FORTRA

beSECURE
21.41 (rev: 11.4.6)

Quick Setup Guide

Copyright Terms and Conditions

202307110155

Table of Contents

Accessing beSECURE

beSECURE is accessible by way of a supported web browser and a valid username and password (supplied to you by your account manager).

To log in to beSECURE, do the following

1. Choose one of the following beSECURE servers, based on your geographical location:
   - US server: https://cloud2.beyondsecurity.com
   - European server: https://cloud3.beyondsecurity.com

   > **NOTE:** If you are unsure of which server address to use, contact Beyond Security Technical Support at support@beyondsecurity.com, or your account manager for login credentials.

2. On the Welcome page, enter your **username** and **password**, and then click **Login**.

> **IMPORTANT:** If three failed log in attempts occur with your username, your account becomes locked and no additional log in attempts can be made for 30 minutes (default). For information on modifying this timer, see ***Creating a Security Profile*** for information on the **Password Failure Location Duration** parameter.

To log out of beSECURE, select your username in the top-right corner of the screen, and then select **Logout**.

Navigation Bar Menu Overview

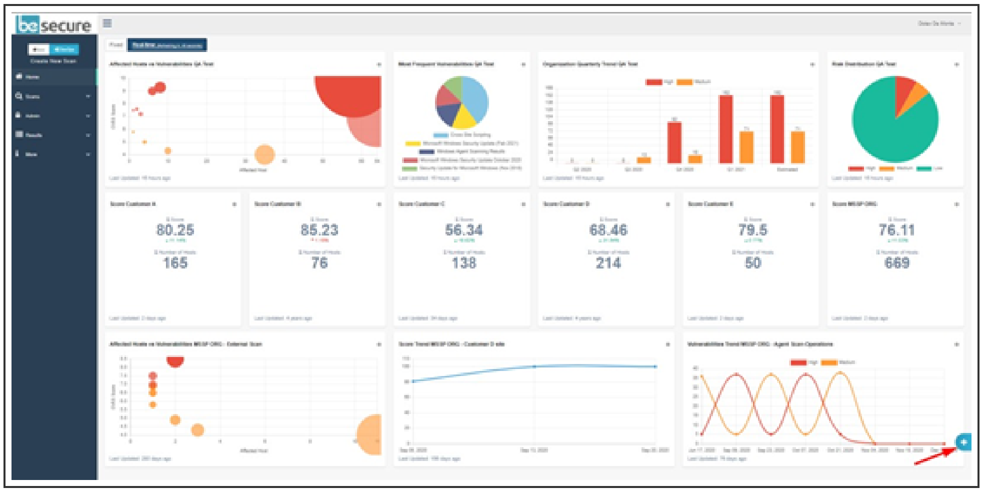
Home - Customize your own personal Homepage. Add widgets for a quick overview for future log ins to see vulnerability details.

Scans - Create new scans and web scans, edit existing scan details, credentials storage (Credential storage allows the login details for windows or SSH (for Linux servers) to be saved in the system for authenticated scans).

Admin - Add/Edit account users, Contacts, account profile (like a set of rules for all assigned users) and Organizations.

Results - Shows summary, search for results, generate and view reports, assets.

Most Commonly used Widgets (not a part of the menu but is found and added using the + icon in the right bottom corner) - Widgets are visual tools that can provide a user with analytical overview of Most Frequent Vulnerabilities, Monthly/Quarterly Trend (option to export results as CSV).



Admin Tab

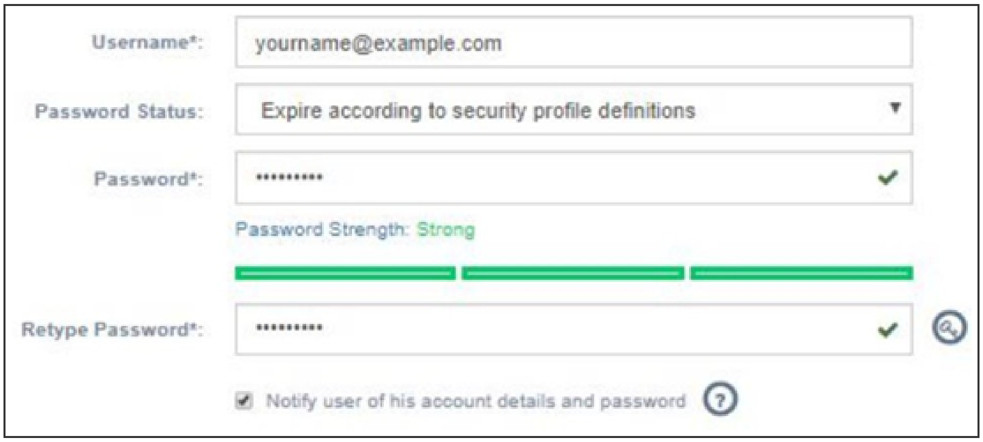
The main organization and first user will have been created for you. Additional Users, Contacts and Organizations can be created from the user interface. Accounts are users who can log in to beSECURE, contacts are people who receive email notifications and report but cannot log in to beSECURE, and the organization is the main group that contains users, contacts and scans.

> **NOTE:** Before creating a user account, an account profile and security profile should be created because during the creation of a user account, one is asked to select account profile and security profile.

Setting up new users

1. Log in to **beSECURE**.
2. In the upper-left corner of the **Home** page, select **DevOps**.
3. Select **Admin** > **Accounts** > **List**.
4. Select the **New** ⊕ button.
5. On the **Account Details (New)** page, enter the following information:
   a. **Username** - Enter the user's email address.
   b. **Password Status** - Select a password expiration policy for this user.
   c. **Password** - Enter a password that will correspond with the **Username**.
   d. **Retype Password** - Reenter the password from the **Password** box.
   e. **Security Profile** - Select the desired profile for this user.
   f. **Account Profile** - Select either Scanning user (ability to create or edit scan settings) or Reporting user (only has the ability to view scan results for the assigned organization(s).
   g. **Language** - Select the preferred language for this user.
   h. **Timezone** - Select the user's local time zone.
   i. **New Contact Person** - Enter the user's contact information in the fields provided in this section.

j. Select **Create**.



Username*: yourname@example.com

Password Status: Expire according to security profile definitions

Password*: ••••••••••

Password Strength: Strong

Retype Password*: ••••••••••

☑ Notify user of his account details and password

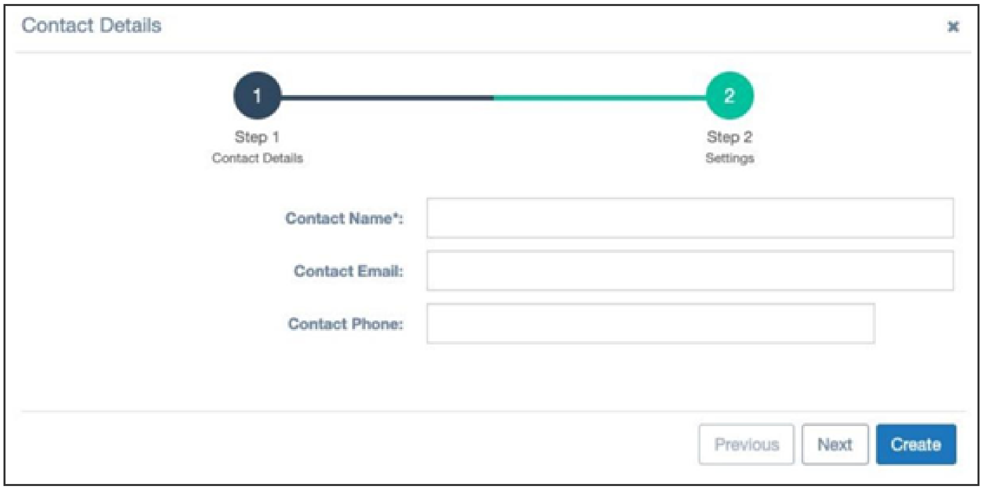
Setting Up Contacts and Group Contacts

There are two contact options. A contact is for one email address and group contacts (G) are like distribution lists. Multiple people can receive the scan notifications and reports.

Individual contacts can be added when creating a new user like in the directions above or by the Contacts option under Admin. A Contact Group can only be added from under the Admin tab using the Group Contacts option.

To create a new contact or group, do the following

1. Log in to **beSECURE**.
2. In the upper-left corner of the **Home** page, select **DevOps**.
3. Select **Admin** > **Accounts** > **Contacts** or **Group Contacts**.
4. Select the **New** + button.
5. In the boxes provided, enter the contact's or contact group's information.
6. Select **Create**.

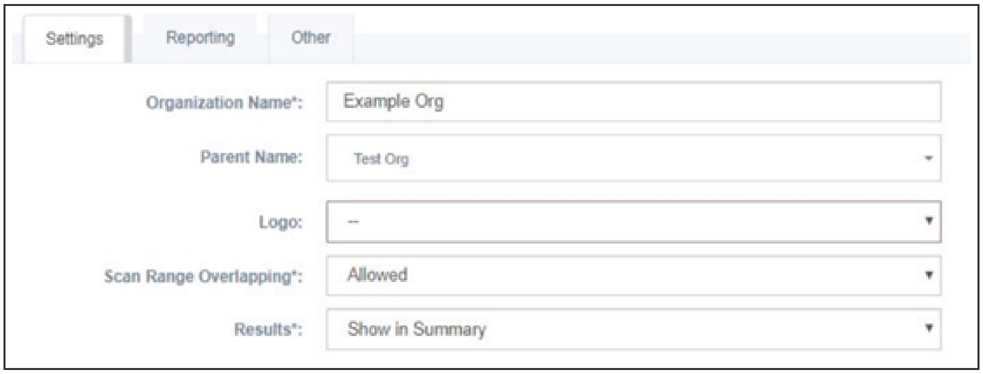


Create Organizations

Organizations are utilized to create divisions within a company. This can be useful for reseller clients or businesses that have multiple divisions or locations.

To create an organization, do the following:

1. Log in to **beSECURE**.
2. In the upper-left corner of the **Home** page, select **DevOps**.
3. Select **Admin** > **Organizations** > **List**.
4. Select the **New** ⊕ button.
5. On the **Settings** tab, enter the following information:
   a. **Organization's Name** - Enter the desired name for the organization.
   b. **Parent Name** - The parent name for reporting hierarchy.
   c. **Logo** - Select a preexisting logo. To add a logo, select **My Logo** from the left-side pane.
   d. **Scan Range Overlapping** - Specifies if a host is on more than one scan.
   e. **Results** - Select to show or hide the organization's name in reports.
   f. **Contact Person** - Select the contact person for the organization.
6. Select the **Permissions** tab.
7. Under **Owned By**, select a user from the **Available** box to move it to the **Assigned** box.
8. Select the **Reporting** tab.
9. Select when to send the assigned contact or contact group email notifications regarding the scan's progress.
10. Select **Create**.



Organization Name*:	Example Org
Parent Name:	Test Org
Logo:	--
Scan Range Overlapping*:	Allowed
Results*:	Show in Summary

Creating a Scan

IMPORTANT: You must have Scanning or Administrator permissions to access this feature.

You can create scans in beSECURE using either of the following methods:

- Quick - **Create New Scan** link at the top of the navigation bar - Provides a simplified interface to allow a scan to be created and run quickly.
- Extensive - **Scan List** page- Provides access to all scan parameters at the time of creation.

Create New Scan link

1. Log in to **beSECURE**.
2. In the upper-left corner of the **Home** page, select **Create New Scan**.
3. In the **Scan Name** box, enter a name for the scan.
4. In the **Range** box, enter the IP address(es) and/or hostname(s) to scan.

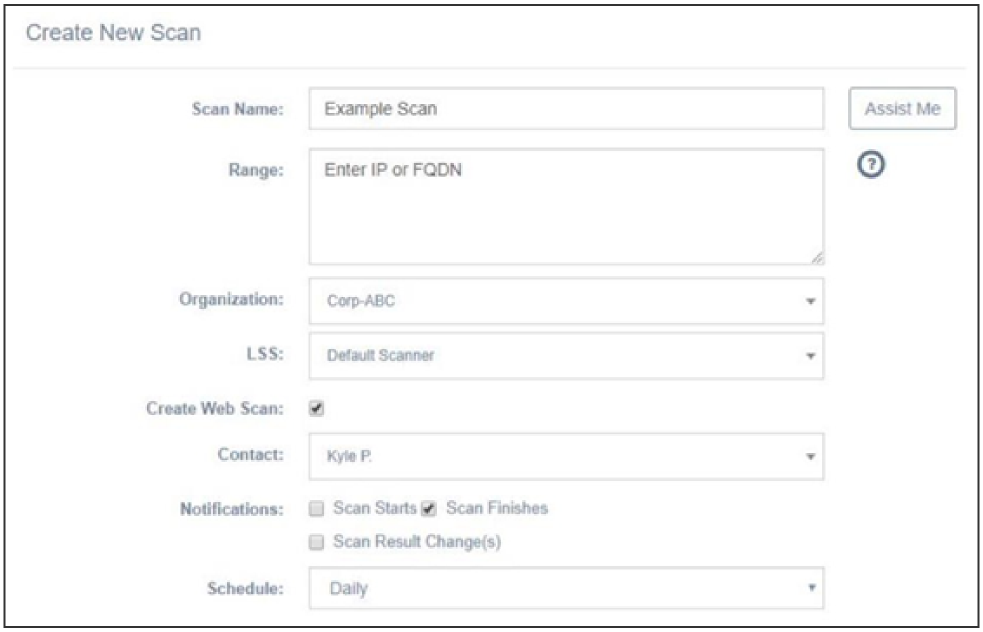
   NOTE: Hostnames/IP addresses provided must be unique for the specified Parent Organization, two different Scans assigned to the same organization should have no common target hosts. Use a comma or a new lines to separate different IPs or Hostnames. Use network dividers such has /8 (A-class) or /24 (C-class) to define subnets. Use '-' to define ranges (For the last digits only, i.e. 192.168.1.100-120).

5. In the **Organization** box, select an organization registered in your beSECURE account to scan.

   NOTE: Do not select an organization you could also register your SOC/ IT / Production as your company’s organization.

6. In the **LSS** box, select the desired local scanning server (LSS) to use with the scan.
7. To perform scans on the application layer (that is, the 7th OSI layer), leave the **Create Web Scan** check box selected.
8. In the **Contact** box, select a contact registered in your beSECURE account to receive notifications regarding the scan.

9. To send real-time email notifications regarding the scan to the Contact selected, leave the **Scan Starts**, **Scan Finishes**, and **Scan Result Change(s)** check boxes selected in the **Notifications** group.
10. In the **Schedule** box, select if you want the scan to run **Immediately**, **Daily**, **Weekly**, or **Monthly**.
11. If you selected Daily, Weekly, or Monthly for the **Schedule** parameter, in the **Every** or **Every day** box, select the number of day(s), the day of the week, or calendar day, based on the corresponding scanning schedule.
12. Click **Create**.



Create New Scan

Scan Name: Example Scan

Range: Enter IP or FQDN

Organization: Corp-ABC

LSS: Default Scanner

Create Web Scan: ☑

Contact: Kyle P.

Notifications: ☐ Scan Starts ☑ Scan Finishes ☐ Scan Result Change(s)

Schedule: Daily

IMPORTANT: The scan runs an infrastructure scan while the web scan specifically runs vulnerability tests for websites for example SQL injection and cross site scripting.

From the Scans List page

1. Log in to **beSECURE**.
2. In the upper-left corner of the **Home** page, select **DevOps**.
3. Select **Scans** > **Scans List**.
4. Select the **New** + button.
5. On the **Scan Details** page, under the **Main** tab, configure the following parameters:
   a. In the **Scan Name** box, enter a name for the scan.
   b. In the **LSS** box, select the desired local scanning server (LSS) to use with the scan.

c. In the **Organization** box, select an organization registered in your beSECURE account to scan.

> **NOTE:** Do not select an organization you could also register your SOC/ IT / Production as your company's organization.

d. In the **Hostname / IP Address Range** box, enter the IP address(es) and/or hostname(s) to scan. Optionally, click **Import** to import a CSV file, or **Resolve** to resolve the host.

> **NOTE:** Hostnames/IP addresses provided must be unique for the specified Parent Organization, two different Scans assigned to the same organization should have no common target hosts. Use a comma or a new lines to separate different IPs or Hostnames. Use network dividers such has /8 (A-class) or /24 (C-class) to define subnets. Use '-' to define ranges (For the last digits only, for example, 192.168.1.100-120).

6. If the scan requires Windows authentication, click the **Authentication** sub-tab and configure the following parameters (*skip to step 6 if WIndows Authentication is not required*):
    a. In the **Stored Credentials** box, select credentials from the Credentials Storage section of your beSECURE account to use with the scan, or manually enter your credentials in the **Windows Username**, **Windows Password**, and **Windows Domain** boxes.
    b. To add SSH Authentication, click **Host List** to select from existing hosts registered in your account, or click **Add New Host** to enter a **Hostname** and **Port** to use with this scan.
7. Click the **Hostname / IP Address Range** tab and configure the following parameters:
    a. In the **Include** box, enter the IP address(es) and/or hostname(s) to include in the scan. Optionally, click **Import** to import a CSV file containing hostnames and/or IP addresses, or **Resolve** to resolve the host.
    b. In the **Exclude** box, enter the IP address(es) and/or hostname(s) to exclude from the scan. Optionally, click **Import** to import a CSV file containing hostnames and/or IP addresses, or **Resolve** to resolve the host.
8. Click the **Additional Settings** sub-tab and configure the following parameters:

   a. By default, the **Ping Host** check box is selected. See note before you opt to clear this setting.

      > **NOTE:** Disabling **Ping Host(s)** causes the scan to skip the first phase where it attempts to detect live hosts in the range provided. This causes the scan to run on hosts that do not answer the Scan Setting ping and do not listen to standard ports. This is beneficial when scanning high-security Scan Settings like a DMZ. However, clearing this check box may also cause the scan to run much longer due to all of the possible Scan Settings in the range being scanned, even if there are no actual machines configured to the IP address.

   b. In the **Port Range** box, enter the desired range of ports to scan, or select the **Full Port Range** check box to enter the full range of ports (1-65535).
   c. Optionally, in the **Exclude Ports** box, enter any ports to exclude from the scan.
   d. In the **SNMP Community Name** box, enter the desired SNMP name to use with the scan.
   e. In the **Scanning Profile** box, select a profile to use with the scan.
   f. Optionally, in the **Tests to Exclude** box, enter any tests to exclude from the scan.
   g. Optionally, in the **Tests to Include** box, enter any tests to include with the scan.

9. Click the **Permissions** tab and assign the contacts who need rights to access and modify this scan by clicking on each desired contact name in the **Available** box to move it to the **Assigned** box.

   > **NOTE:** A scan without assigned owners is automatically owned by any Scanning or Administrator Account User in the account.

10. Click the **Reporting** tab and configure the following parameters:
    a. In the **Contact Person** box, select a contact registered in your beSECURE account to receive notifications regarding the scan.
    b. To send real-time email notifications regarding the scan to the selected **Contact Person**, leave the **Scan Starts**, **Scan Finishes**, and/or **Scan Result Change(s)** check boxes selected in the **Notifications** group.
    c. In the **Customization Name** box, select a preconfigured report stored in your beSECURE account (if any), or select **New** to create a new report.
    d. In the **Format** box, select **PDF** or **XML** for the report's format.
    e. In the **Report Type** box, select **Complete** (full report), **Filtered** (results filtered by way of vulnerability name), or **Differential** (compares results from two different scans) for the type of report to generate.

   f. If **Format** is set to **PDF**, in the **PDF User Password** box, optionally type a password to password protect the report once it is generated.
   g. In the **Report Style** box, select the style of report to view the scan results in. For a description of each Report Style, see Report Styles.
   h. To hide the Host Information section of the report when it is generated, select the **Hide Host Information section** check box.
   i. If the **Report Type** box is set to **Filtered**, configure the parameters in Filtered Report group:
      i. In the Vulnerability box, enter a name for the vulnerability

11. Click the **Other** tab and if desired, enter a comment regarding the scan in the Comment box.
12. Select **Create** to save the scan and add it to the Scan List.

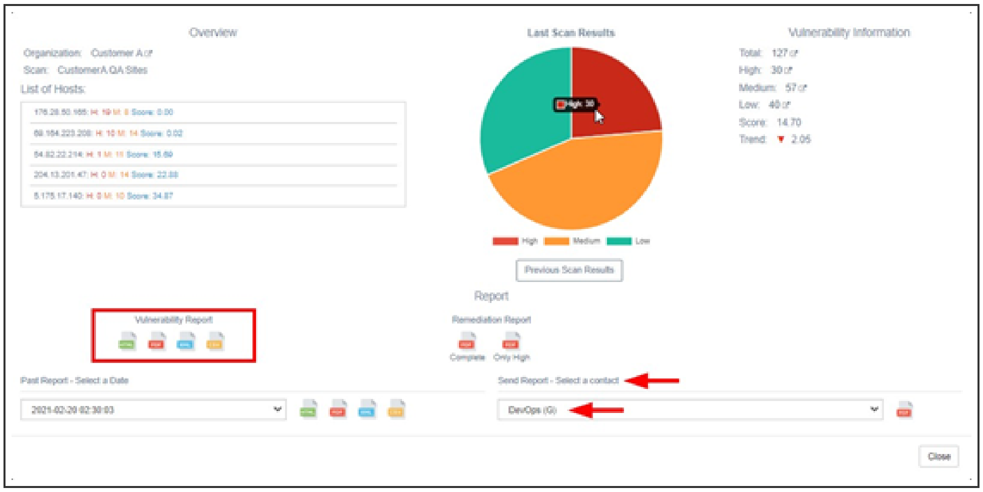
Results

After a scan has been completed the report will be sent automatically by way of email to the contact person or contact group for that scan. The beSECURE system offers a few different ways of reviewing the results.

Vulnerability Scan Summary Results

The Vulnerability Scan Summary Results page has a dashboard that dynamically displays data from scans, allowing you to select hyperlinks/smart object going from an overview of the entire organization, to overview of a specific scan, down to an overview of one specific host from a scan. To view the Vulnerability Scan Summary Results page, do the following:

1. Sign in to **beSECURE**.
2. Select **Results** > **Summary**.
3. In the **Organization** box, select an organization.
4. Select a report from the list.



Overview

Organization: Customer A

Scan: CustomerA QA Sites

List of Hosts:

176.28.50.165: H: 19 M: 8 Score: 0.00

69.164.223.208: H: 10 M: 14 Score: 0.02

54.82.22.214: H: 1 M: 11 Score: 15.69

204.13.201.47: H: 0 M: 14 Score: 22.88

5.175.17.140: H: 0 M: 10 Score: 34.87

Vulnerability Information

Total: 127

High: 30

Medium: 57

Low: 40

Score: 14.70

Trend: ▼ 2.05

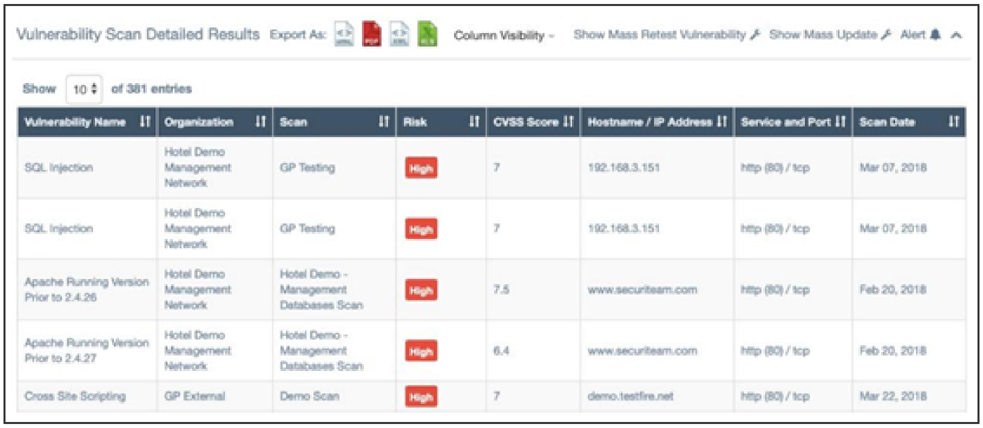
Past Report - Select a Date: 2021-02-20 02:30:03

Send Report - Select a contact: DevOps (G)

Under the **List of Scans**, selecting a scan name will show the data for that scan.

Select the **HTML**, **PDF**, **XML**, or **CSV** icon to download a copy of the report in the corresponding format. You can also send reports to any existing contact in your beSECURE account.

The **Last Scan Results** pie chart displays how many high, medium, and low vulnerabilities were found. Selecting a section of pie chart will display the Vulnerability Scan Detailed Results. Select the **HTML**, **PDF**, **XLS**, **CSV**, or **XML** icon to download a copy of the report in the corresponding format.

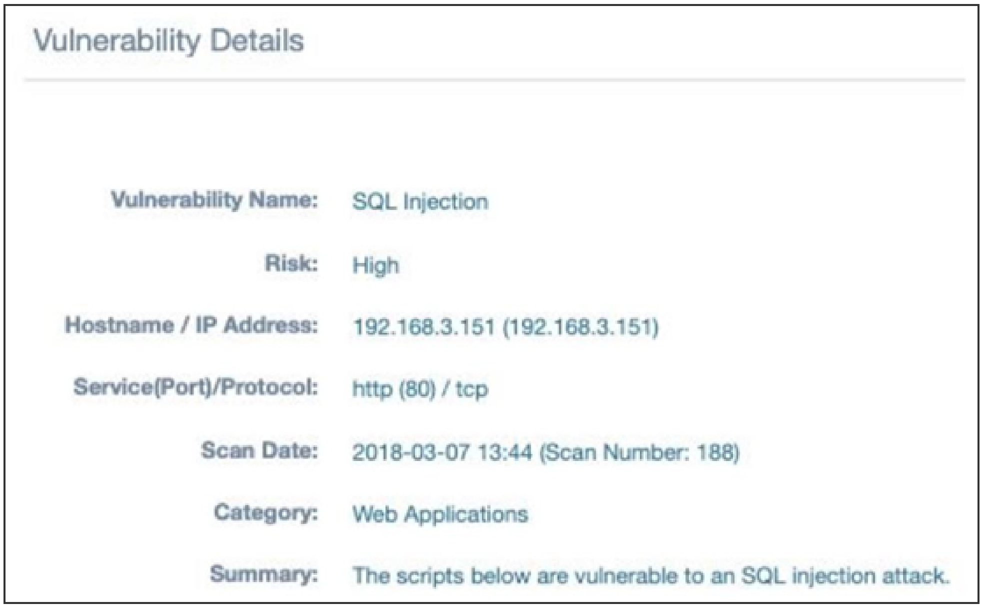


Vulnerability Scan Detailed Results Export As: Column Visibility Show Mass Retest Vulnerability Show Mass Update Alert

Show 10 of 381 entries

Vulnerability Name	Organization	Scan	Risk	CVSS Score	Hostname / IP Address	Service and Port	Scan Date
SQL Injection	Hotel Demo Management Network	GP Testing	High	7	192.168.3.151	http (80) / tcp	Mar 07, 2018
SQL Injection	Hotel Demo Management Network	GP Testing	High	7	192.168.3.151	http (80) / tcp	Mar 07, 2018
Apache Running Version Prior to 2.4.26	Hotel Demo Management Network	Hotel Demo - Management Databases Scan	High	7.5	www.securiteam.com	http (80) / tcp	Feb 20, 2018
Apache Running Version Prior to 2.4.27	Hotel Demo Management Network	Hotel Demo - Management Databases Scan	High	6.4	www.securiteam.com	http (80) / tcp	Feb 20, 2018
Cross Site Scripting	GP External	Demo Scan	High	7	demo.testfire.net	http (80) / tcp	Mar 22, 2018

On the **Vulnerability Scan Detailed Results** page, select a Vulnerability Name to view its details.



Vulnerability Details

Vulnerability Name: SQL Injection

Risk: High

Hostname / IP Address: 192.168.3.151 (192.168.3.151)

Service(Port)/Protocol: http (80) / tcp

Scan Date: 2018-03-07 13:44 (Scan Number: 188)

Category: Web Applications

Summary: The scripts below are vulnerable to an SQL injection attack.

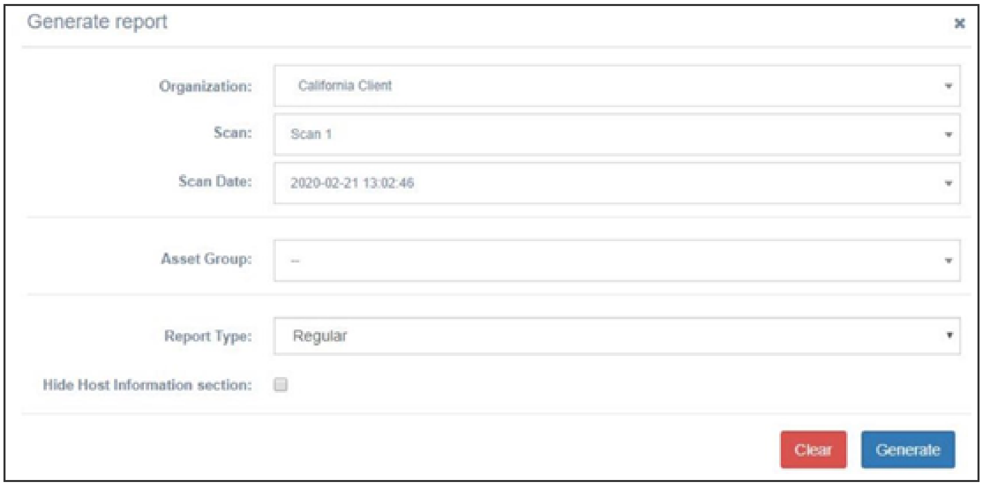
Generating Reports

beSECURE includes areport generator that creates reports based on specific criteria. It allows the report to show data for the entire organization or one scan. It also allows you to generate a report showing specific data, such as an asset group.

To generate a report, do the following:

1. Sign in to **beSECURE**.
2. Select **Reports** > **Results**.
3. Select **Generate Report**.

4. On the **Generate report** dialog, make a selection for each box.
5. Select **Generate**.



Generate report

Organization: California Client

Scan: Scan 1

Scan Date: 2020-02-21 13:02:46

Asset Group: --

Report Type: Regular

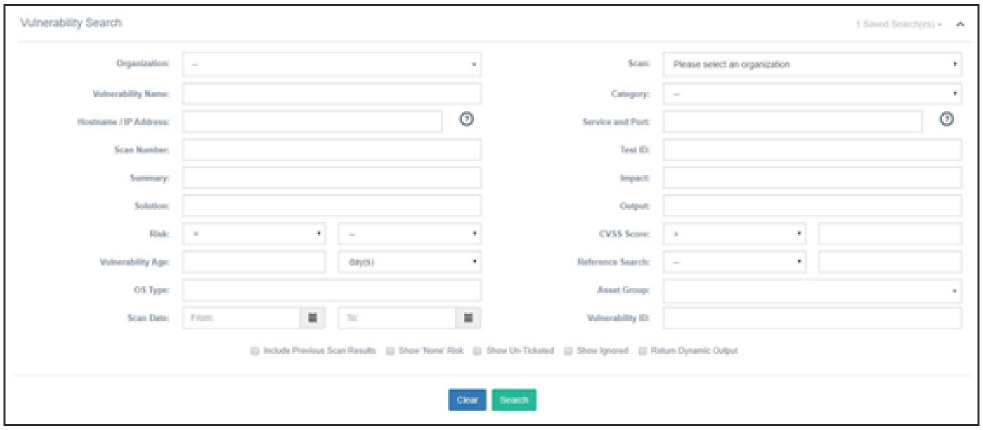
Hide Host Information section: □

Search for Results

The search function offers filters to find specific results data. Some of the filters by Hostname/IP Address, High/Medium/Low Risk, Vulnerability Age, Service and Port.

To perform a search, do the following:

1. Sign in to **beSECURE**.
2. Select **Reports** > **Search**.
3. Enter information in the boxes that fit your search criteria.
4. Select **Search**.



Vulnerability Search

Organization: --

Scan: Please select an organization

Vulnerability Name:

Category: --

Hostname / IP Address:

Service and Port:

Scan Number:

Test ID:

Summary:

Impact:

Solution:

Output:

Risk: = --

CVSS Score: >

Vulnerability Age: day(s)

Reference Search: --

OS Type:

Asset Group:

Scan Date: From: To:

Vulnerability ID:

□ Include Previous Scan Results □ Show 'None' Risk □ Show Un-Ticketed □ Show Ignored □ Return Dynamic Output

On Premise IS Deployment - Enabling Email Notifications

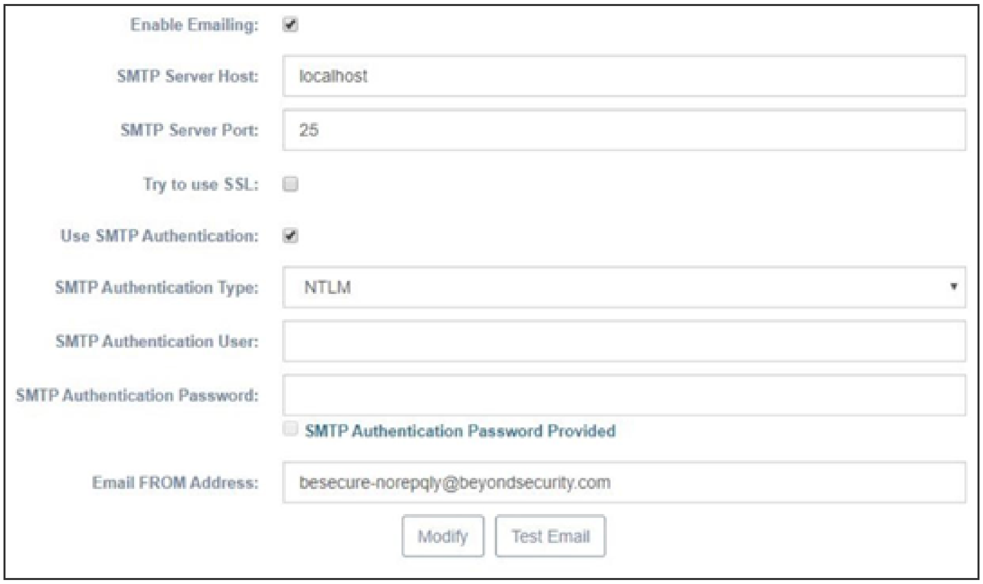
> **NOTE:** This section is not relevant for on premise scanner (LSS) deployments. If you are configuring an on-premise scanner (LSS) you can skip this section.

You only need to manually configure email notifications when using beSECUREII or the on-premise information system (IS) (automatic email notifications are disabled by default). To use your own corporate SMTP server or the internal SMTP server on your on-premise IS, you must configure the email notification settings in beSECURE.

To enable email notifications, do the following:

1. Log in to the on-premise IS.
2. Select **More** > **Server** > **Notifications**.
3. Select **Enable Emailing**.
4. In the **SMTP Server Host** box, enter one of the following:
    a. **localhost** - Enables and uses the built-in SMTP server.
    b. The FQDN or IP address of your third-party SMTP server / corporate SMTP server.
5. In the **SMTP Server Port** box, the default port is 25. If you enable **Try to use SSL**, adjust the port number accordingly (this is not required for an internal SMTP server).
6. Optionally, in the **Email FROM Address** box, you can change the default value from "besecure-noreply@beyondsecurity.com" to any other email address you want to

receive bounce emails at.



Enable Emailing: ☑

SMTP Server Host: localhost

SMTP Server Port: 25

Try to use SSL: □

Use SMTP Authentication: ☑

SMTP Authentication Type: NTLM

SMTP Authentication User:

SMTP Authentication Password:

□ SMTP Authentication Password Provided

Email FROM Address: besecure-norepqly@beyondsecurity.com