Vulnerability Management System & Risk Analysis Tool (VMS-RANT)

User guide (ITR-UsgVMSRANT)

General information

Type	Standard
Reference	R004 (ATENA)
Version	1.0
State	Final version
Owner	R. Ebene
Date of application	29/04/2019
Classification	Public

Distribution list

Recipient	Channel	Reason
J. Lancrenon	Internal repository	Validation
E. Omar	Internal repository	Validation
C. Harpes	Internal repository	Validation

History

Version	Date	Author	Modifications
1.0	29/04/2019	R. Ebene	Finalization

Working group

Name	Organisation
CHA, JLA, EOM, REB	itrust consulting

Approval

Name	Role	Responsibility	Date	Signature
Rose Ebene	Author	Content creation Tool testing	29/04/2019	Email to JLA
Jean Lancrenon	Product owner	Validation	29/04/2019	Email to CHA

Table of contents

1 Introduction....5
1.1 Context....5
1.2 Objectives of the document....5
1.3 Structure of the document....5
1.4 References....5
1.5 Acronyms....5
1.6 Glossary....5
2 Vulnerability management (VMS part)....7
2.1 Connection to the VMS-RANT tool....7
2.1.1 Create an account....7
2.1.2 Login....8
2.1.3 Reset password....8
2.1.4 Two-Factor Authentication (2FA)....9
2.2 Home screen....9
2.3 CERT/CSIRT....10
2.3.1 Editing a custom CVE....10
2.3.2 Description....11
2.3.3 References....12
2.3.4 Vulnerability....12
2.4 Modelling....13
2.4.1 Editing a template....13
2.4.2 Viewing a model....14
2.4.3 Modifying a model....15
2.5 Search....16
2.6 Profile....17
2.6.1 Account information:....17
2.6.2 Sign-in settings....17
2.6.3 Activation of 2FA for mobile devices....18
2.7 Sign out....18
3 Risk analysis tool (RANT part)....19
3.1 Threats....19
3.2 Asset....20
3.3 Layer....21
3.4 Events....22
3.5 Features....22
3.6 Location....23
3.7 Risk Factor....23

List of figures

Figure 1: Connection pages....7
Figure 2: Additional information for registration....7
Figure 3: Reset password....8
Figure 4: Reset passwords and sign in....8
Figure 5: Two-Factor Authentication screen....9
Figure 6: Home screen....9
Figure 7: Presentation of the CERT/CSIRT tab....10
Figure 8: The basic information of a CVE....11
Figure 9: Description field of a custom CVE....11
Figure 10: References....12
Figure 11: Add a vulnerability....12

Figure 12: Add a new template 13
Figure 13: Add a new node 14
Figure 14: play button 15
Figure 15: visualisation of a model 15
Figure 16: button to modify a model 16
Figure 17: modify a model 16
Figure 18: page Search 16
Figure 19: Profile page 17
Figure 20: enable two-factor authentication. 17
Figure 21: RANT page 19
Figure 22: Threats page 19
Figure 23: Asset page 20
Figure 24: Add an asset 21
Figure 25: List of the different layers 22
Figure 26: Features page. 22
Figure 27: Risk Factor page 23
Figure 28: Edit a risk factor page 24

1 Introduction

1.1 Context

In the ATENA project, partner ITRUST has developed a tool called VMS-RANT, which makes it possible to manage vulnerabilities (VMS part) and to calculate risks in critical infrastructures (RANT part) compared to the models built in the VMS part. For more details, consult the documents [2] and [3].

1.2 Objectives of the document

The purpose of the VMS-RANT tool user guide is to introduce the user to all the features of the application. It explicitly describes all the functionalities of the service in order to answer any questions that a user may have.

1.3 Structure of the document

The structure of the document is as follows:

- the first part deals with vulnerability management (VMS part);
- the second part deals with the risk analysis tool (RANT part).

1.4 References

[1] National Vulnerability Database (NVD) website: https://nvd.nist.gov/
[2] D3.5 - Risk analysis methodology and tools_v2.0
[3] D3.6 ATENA system requirements and specifications final report_v1.0

1.5 Acronyms

CERT	Computer Emergency Response Team.
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
RANT	Risk Analysis Tool
VMS	Vulnerability Management System
IADS	Intrusion and Anomaly Detection System
IEC	Israel Electric Corporation
TOTP	Time-based One-Time Password
NVD	National Vulnerability Database
QR code	Quick Response Code
CVSS	Common Vulnerability Scoring System

1.6 Glossary

CSIRT	A CSIRT (Computer Security Incident Response Team), or CERT, is a service organisation responsible for receiving, reviewing and responding to computer security incident reports and

	activities. Their services are usually provided for a defined group that could be a parent entity such as a company, government or educational organisation, a region or country, a research network or a client who remunerates them for their expertise.

2 Vulnerability management (VMS part)

2.1 Connection to the VMS-RANT tool

The VMS-RANT application is available on the IEC testbed at http:// 172.27.23.23.46:2000. Once connected to the application URL, the user sees the connection interface below (see Figure 1). He has the possibility to:

- create an account (see 2.1.1);
- login (see 2.1.2);
- reset the password (see 2.1.3).

The different options are explained in the following subsections.

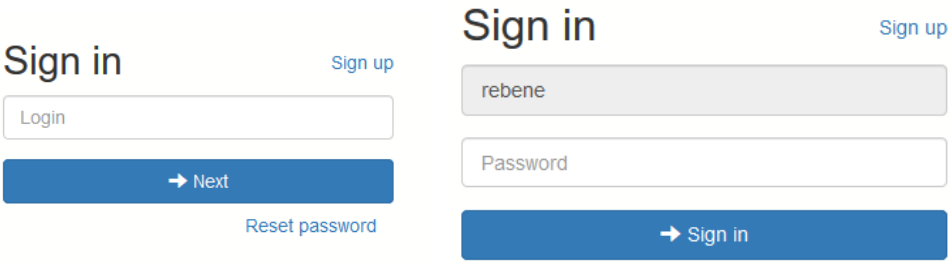

Figure 1: Connection pages

2.1.1 Create an account

To use the VMS-RANT application, the user shall first create an account. To create an account, he clicks on the "Sign up" button (see Figure 1).

After clicking on the "Create an Account" or "Sign up" button, the user is prompted to enter the additional information required to set up his account (see Figure 2 below).

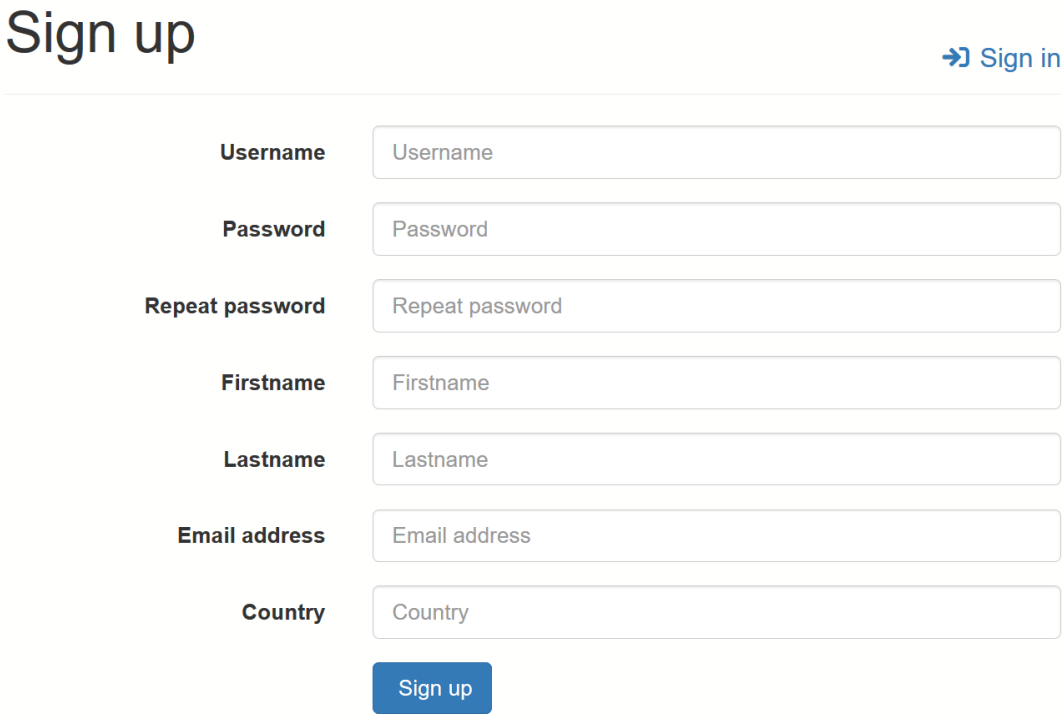

Figure 2: Additional information for registration

The user shall complete the form and confirm by clicking on "Sign up". The seven fields in Figure 2 above are mandatory. When he has finished correctly, he can log in (see Figure 1).

2.1.2 Login

Once his account has been created, the user can log in to the VMS-RANT application. The login screen is visible in Figure 1, where he must enter the username and password, then click on "Login".

2.1.3 Reset password

If the user has forgotten his password, he can reset it by clicking on the "Reset password" link on the VMS-RANT login interface (see Figure 1).

The user is redirected to the password reset interface where he enters his username or email address that he entered when he registered. See Figure 3.

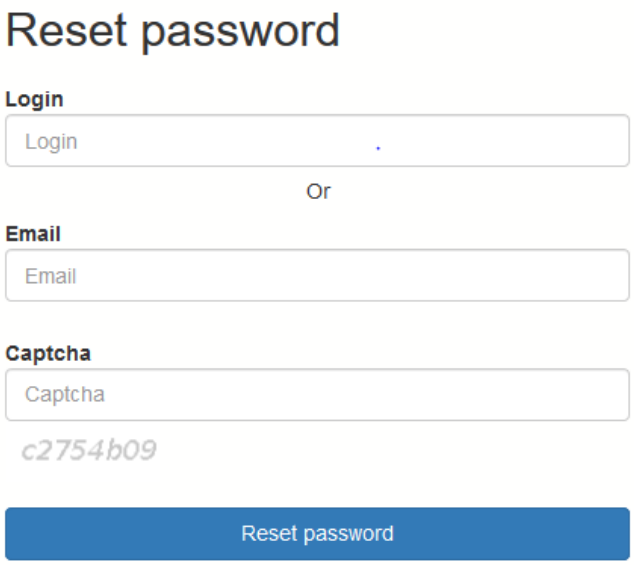

Figure 3: Reset password

After clicking on the "Reset password" button, the user will receive an email containing a link that will redirect him to a web page where he can choose a new password. Then he can already sign in. See Figure 4.

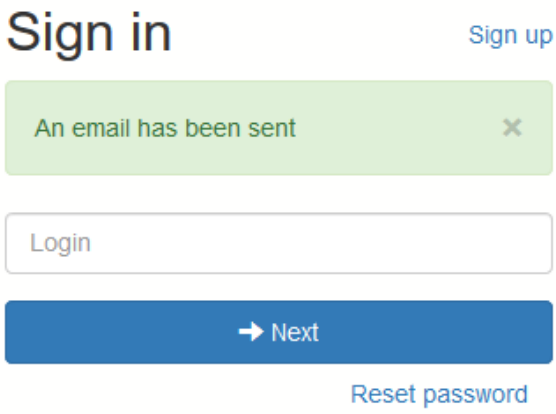

Figure 4: Reset passwords and sign in

Be careful, the configuration may not be present if the administrator has not activated the "send email" functionality.

2.1.4 Two-Factor Authentication (2FA)

When Two-Factor Authentication (2FA) is enabled (if this is done by the user), the user is prompted to enter an additional security code. This code is received via a smartphone application that supports the TOTP (Time-Based One-Time Password) protocol. Such an application is available for all major smartphones (Android, iOS, Windows Mobile) in their respective stores.

2FA via mobile application

For the user who has configured 2FA via mobile applications in the profile settings (see 2.6.2), an additional entry, "Use mobile application", appears in the selection area. The user has to open the two-factor authentication application on his mobile phone and copy the 6-digit code indicated in the VMS-RANT application text box (see Figure 5).

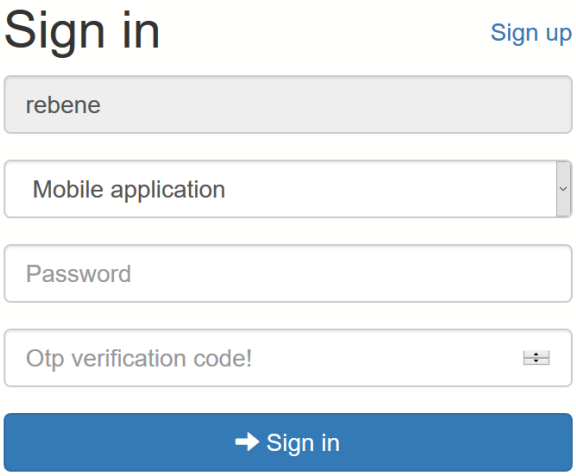

Figure 5: Two-Factor Authentication screen

2.2 Home screen

After connecting to the VMS-RANT application, the following screen shows the VMS part, see Figure 6 below.

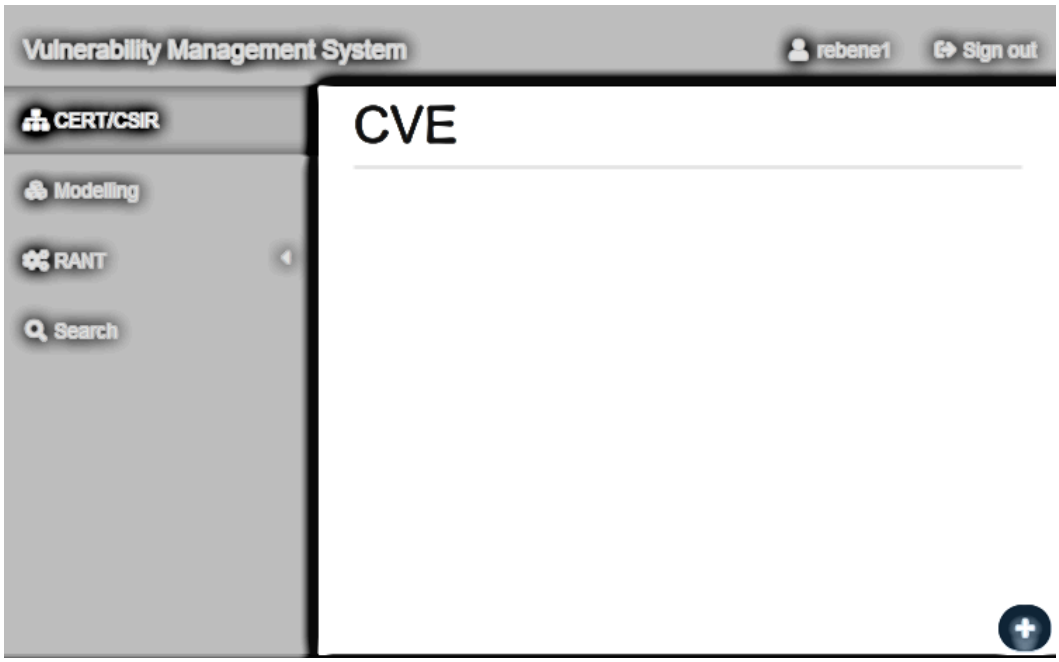

Figure 6: Home screen

The following sub-chapters explain in more detail the content of the different navigation tabs CERT/CSIRT, Modelling, Search, Profile, Sign out, and RANT.

2.3 CERT/CSIRT

This tab leads to two main parts which are CVE and Vulnerability, and contains a custom CVE entry list (customised CVE), where each item contains an identification number, description, public reference and information on the type of impact affected by this CVE. This information can be added, modified and deleted using the corresponding buttons (see Figure 7).

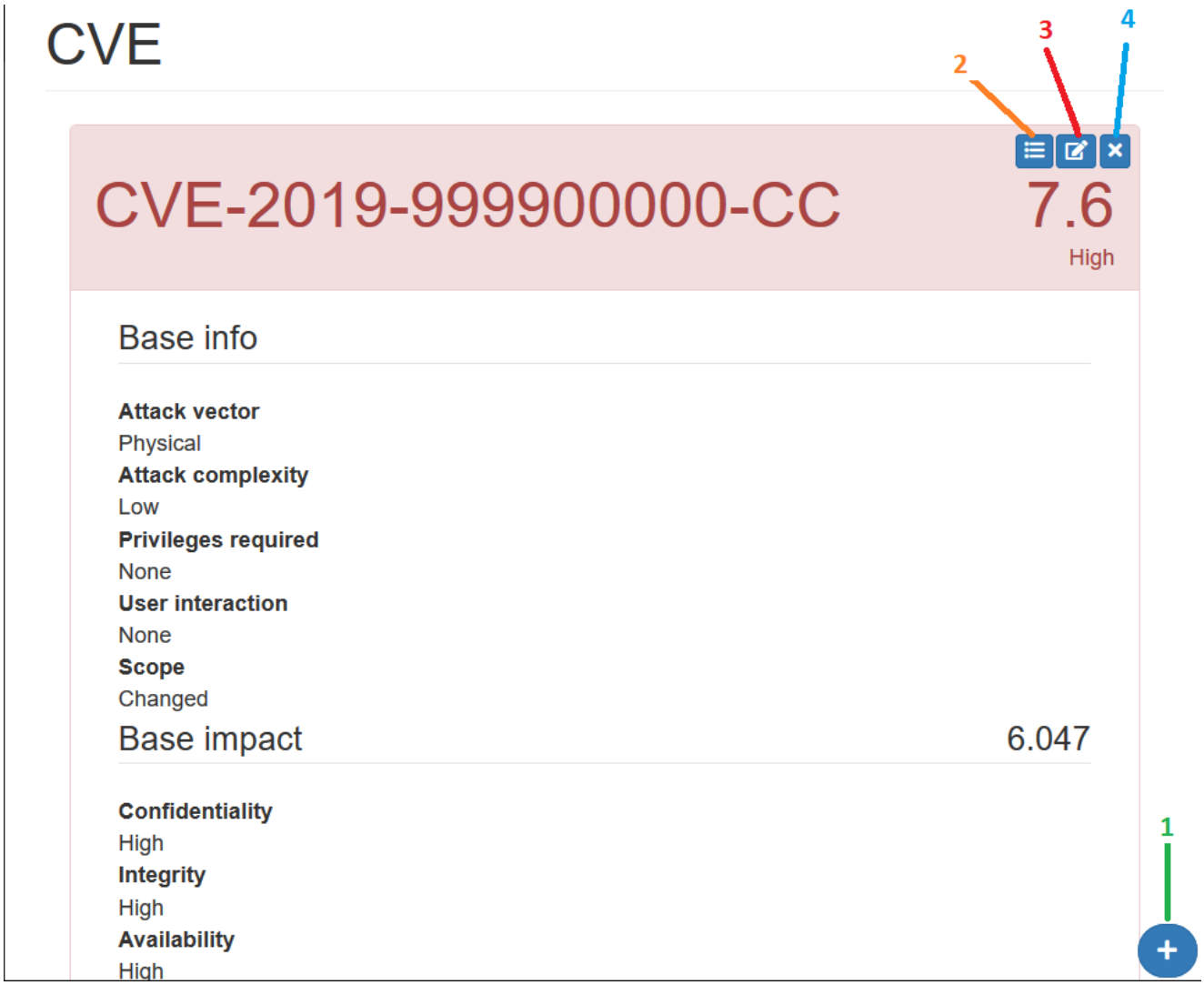

Figure 7: Presentation of the CERT/CSIRT

- 1: button to add a new CVE;
- 2: button to perform a search;
- 3: button to edit/modify an existing CVE;
- 4: button to delete a CVE.

2.3.1 Editing a custom CVE

This section allows the user to define the characteristics of the custom CVE.

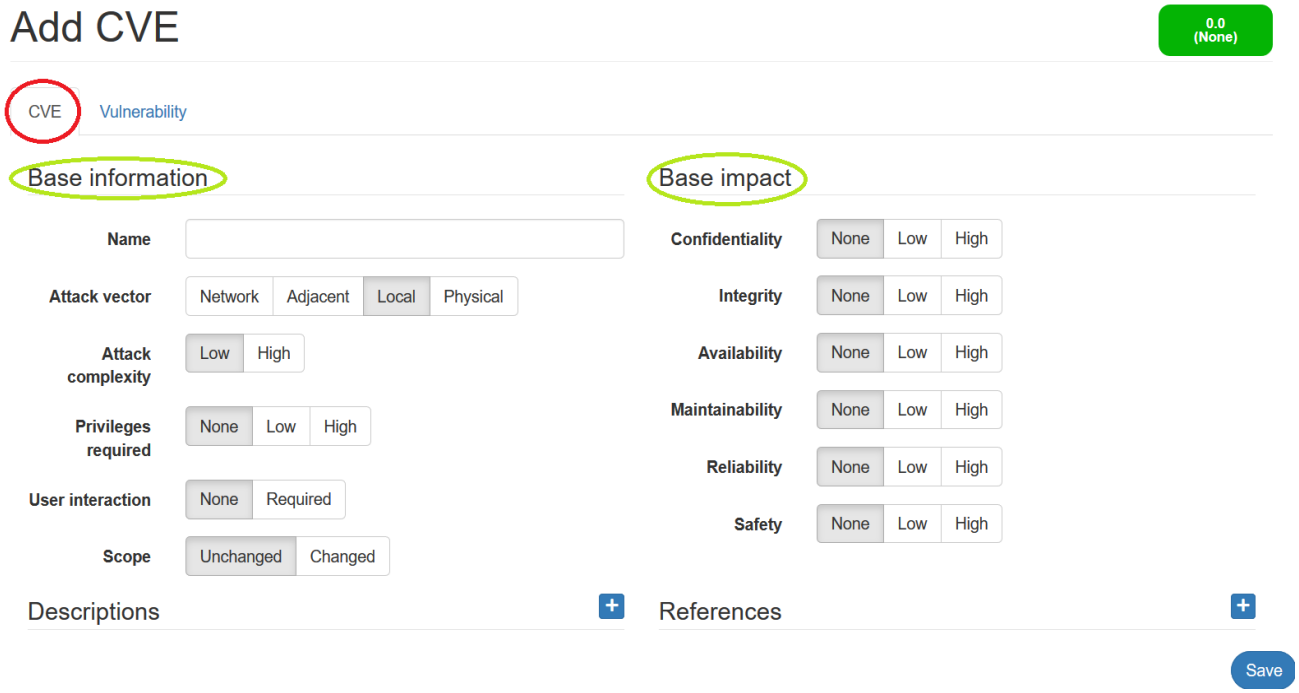

Figure 8: The basic information of a CVE

The name of the CVE is not mandatory but if the user fills it in, it should start with CVE-YYYY-DIGIT-CC. If the CVE name already exists in the NVD database [1], a suffix "-CC" will automatically be added at the end of the name. The suffix "-CC" means CVE Custom. Note that in the "Base Impact" section, the last three elements are not part of the CVSS3.0 standard.

2.3.2 Description

To complete the CVE description, the user clicks on the button "+". A small window then opens, and the user must fill in the fields "Language" and "Description", see Figure 9.

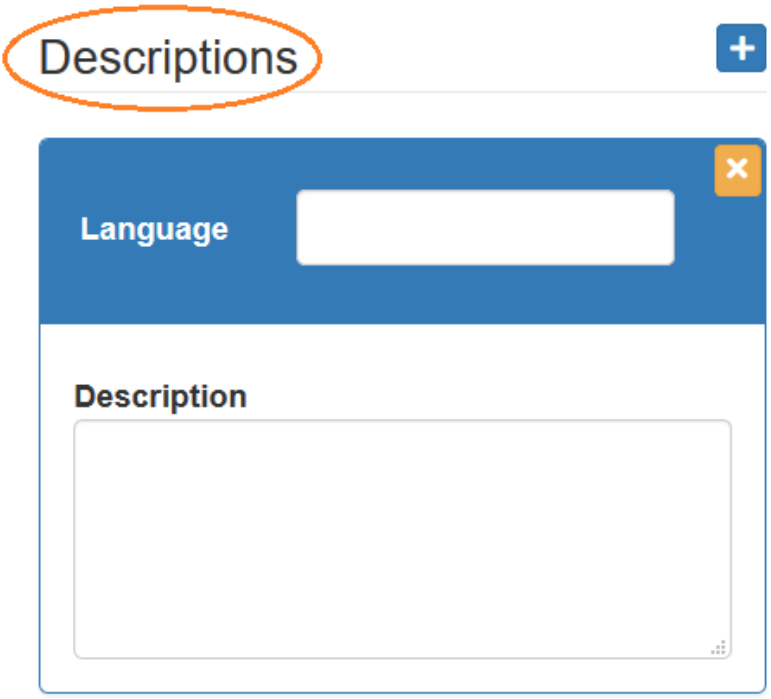

Figure 9: Description field of a custom CVE

2.3.3 References

Similarly, for the "References" part, the user clicks on the button " + " on the right. A small window opens with field lines to fill in, which are "name", "source", and "URL", see Figure 10.

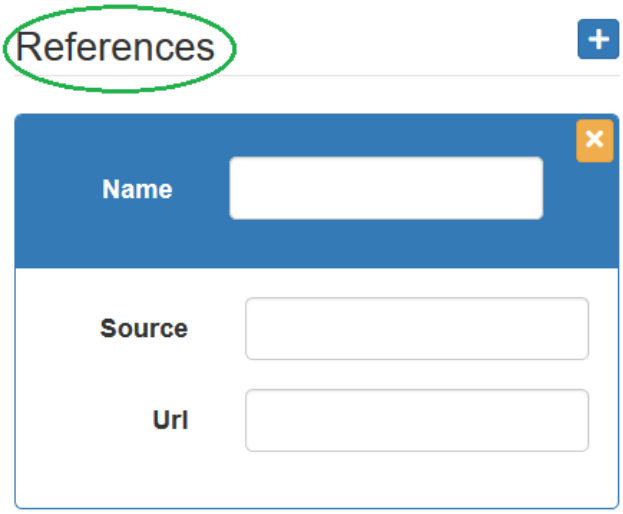

Figure 10: References

Warning: If the user leaves the page without saving changes (by clicking on the "save" button, see the bottom right of Figure 8), these changes will be lost.

2.3.4 Vulnerability

This section allows the user to enter information on computer software or hardware that has vulnerabilities related to the CVE. Each entry must have a name, a vendor/manufacturer and a version.

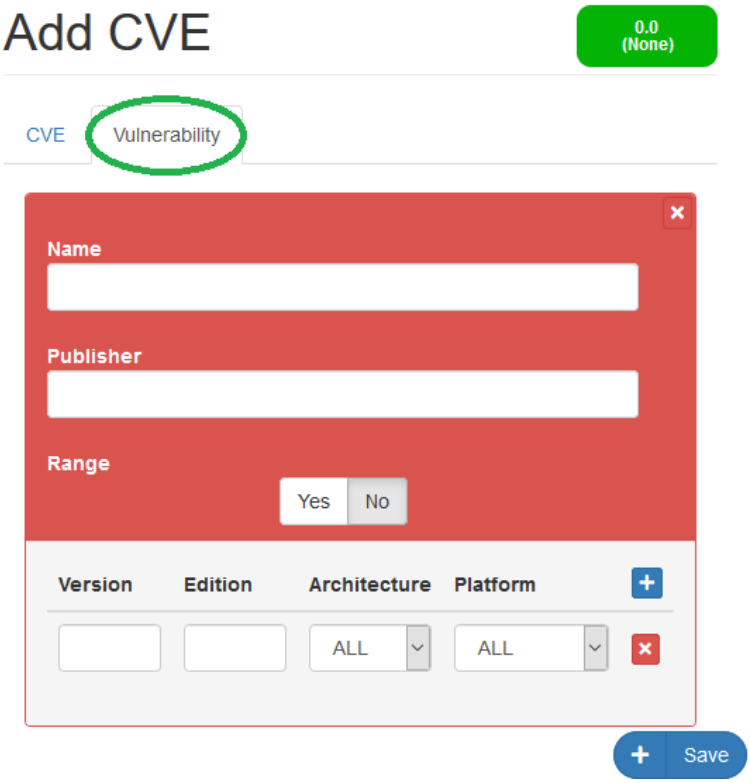

Figure 11: Add a vulnerability

To modify a vulnerability, the user has to click on the "modify" button (see Figure 7) and choose the "Vulnerability" tab (see Figure 11).

Warning: If the user leaves the page without saving his changes by clicking on the "save" button, see Figure 11, these changes will be lost.

2.4 Modelling

In the "Modelling" tab, the user can model a tree or dependency graph.

2.4.1 Editing a template

To add a new model element, the user clicks on the "add" button. He can define whether his model is public or private.

The principles of the private / public modelling choices are discussed below.

- A private model is displayed in red and is visible to, and accessible by, only the user that created the model.
- A public model is displayed in green and is visible and accessible to all.
- Models displayed in green in the private area are shared.

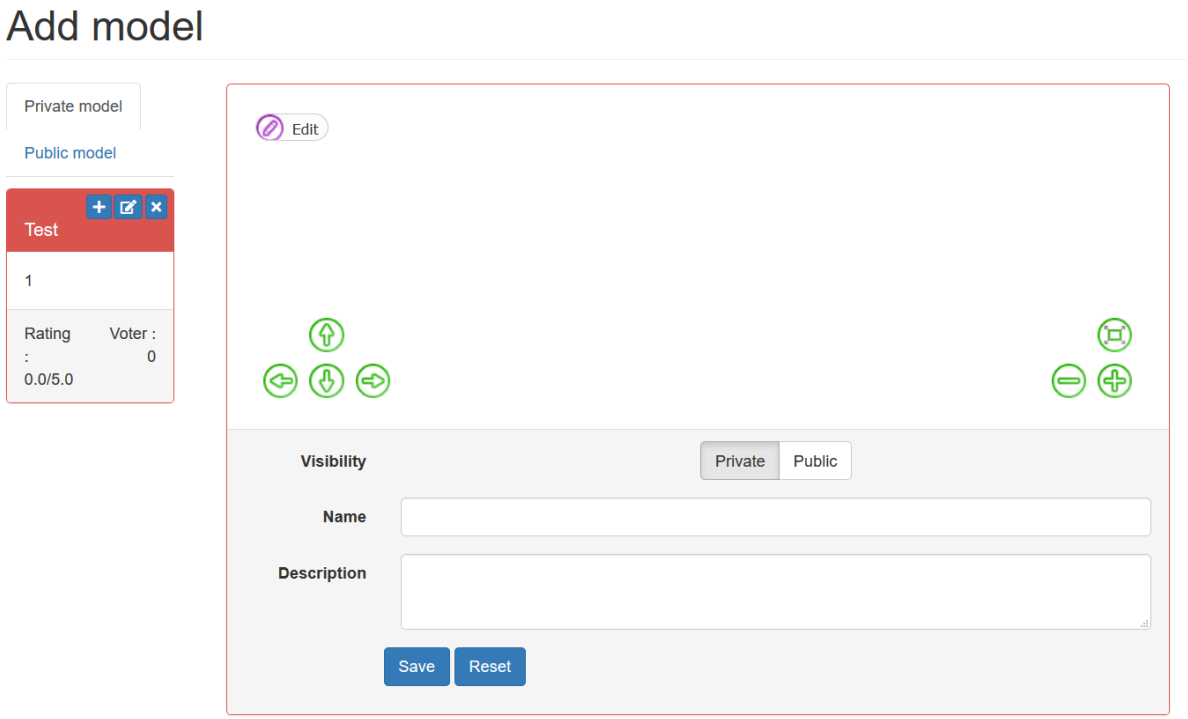

Figure 12: Add a new template

To add modelling elements to his workspace, the user must click on the "Edit" button (see Figure 12). Then on "Add Node", to add nodes.

The window in Figure 13 appears when the user makes a simple click in the workspace. The user must enter the information in the various fields below:

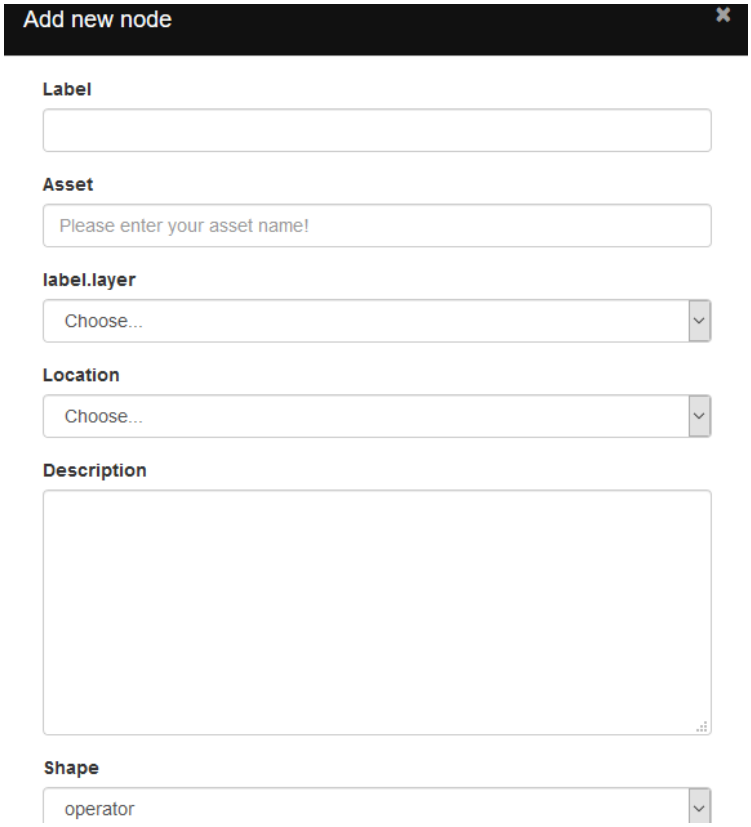

Figure 13: Add a new node

- **Label:** name of the model;
- **Asset:** name of the asset linked to this node;
- **Location:** location of the node based on the asset location;
- **Description:** a brief description of the node;
- **Shape:** type or shape of the node, to be chosen from the following shapes in the drop-down list: Operator, Icon, Box, Database, Ellipsem Square, Star, Text, Triangle, Triangledown;
- **Icon:** if the form "**Icon**" is chosen in the field "**Shape**", a drop-down list is activated and the user must choose the corresponding icon;
- **Operator**: depending on the type of "**Shape**" chosen, the "**Operator**" field is activated or not. When the field is activated, the user must choose the type of operator (AND or OR) from the drop-down list;
- **The entry point:** depending on the type of "**Shape**" chosen, the "**Entry point**" field is activated or not. When the field is activated, the user must choose between the two selections "Yes" or "No" depending on whether the element is an entry point or not;
- **Size:** the user chooses between "normal" and "wide" according to the size of his graph or tree;
- **Physics simulation:** the user chooses between "normal" and "wide" depending on the size of his graph or tree;
- **Cancel:** allows the user to cancel the operation;
- **Save:** To save all the information entered.

2.4.2 Viewing a model

To see the vulnerability status of a model, the user must click on the "play" button. See Figure 14 below.

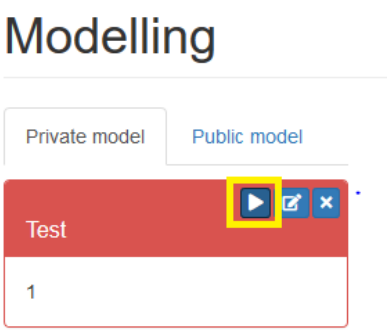

Figure 14: play button

After clicking on the "play" button, another window appears and the user can now view the vulnerability status of his model. The level of vulnerability of a given element in the model is colour-coded. The colour green means no vulnerability and red shows the vulnerable elements of the model (See Figure 15).

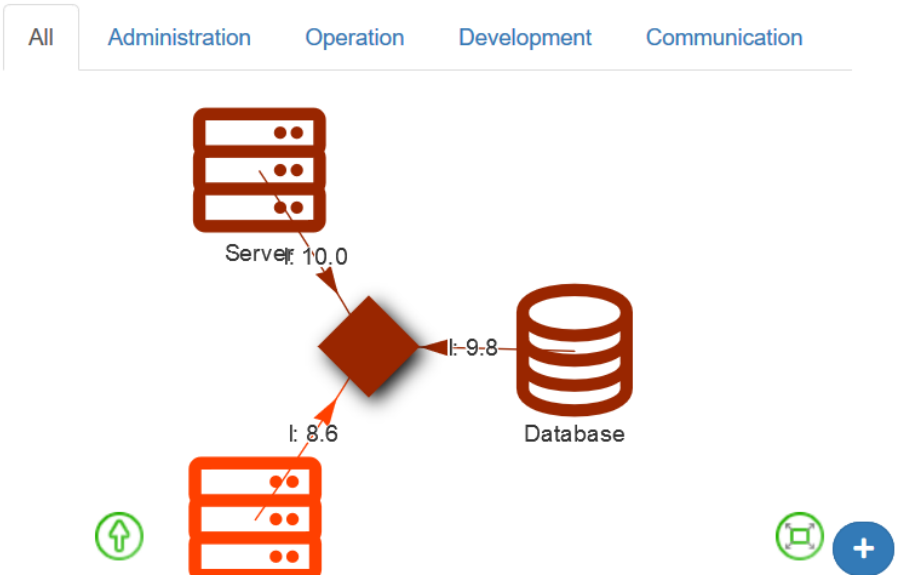

Figure 15: visualisation of a model

The "All" tab gives an overview of the model. The other tabs correspond to layers that can be edited in the Layer section of the RANT part, see 3.3.

- Navigation in layers with the mouse:
  - To reach the lower layers, the user selects the unblemished elements and scrolls up.
  - To raise the layers, the user simply scrolls down.
- Navigation by layer selection:
  - Same principle as mouse navigation, except that here the user directly selects the desired layers.

2.4.3 Modifying a model

To modify a model element, the user clicks on the "Edit" button, see Figure 16. The "Edit model" window appears and the user can modify his model. To duplicate a model, the user must left-click on the tab " " (see Figure 17below).

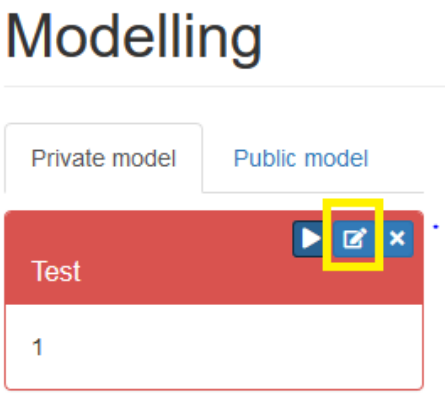

Figure 16: button to modify a model

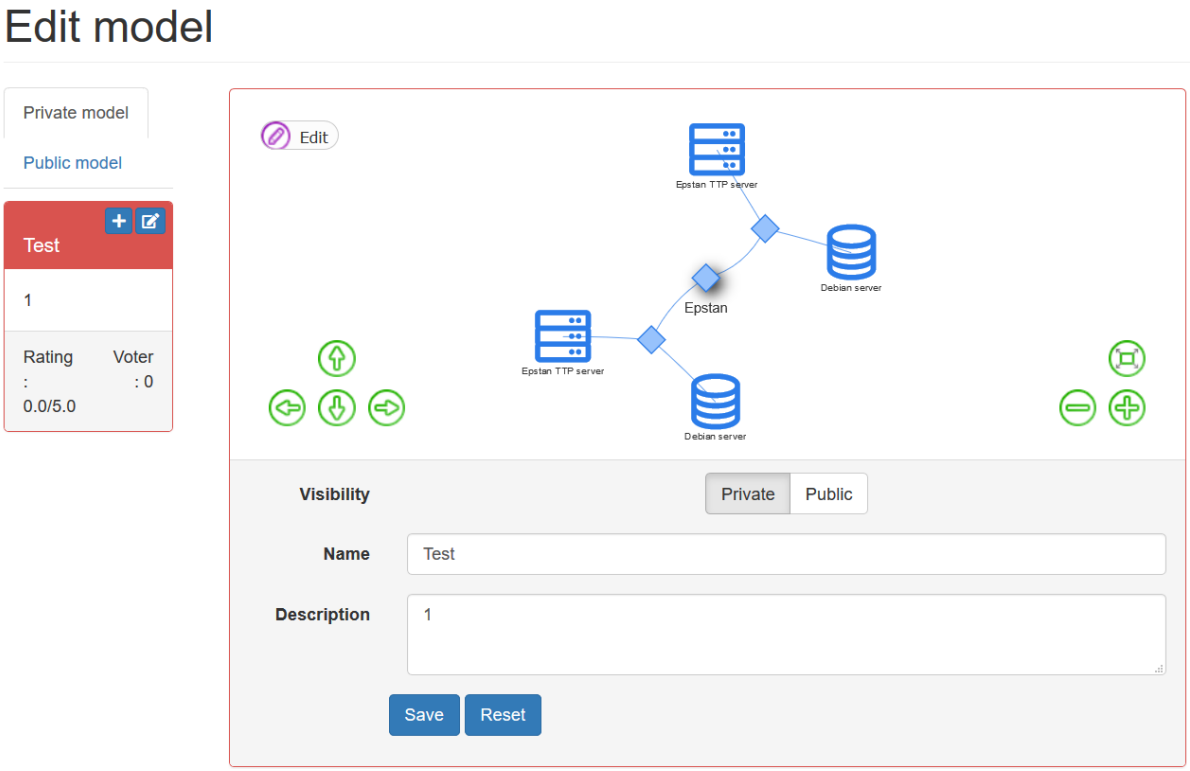

Figure 17: modify a model

2.5 Search

The "Search" tab allows the user to search the existing CVE in the database. To do this, he must enter the name of the custom CVE he is looking for and click on "OK" to validate his search.

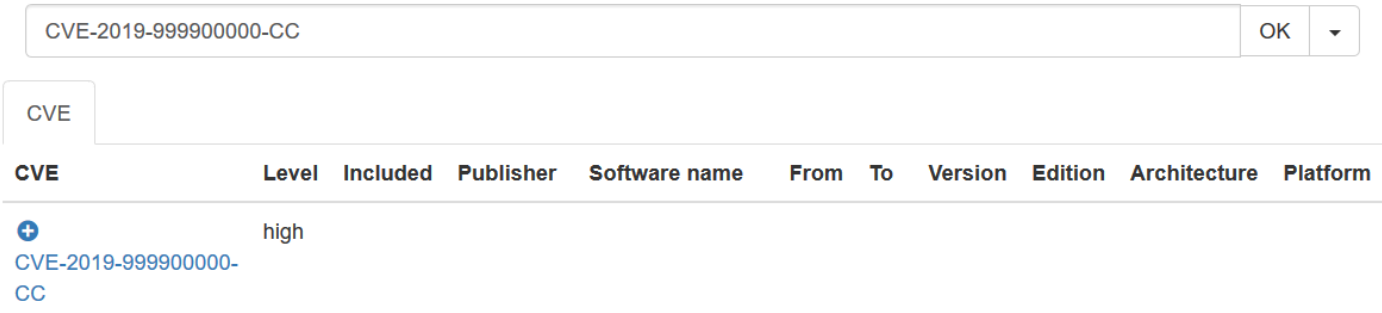

Figure 18: page Search

2.6 Profile

To go to the "Profile" page, the user must click on the icon . The "Profile" page is accessible from the right side of the ribbon. He can enter or update his personal information. See Figure 19. The "Profile" page has two different columns: "Account information" and "Sign-in settings".

2.6.1 Account information:

This column contains seven fields to be filled in:

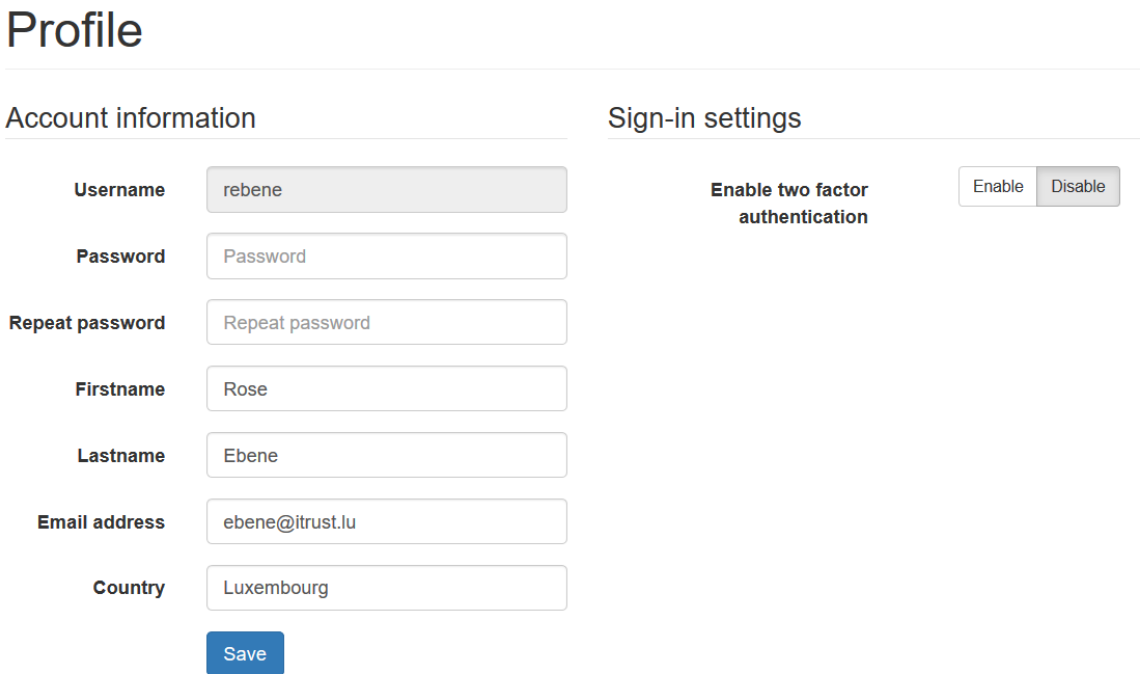

Figure 19: Profile page

2.6.2 Sign-in settings

In the login settings, the user can enable or disable Two-Factor Authentication (2FA) for his account. When he activates 2FA by clicking on the corresponding button, he will need to confirm his identity to log in later by forcing him to enter a security code sent to his email address. See 2.1.4 for more details on the two-factor authentication process. See below Figure 20.

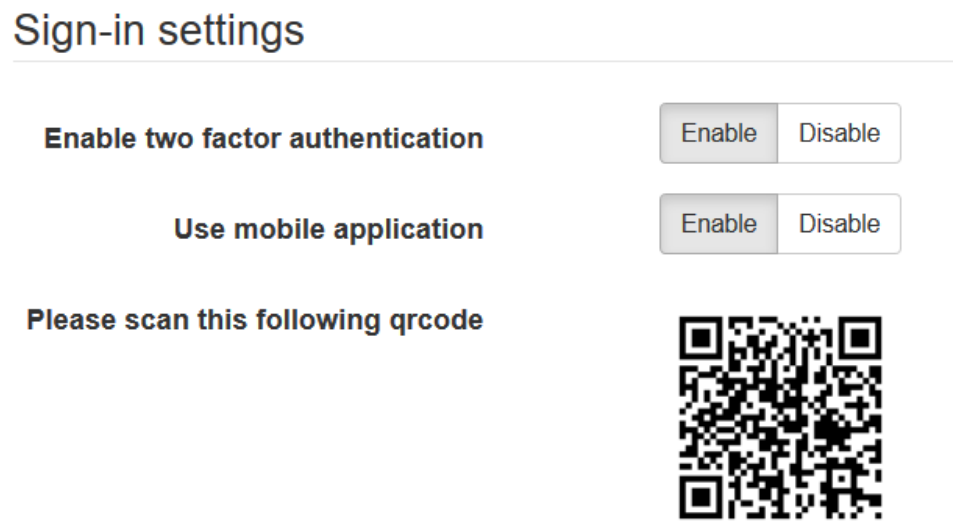

Figure 20: enable two-factor authentication

2.6.3 Activation of 2FA for mobile devices

When the user also activates the "Use mobile application" function, he also has the option of entering a one-time password, generated each time by his mobile device.

The 2FA activation procedure for his mobile is as follows:

- Enable double-factor authentication by clicking on the "Enable" button.
- Activate "Use mobile application" by clicking on the "Enable" button.
- Install an application that supports the TOTP protocol (time-based one-time password) from the application store on his device. Such an application is available for all major platforms (Android, iOS, Windows Mobile) (for example, "Microsoft Authenticator").
- Open the application and scan the QR code indicated on VMS-RANT.

2.7 Sign out

The "Sign out" button on the far right of the ribbon can be used to disconnect from the VMS-RANT.

3 Risk analysis tool (RANT part)

The Risk Analysis Tool (RANT), which calculates the risks to which the models built in the VMS part are exposed, must receive information from the IADS indicating whether or not there are problems on the nodes.

The RANT part has seven tabs (see Figure 21):

Figure 21: RANT page

3.1 Threats

Depending on the criteria "Confidentiality", "Integrity", "Availability", "Maintainability", "Reliability", "Safety" (see Figure 22), the "Threats" page allows the user to view the threat status on the models. To do this, the user must select a criterion from the drop-down list and then click on the "play" button. The page in Figure 22 appears.

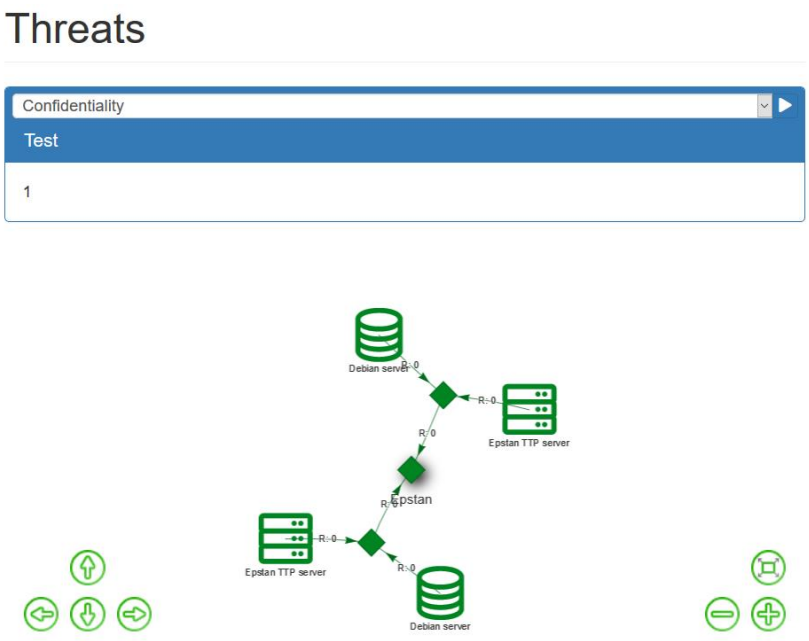

Figure 22: Threats page

- To enlarge the model, click on the button ⊕;
- to reduce, on the button ⊖;
- to refocus, on the button ⊡;
- to move from left to right, from bottom to top, play with the following buttons ⇦ ⇧ ⇨.

3.2 Asset

The "Asset" page allows the management of assets.

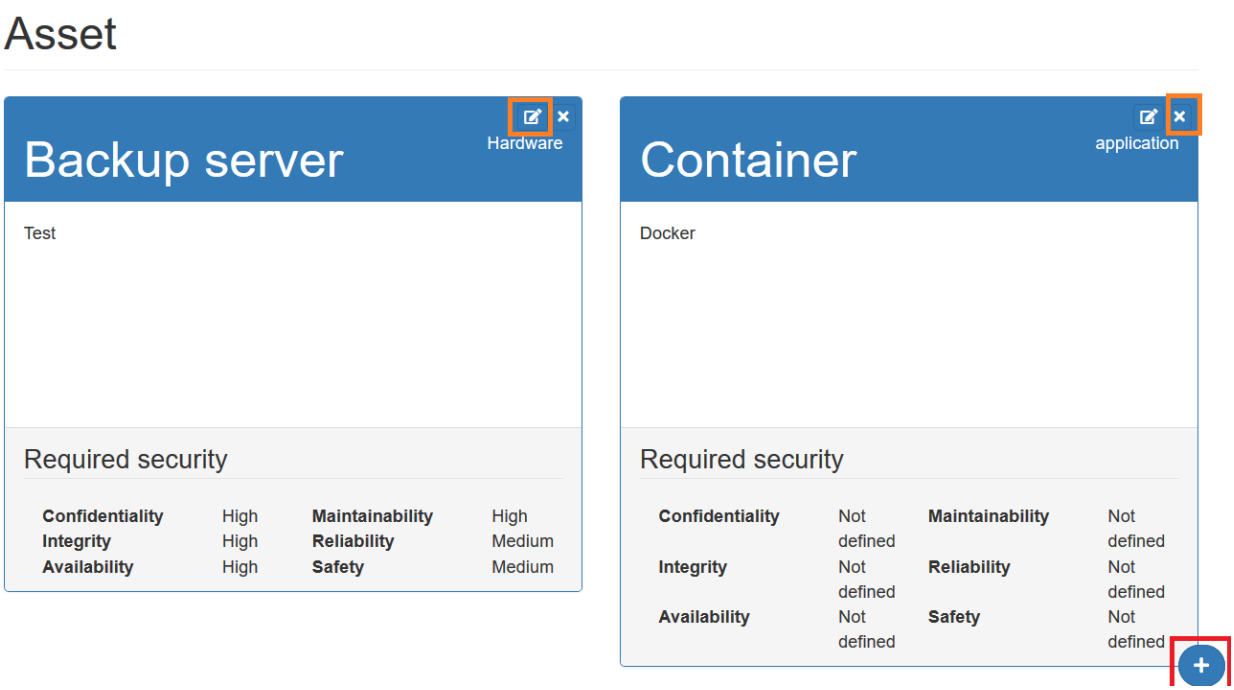

Figure 23: Asset page

To add a new "Asset" or active, the user clicks on the "more" button on the right, and at the bottom of the page (see Figure 23), the window below appears, the user must fill in the different fields (see Figure 24).

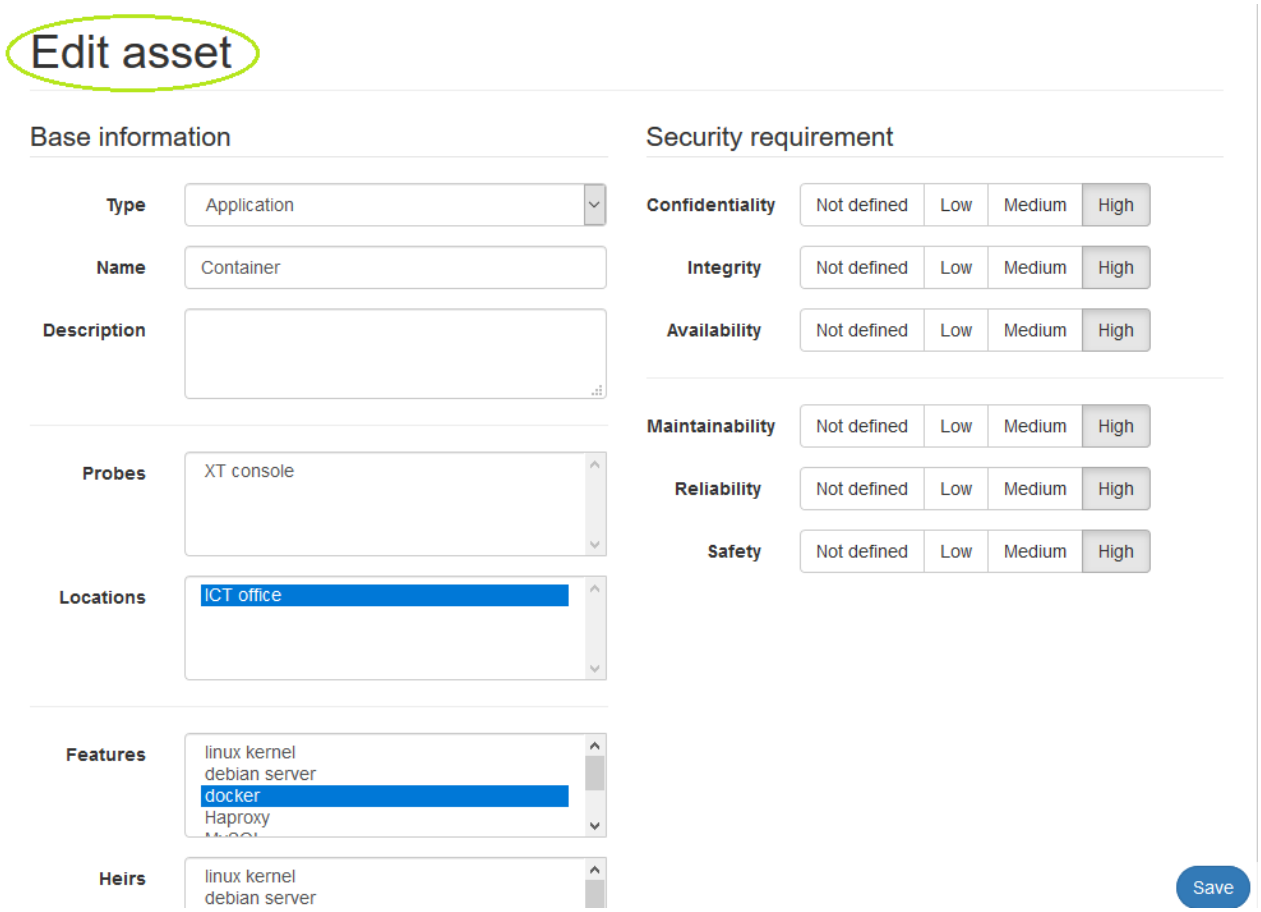

Figure 24: Add an asset

To complete the asset information to add the features and/or secondary assets attached, the user selects the "Features" and "Hedges" fields.

To modify or delete an asset, he uses the corresponding buttons (see Figure 23).

3.3 Layer

This section allows the user to manage the different layers of the modelling. The layers are defined by levels, the levels being ordered in an increasing way. Example: level 1 is considered higher than level 2.

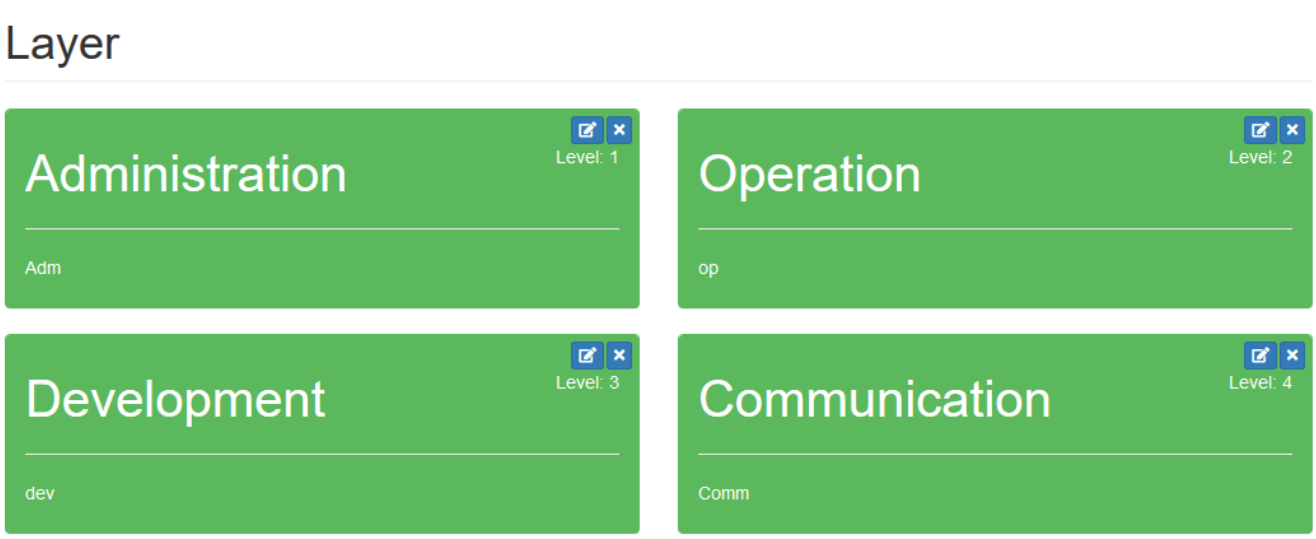

Figure 25: List of the different layers

3.4 Events

The "Events" page allows the user to simulate the management of events. This is optional.

3.5 Features

This page allows the user to add features directly to assets without going through the "Asset" page. All the features added to the different assets appear here. See Figure 26.

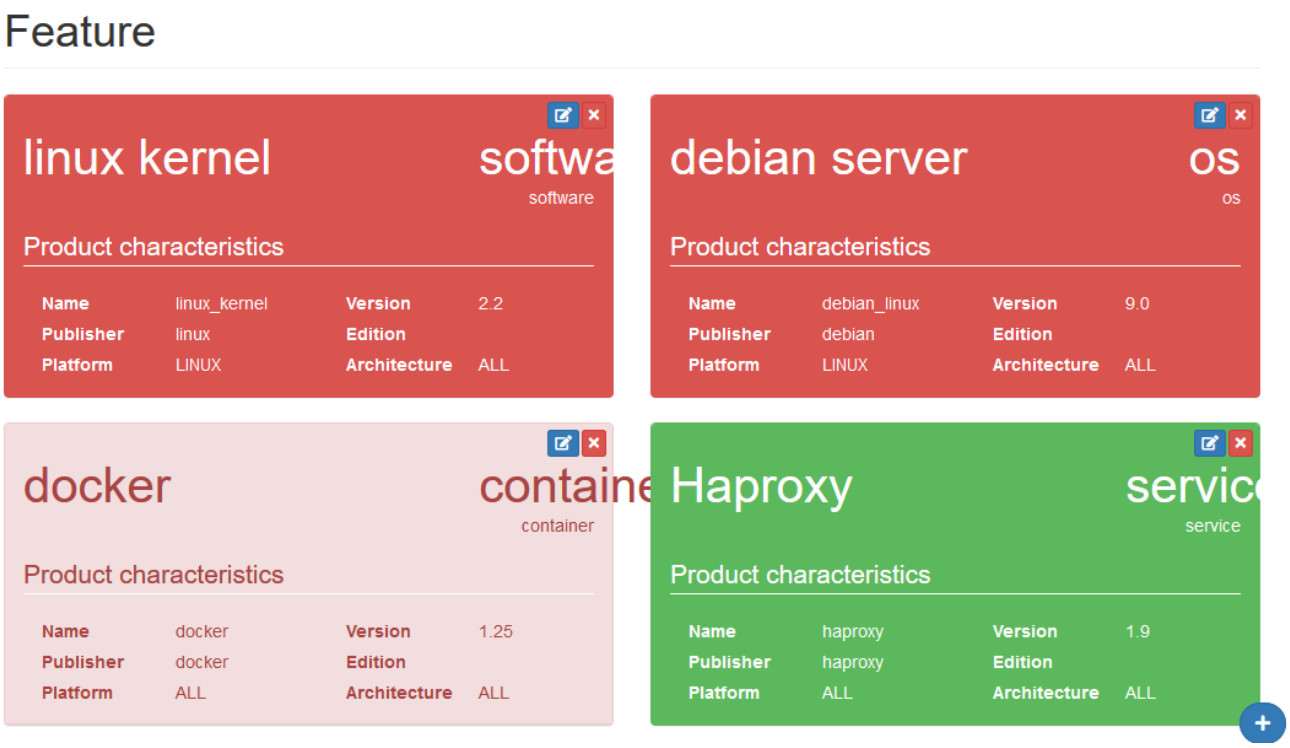

Figure 26: Features page.

Colours may vary from green (no vulnerability detected) to scarlet red (critical vulnerability).

3.6 Location

This page allows the user to manage the locations of each asset group. These locations are used during modelling to link each asset in the database.

3.7 Risk Factor

Risk Factor is a factor that mitigates the probability of events increasing. It allows events to be corrected by reducing their probability.

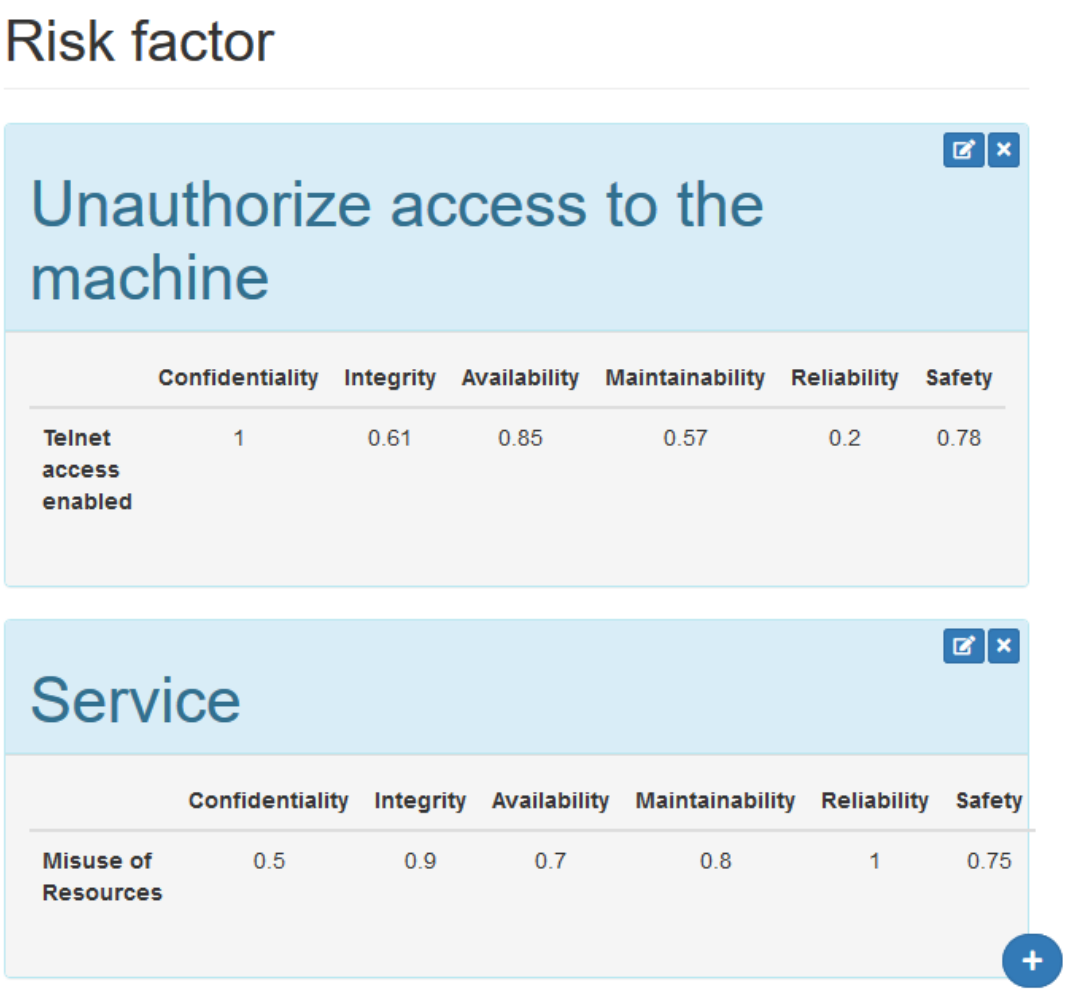

Figure 27: Risk Factor page

The user can add or modify risk factors. For each factor there may be zero or more types of threats defined.

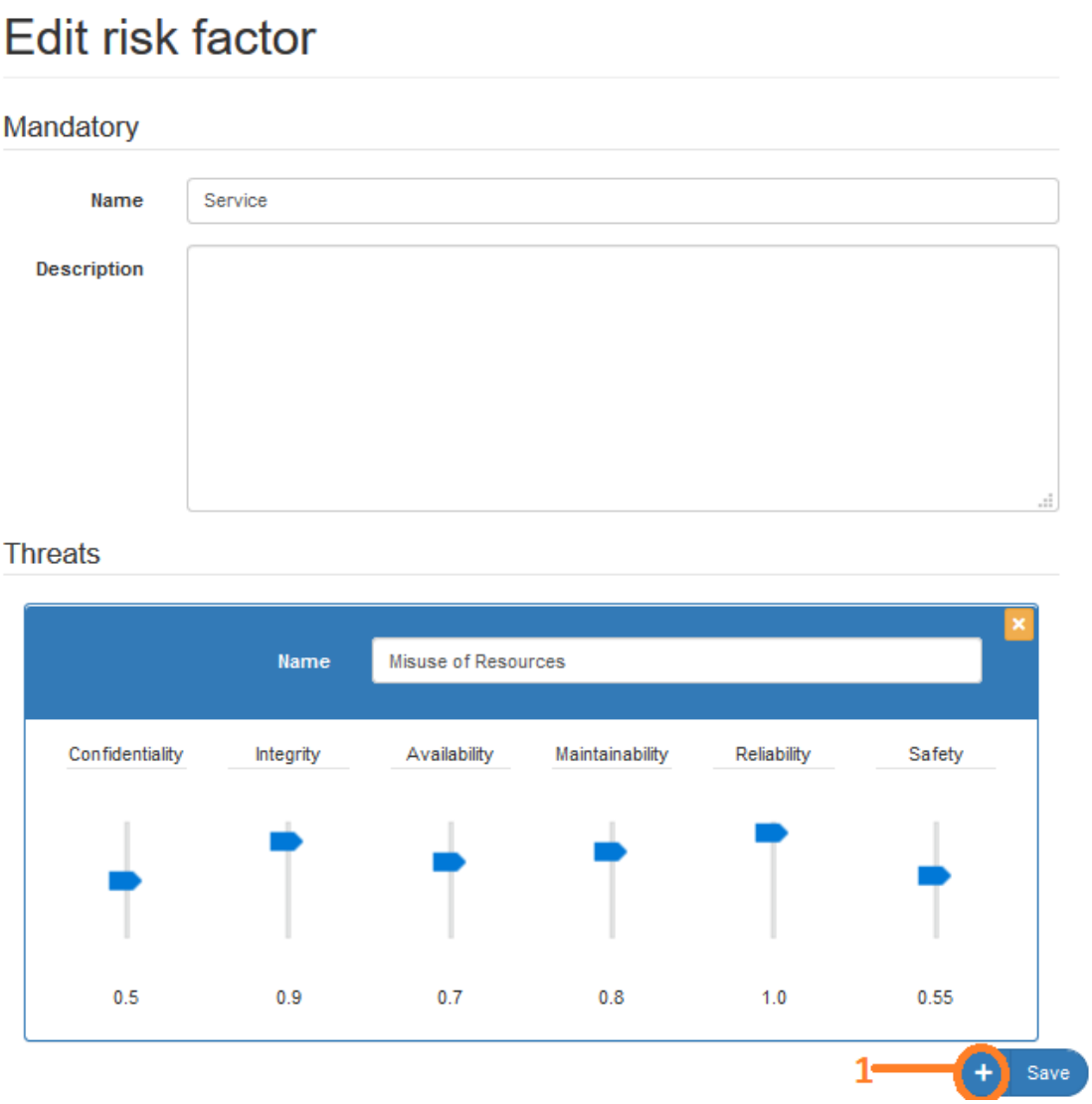

Figure 28: Edit a risk factor page

To add a new type of threat, the user shall select the "plus" button (button 1, see Figure 28) and define a name and associated criteria (confidentiality, integrity, availability, etc.). The values of the latter vary between **0** and **1** in steps of **0.05**.