)  
 yahoo.yandex.google.com:444  
 localhost  
 localhost:135

**Submit**

## 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

Nº	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)

**Issues list**

Pentest Collaboration Framework: Internal pentest

**i Issues**

**IP**

name	description	addresses	CVSS	status
sql injection	sql injection at ...	8.8.8.8:44 wefwef.wefwef:44	10.0	PoC creation
XXE	XXE vulnerability in profile update form		10.0	Pending...
Local File Reading	Can read files with ../../..		7.5	Not confirmed
Admin easy password	admin/admin		7.0	PoC creation
XSS	XSS in GET-parameter id		5.0	Not confirmed
CSRF	CSRF vulnerability in form		3.0	Need to check
Information disclosure	Disclosure of server version		0.0	Need to recheck

Projects Teams Profile

Search... Search Add

name='admin page' & description='index.php'; addressess > 0

Open Open Open Open Open Open Open Open

New issues form button

Search form

Issues list

## 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

Pentest Collaboration Framework Example pentest

**Create new issues**

Vulnerability name: SQL injection...

URL path or service name: /admin/

Description:

CVSS: 0

CVE number: 2020-1337

CWE number: 123

Fix: To fix this vulnerability you need ...

Services:

- ip: 1.1.1.1, 1.1.1.22, 1.1.1.80, 2.2.2.2, 2.2.2.53 (udp), 3.3.3.3, 3.3.3.8080, 4.4.4.4
- hostname: google.com, google.com:22, google.com:80, amazon.com, amazon.com:53 (udp), mail.google.com, mail.google.com:8080

Status: PoC creation

Criticality: use CVSS criticality

Parameter: GET id=123

Type: Custom

Submit

## 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

Issue name

Issue info tabs

Tab's workspace

**Issue: SQL injection**

Vulnerability name: SQL injection

Description: SQL injection description.

Fix: To fix it you just need...

Services:

- IP: 3.3.3.8080, checked
- 2.2.2.2, checked
- 1.1.1.1, unchecked
- 1.1.1.22, unchecked
- 1.1.1.80, unchecked
- 2.2.2.53 (udp), unchecked
- 3.3.3.3, unchecked
- 4.4.4.4, unchecked

hostname: google.com, checked

URL path or service name: /phpmyadmin/index.php

CVSS: 9.5

CVSS Calculator

CVE number: 2020-1234

CWE number: 88

Status: Confirmed

Criticality: use CVSS criticality

Parameter: GET id=1

Type: web

Submit, Delete, Share

### Issue information: edit form

## Issue edit form

Share button

**Issue: SQL injection**

Vulnerability name: SQL injection

Description: SQL injection description.

Fix: To fix it you just need...

Services:

- IP: 3.3.3.8080, checked
- 2.2.2.2, checked
- 1.1.1.1, unchecked
- 1.1.1.22, unchecked
- 1.1.1.80, unchecked
- 2.2.2.53 (udp), unchecked
- 3.3.3.3, unchecked
- 4.4.4.4, unchecked

hostname: google.com, checked

URL path or service name: /phpmyadmin/index.php

CVSS: 9.5

CVSS Calculator

CVE number: 2020-1234

CWE number: 88

Status: Confirmed

Criticality: use CVSS criticality

Parameter: GET id=1

Type: web

Submit, Delete, Share

### Issue information: PoC form

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

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

# Issue PoC list

Pentest Collaboration Framework Example pentest

**Issue: SQL injection**

Info PoC

Search:

host comment proof-of-concept

2.2.2.2 Example PoC

3.3.3.3:8080 Example PoC text

```

form = EditNetwork()
form.validate()
errors = []
if form.errors:
    for error in form.errors:
        errors.append(error)
else:
    if form.action.data == 'Delete':
        db.delete_network(current_network['id'])

    is_ipv6 = False

    if not errors:
        is_ipv6 = ':' in form.ip.data

    if form.mask.data > 32 and not is_ipv6:
        errors.append('Mask too large for ipv4')

    services = {}

```

Showing 1 to 2 of 2 entries

No service Example Text Выберите файл файл не выбран Submit

Final PoC version

New PoC form

## 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.

## Shared issue

The screenshot shows a web-based application interface for managing security issues. At the top, there's a navigation bar with tabs for 'Projects', 'Teams', and 'Profile'. Below the navigation, a large title 'Issue: SQL injection' is displayed. The main form is divided into several sections:

- Vulnerability name:** SQL injection
- URL path or service name:** /phpmyadmin/index.php
- CVSS:** 9.5
- CVE number:** 2020-1234
- CWE number:** 88
- Status:** Confirmed
- Criticality:** use CVSS criticality
- Parameter:** GET id=1
- Type:** web

Under the 'Services' section, there are two input fields: 'ip' containing '3.3.3.3:8080' and 'hostname' containing 'google.com'. Both fields have checkboxes next to them, with '3.3.3.3:8080' and 'google.com' checked.

## Issue Templates

### Templates list

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

The screenshot shows a page titled 'Issues templates'. It includes a header with a link to 'More information about issue templates here.' and a search bar. Below the header, there are buttons for creating a new template ('+') and deleting a template ('trash'). There are also download and delete icons.

<input type="checkbox"/>	Name	Action
<input type="checkbox"/>	test template	

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:

The screenshot shows a user interface for managing issue templates. At the top, there's a header 'Issues templates' and a link 'More information about issue templates here.' Below this is a search bar with a placeholder 'Issue name' and a blue '+' button. A yellow box highlights this area. Below the search bar are two buttons: a green one with a download icon and a red one with a trash bin icon. To the right of the search bar is a 'Search...' input field. Underneath these are two rows of buttons. The first row has a checkbox labeled 'Name' and a dropdown menu labeled 'Action'. The second row contains a checkbox labeled 'test template' and three action buttons: a blue one with a gear icon, a green one with a download icon, and a red one with a trash bin icon.

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

This screenshot is identical to the one above, showing the 'Issues templates' section with the same layout and highlighted 'Issue name' input field and '+' button.

### 2. Select owner of template

#### Create new issue template: test

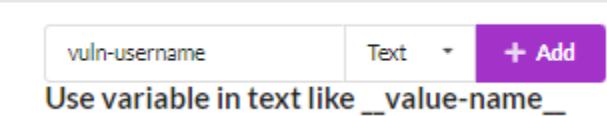
Owner:

### 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:

A screenshot of a software interface titled "Template variables". At the top, there are three tabs: "Info", "Additional fields", and "Required variables", with "Required variables" being the active tab. Below the tabs, the title "Template variables" is displayed. A list item for "\_\_vuln-username\_\_ (Text)" is shown, with its current value "admin" in a text input field. To the right of this field are two buttons: an orange "Copy name" button with a clipboard icon and a red "Delete variable" button with a trash bin icon.

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 fulfill main issue fields. For example, you can fulfill issue description and fix fields and insert into them required variable "\_\_vuln-username\_\_":

**Info**    Additional fields    Required variables

@ Name: Weak password

Description: User "\_\_vuln-username\_\_" has a weak password.

Fix: Change password for user "\_\_vuln-username\_\_".

**+ Submit**

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:

## Issues templates

More information about issue templates [here](#).

The screenshot shows a list of issue templates. At the top left is a search bar labeled "Issue name". To its right are three buttons: a blue one with a plus sign, an orange one with a file icon, and a green one with a download icon. Below these are two red trash can icons and a search bar labeled "Search...". The main area contains a table with columns for "Name" and "Action". Two rows are visible: "weak password" (highlighted with a yellow background) and "test template". Each row has a checkbox in the first column and three action buttons in the last column: a blue link icon, a green plus icon, and a red trash can icon. A yellow oval highlights the blue link icon in the "weak password" row.

	Name	Action
<input type="checkbox"/>	weak password	
<input type="checkbox"/>	test template	

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:

The screenshot shows a modal window titled "Add from template". At the top are two buttons: a green one with a plus sign and the text "Add from template" and a blue one with a plus sign and the text "+ Add". Below these is a search bar with the placeholder "Search template..." and a magnifying glass icon. The main content area is titled "ISSUE TEMPLATES" and contains a list of templates: "Create a new template" (with a yellow star icon), "test template (Personal)" (with a blue circle icon), and "weak password (Personal)" (with a blue circle icon). The "weak password" template is highlighted with a yellow background.

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:

Create new issue from template: weak password

You need to fill this variables:

- vuln-username (text)
- test username

**Issue: Weak password**

**Issue information** Additional fields

@ Name:	Weak password	URL path/service:	/admin/
Description:	User "test username" has a weak password.	# CVSS:	0.0 <a href="#">CVSS calculator</a>
		# CVE:	2020-1337
		# CWE:	0
		Status:	Need to recheck
		Criticality:	use CVSS criticality
		Parameter:	(GET) id=123
		Type:	Custom

+ Create

And next click at blue button "Create":

+ 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:

### Issues templates

More information about issue templates [here](#).

New template name



Search...

Then you will be redirected at /import\_issue\_templates page, which you must to fullfill:

### Import issue templates from file

Owner:

Team: Обучение

JSON-files:

Выбрать файлы

Файл не выбран

# Name prefix:

imported\_

Upload

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:

## Import issue templates from file

Owner: Team: Обучение ▾

JSON-files: Выбрать файлы Файл не выбран

# Name prefix: imported\_

 Upload

### Export

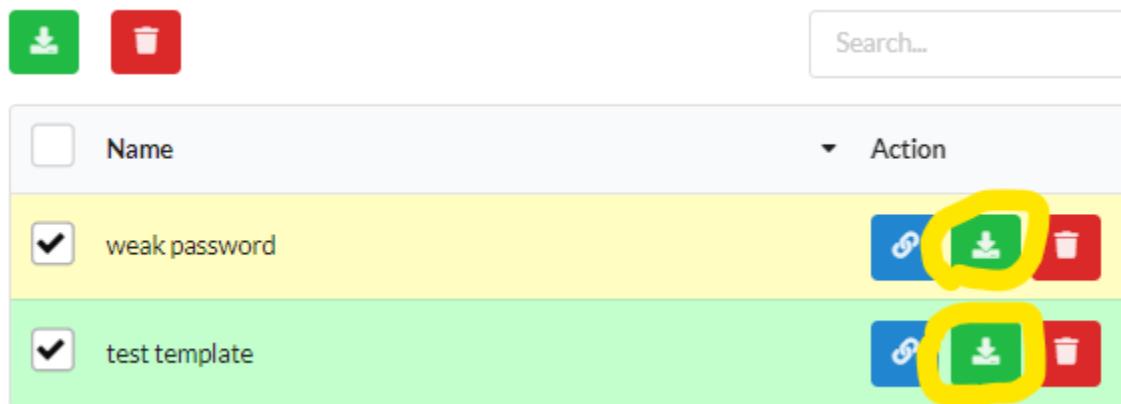
To export

issue

templates, you can:

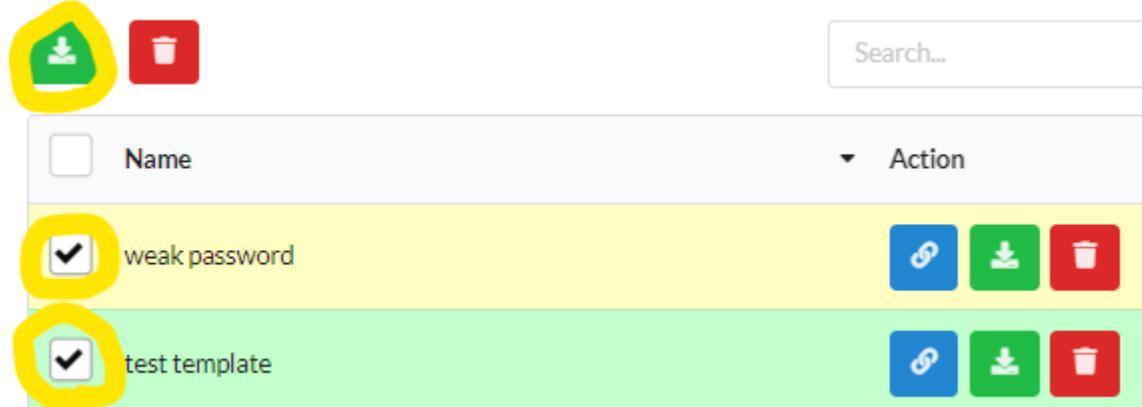
- export one issue template
- export multiple issue templates

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



Name	Action
weak password	  
test template	  

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

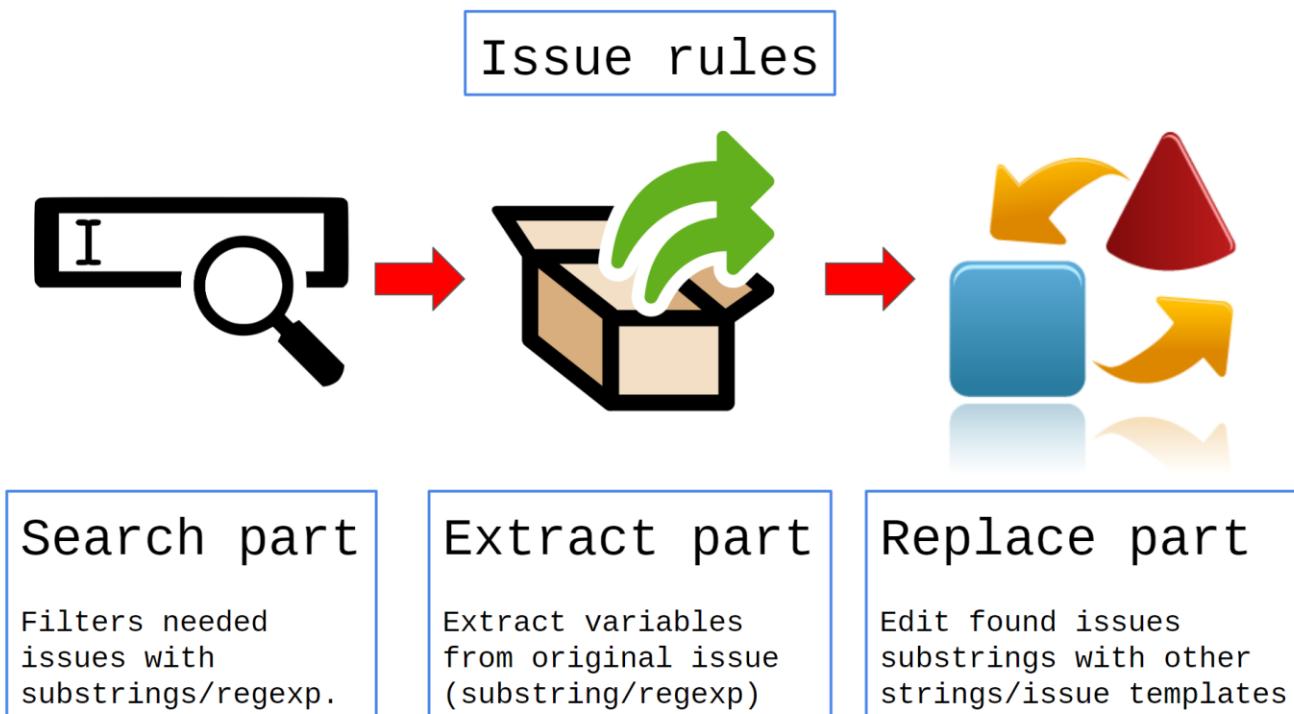


Name	Action
weak password	  
test template	  

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.

The screenshot shows a user interface for managing issue rules. At the top, there is a green oval highlighting the title "Issues rules" and a link "More information about issue rules [here](#)". Below this is a search bar with placeholder text "New rule name" and two buttons: a blue "+" button and an orange file icon button. To the left of the search bar are two icons: a green download icon and a red trash bin icon. To the right is a search input field with placeholder text "Search...". The main area displays a table with three rows, each representing a rule. The columns are "Name" and "Action". The first row is yellow and contains the rule "squid replace". The second row is light green and contains the rule "replace all". The third row is yellow and contains the rule "Nessus plugin id". Each row has a checkbox in the first column and three action buttons in the last column: a blue link icon, a green download icon, and a red trash bin icon.

	Name	Action
<input type="checkbox"/>	squid replace	
<input type="checkbox"/>	replace all	
<input type="checkbox"/>	Nessus plugin id	

## 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 its 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.

### Create new issue rule: dgdfgbsfg

Owner: Team: 456 + Create

Search rule → Extract variables → Replace text Wiki

#	Field name	Type	Filter	Action
1	_nessus_plugin_id_	Substring	1337	↑ ↓ Delete

New search filter

@ Field: Field name @ Type: Substring (% some\_text% another\_text%) @ Value: %some\_text% / son Add filter

Examples

Nessus special plugin ID Issues with "SQL" in name Critical vulnerabilities Certain CWE "XSS" or "CSRF" in description.

## 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!!!).

### Create new issue rule: dgdfgbsfg

Owner: Team: 456 + Create

Search rule → Extract variables → Replace text Wiki

Field name	Variable name	Extract type	Filter	Action
name	issue_name	Substring	<>	Delete

New extract variable rule

@ Field: Field name @ Name: a-zA-Z0-9\_ @ Type: Substring (% some\_text% another\_text%) @ Value: %text>text% / \*tc Add filter

Examples

Nessus ID variable Used username variable Issue name variable Issue name variable(RegExp)

## 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):

The screenshot shows the 'Replace templates' section with one rule: 'wefwef (Team: 456)'. It also shows the 'Add "replace with template" rule' button and a note about selecting team templates.

#	Template name	Template variables	Action
1	wefwef (Team: 456)		<button>Delete</button> <button>Edit</button>

The 'Replace substrings' section shows one rule: 'RegExp' for 'description' field with search filter '^[\s\S]\*\$' and replace string 'Some text example'. It includes configuration for type (Regular expression), field (description), search filter (^[\s\S]\*\$), replace value (Some text example), and a 'Add string replace rule' button.

#	Replace type	Field name	Search filter	Replace string	Action
2	RegExp	description	^[\s\S]*\$	Some text example	<button>Edit</button> <button>Down</button> <button>Delete</button>

Below the tables are 'Add "replace with string" rule' fields and an 'Examples' section with buttons for deleting, replacing descriptions, and replacing names.

## Use rules

### Open project issues

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

## Issues: 14

	Show 10 entries			Criticality:
	25			
	76			
	2			
	14	<input type="checkbox"/>	<b>Nessus: SSL Certificate Cannot Be Trusted</b>	Plugin name: SSL Certificate Cannot Be Trusted Info: The SSL certificate for this service cannot be verified.
	2	<input type="checkbox"/>	<b>Nessus: TLS Version 1.0 Protocol Detection</b>	Plugin name: TLS Version 1.0 Protocol Detection Info: This host uses the TLS 1.0 protocol.
	3			

Select issues and rules

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

## Use issue replace rules

The screenshot shows a user interface for managing security issues and rules. It consists of three main sections:

- Issues to change:** A table listing four security issues. The first two issues have checkboxes checked, indicating they are selected for replacement. The third issue has an unchecked checkbox.
- Rules to use:** A table listing three rules. The second and third rules have checkboxes checked, indicating they are selected for application to the selected issues.
- Additional options:** A blue "Submit" button.

Below the interface, a text summary states: "It will use selected rules at selected issues."

Name	Description	CVSS	Action
Nessus: SSL Certificate Cannot Be Trusted	Plugin name: SSL Certificate C...	6.5	
Nessus: TLS Version 1.0 Protocol Detection	Plugin name: TLS Version 1.0 P...	6.5	
Nessus: SSH Weak Key Exchange Algorithms Enabled	Plugin name: SSH Weak Key Exch...	3.7	
Nessus: SSH Server CBC Mode Ciphers	Plugin name: SSH Server C CBC M...	2.6	

Name	Owner	Action
squid replace	Team: 456	
replace all	Team: 456	
Nessus plugin id	Team: 456	

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:

# Issues rules

More information about issue rules [here](#).

The screenshot shows a user interface for managing issue rules. At the top, there is a search bar labeled "Search..." and two buttons: a blue "+" button and an orange file icon button. Below this is a table with columns for "Name" and "Action". Two rows are visible:

Name	Action
squid replace	
replace all	

Both the "squid replace" row and its "download" action button are circled in black.

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-41a2-81a9-7b30ba04dfffb",  
        "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:

# Issues rules

More information about issue rules [here](#).

The screenshot shows a user interface for managing issue rules. At the top, there is a text input field labeled "New rule name" and a blue button with a plus sign. To the right of the plus sign is an orange button with a white file icon, which is circled in black. Below these are two small buttons: a green one with a download icon and a red one with a trash icon. To the right is a search bar with the placeholder "Search...". A vertical scroll bar is on the far right. The main area displays a table with two rows. The first row, "squid replace", has a checked checkbox in the first column, followed by the name "squid replace" and three action buttons: a blue link icon, a green download icon, and a red trash icon. The second row, "replace all", has an unchecked checkbox, followed by the name "replace all" and the same three action buttons. The rows have yellow and green backgrounds respectively.

	Name	Action
<input checked="" type="checkbox"/>	squid replace	
<input type="checkbox"/>	replace all	

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

Nº	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:

# Project reports

**Zip/plaintext file**

Test team - Pentest report zip

or upload one

Выберите файл Файл не выбран

**Edit file extensions**

tex

**Download**

**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:

# Project reports

## Zip/plaintext file

Test team - Pentest report zip

Select one...

Test team - Pentest report zip

Test team - Statistics report tex

Dropzone (empty) New file...

## Edit file extensions

tex

Download

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	-

**Reports generation**

Pentest Collaboration Framework: Example pentest    Projects    Teams    Profile

### Project reports

**Zip/plain/text file**

Test team - Pentest report zip

or upload one

Выберите файл new 54.txt

Edit file extention  
tex

Download

Generate project JSON button

Report generation form

## 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":"new54.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":"new54.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": "new54.txt", "type": "text", "url": "/static/files/poc/9a215828-fa20-4e09-8713-f66625d067b8"}], "port": 8080}, {"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\n\nmultiline\r\n\ndescription", "fix": "", "id": "9fefbbc3-27c8-4499-b09c-e4f774e02e7b", "name": "XXE", "param": "", "project_id": "dfe91b40-1854-48ad-a127-01ff201f2884", "services": []}, {"status": "Not confirmed", "type": "custom", "url_path": "", "user_id": "c94ff3d3-8217-4242-914a-052ac29dde22"}, {"cve": "", "cvss": 2.0, "cwe": 0, "description": "CSRF example description", "fix": "", "id": "c055de07-6977-43e5-872ba87ea005172c", "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

Nº	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**

**i Project files: 3**

filename	description	services
new 54.txt	File with hosts	
new 54.txt		
test.html	example html index page	1.1.1.1:80

Выберите файл: Example description

IP: 1.1.1.1  
1.1.1.22  
1.1.1.80

Binary file

Submit

## 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**

```

<!DOCTYPE html>
<!-- This site was created in Webflow. http://www.webflow.com -->
<!-- Last Published: Mon Jul 06 2020 16:48:25 GMT+0000 (Coordinated Universal Time) -->
<html data-wf-page="5eecd0654b70280a91b25d4" data-wf-site="5ec2ba8457c5c50b20b387c9">
<head>
    <meta charset="utf-8">
    <title>File</title>
    <meta content="width=device-width, initial-scale=1" name="viewport">
    <meta content="Webflow" name="generator">
    <link href="/static/css/normalize.css" rel="stylesheet" type="text/css">
    <link href="/static/css/webflow.css" rel="stylesheet" type="text/css">
    <link href="/static/css/drakylars-stellar-project.webflow.css" rel="stylesheet" type="text/css">
    <link href="/static/css/chats.css" rel="stylesheet" type="text/css">
    <script src="/static/js/webfont.js" type="text/javascript"></script>
    <script src="/static/js/cvss.js"></script>
    <link rel="stylesheet" type="text/css" media="all" href="/static/css/cvss.css">
    <!--
        <script type="text/javascript">
            WebFont.load({
                google: {
                    families: ["Inconsolata:400,700"]
                }
            });
        </script>
    -->
</head>
<body>
    <div>
        <div>
            <div>
                <div>
                    <div>
                        <div>
                            <div>
                                <div>
                                    <div>
                                        <div>
                                            <div>
                                                <div>
                                                    <div>
                                                        <div>
                                                            <div>
                                                                <div>
                                                                    <div>
                                                                        <div>
                                                                            <div>
                                                                                <div>
                                                                                    <div>
                                                                                        <div>
                                                                                            <div>
                                                                                                <div>
                                                                                                    <div>
                                                                                                        <div>
                                                                                                            <div>
                                                                                                                <div>
                                                                                                                    <div>
                                                                                                                        <div>
                                                                                                                            <div>
                                                                                                                                <div>
                                                                                                                                    <div>
                                                                                                                                        <div>
                                                                                                                                            <div>
                                                                                                                                                <div>
                                                                                                                                                    <div>
                                                                ................................................................

```

## 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

Nº	Action
1	Open project credentials

Nº	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	-

# Credentials list

Pentest Collaboration Framework: Example pentest

**i Credentials: 2**

Show 10 entries Search:

login / email	hash	password	comment	service
test	098f6bcd4621d373cade4e832627b4f6	test	Admin credentials	3.3.3.3:8080
admin		admin	default password	google.com:80

Showing 1 to 2 of 2 entries Previous 1 Next

**Export**

- Take raws with empty passwords
- Add logins to password list
- Just show result in browser

Login:Password separator :

**Add credentials buttons**

**List of credentials**

**Export credentials form**

## Add single credentials

Name	Value
URL	/project/{{project_uuid}}/credentials/new_creds
URL example	/project/53ade0ed-ea2d-4812-9676-8bd5b7412c/credentials/new_creds
Description	Add new single credentials.
Capabilities	Add new project single credentials form.
Comments	-

## Add single credentials form

Pentest Collaboration Framework Example pentest Projects Teams Profile

### New credentials

**IP**

Login / email: admin

Hash: 21232f297a57a5a743894a0e4a801fc3

Hash type: None

Check hash in wordlist: -

Cleartext password: admin

Comment: Credentials description

Information source: Where did you find these credentials

Submit

**ip-service:** ip  
1.1.1.1:22  
1.1.1.1:80  
2.2.2.2:53 (udp)  
3.3.3.3:8080

**domain-service:** hostname  
google.com:22  
google.com:80  
amazon.com:53 (udp)  
mail.google.com:8080

## 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

The screenshot shows a web-based configuration interface for importing multiple credentials. On the left, there's a sidebar with icons for IP, Network, Services, and Tools. The main area has two sections: 'Rows configuration' and 'Static row fields'. In 'Rows configuration', there are fields for 'Username column number' (set to 0), 'Hash column number' (set to 0), 'Cleartext password column number' (set to 0), 'Comment column number' (set to 0), 'Source column number' (set to 0), and 'Column delimiter' (set to ':'). In 'Static row fields', there are fields for 'Username (every row)' (set to 'admin'), 'Hash (every row)' (set to '21232f297a57a5a7438940e4a801fc3'), 'Hash type (every row)' (set to 'None'), 'Check hash in wordlist (every row, CAREFUL!)' (set to '-'), 'Cleartext password (every row)' (set to 'admin'), 'Comment (every row)' (set to 'Credentials description'), and 'Information source (every row)' (set to 'Where did you find this credentials'). Below these, there's a file input field with the placeholder 'Выберите файл' (File not selected) and a text area for 'Or insert file content here' containing '1;2;3'. At the bottom, there are two checkboxes: 'Do not check columns amount at every row' and 'Do not check duplicate credentials', followed by a blue 'Submit' button.

## 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

The screenshot shows a 'User info' form within a web-based application. The top navigation bar includes 'Projects', 'Teams', and 'Profile'. The main form has sections for 'Login / email' (containing 'test'), 'Hash' (containing '098f6bcd4621d373cade4e832627b4f6'), 'Hash type' (set to 'md5\_hex'), 'Cleartext password' (containing 'test'), 'Comment' (containing 'Admin credentials'), and 'Information source' (containing 'Where did you find this credentials'). On the right side, there are sections for 'ip-service' (with checkboxes for 'ip', '3.3.3.3:8080', '1.1.1.1:80', '1.1.1.1:22', and '2.2.2.2:53 (udp)') and 'domain-service' (with checkboxes for 'hostname', 'google.com:22', 'google.com:80', 'amazon.com:53 (udp)', and 'mail.google.com:8080'). At the bottom are 'Update' and 'Delete' buttons.

## Notes moderation

### Sequencing

Nº	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

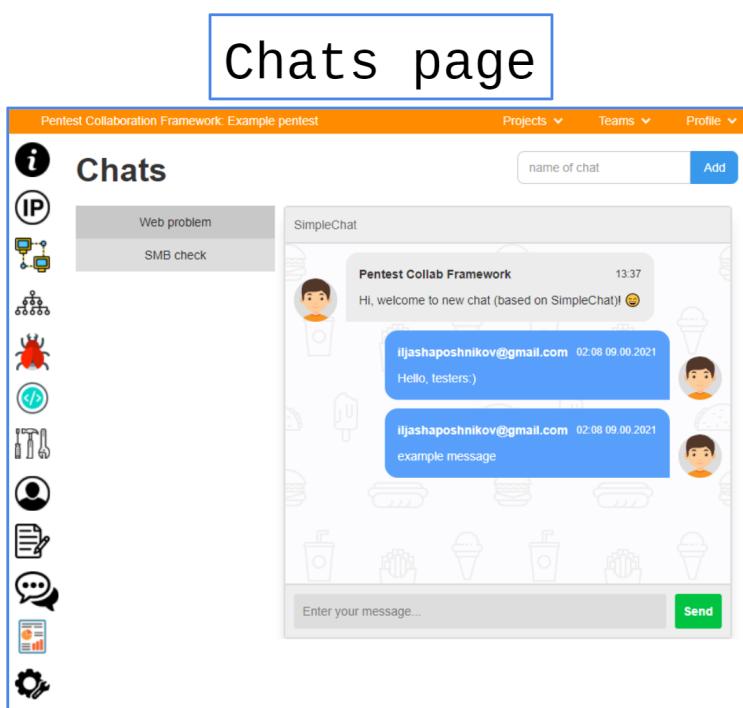
### Sequencing

Nº	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	-



# 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)

<b>Tool name</b>	<b>Integration type</b>	<b>Description</b>
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)
<a href="#"><u>BurpSuite</u></a>	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)
Scanvas	Import	Import JSON report (issue)