RAPID7

AppSpider Enterprise

User Guide

Contents

Contents 2
Revision history 4
About this guide 5
Login page 6
Forgot password 6
Dashboard 8
Impersonation 8
System admin's dashboard 9
Impersonated system admin's dashboard 10
External user's dashboard 12
Profile page 13
Change password 14
System menu 15
Clients 15
System Admin Accounts 16
Scan Engines 17
Scan Engine Groups 19
System events 21
Attack modules 21
Security 23
Authentication / authorization 23
Roles 23
Administration menu 27
Accounts 27
All accounts (SA) 29

Groups 29
All groups 31
Notifications 32
Targets based security 32
Integration 34
Targets 35
All targets 37
Organization profile 39
Scanning menu 41
Configs 41
Attack Policy 57
Blackouts 62
Scans 63
All scans (SA) 72
Scheduled scans 73
Defend scans 76
Findings menu 82
Discovered Issues 82
All discovered Issues (SA) 88
Issues summary 89
Charts 90
Trending chart 91
Discovery chart 92
Presets functionality 94
Targets security schema 95

Revision history

Revision date	Description
September 21, 2015	Created Rapid7 branded version of document.

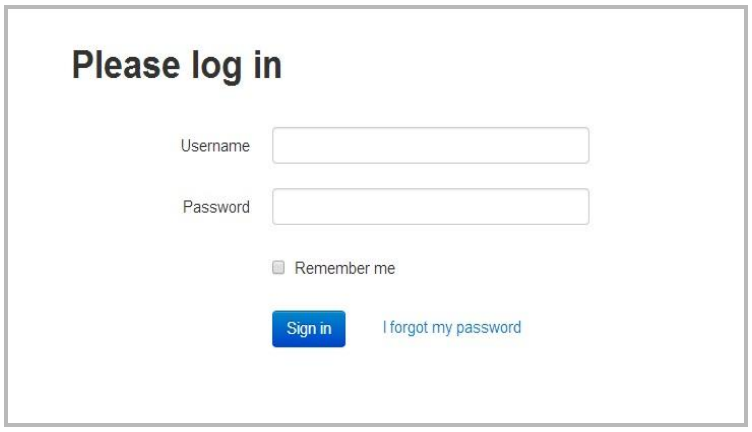
About this guide

This guide explains the features in the AppSpider Enterprise user interface that enable your team to configure and run scans and perform other important operations.

You should have AppSpider Enterprise installed. If not, refer to the *AppSpider Enterpise Installation Guide*, which you can download from the Rapid7Community.

Login page

To access the *Login* page, start a browser and enter the URL of the AppSpider installation in your navigation bar.



The **Username** and **Password** fields are mandatory.

I forgot my password links to the *Password recovery* page.

Users are informed when they have been locked out. User accounts become locked on entering an incorrect password 5 times.

Forgot password

Enter your username or email address to access the *Password recovery* page.

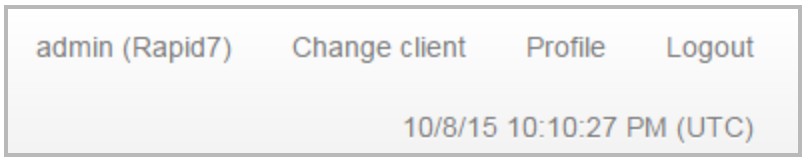
If the username or email address is not found, the screen will display the *Username or email validator*. If the username or email address is found, then the *Security question* screen will display.

If the correct answer is entered, an email with a new password will be sent to your email address. If an incorrect answer is entered, you will be prompted to try again.

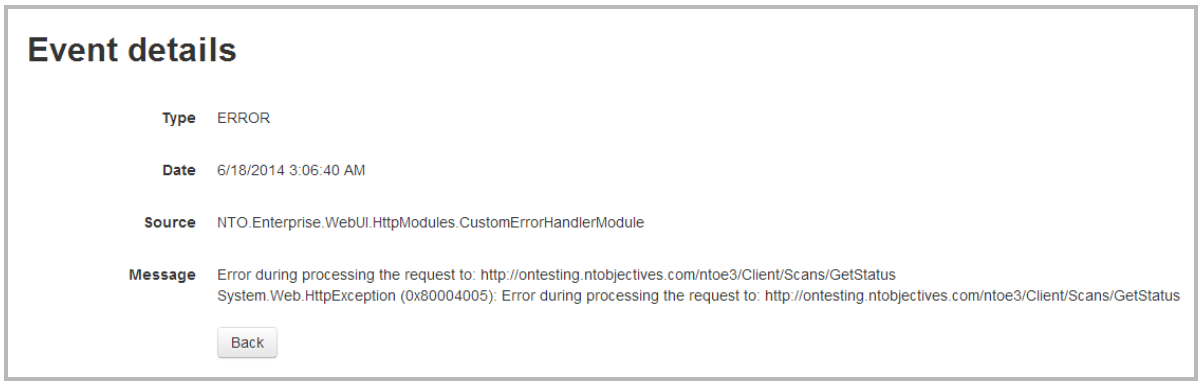
If a security question is not set in the profile, an email with the new password will be sent to the user without entering the security question.

Dashboard

The *Dashboard* includes several options on a bar to the top right. It displays the user's time zone and user name, as well as links to the user **Profile**, **Change client**, and **Logout** options.



All dates on the *Portal* are presented in the current user's time zone.

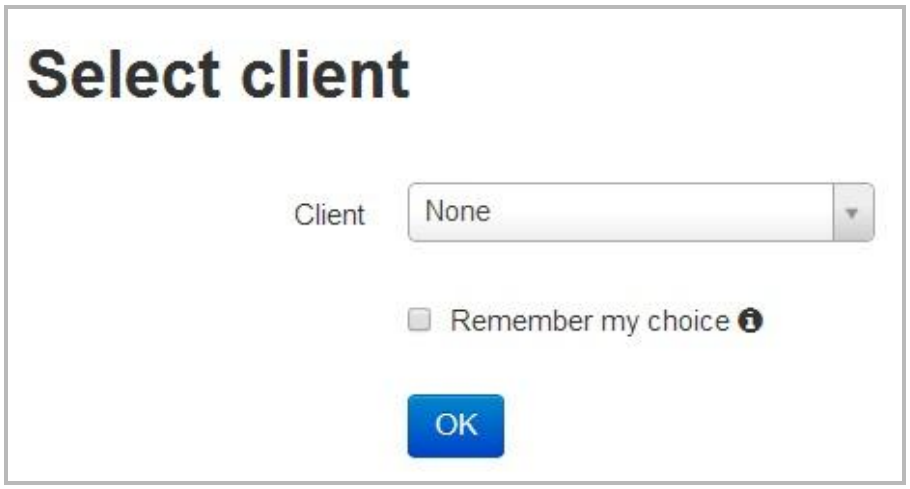


Impersonation

The **Change client** link on the Dashboard will take you to the *Select client* page. This page is only accessible to system admins.

On the *Select client* page, there is **Client** drop down menu which lists all available client options as well as a **None** option.

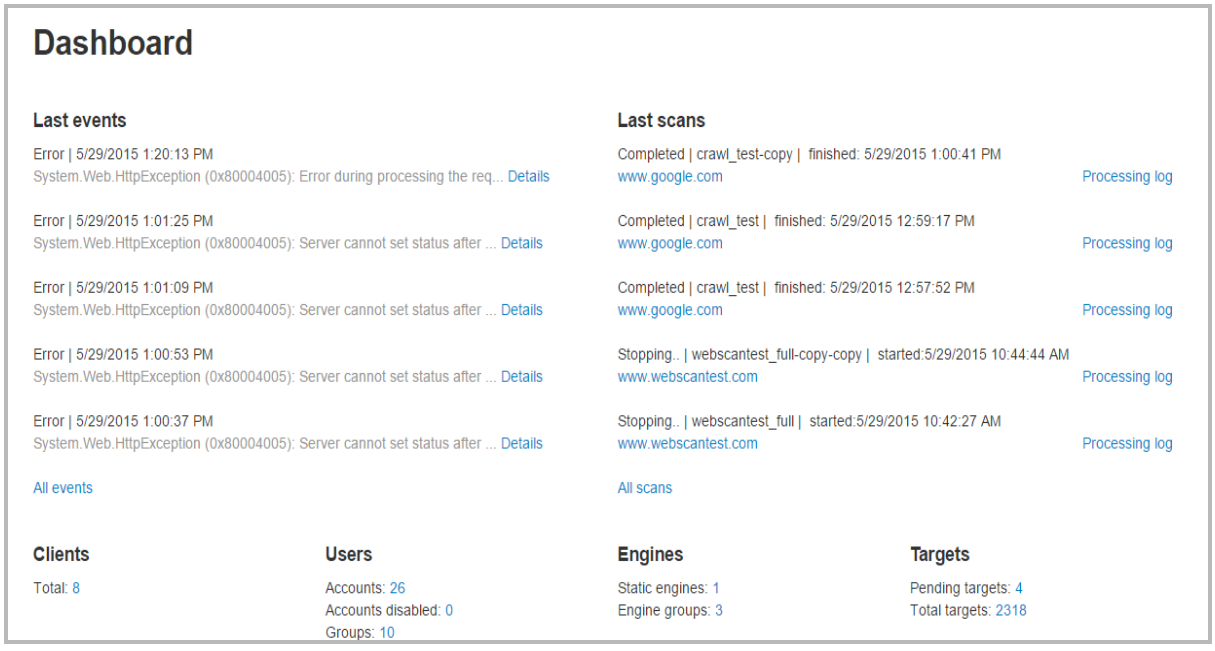
If **None** is selected, the user will be authenticated as a system admin.



If you choose any option on the **Client** drop down other than **None**, then all client-specific operations will be performed using that selected client.

System admin's dashboard

If you select the **None** option on the **Client** drop down menu of the *Select client* page, you will see the options that are part of the system admin's *Dashboard*.

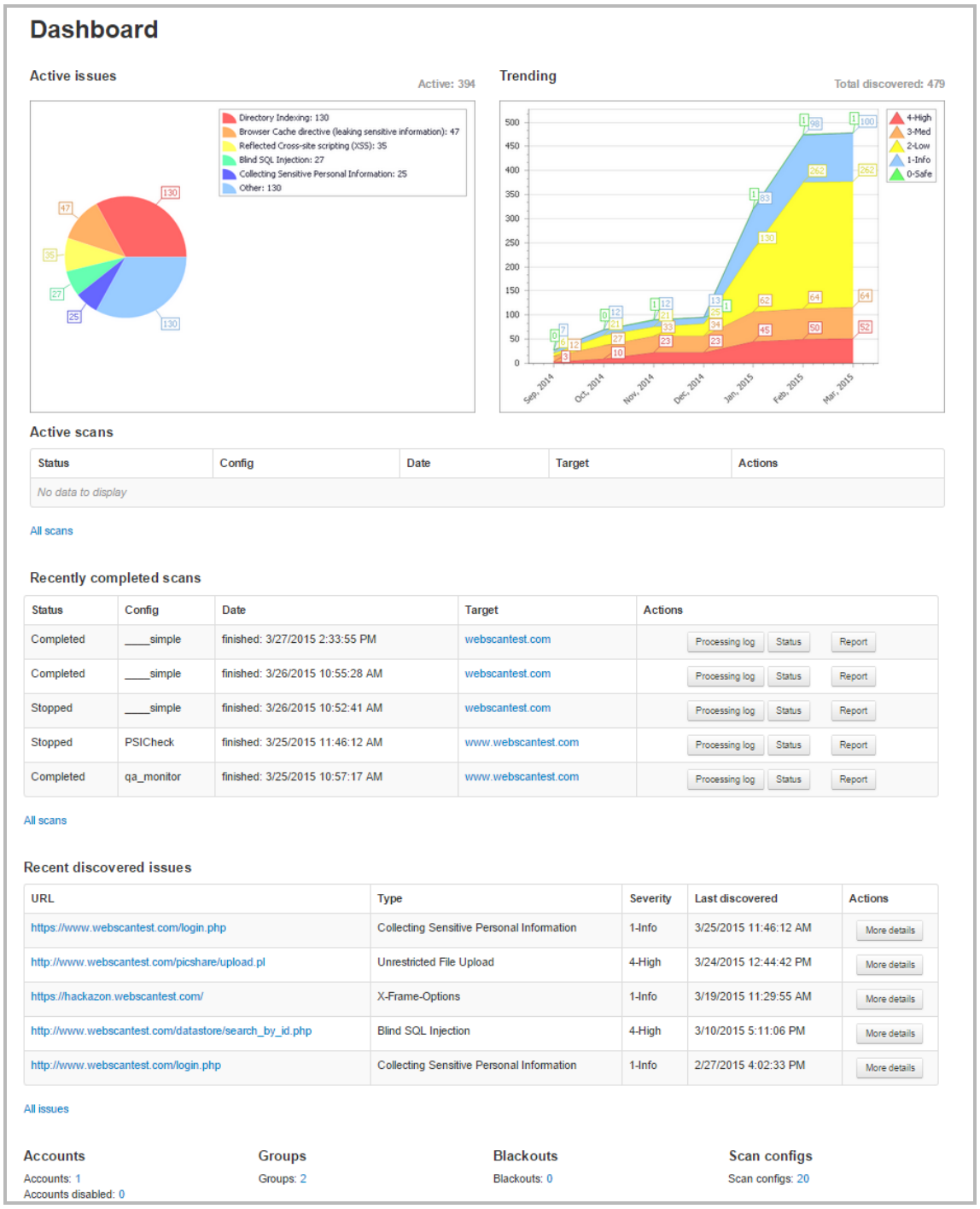


Towards the top, the dashboard has the *Last events* panel with links to event *Details* pages and the *All events* page. Additionally, the system admin's dashboard has the *Last scans* panel with links to the scan *Processing log* page, the *All scans* page, and an external link to target hosts.

At the bottom of the dashboard is counter information on *Clients*, *Users*, *Engines*, and *Targets*. Each item includes a numerical counter which is a link to a page with a listing of the relevant clients.

Impersonated system admin's dashboard

If you select any option other than **None** on the **Client** drop down menu of the *Select client* page, the *Dashboard* you will see will be for the Impersonated system admin.



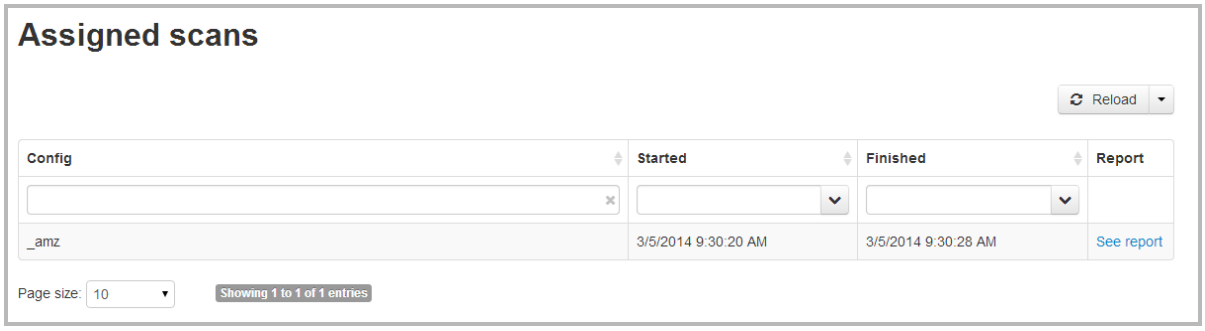
The *Active issues* pie chart is a diagram of all active issues for the current client divided by type. The *Trending* graph displays the number of issues by priorities for different dates. Both display information that is cached every 15 minutes.

The *Active scans* table displays the 5 scans that are currently in progress. It has **Processing log** and **Status** links. The **All scans** link leads to the *Scans* page.

The *Recently completed scans* table displays the 5 most recently completed scans. Like the *Active scans* table, it has **Processing log** and **Status** links, and the **All scans** link leads to the *Scans* page.

The *Recent discovered issues* table displays the 5 most recently discovered issues. It has the **More details** link which leads to the *Issue details* page.

External user's dashboard



The table contains the following columns:

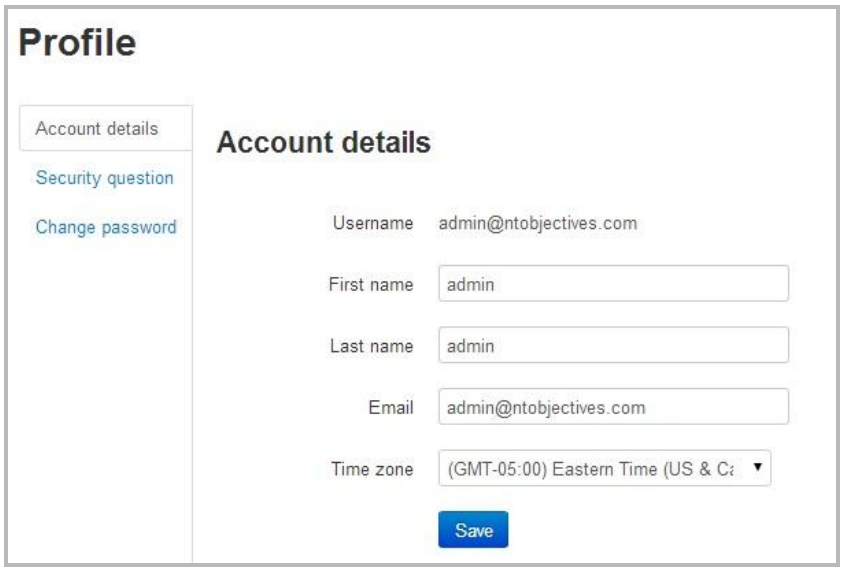
- *Config* - the name of scan config.
- *Started* - the start date and time of the scan.
- *Finished*" - the finish date and time of the scan.

Action button:

- *See report* - opens report page.

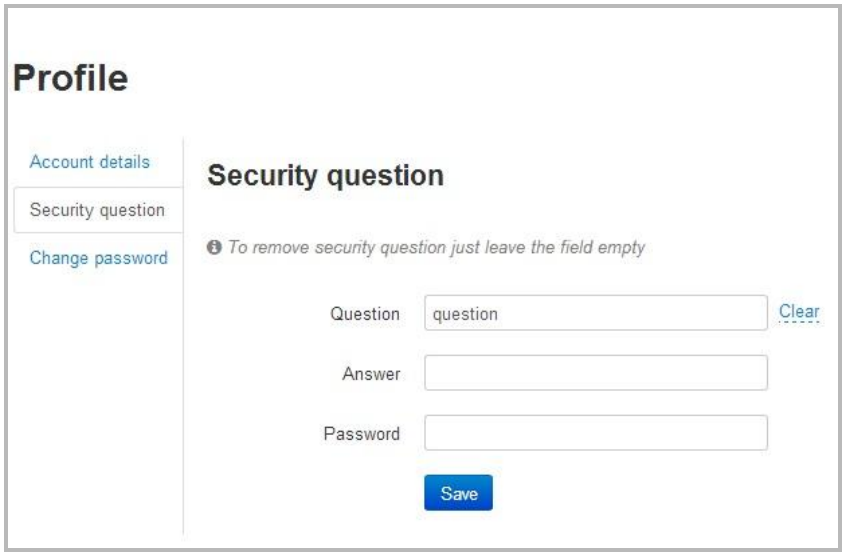
Profile page

The *Profile* page displays and allows you to change user data.



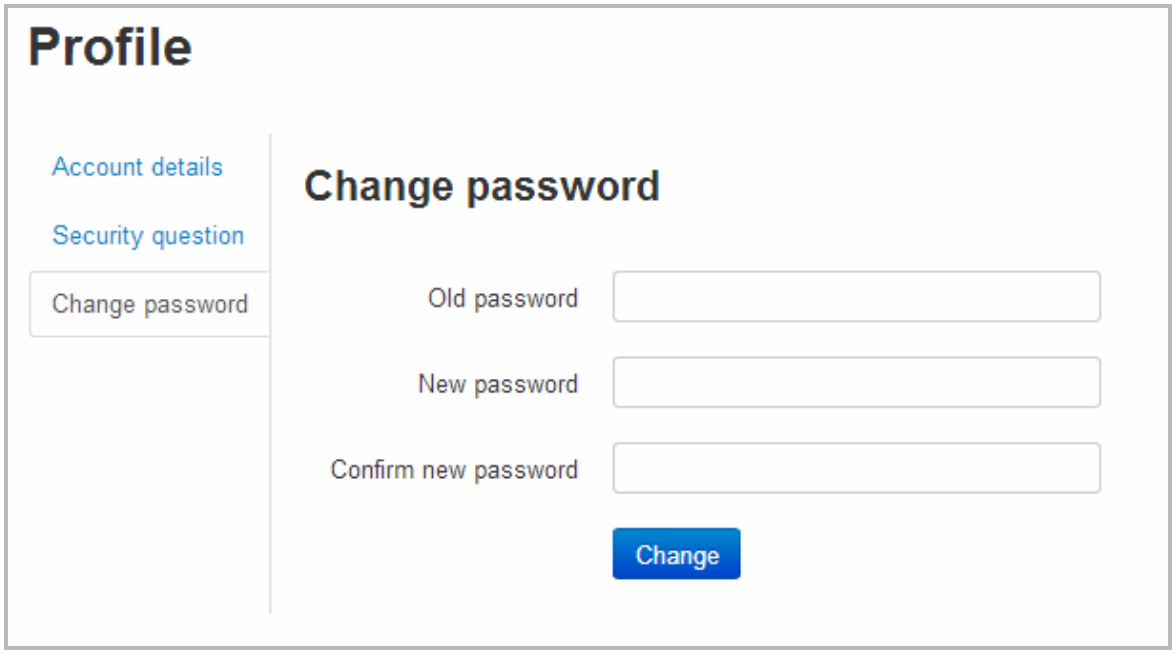
Email is a mandatory field.

You may change a Time zone using the **Time zone** drop down menu. All dates across the entire portal will reflect the selection you have made.



To change your *Security question*, enter a **Question**, **Answer**, and **Password**, then click the **Save** button.

Change password

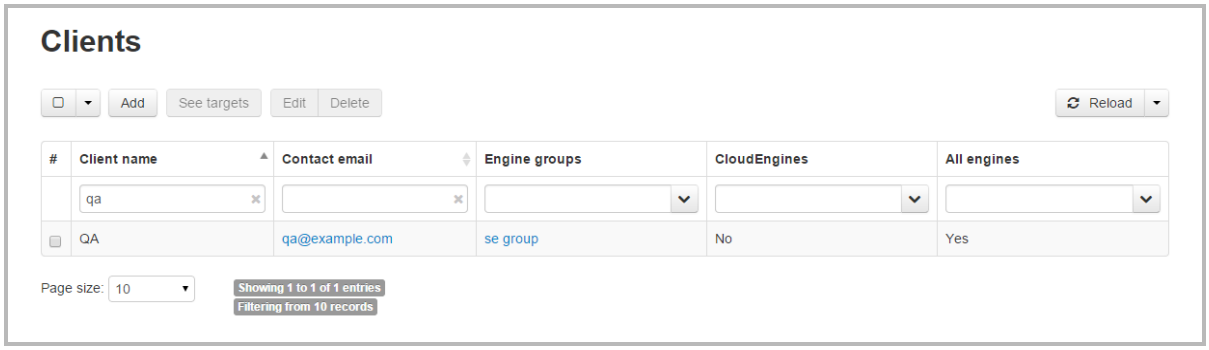


To change your password, complete the **Old password**, **New password**, and **Confirm new password** fields, then click the **Save** button.

System menu

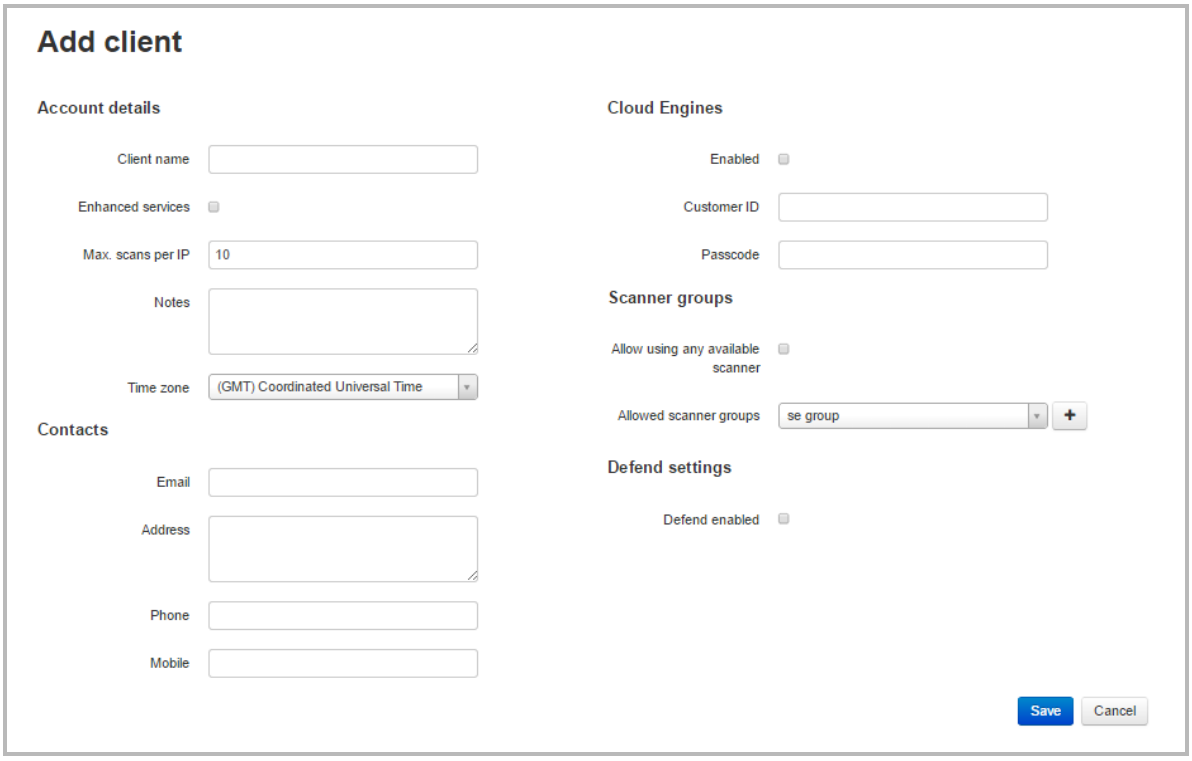
Clients

The *Clients* page displays an alphabetical list of clients. It also has buttons to **Add**, **Edit**, or **Delete** clients.



The **See targets** button leads to the *Targets* page for the selected client.

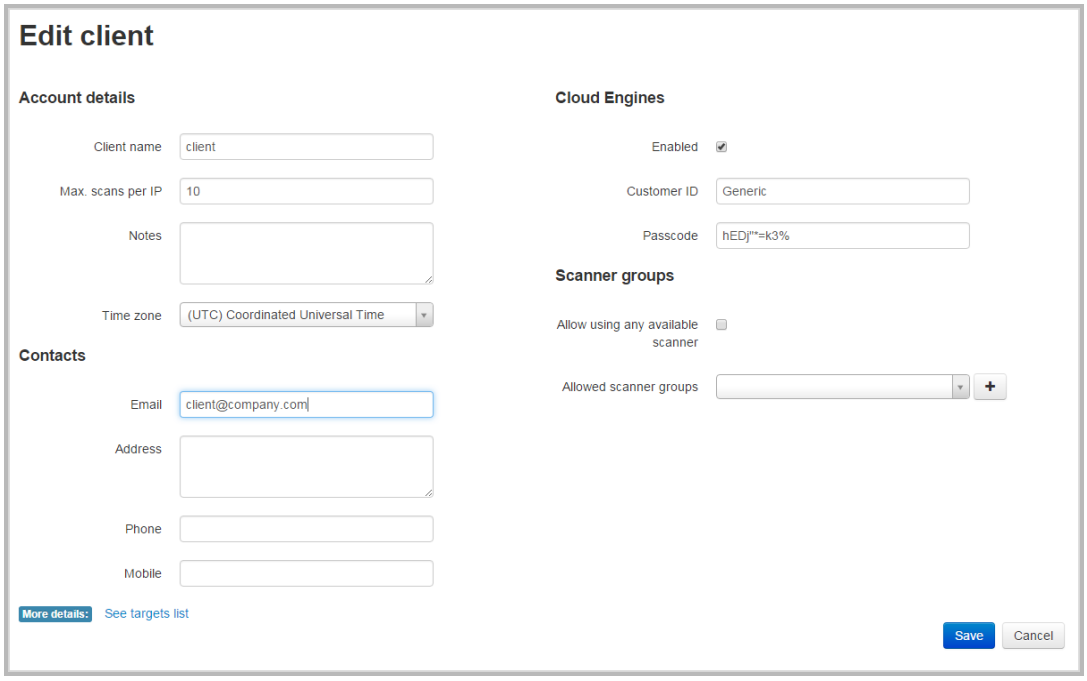
Add client page



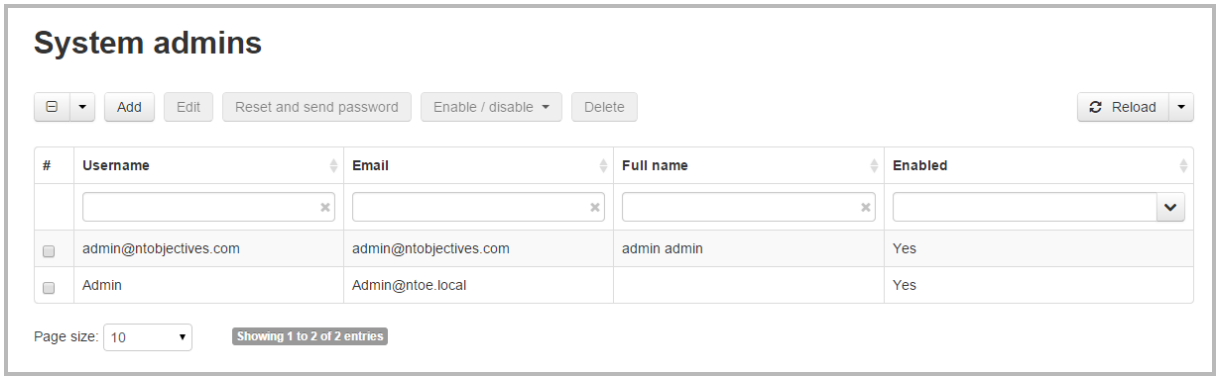
If you are a system admin, you can add a client by filling out the fields on the *Add client* page and clicking the **Save** button. The mandatory fields to create a client are **Client name** and **Email**.

Edit client page

If you are a system admin, the *Edit client* page allows you to edit information for an existing client. The fields on this page are the same as those on the *Add client* page.

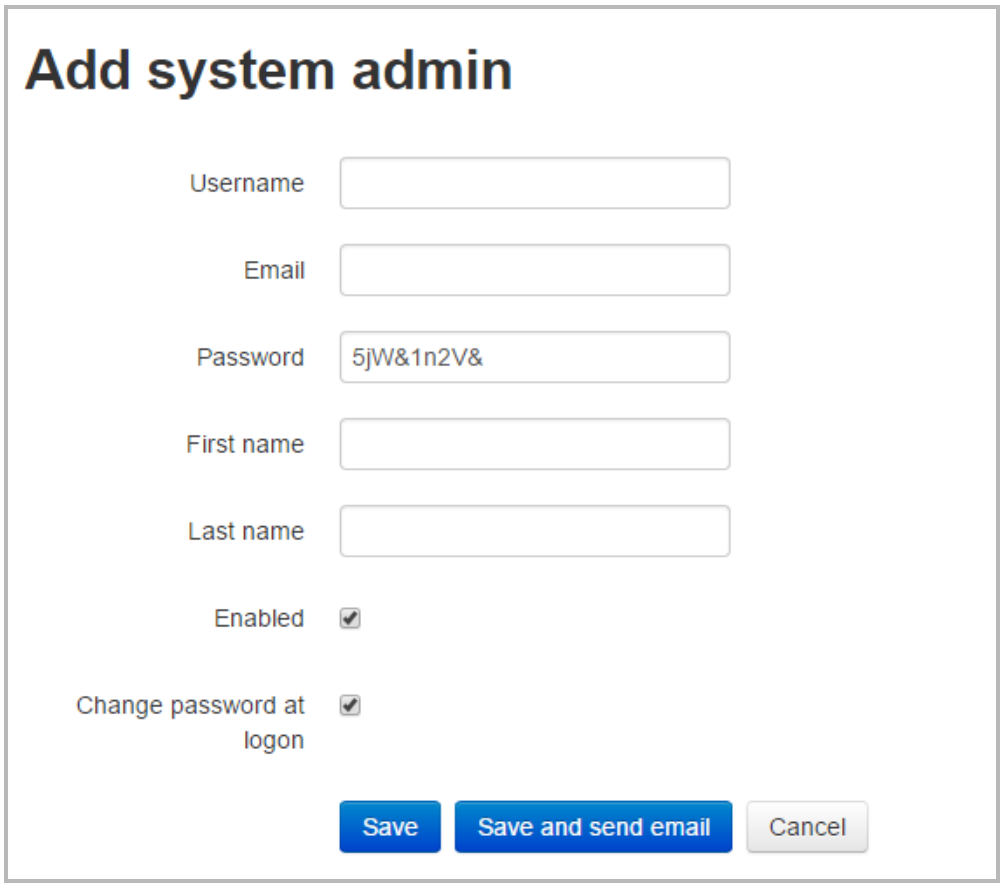


System Admin Accounts



On the *System admins* page is a listing of all system admins. you can **Add**, **Edit**, **Reset and send password**, **Enable / disable**, or **Delete** a system admin account.

Add system admin account



From this page, you can add a new system admin. The **Username** and **Email** fields are mandatory. The **Password** field is predefined and editable.

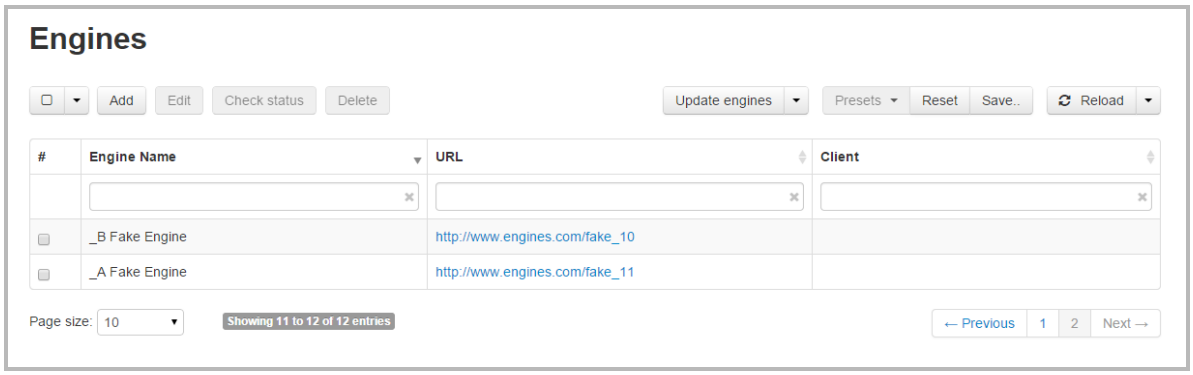
If you want the new user to be active and able to authenticate on the portal, check the **Enabled** box. Uncheck it if you would like to create an inactive user that will be unable to authenticate on the portal.

To force the new user to change password after first login, check the **Change password at logon** box.

Click the **Save** button to create the new system admin account. To create the new system admin account and send the user an email containing login credentials, click **Save and send email**.

Scan Engines

The *Engines* page lists and allows you to **Delete**, **Add**, **Edit**, or **Check Status** of the scan engines.

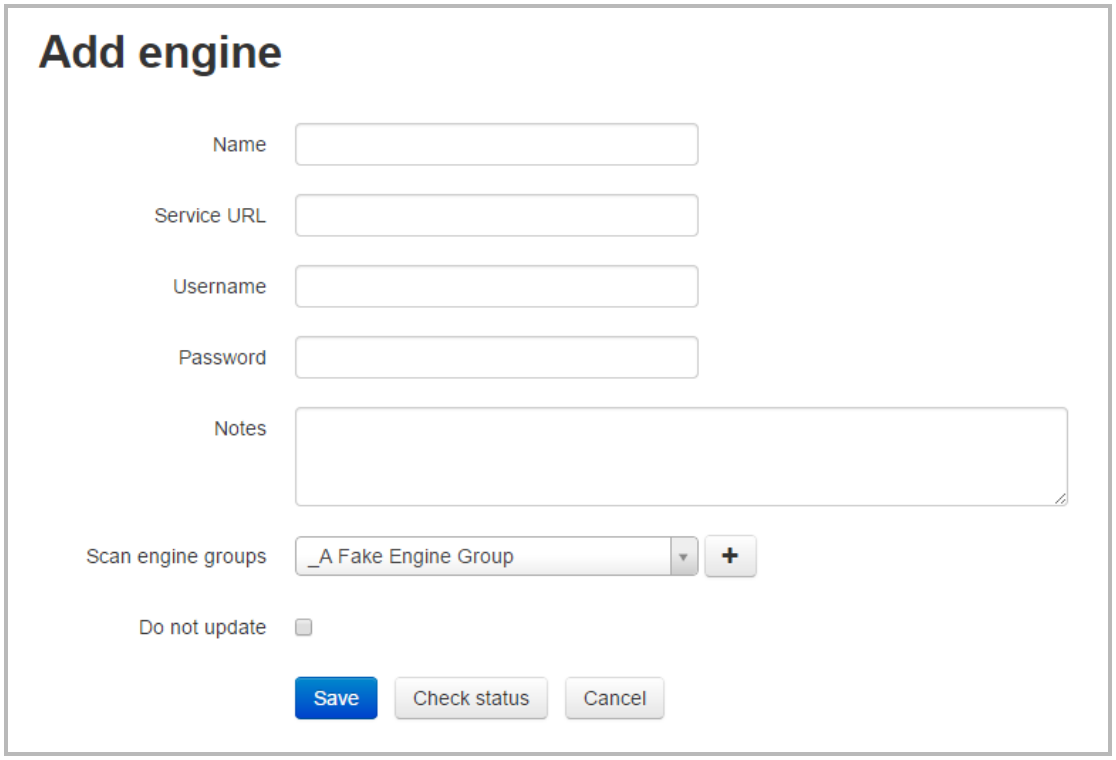


Click the **Update engines** button to update all scan engines. The drop down arrow next to **Update engines** opens a menu with the **See history** option, which leads to the Updates history page, and the option to **Cancel upgrade** for an engine.

Click **Reload** to refresh the page. The drop down arrow next to the **Reload** button allows you to **Enable auto reload** for the page.

Add or edit scan engines

To add a scan engine, use the **Add** button on the *Engines* page.



To add an engine, complete the fields on this page. The **Name**, **Service URL**, **Username**, and **Password** fields are mandatory.

Check the **Do not update** box if you do not want the scan engine to be updated.

When you are finished, click the **Save** button to create the new engine.

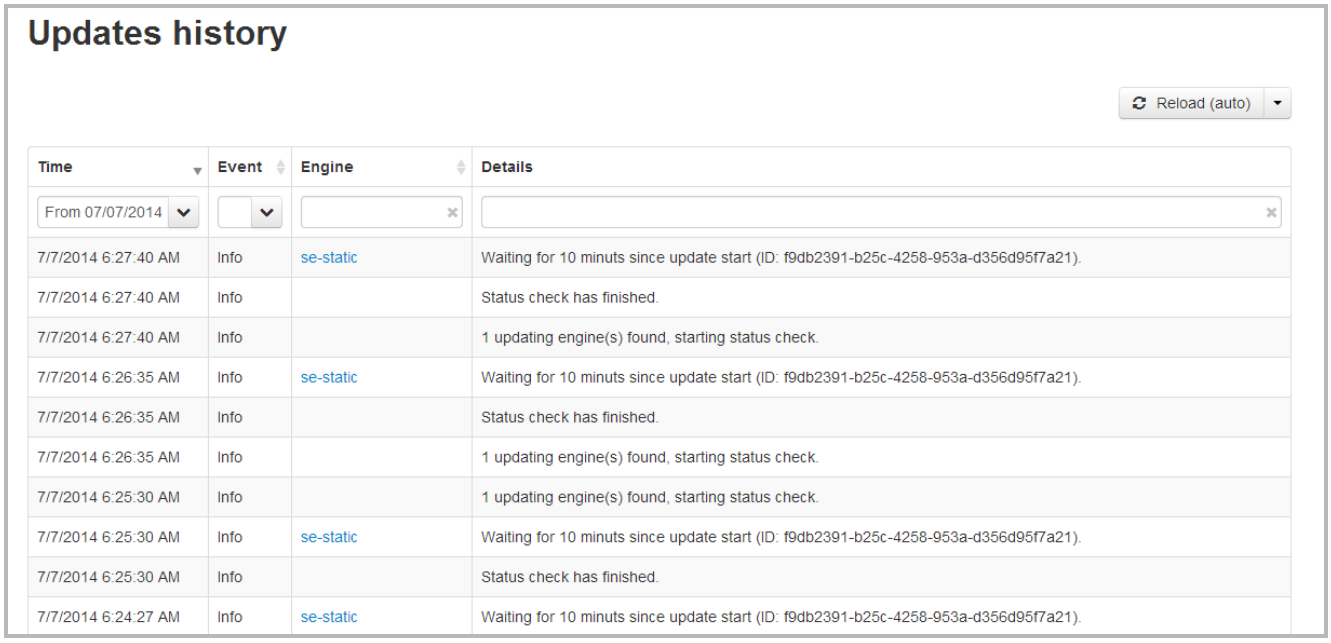
The **Check status** button can be used if all the required fields are filled out and checks the scan engines.

To edit a scan engine, click the **Edit** button on the *Engines* page. The fields on this page will be the same as the ones on the *Add engine* page.

Update engine

Click the **Update engines** button to access the *Select installer* popup window. Select the file for the AppSpider installer.You will see the name of the installer as well as a status bar. When the import is complete, the popup window will close.

On the *Updates history* page, you can monitor updates for your engines.



You can use any of the columns to filter the display order.

Click **Reload** to refresh the page. The drop down arrow next to the **Reload** button allows you to **Enable auto reload** for the page.

Scan Engine Groups

On this page, you can view a listing of and **Add**, **Edit**, or **Delete** scan engine groups.

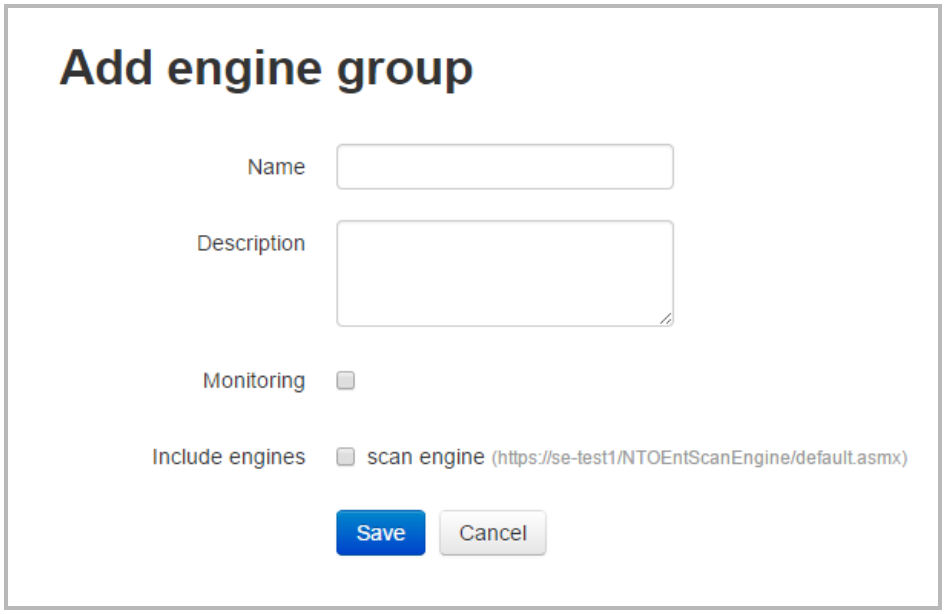
Action buttons:

- **Add** - creates a new scan engine group
- **Edit** - edits an existing scan engine group
- **Delete** - removes an existing scan engine group

Click **Reload** to refresh the page. The drop down arrow next to the **Reload** button allows you to **Enable auto reload** for the page.

Add Scan Engine group

Click the **Add** button on the *Engine groups* page to access the *Add engine group* page.

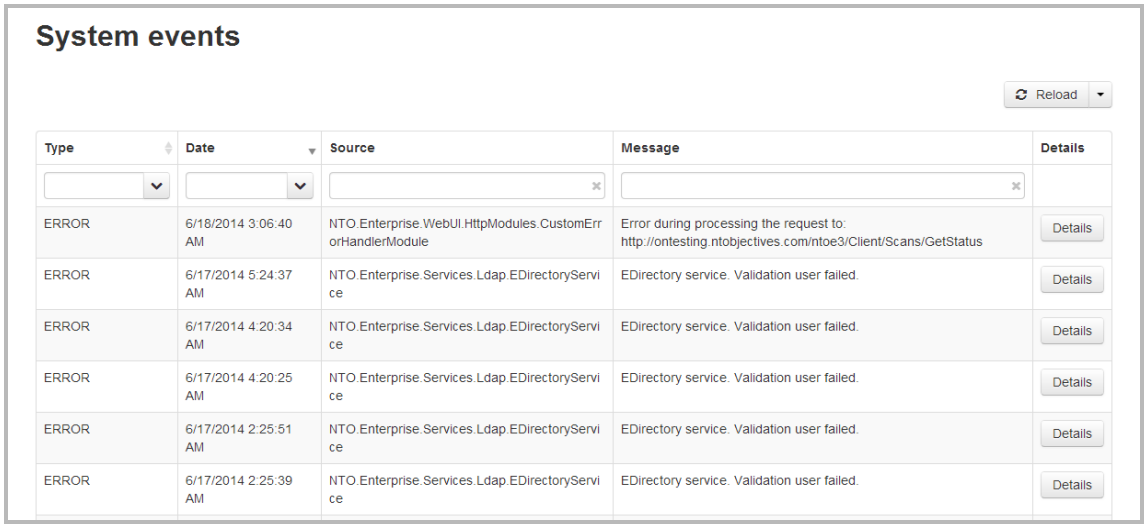


Complete the **Name** and **Description** fields with the appropriate information. Check the **Monitoring** box to enable monitoring status for a group.Then, check the box for the scan engines you would like to include in the group. Click the **Save** button to create the new group.

Click the **Edit** button on the *Engine groups* page to access the *Edit engine group* page. It has the same fields as the *Add engine group* page does.

System events

This page contains a table that lists system events.

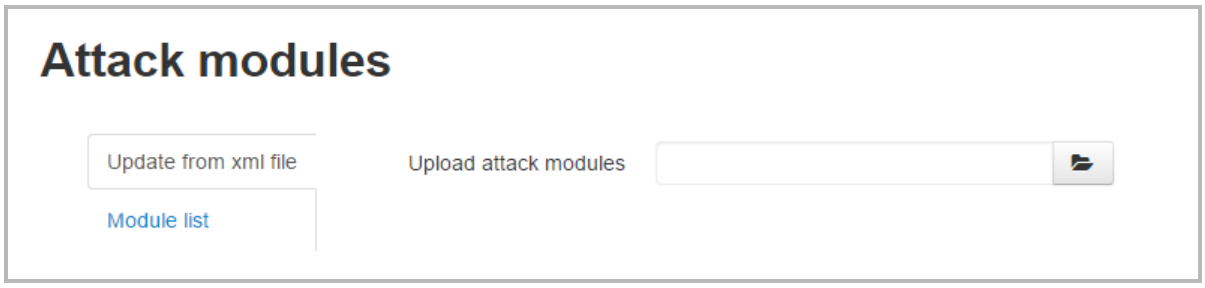


To view the *Event details* page for an event, click the **Details** button.

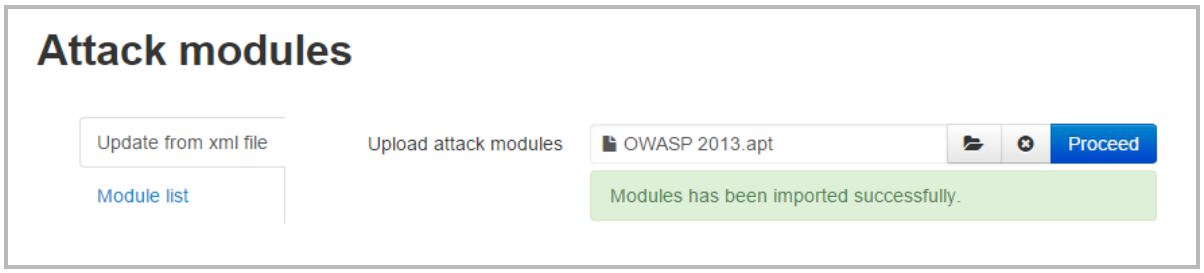
Click **Reload** to refresh the page. The drop down arrow next to the **Reload** button allows you to **Enable auto reload** for the page.

Attack modules

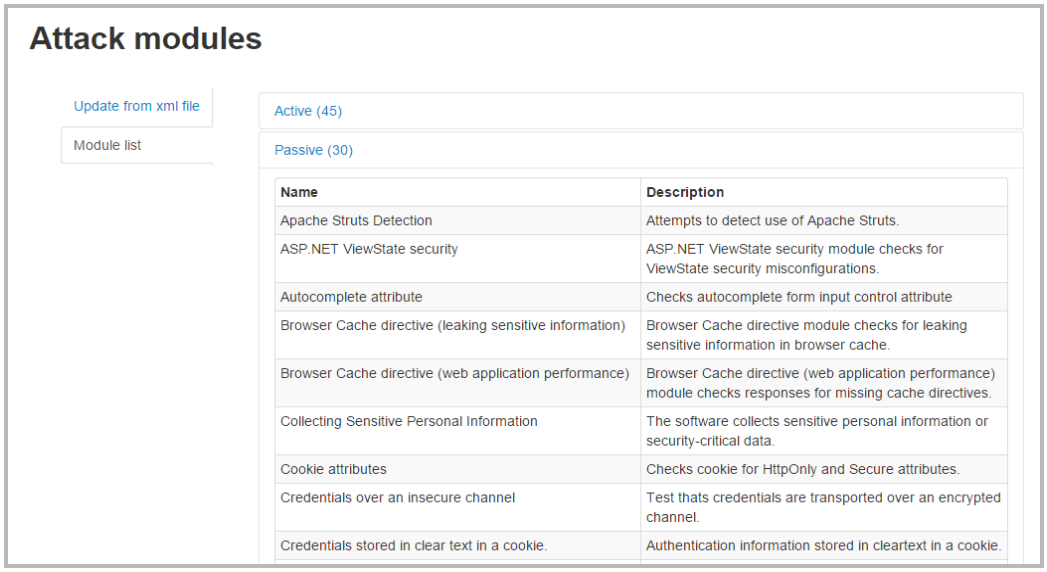
The *Attack modules* page is where you import attack modules to the portal. Use the **Upload attack modules** field to import .apt files that have been exported from AppSpider.



Select the attack policy file to uploads the file to the web portal.



The list of available attack modules is divided into Active and Passive attacks and presented under the upload field:



Security

Authentication / authorization

The application requires authentication. A non-authenticated user is redirected to the login page if any portal page is requested. Unauthenticated requests are allowed to validation applet files: validate.jar and launch.jnlp (workaround for JVM cookies issues).

If a user is authenticated but not authorized to access a page, a 403 error is shown.

Roles

System admins pages and menu items are always visible if a user is a system admin (no matter if impersonated or not). Impersonated system admins always have all roles.

Client account pages are visible only for impersonated system admins and client accounts.

Pages visible for non-system-admin roles require current client (client account or impersonated system admin).

The following tables list permissions and the user roles associated with them:

- Sys admin (SA)
- Client admin (CA)
- Blackout viewer (BV)
- Blackout manager (BM)
- Config manager (CM)
- Report assigner (RA)
- Report viewer (RV)
- Report manager (RM)
- Scan runner (SR)
- Vunerabilities manager (VM)
- Vulnerabilities viewer (VV)
- WAF manager (WM)

System permissions

Permission	SA	CA	BV	BM	CM	RA	RV	RM	RR	SR	VV	VM	WM
System	x												
Clients	x												
System admins	x												
Engines													
Engine groups													
Targets													
System events													
Attack modules													

Administration permissions

Permission	SA	CA	BV	BM	CM	RA	RV	RM	RR	SR	VV	VM	WM
Accounts	x	x											
All accounts	x												
Groups	x	x											
All groups	x												
Targets	x												
Notifications	x	x											
Integration	x	x											
Targets	x	x											
Target Groups	x	x											
Organization profile	x	x											

Scanning permissions

Permission	SA	CA	BV	BM	CM	RA	RV	RM	RR	SR	VV	VM	WM
Scanning	x	x	x	x	x	x	x	x	x	x	x	x	x
Scan configs	x				x					x			
Add/edit buttons	x	x			x								
Add/edit page	x				x								
Save and run	x									x			
Bulk add page	x				x								
Import as XML	x	x			x								
Copy	x	x			x								
Save as	x	x			x								
Delete	x	x			x								

Permission	SA	CA	BV	BM	CM	RA	RV	RM	RR	SR	VV	VM	WM
Monitoring turn on/off					x								
Run										x			
Schedule										x			
View scans						x	x	x	x	x			
Attack policy					x								
Blackouts	x		x	x									
Add/edit blackouts				x									
Delete blackouts				x									
All scans	x												
Scans	x					x	x	x	x	x	x		x
View/download reports	x						x						
View/download logs	x						x						
Approve	x								x				
Delete	x							x					
Status	x									x			
Pause, Resume	x									x			
Stop	x									x			
Assign	x					x							
Update scan	x							x					
Update report	x							x		x			
Defend button	x												x
Scheduled scans	x									x			
Add/edit scheduled scans	x									x			
Delete scheduled scans	x									x			
Defend scans	x												x

Vulnerabilities permissions

Permission	SA	CA	BV	BM	CM	RA	RV	RM	RR	SR	VV	VM	WM
Vulnerabilities	x										x	x	
Vulns summary	x										x	x	
All discovered vulns	x												
Discovered vulns	x										x	x	
Change status	x											x	

Permission	SA	CA	BV	BM	CM	RA	RV	RM	RR	SR	VV	VM	WM
Vulnerability details/ edit/delete	x										x	x	
Discovery chart	x	x									x	x	
Trending chart	x	x									x	x	
Charts	x	x									x	x	

Profile, change client, and dashboards permissions

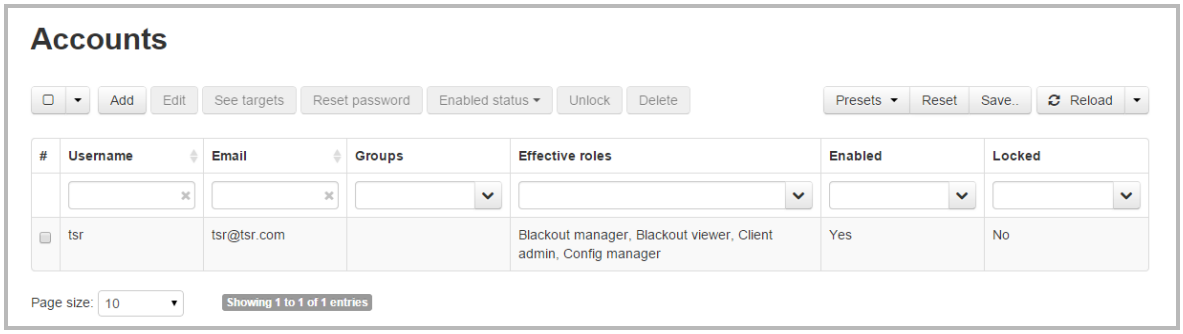
Permission	SA	CA	BV	BM	CM	RA	RV	RM	RR	SR	VV	VM	WM
Pofile	x	x	x	x	x	x	x	x	x	x	x	x	x
Change client	x												
Dashboards													
System admin dashboard	x												
Assigned scans	x									x			
Client admin dashboard	x				x								
Assigned scans	x	x			x								
Client account dashboard		x	x	x	x	x	x	x	x	x	x	x	x
Accounts/groups summary		x											
Blackouts summary			x	x									
Configs summary					x								
Active vulns											x	x	
Trending											x	x	
Active scans						x	x	x	x	x			x
Recently completed scans						x	x	x	x	x			x
Recently discovered vulns											x	x	

Administration menu

This menu provides access to several administrative operations.

Accounts

The *Accounts* page displays the list of accounts for the current client.

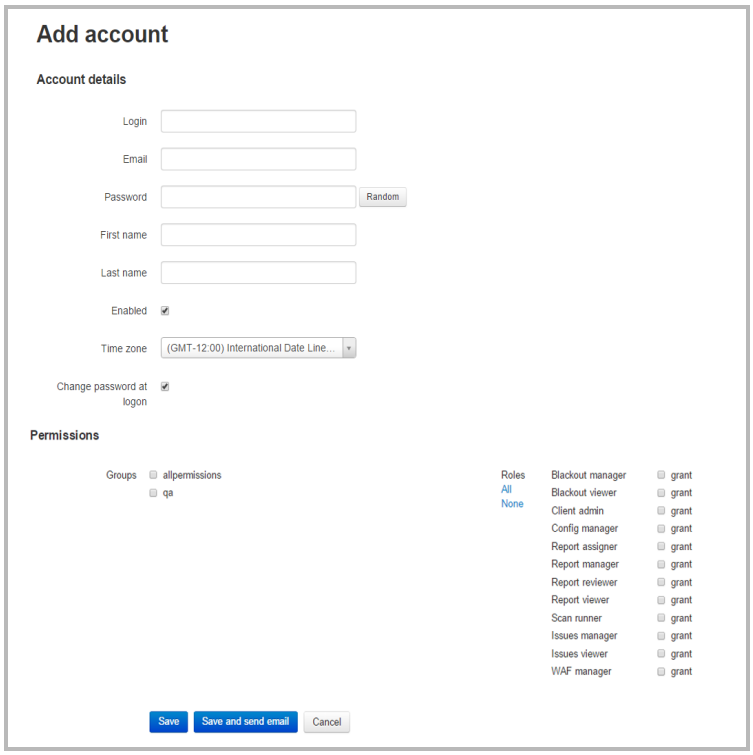


On this page, you can **Add**, **Edit**, **Unlock**, or **Delete** an account. You can also **See targets**, **Reset Password**, or **Enabled status** for an account.

Click **Reload** to refresh the page. The drop down arrow next to the **Reload** button allows you to **Enable auto reload** for the page.

Add account

To access the *Add account* page, click the **Add** button on the *Accounts* page.



In order to add an account, you must fill out the **Login**, **Email**, and **Password** fields. You can use the **Random** button next to the **Password** field to auto-generate a password.

If you want the new user to be active and able to authenticate on the portal, check the **Enabled** box. Uncheck it if you would like to create an inactive user that will be unable to authenticate on the portal.

To force the new user to change password after first login, check the **Change password at logon** box.

The **Time zone** drop down contains all Time zones. The client's time zone is predefined.

Check the box next to any group whose permissions you would like to add to the new account.

Check the box next to the role whose permissions you would like to add to the new account.

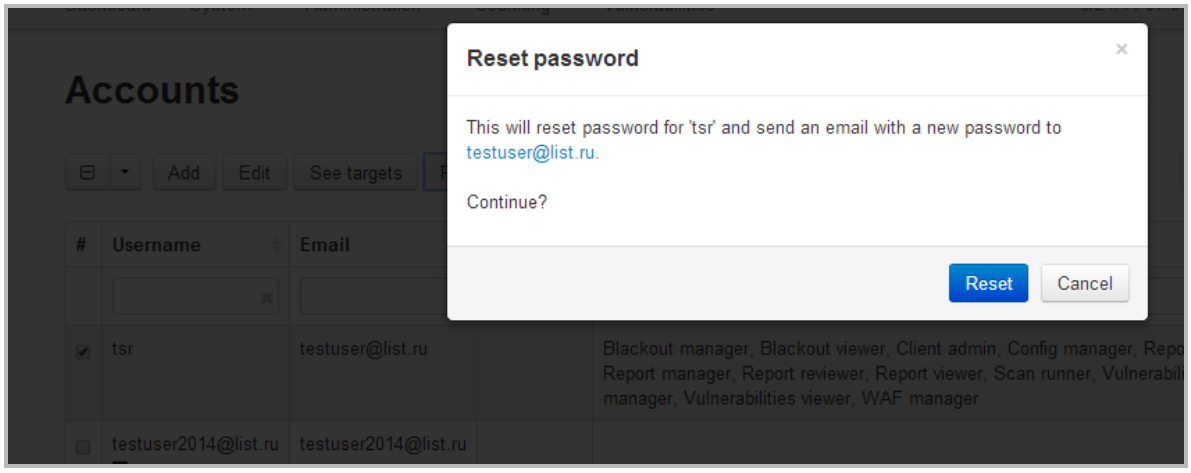
Click the **Save** button to create the new system admin account. To create the new system admin account and send the user an email containing login credentials, click **Save and send email**.

Edit account

To access the *Edit account* page, click the **Edit** button on the *Accounts* page. The details and fields on that page are the same as on the *Add account* page.

Reset Password

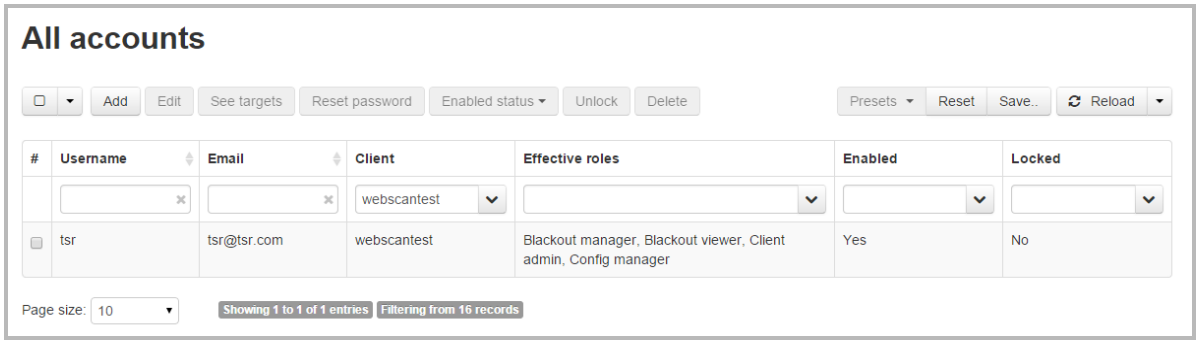
On the *Accounts* page,click the **Reset password** button after selecting the account(s) whose password(s) you would like to reset.



You will see a confirmation popup. Click the **Reset** button to confirm the password reset. A message with login details will be sent to the user(s).

All accounts (SA)

The *All accounts* page displays a list of all clients. It displays and functions the same as the *Accounts* page.



Groups

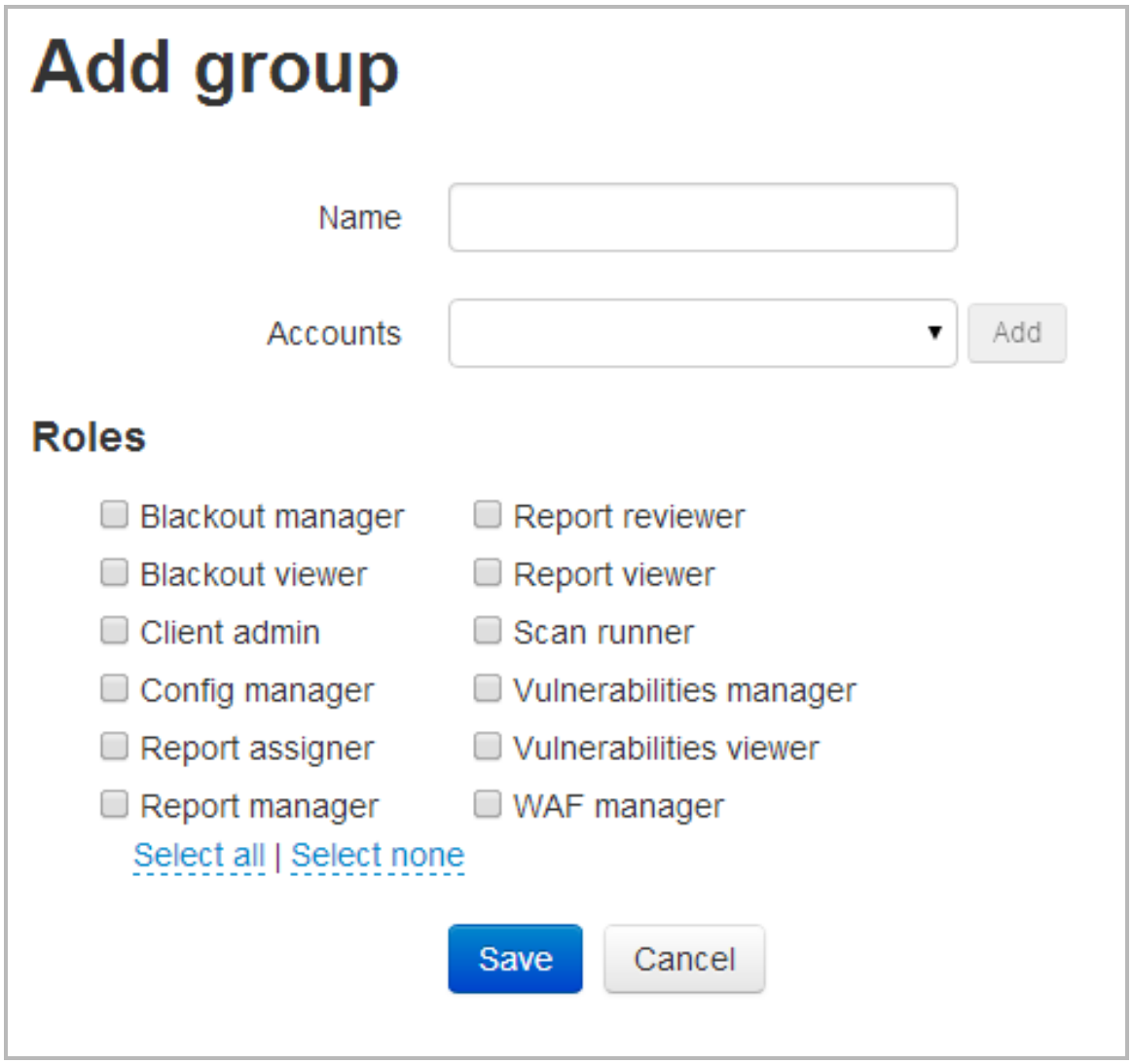
This page displays the list of groups for the current client.

You can **Add**, **Edit**, or **Delete** groups on this page.

Click **Reload** to refresh the page. The drop down arrow next to the **Reload** button allows you to **Enable auto reload** for the page.

Add or edit group

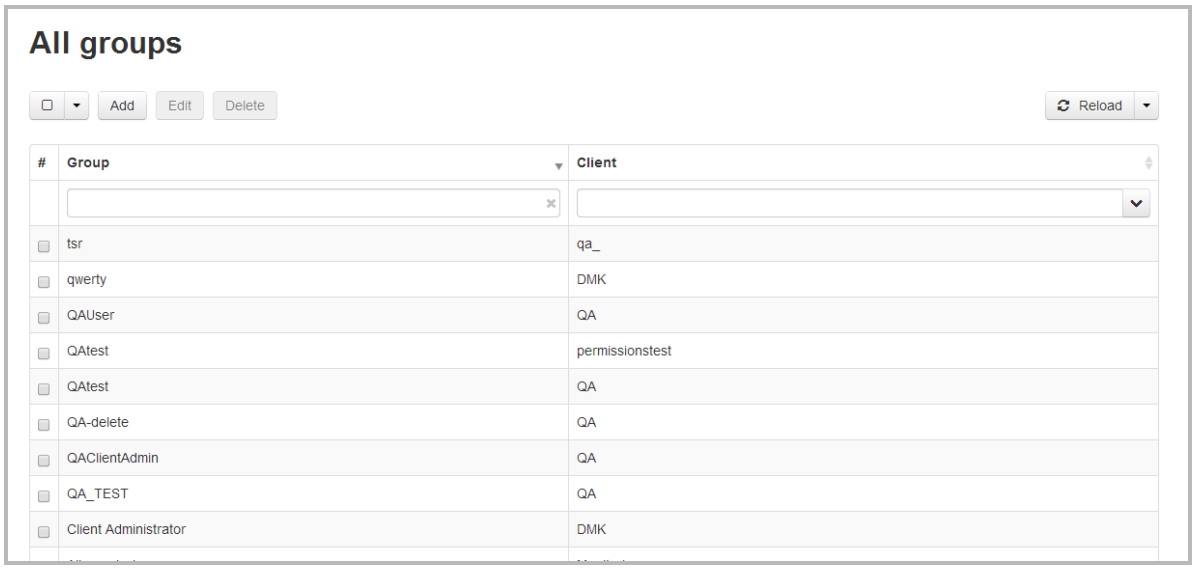
This is the page that allows users to add and edit groups.



Add or edit the **Name** for the group. Then select the account(s) you want from the **Accounts** drop down menu and click the **Add** button to include them in the group. To add or remove permissions for a group, check or uncheck the boxes next to the listed *Roles*. When you are finished making changes, click the **Save** button.

All groups

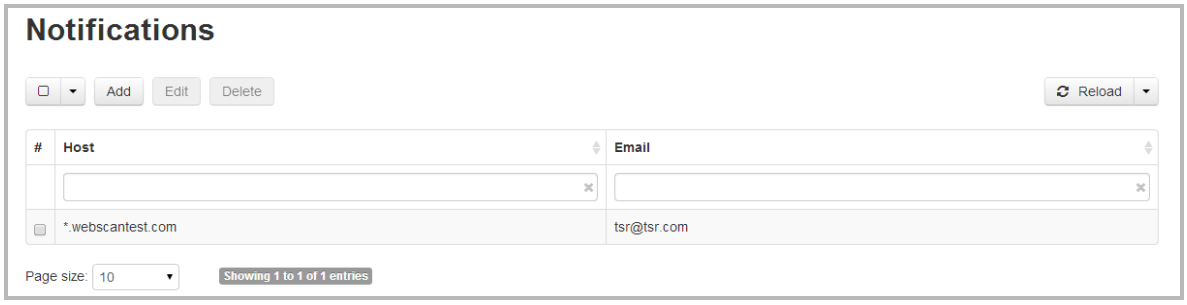
The *All groups* page is only accessible to system admins. It allows system admins to **Add**, **Edit** or **Delete** any client's group.



This page displays and functions the same as the *Groups* page, with one additional option: sorting groups by client.

Notifications

The *Notifications* page displays notifications of the current client. A notification is an email that is sent to an email address when a scan against the selected host is started. Each client has its own set of notifications.



You can **Add**, **Edit**, or **Delete** notifications on this page.

Click **Reload** to refresh the page. The drop down arrow next to the **Reload** button allows you to **Enable auto reload** for the page.

Targets based security

Action buttons will be disabled for blackouts targets that are not approved for the current user. If the target is not allowed, the blackout won't be created. Instead, an error message will appear.

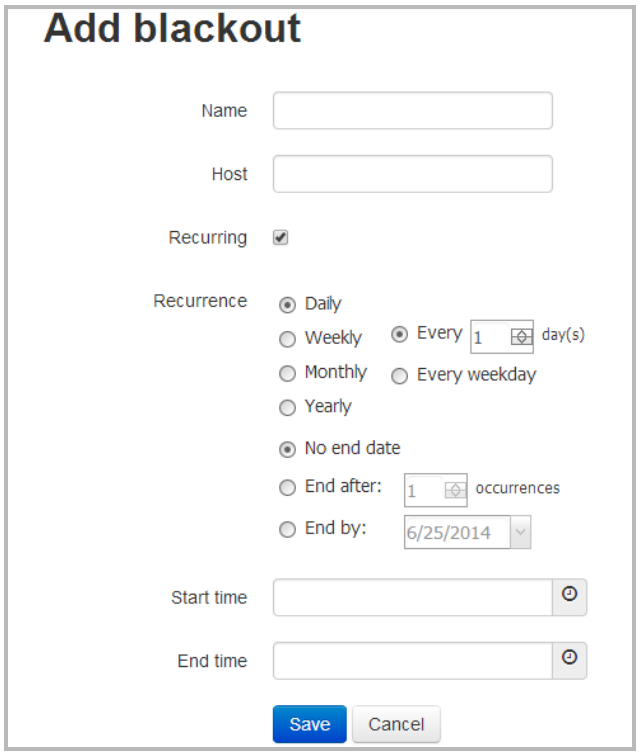
The impersonated system admin can create any blackout. If a blackout is created for a nonexistent target, the target will be created in theAll targets page and auto assigned to the current client with pending status if the target does not exist or is not approved for the client, or approved status if the target is approved for the client.

The client admin has all targets approved for the current client. Other accounts must have targets explicitly approved for them. If blackouts are created for nonexistent targets, the targets will be created. If the target is not attached to the client and the account, it will be assigned pending status.

Wildcard targets are processed: approved * means all targets are approved, approved *.com means all targets in .com domain zone are approved, and so on.

Add Blackout

This page allows users to add and edit blackout rules.



All fields are mandatory.

The **Host** field should be a host without protocol. IPs are also valid. Asterisk (*) is supported only at the beginning of the field (*, *.host.com, *host.com).

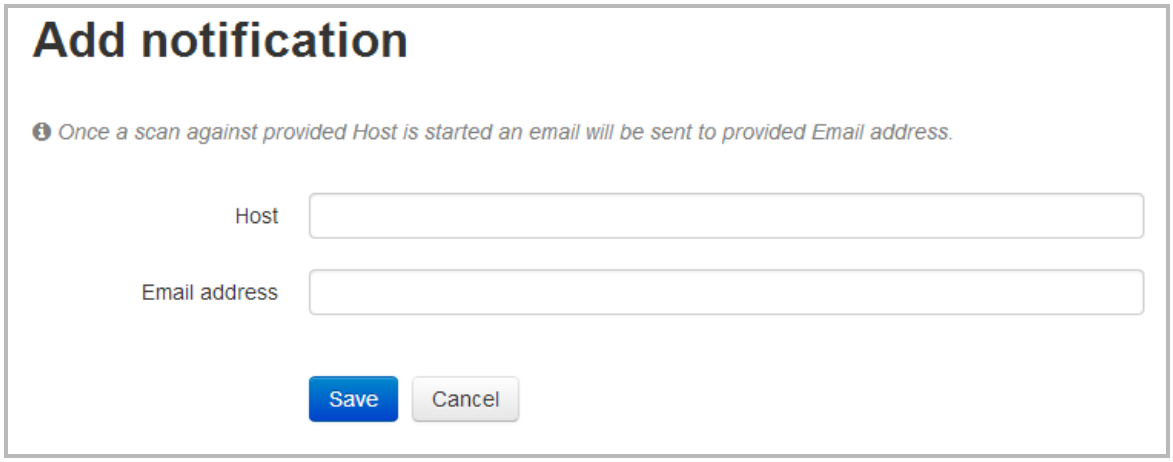
For a non-recurrent blackout, add a **Start/end date** and **time**. For a recurrent blackout, add a **time** only. The blackout will occur between the start and end time.

Check **Recurring** if you want the blackout to repeat.

Click the **Save** button to create the blackout.

Add notification

Use this page to create email notifications. Notifications will be sent to the indicated email address when every scan against the indicated host is executed, started, or completed.



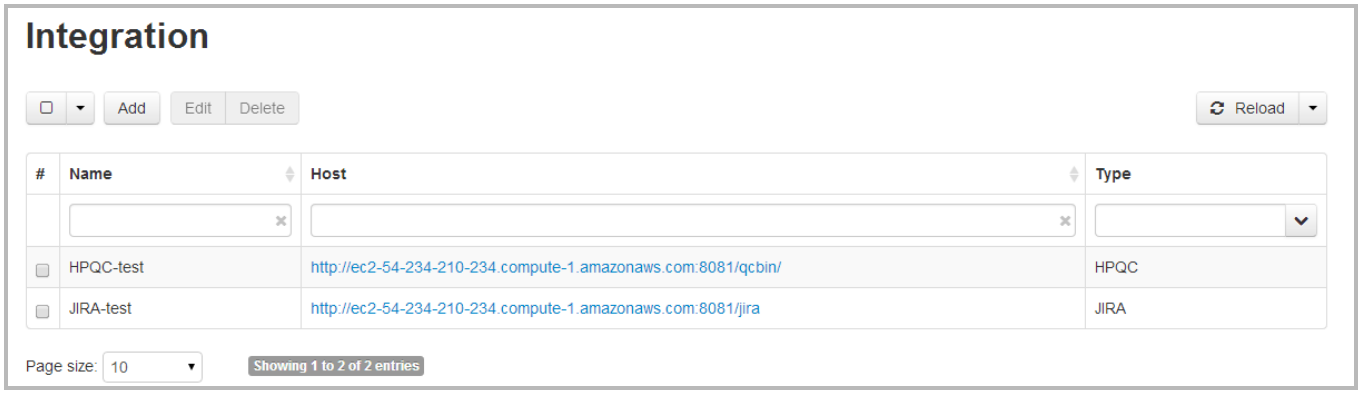
After adding the **Host** name and **Email address**, click the **Save** button to activate the notification.

Edit notification

You can edit a notification that has already been created here. The *Edit notification* page has the same fields as the *Add notification* page.

Integration

On this page, you can manage integration services such as Jira and HP Quality Center.

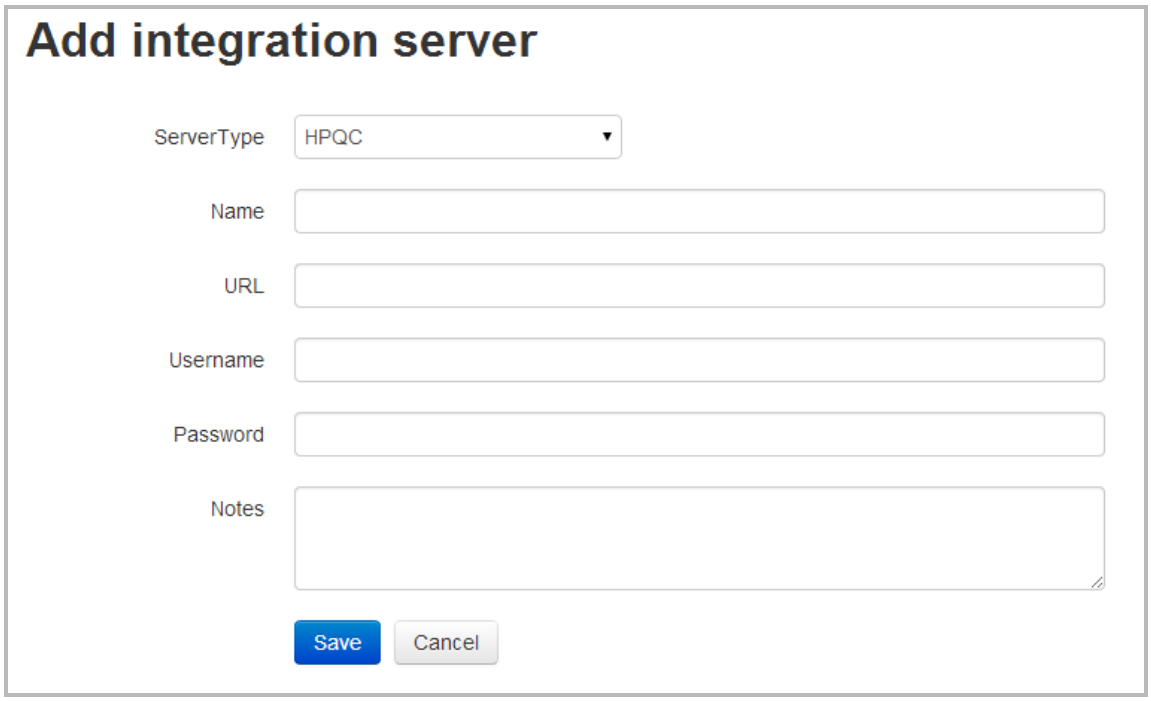


The buttons allows you to **Delete**, **Add**, or **Edit** integration engines.

Click **Reload** to refresh the page. The drop down arrow next to the **Reload** button allows you to **Enable auto reload** for the page.

Add integration server

This page allows users to add or edit integration server information.



The **ServerType** drop down includes the JIRA or HPQC options. All fields are mandatory except for **Notes**. Click the **Save** button to create new server settings.

Targets

Targets security

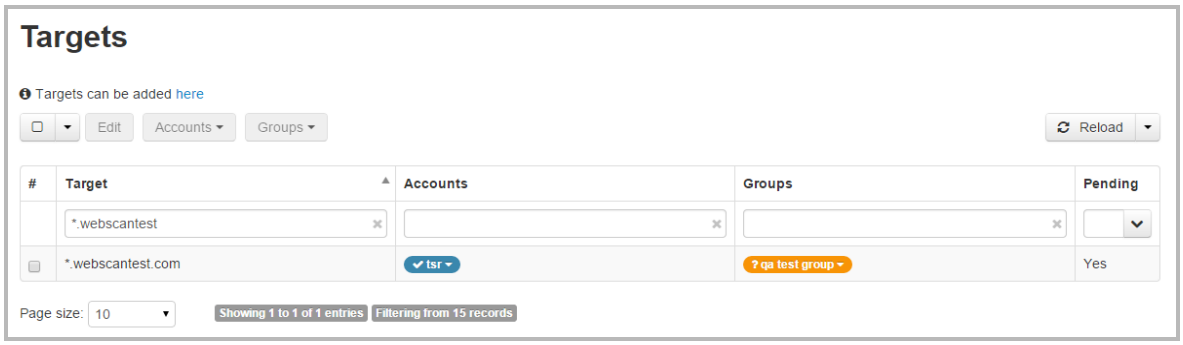
Globally, you may access data related to a target that you are approve to view. Targets may be approved at client and at the account/group level.

System admins have access to the *All targets* page.

Client admins have access to all approved client targets.

Other accounts have access to targets approved for their account or assigned groups. Accounts or groups can only be assigned targets that are approved for a client which owns that account or group.

Targets may start with an asterisk (*). There is also a special * target. Approving *.host.com means approving www.host.com, www2.host com, etc., while approving * means approving any target.



The table displays all targets assigned to the current client as well as *Account*, *Group*, and Target information (under *Pending*).

On this page, you can select a target then click the **Edit** button to make changes to it.

Click the **Accounts** button after selecting multiple targets to access the *Accounts approval menu*.

To access the groups approval menu, select one or more targets then click the **Groups** button.

Click the down arrow next to the **Accounts** or **Group** button to access each of their drop down menus. From there, you can:

Set pending approved to make all pending accounts / groups of all selected targets approved.

Set pending not approved to make all pending accounts / groups of all selected targets not approved.

Set all pending to make all accounts / groups of all selected targets pending.

Set all approved to make all accounts / groups of all selected targets approved.

Set all not approved to make all accounts / groups of all selected targets not approved.

If you are logged in as an impersonated system admin or client admin, you will see the **Targets can be added here option**, which leads to the *All targets* page.

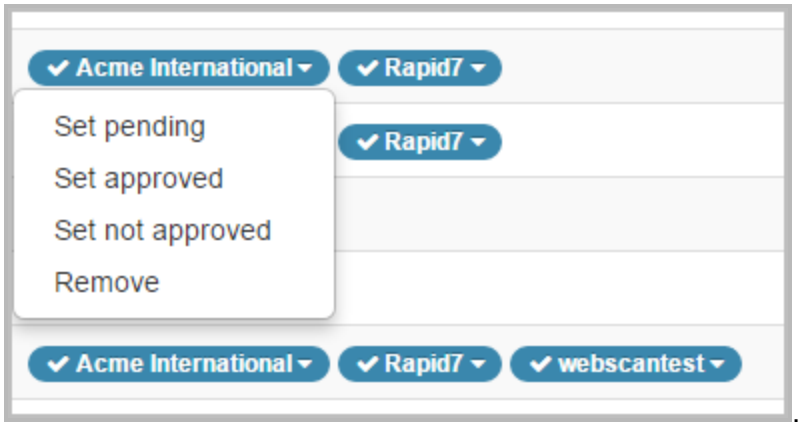
Click **Reload** to refresh the page. The drop down arrow next to the **Reload** button allows you to **Enable auto reload** for the page.

All targets

This page is only available to system admins and displays all targets in the system and the clients assigned to each target.

Use the **Add** button to add a target. Select a single target and click the **Edit** button to make changes to that target.

All clients are assigned to a target. Blue means the client is approved, red ones are not approved, and yellow targets are pending. Click on a client to access a drop down menu where you can change its individual status.



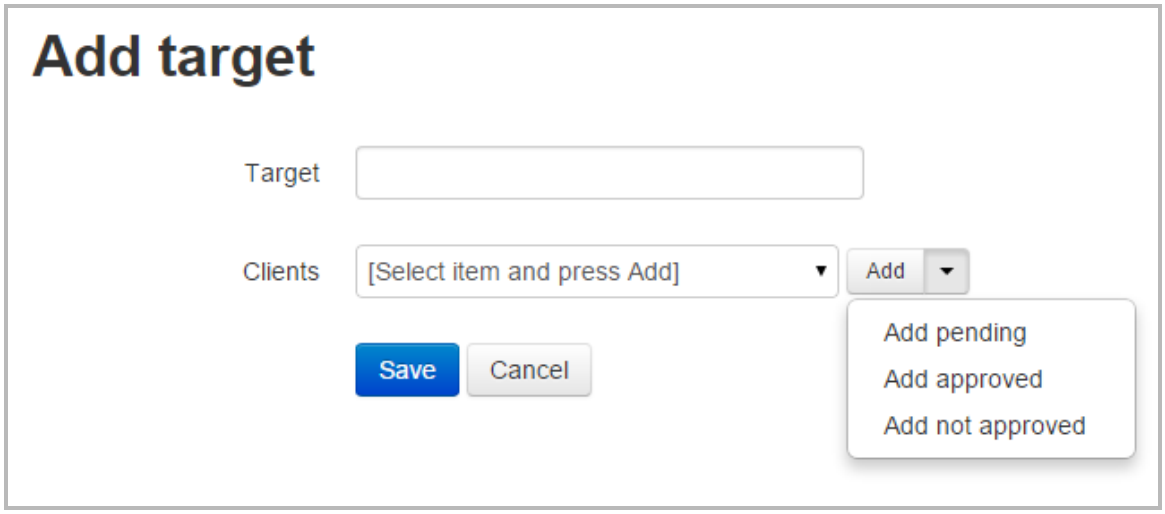
If you would like to make changes to the statuses of all clients attached to a particular target or targets, click the **Approval** button after selecting the desired targets to access a drop down of status change options. **Set pending approved** will make all pending clients of all selected targets approved. **Set pending not approved** will make all pending clients of all selected targets not approved. **Set all pending** will make all clients of all selected targets pending. **Set all approved**

will make all clients of all selected targets approved. **Set all not approved** will make all clients of all selected targets not approved.

The **Delete** button removes all related scans, configs, issues, blackouts and notifications.

Add target

This page allows the system admin to add a target.



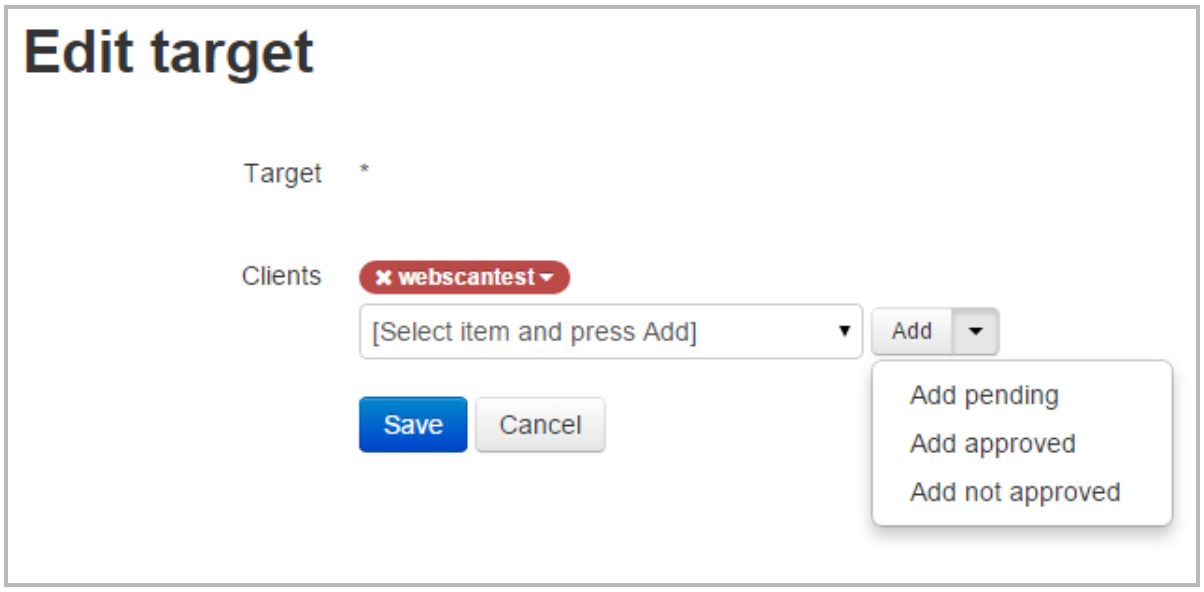
All fields are mandatory.

Add the name into the **Target** field. Then, select the desired client in the **Clients** drop down menu. If you click the **Add** button, the client will be added in pending status. If you want to add the client as approved or not approved rather than pending, use the arrow next to the **Add** button to access the drop down menu and select the desired option.

After adding all desired clients, click the **Save** button.

Edit target

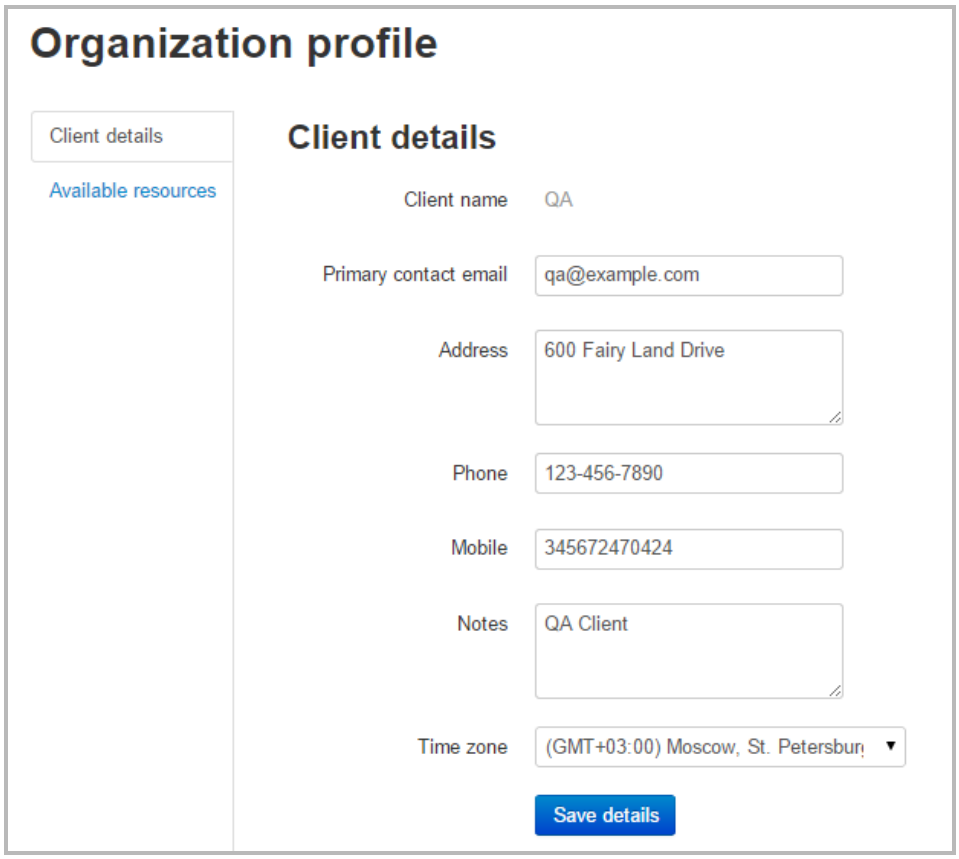
Use this page to edit a target.

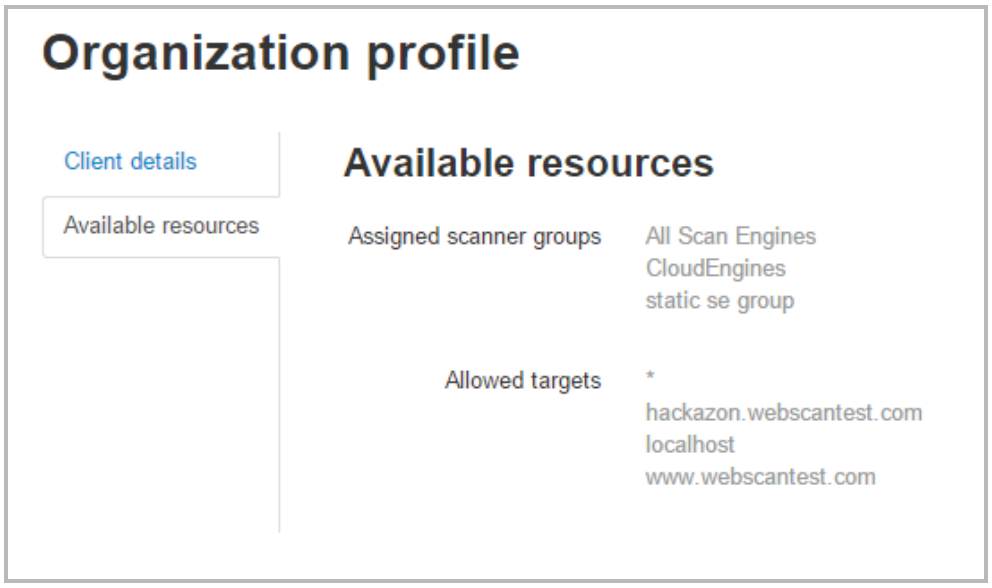


The *Edit target* page contains the same fields and options as the *Add target* page.

Organization profile

This page displays the profile of the organization.





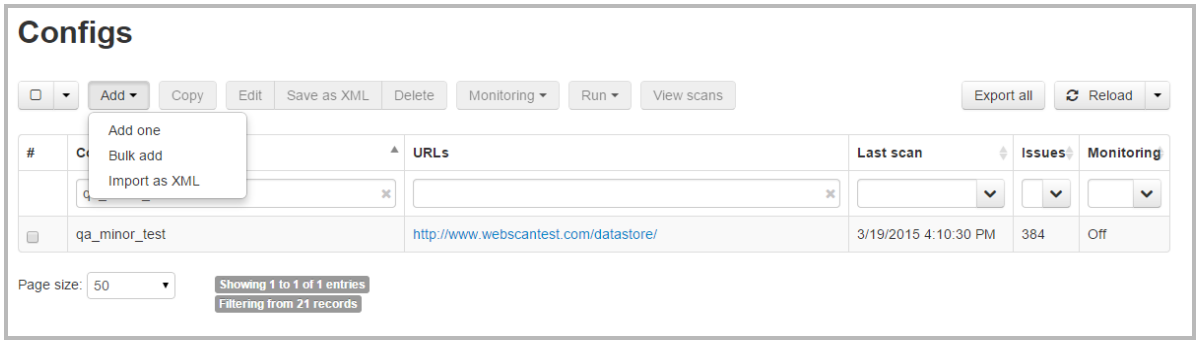
The page displays **Client details** information and *Available resources* data. **Client details** fields are editable, while *Available resources* displays a list of available scanner groups and allowed targets for the current client.

After making changes to **Client details**, click the **Save** button.

Scanning menu

Configs

The *Configs* page displays all scan configs for the current client.



The table includes information regarding the name of the config, the attacked *URL*, the start date/time of *Last scan*, a count of found *Issues* by the config, and whether or not *Monitoring* has been enabled.

Click the **Add** button to access its drop down menu. **Add one** opens the *Add config* page. **Bulk add** opens the *Bulk add* page. **Import as XML** opens the *Import as XML* page.

The **Copy** button copies any selected scan configs.

If you select a single scan config and click the**Edit** button, it will open the *Add config* page with config properties predefined.

If you select a single scan config and click the **Save as XML** button, it will export the config to an xml file.

The **Delete** button removes any selected scan configs.

Clicking the **Monitoring** button changes the *Monitoring* status for any selected scan configs.

To open the *Schedule/Run Scan* page, click the **Run/Schedule** button.

To open the *Scans for scan config* page, select a single scan config and click the **View scans** button.

Use the **Export all** button to export configs data to a CSV file (any selected filters are applied).

All columns are sortable and have search filters.

Click **Reload** to refresh the page. The drop down arrow next to the **Reload** button allows you to **Enable auto reload** for the page.

Targets-based security

If scanning is not approved for current user targets, the buttons will be greyed out to show that they have been disabled. An impersonated system admin will have all targets approved.

Target wildcards are supported.

Configs can be created with any URLs. The **Save and Run** feature for a config with URLs pointing to unapproved targets will save the config, redirect to the *Configs* page, and display a warning.

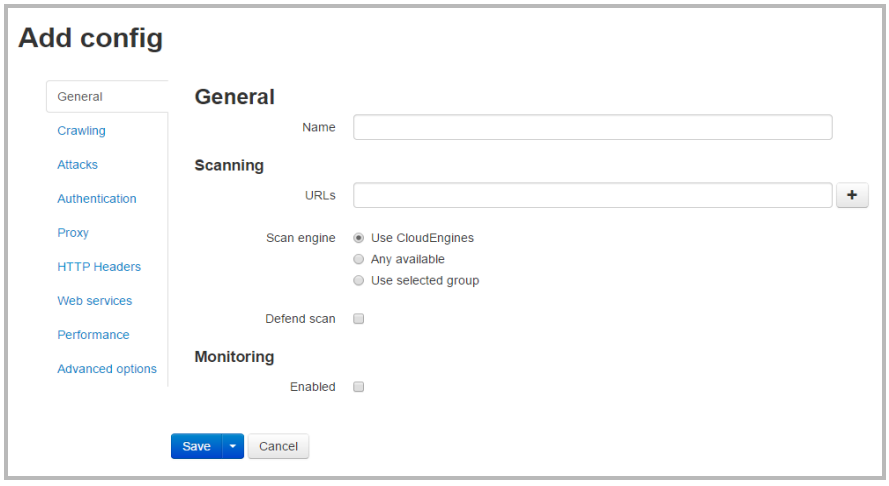
If a config is created that scans a non-existing target, the target will be created and will attach to the current client (i.e. the client account including the client admin) and account (i.e. all client accounts except the client admin) in pending state if the target does not exist or is not approved, or in approved state if the target exists and is approved.

Configs/Add one

Use this page to add simple scan configs for sites that are to be scanned.

To create a new scan config or update an existing config, click the **Save** button. The **Save and run** button creates/updates a scan config and runs a scan based on config settings.

The **General** tab, which displays the main config options.

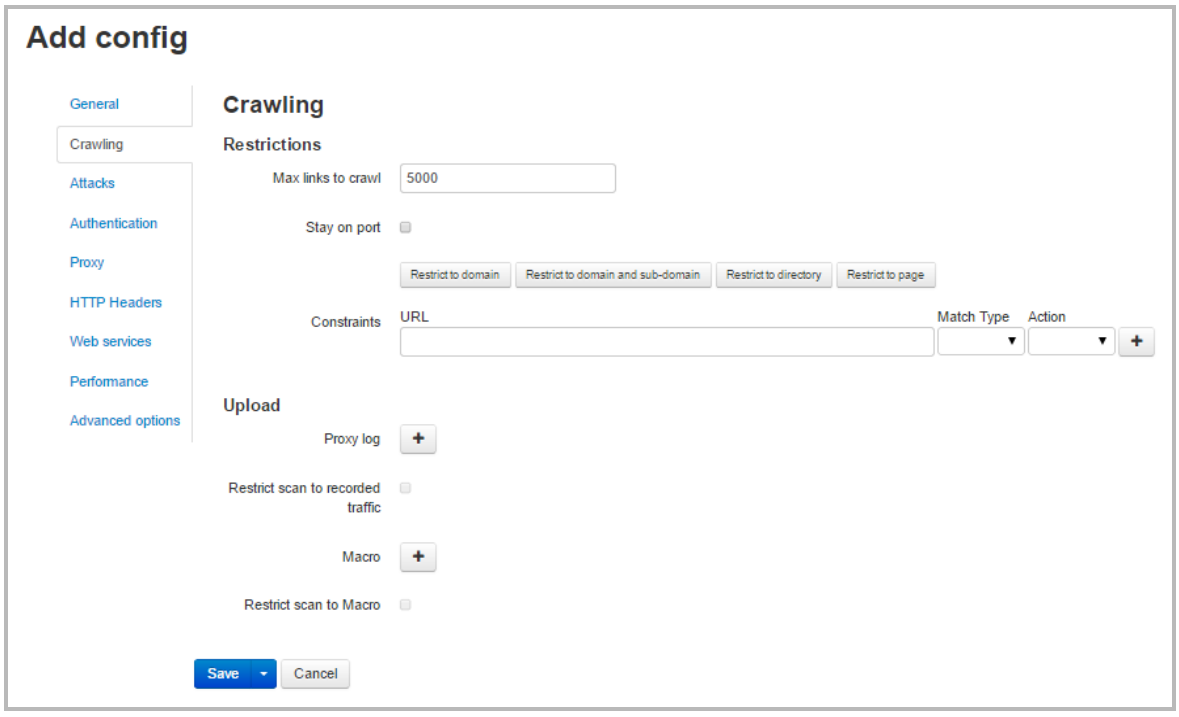


Give the config a **Name**. Then, in the *Scanning* section, complete the following fields.

- Add attacked **URLs**. Targets are added in accordance with the *Targets security schema*. Use the **plus-sign** button to add more than one **URL**.
- Select a **Scan engine**. Click on the **Use selected group** will generate a list of available groups.
- Check the **Defend scan** box to enable that option.

Checking the **Monitoring**box opens a menu for choosing further options, **Triggers scan** and **Delay**.

The *Crawling* tab



The *Restrictions* section offers the following options.

- A number of **Max links to crawl**. 5000 is the default.
- Check box to enable or disable **Stay on port**.
- Buttons to **Restrict to domain**, **Restrict to domain and sub-domains**, **Restrict to directory**, and/or **Restrict to page**.
- **Constraints URL** field with **Match Type** and **Action** lists. You can set URLs as Black or White list. To add a URL, type it into the field and click the plus-sign icon.

The *Upload* section offers the following options.

- The **Proxy log** button, which exports a proxy file from the web portal. To add a file, click the **Add** icon and select the file.
- The **Restrict to recorded traffic** check box.
- The **Macro** button, which exportsa macro file from the web portal. To add a file, click the **Add** icon and select the file.
- The **Restrict scan to Macro** check box.

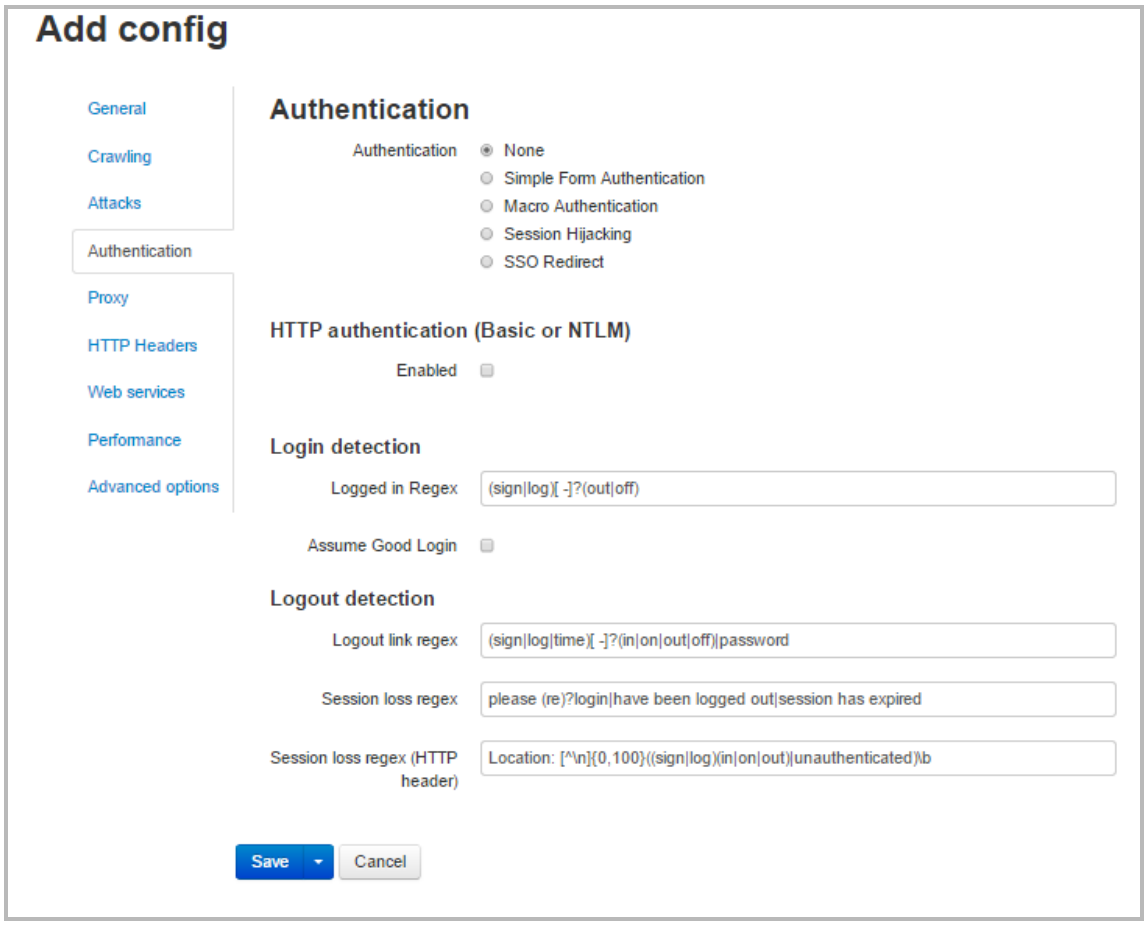
The *Upload* tab

Predefined policies is a drop down list with all your attack policy lists. **Crawl only** and **All modules** are predefined lists. If you do not use a predefined list, then select the attacks desired from the **Active** and **Passive attacks** lists.

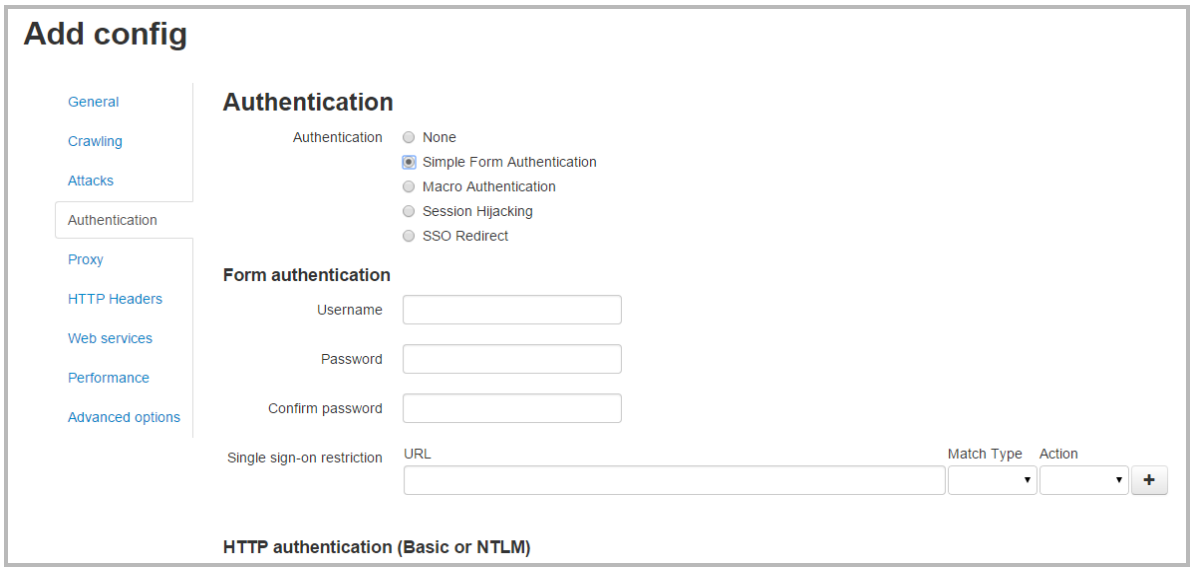
The *Authentication* tab

In the *Authentication* section, selecting different options under the first **Authentication** list will generate different options below it.

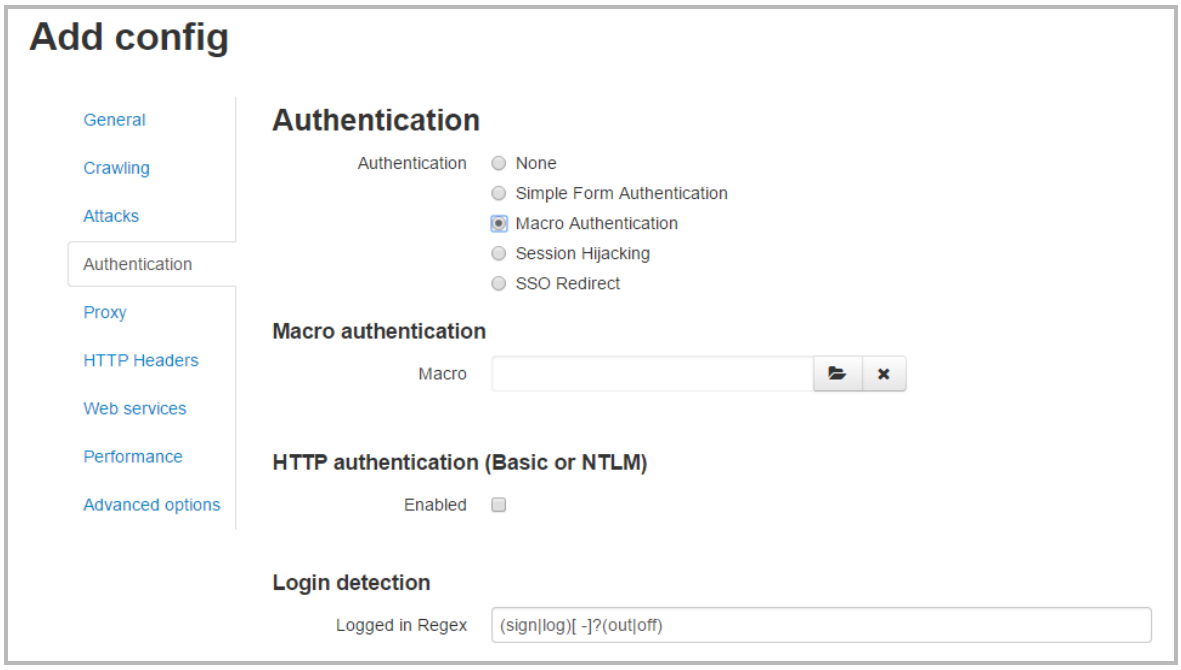
Selecting **None** will show **HTTP authentication**, **Login detection**, and **Logout detection** options.



Selecting **Simple Form Authentication** opens a Form authentication block with **Username**, **Password**, **Confirm password**, and **Single sign on link** options.



Selecting **Macro authentication** will generate a **Macro** field which can be used to export a macro file from the web portal.



Choosing **Session Hijacking** will enable that method.

Selecting **SSO Redirect** will allow initial redirect for SSO (no forms used).

Checking the **Enable** box presents the **HTTP authentication (Basic or NTLM)** option.

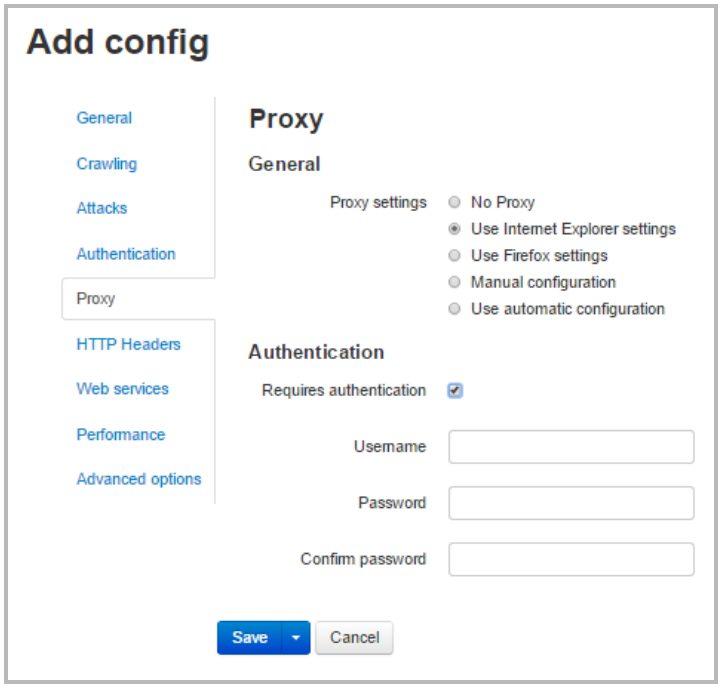
Login detection section:

- **Logged in Regex** - text field, predefined as (sign|log)[-]?(out|off)
- **Assume Good Login** checkbox

Logout detection section:

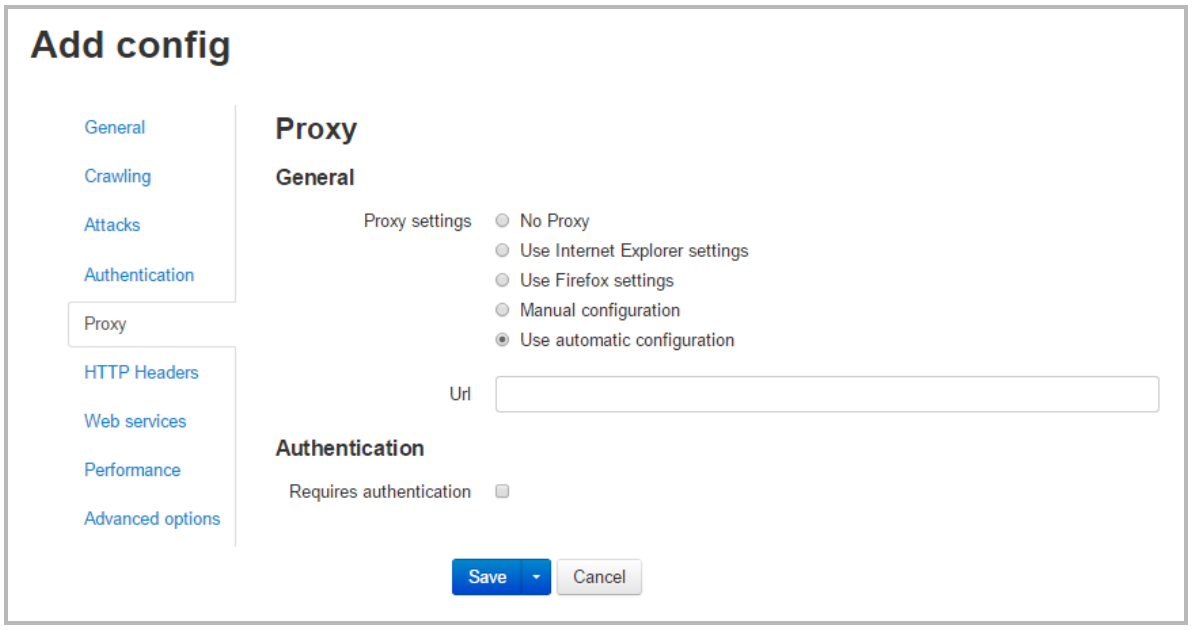
- **Logout link regex** - text field, predefined as *(sign|log|time)[-]?(in|on|out|off)|password*
- **Session loss regex** - text field, predefined as *please (re)?login|have been logged out|session has expired*
- **Session loss regex (HTTP header)** - text field, predefined as *Location: [^\n]{0,100} ((sign|log)(in|on|out)|unauthenticated)\b*

The *Proxy* tab displays the following options:



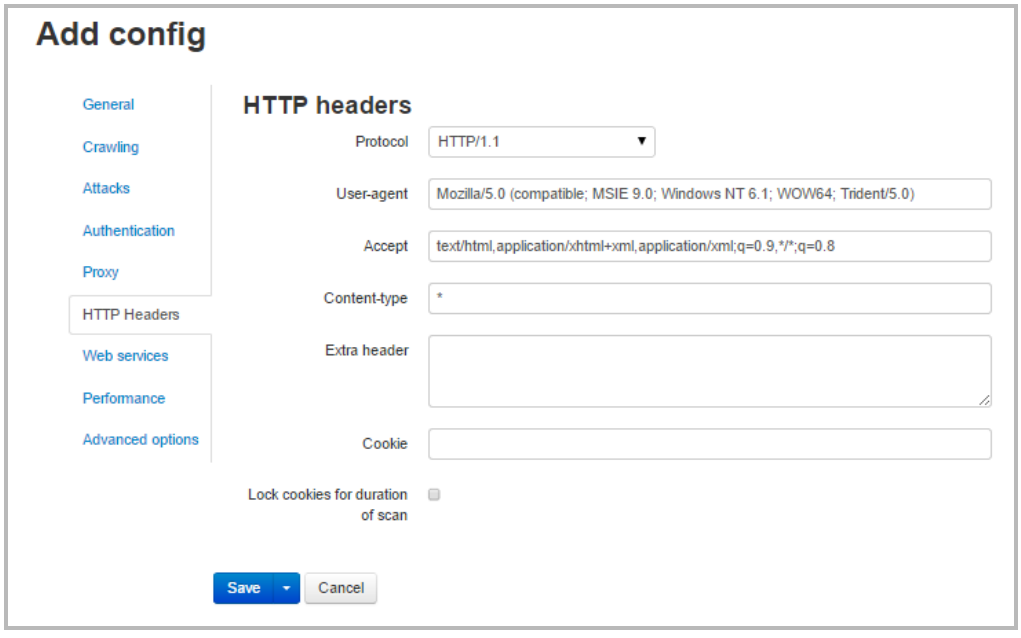
General proxy settings - chooses one proxy setting for the scan config:

- **No proxy**;
- **Use Internet Explorer settings**;
- **Use Firefox settings**;
- **Manual configuration** - opens HTTP and HTTPS fields for adding URLs and ports;
- **Automatic configuration** - opens URL field.



Enabled Requires authentication option, opens the form **Username**, **Password**, **Confirm password** fields presented.

The *HTTP headers* tab displays the following options:



Protocol - protocol list with two options: *HTTP/1.1 (predefined) and HTTP/1.0*

User-agent - text field, predefined as *Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)*

Accept - text field, predefined as *text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8*

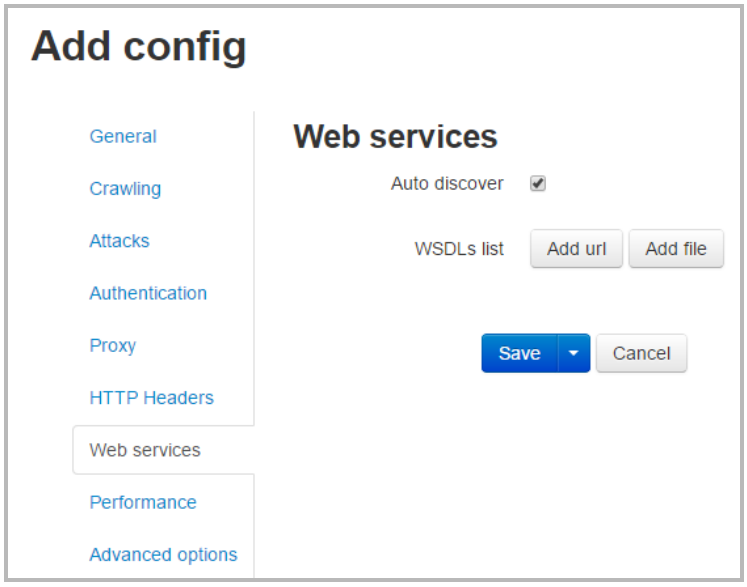
Content-type - text field, predefined as */*

Extra header- text field

Cookie- text field

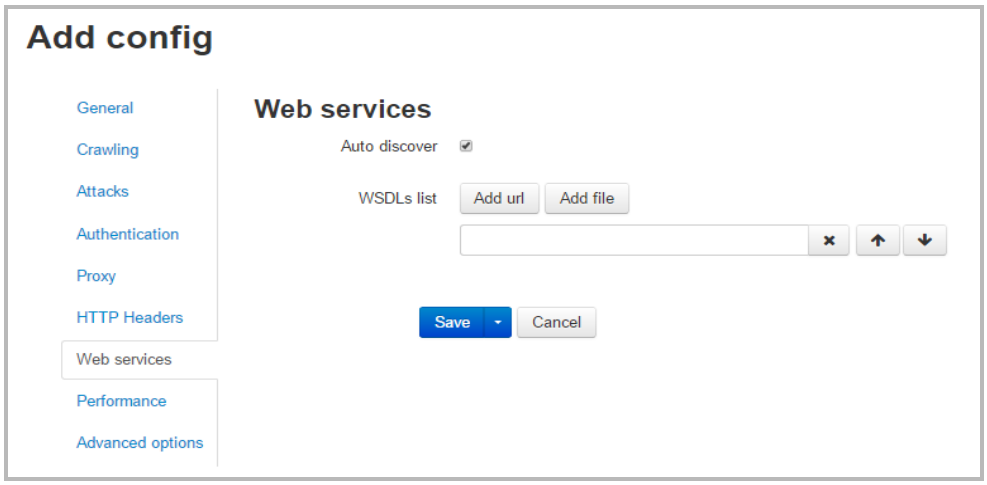
Lock cookies for duration of scan is unchecked by default

The *Web services* tab displays the following options:

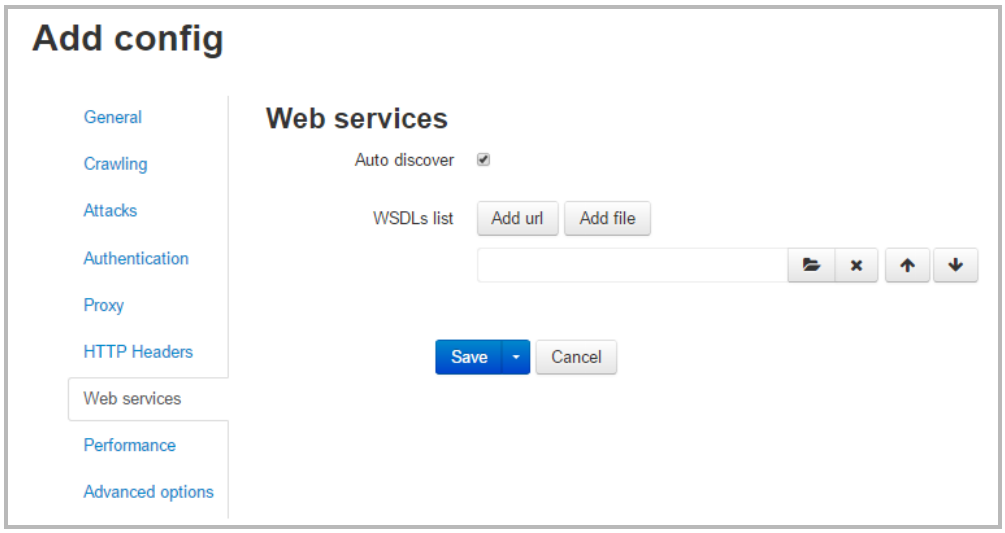


Auto discover checkbox is enabled by default.

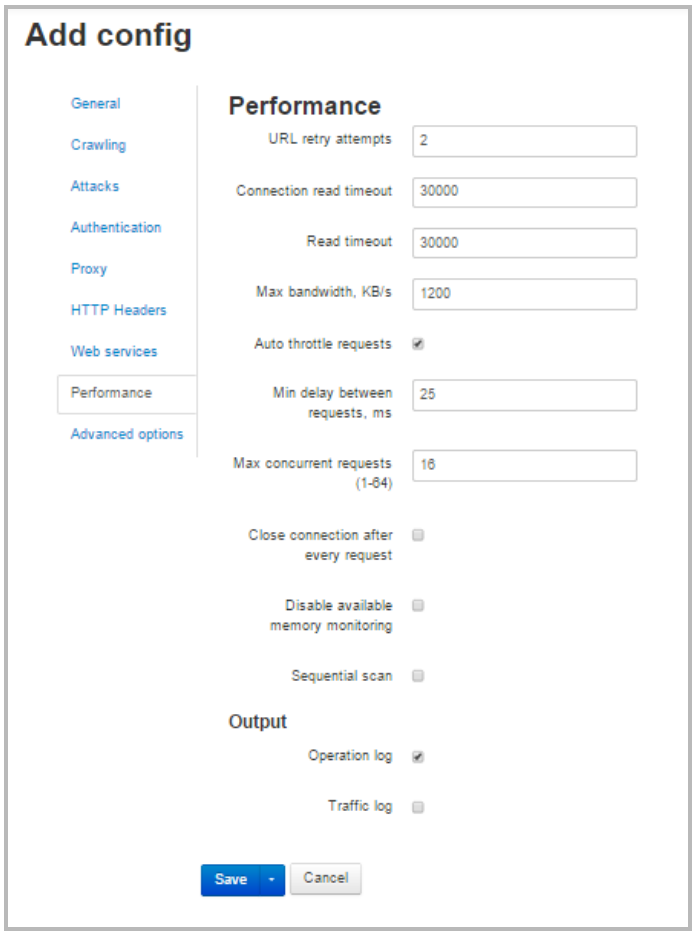
Add URL - the standard options to add multiple URLs. To add a URL press the button and type it in text field:



Add file - the standard options to add file. Press the button and field appears for the exporting a file from the web portal:



The *Performance* tab displays the following options:



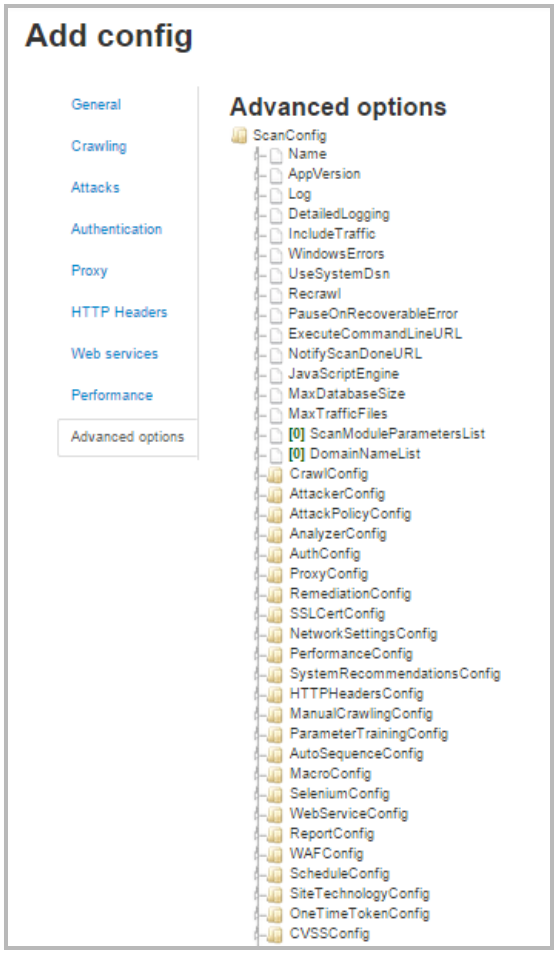
Performance options:

- **URL retry attempts** - text field, predefined as 2
- **Connection read timeout** - text field, predefined as 30000
- **Read timeout** - text field, predefined as 30000
- **Max bandwidth, KB/s** - text field, predefined as 500
- **Auto throttle requests** - is checked by default; to prevent server showdown
- **Min delay between requests, ms** - text field, predefined as 25; for example, 100 ms means max 10 requests per second.
- **Max concurrent requests (1-64)** - text field, predefined as 16
- **Close connection after every request** - is unchecked by default
- **Disable available memory monitoring** - is unchecked by default
- **Sequential scan** - is unchecked by default

Output options:

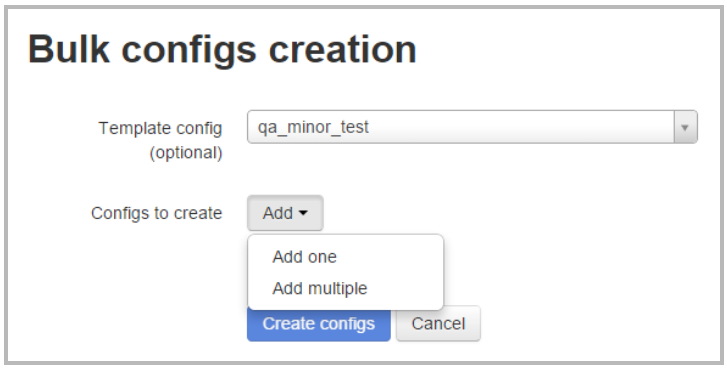
- *Operation log* - is checked by default
- *Traffic log* - is unchecked by default

The *Advanced* tab tree structure of all scan configs options:



Bulk add

This page allows the user to create new scan configs based on a template (optional). The user creates a list of configs to create (name and URLs) and presses the submit button and the system creates new configs. If a template is selected, everything is the same as in the template except the name and URLs from the list.



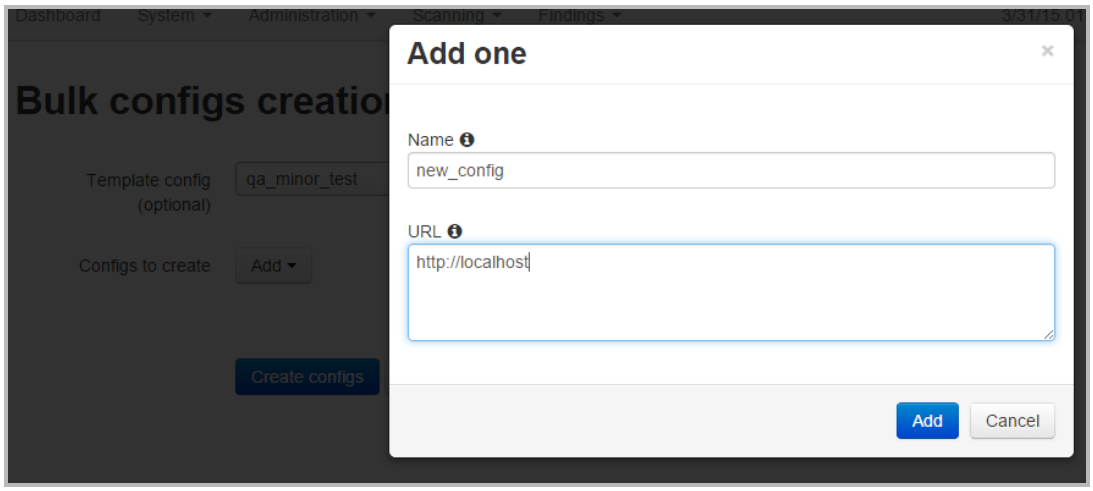
Template config - is a scan config to be used as a template to create new configs, this is optional. Help text is *Please enter 3 or more characters*.

Configs to create - is an editable list of configs to create. There is an Add button to add items to list, items are editable and removable.

Add button - is a drop-down menu button. Items are: Add one, Add multiple.

Add one scan config

Add onepopup allows the user to add one scan config against several URLs



Name field allows only alpha-numeric dash, dots and underscore characters. Max length is 38 symbols. On the right of **URLs** there is a help icon with tooltip text: *Multiple URLs allowed, each URL should start with protocol (e.g. http:// or https://), each URL should be put on a new line.*

Creating a scan config :

1. Find existing config in **Template config** list
2. Select *Add one* in ***Configs to create*** list
3. Enter new scan config name to **Name** field in opened popup window
4. Enter requested URL to **URL** field
5. Enter one more requested URL to **URL** field on a new line
6. Press **Add** button

Popup closed. New scan config with new URLs and name and the same settings is added to *Bulk config creation* page.

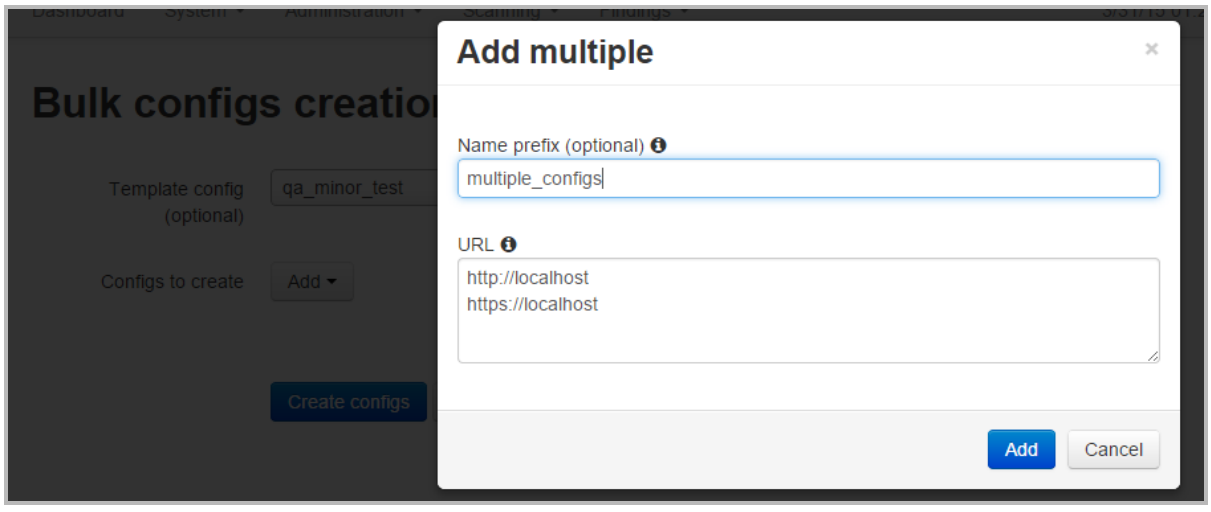
Add multiple scan configs

Add multiple - allows user to add several scan configs against several URLs.

Name prefix (optional) field allows only alpha-numeric dash, dots and underscore characters. Max length is 38 symbols. On the right of the field, there is a help icon with the tooltip text: *Optional prefix to be added to config names, optional. Resulting name will be made of prefix and appended URL.*

URLs also has Help icon, text : *Config will be created for each URL in the list. Enter valid URLs starting with protocol (e.g. http:// or https://). Each URL goes to a new line.*.

Generated config names are 38 characters max, all invalid characters are replaced with _ (valid are english alphabet, digits, - and _).



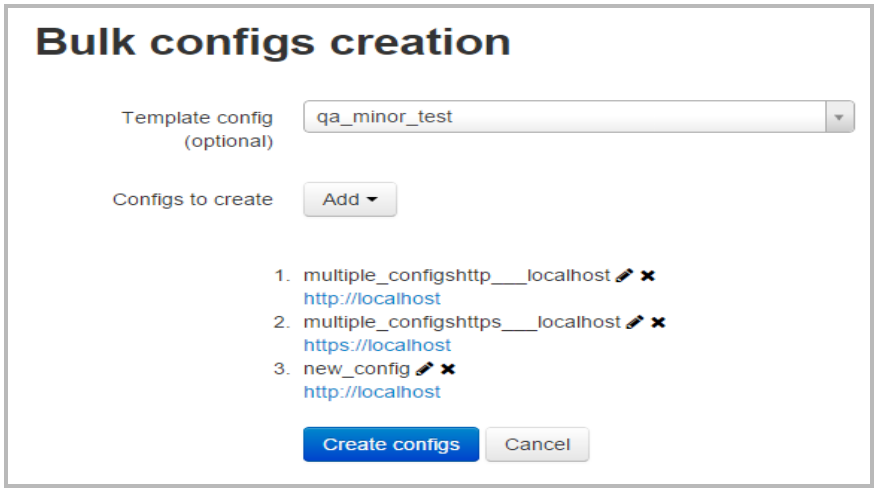
Creating multiple scan configs:

1. Find existing config in *Template config* list
2. Select **Add multiple** in *Configs to create* list
3. Enter new scan config name to **Name prefix (optional)** field in opened popup window
4. Enter requested URL to **URL** field
5. Enter one more requested URL to **URL** field on a new line
6. Press **Add** button

Popup closed. New scan configs with new URLs and names and the same settings are added to Bulk config creation page.

Bulk config results page

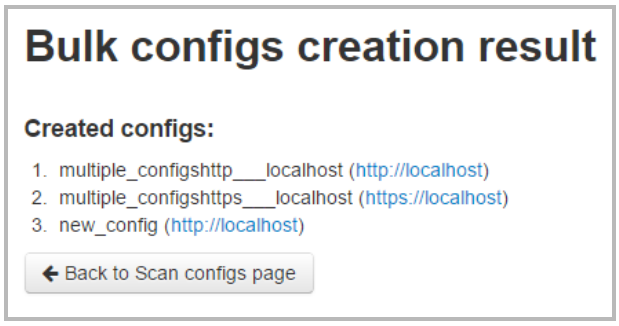
After clicking to **Add** button in popup window a user redirected to *Bulk config creation* page.



Bulk config creation page displays an ordered list (1, 2, 3, ...).

On the first line of the list, the config name is entered. On the right of the config name (on the same line, w/o margin) there are edit and delete icon buttons. On the next lines, the user places the URLs.

After clicking to **Create configs** the user is redirected to the Bulk configs creation result page.

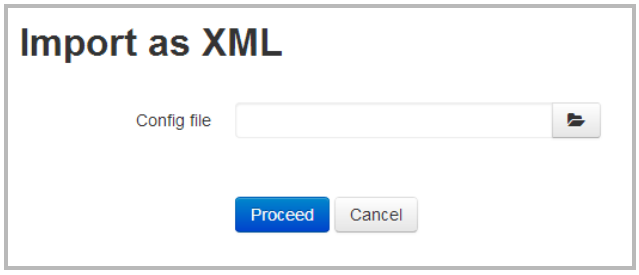


There are two possible groups: *Created configs* and *Creation errors* listing the created and not created configs.

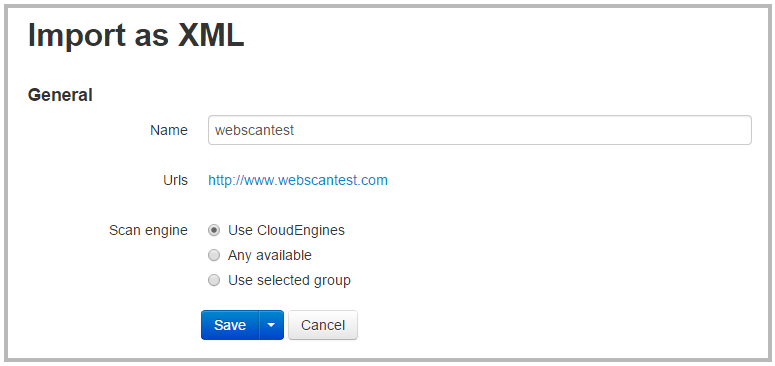
The user is redirected to *Scan configs* page when he clicks to *Back to Scan configs page*.

Import as XML

Import as XML page allows the user to import a scan config as XML to the portal.



The page contains **Config file**. This is the field for importing XML configs that have been exported from the web portal or AppSpider. The user uploads the scan config and clicks to the Proceed button. The following form is opened:



The form contains general info about the scan config:

Name - imported scan config name

URLs - link to hostname (target)

Scan engine option allows user to select one type: Use CloudEngines, Any available, Use selected group.

Action buttons are:

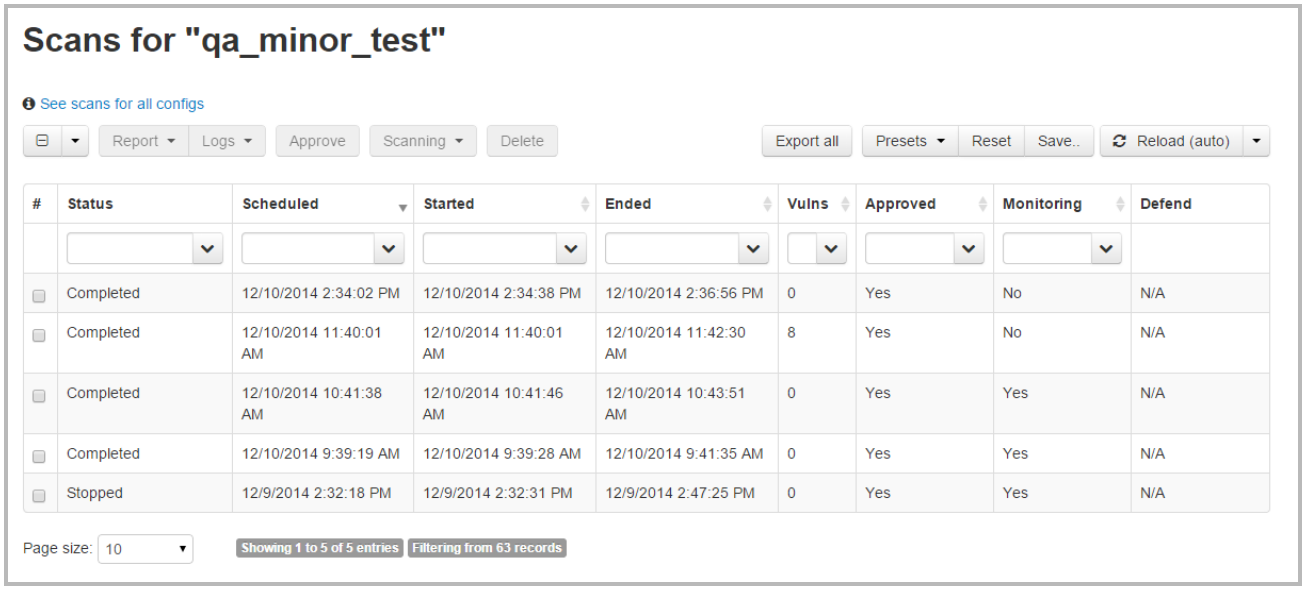
Save button – creates new scan config on the Portal; returns to the Scan configs.

Save and run button - creates a new scan config and run scan based on config settings; opens Scans page.

Cancel button – returns to the Scan configs page without saving.

Scans for scan config

The page contains scans grid for selected scan config. The user checks a scan config on the *Configs* grid and clicks the View scans button.



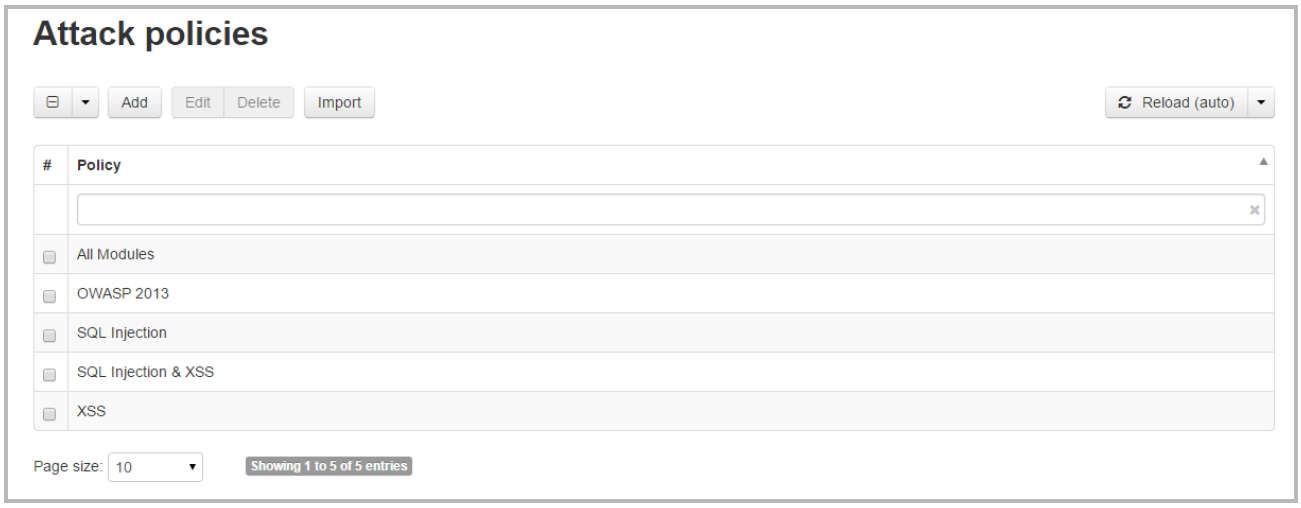
#	Status	Scheduled	Started	Ended	Vulns	Approved	Monitoring	Defend
	Completed	12/10/2014 2:34:02 PM	12/10/2014 2:34:38 PM	12/10/2014 2:36:56 PM	0	Yes	No	N/A
	Completed	12/10/2014 11:40:01 AM	12/10/2014 11:40:01 AM	12/10/2014 11:42:30 AM	8	Yes	No	N/A
	Completed	12/10/2014 10:41:38 AM	12/10/2014 10:41:46 AM	12/10/2014 10:43:51 AM	0	Yes	Yes	N/A
	Completed	12/10/2014 9:39:19 AM	12/10/2014 9:39:28 AM	12/10/2014 9:41:35 AM	0	Yes	Yes	N/A
	Stopped	12/9/2014 2:32:18 PM	12/9/2014 2:32:31 PM	12/9/2014 2:47:25 PM	0	Yes	Yes	N/A

The page has a **See scans for all configs** link that leads to the *Scans* page.

Action buttons are the same as on *Scans* grid. This table has pagination, **Reload / Auto reload** buttons and *Presets* menu.

Attack Policy

The *Attack policies* table consists of all of the user's attack policies.



It contains following column - *Policy* (name of the attack policy)

Action buttons:

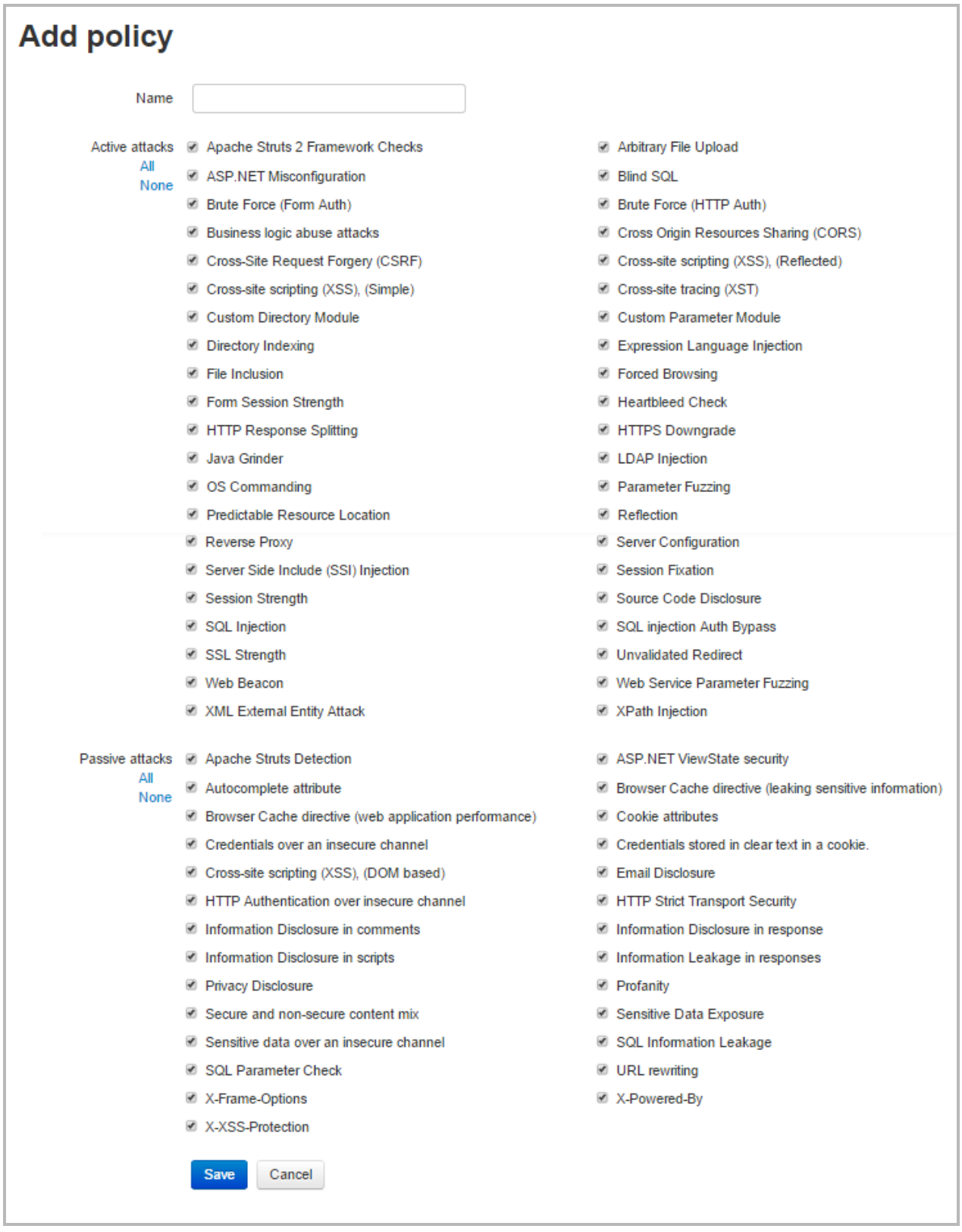
- **Add** - opens Add policy page;
- **Edit** – opens Edit policy page with predefined settings;
- **Delete** – removes the selected attack policy;
- **Import** - opens popup window for import an attack policy as XML to the portal.

The list of attack configs is displayed on the *Add/edit config* page on the *Attacks* tab in the *Predefined policies* list. On the selection of the desired item in the combo box, the appropriate attack config options are represented.

This table has pagination and **Reload/Auto reload** button.

Add Policy

This page allows users to create an attack policy for using it when creating a scan config.



The **Name** field is the name of the attack config.

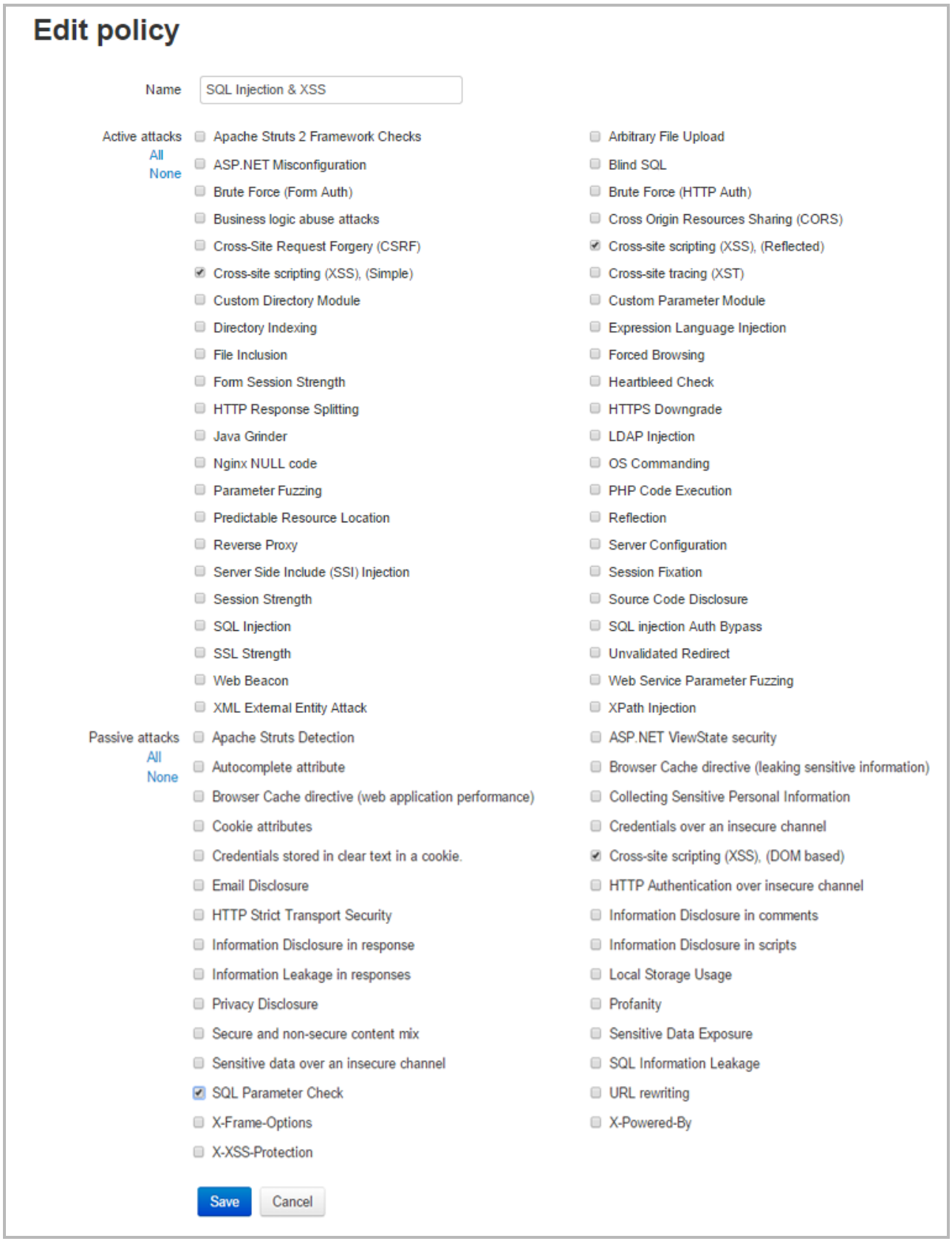
The list of all attacks with check boxes is displayed. The user may select any of the attack types stored in the config or click **All/None** link for unchecking/checking all modules in *Active* or *Passive* blocks.

Save - create new config.

Cancel - return to Attack policy page without saving.

Edit Policy

This page allows users to edit an existing attack policy.



Edit policy

Name: SQL Injection & XSS

Active attacks (All / None)

- [ ] Apache Struts 2 Framework Checks
- [ ] ASP.NET Misconfiguration
- [ ] Brute Force (Form Auth)
- [ ] Business logic abuse attacks
- [ ] Cross-Site Request Forgery (CSRF)
- [x] Cross-site scripting (XSS), (Simple)
- [ ] Custom Directory Module
- [ ] Directory Indexing
- [ ] File Inclusion
- [ ] Form Session Strength
- [ ] HTTP Response Splitting
- [ ] Java Grinder
- [ ] Nginx NULL code
- [ ] Parameter Fuzzing
- [ ] Predictable Resource Location
- [ ] Reverse Proxy
- [ ] Server Side Include (SSI) Injection
- [ ] Session Strength
- [ ] SQL Injection
- [ ] SSL Strength
- [ ] Web Beacon
- [ ] XML External Entity Attack
- [ ] Arbitrary File Upload
- [ ] Blind SQL
- [ ] Brute Force (HTTP Auth)
- [ ] Cross Origin Resources Sharing (CORS)
- [x] Cross-site scripting (XSS), (Reflected)
- [ ] Cross-site tracing (XST)
- [ ] Custom Parameter Module
- [ ] Expression Language Injection
- [ ] Forced Browsing
- [ ] Heartbleed Check
- [ ] HTTPS Downgrade
- [ ] LDAP Injection
- [ ] OS Commanding
- [ ] PHP Code Execution
- [ ] Reflection
- [ ] Server Configuration
- [ ] Session Fixation
- [ ] Source Code Disclosure
- [ ] SQL injection Auth Bypass
- [ ] Unvalidated Redirect
- [ ] Web Service Parameter Fuzzing
- [ ] XPath Injection

Passive attacks (All / None)

- [ ] Apache Struts Detection
- [ ] Autocomplete attribute
- [ ] Browser Cache directive (web application performance)
- [ ] Cookie attributes
- [ ] Credentials stored in clear text in a cookie.
- [ ] Email Disclosure
- [ ] HTTP Strict Transport Security
- [ ] Information Disclosure in response
- [ ] Information Leakage in responses
- [ ] Privacy Disclosure
- [ ] Secure and non-secure content mix
- [ ] Sensitive data over an insecure channel
- [x] SQL Parameter Check
- [ ] X-Frame-Options
- [ ] X-XSS-Protection
- [ ] ASP.NET ViewState security
- [ ] Browser Cache directive (leaking sensitive information)
- [ ] Collecting Sensitive Personal Information
- [ ] Credentials over an insecure channel
- [x] Cross-site scripting (XSS), (DOM based)
- [ ] HTTP Authentication over insecure channel
- [ ] Information Disclosure in comments
- [ ] Information Disclosure in scripts
- [ ] Local Storage Usage
- [ ] Profanity
- [ ] Sensitive Data Exposure
- [ ] SQL Information Leakage
- [ ] URL rewriting
- [ ] X-Powered-By

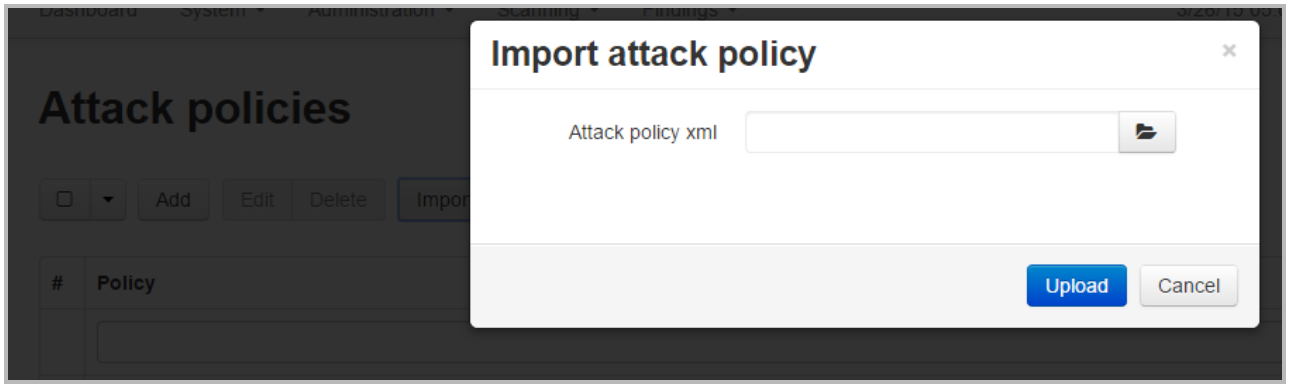
Save | Cancel

This is the same page as *Add policy* with following difference:

The title is *Edit policy*. All fields are predefined.

Import policy

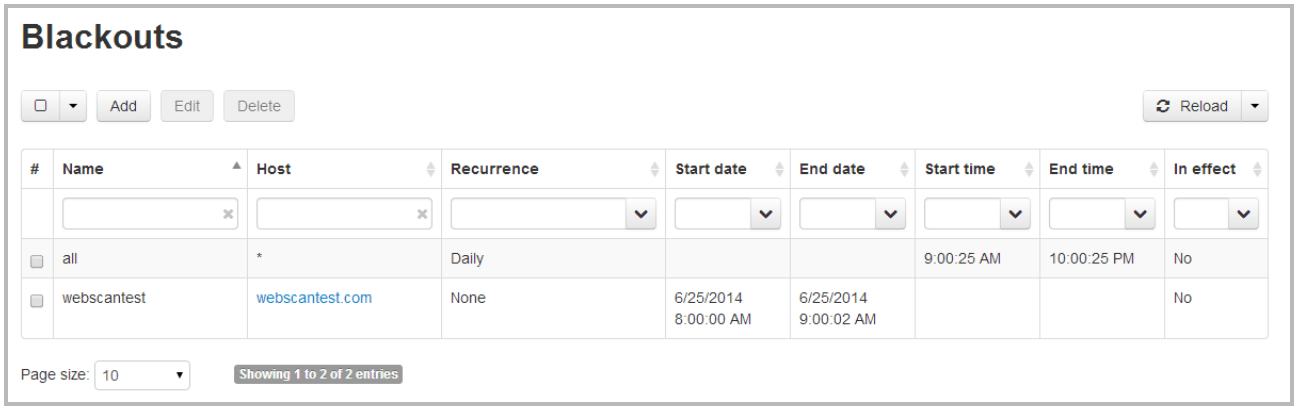
Import attack policy allows the user to import an attack policy as XML to the portal.



The popup contains **Attack policy xml** field. This is the field for importing XML policy that have been exported to the web portal. The user uploads the attack policy and clicks to the Upload button. The selected xml file uploads and placed into Attack policy grid. User is able to edit it and resave.

Blackouts

The table shows all blackouts for the current client.



Blackout is a time when a scan for a host is not performed.

The *Blackouts* table contains the following columns:

- **Name** – the name of the blackout.
- **Host** – IP address/Hostname affected
- **Recurrence** – recurrence type: None, Daily, Weekly, Monthly, Yearly
- **Start date** – start date for non-recurrent blackouts only
- **End date** - end date for non-recurrent blackouts only
- **Start time** - start time for recurrent blackouts only
- **End time** - end time for recurrent blackouts only
- **In Effect** - indicates whether the blackout is active or not.

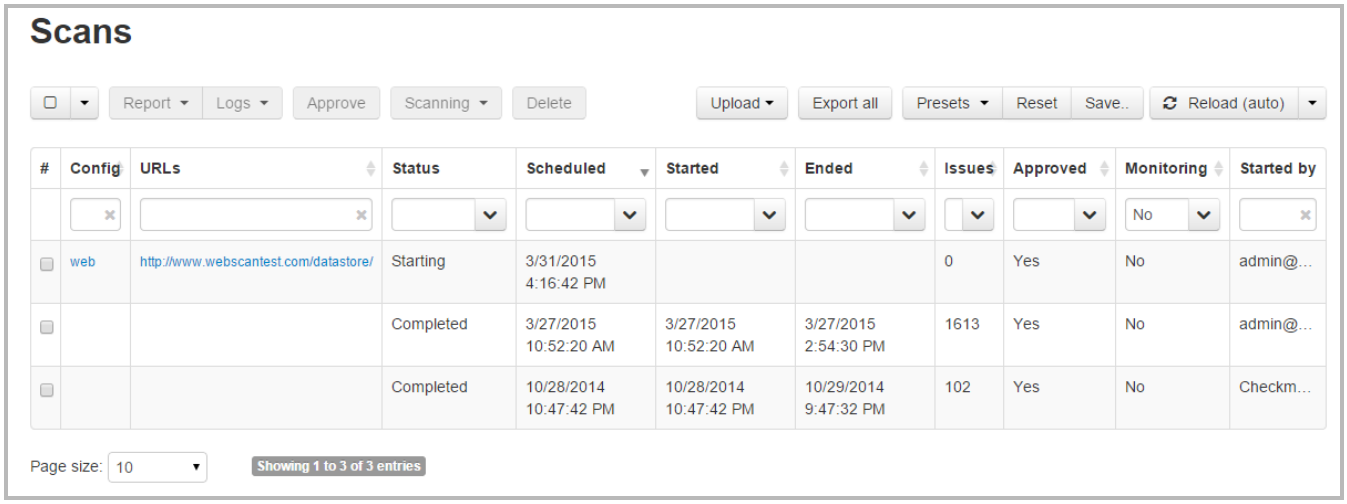
Action buttons:

- **Add** - opens Add blackout page, always enabled , requires Blackouts manager permissions.
- **Edit** - opens Edit blackout page, enabled if only one blackout is selected, requires Blackouts manager permissions.
- **Delete** - shows deletion dialog, enabled if one or more blackouts are selected, requires Blackouts manager permissions.

This table has pagination and **Reload / Auto reload** button.

Scans

The *Scans* table consists of all scans for the current client.



The *Scans* table contains the following columns:

- *Config* - scan configuration name
- *URLs* - attacked URLs
- *Status* - current scan status
- *Scheduled* - schedule scan time
- *Started* - start scan time
- *Ended* - stop scan time
- *Issues* - the number of discovered issues
- *Monitoring* - enable or disable monitoring status for the scan.

Action buttons are:

Report -

- '**View**' - opens the HTML report page.
- '**Download**' - download the report as ZIP archive.
- '**Update**' - opens Update report popup window; allows users to download a new report and updates the existing report.
- '**Assign**' - opens 'Assign report' page for the report.

Logs -

- '**View processing log**' - opens Processing log page; allows the user to see report logs if they have been created.
- '**Download engine log**' - downloads the engine log for the scan.

Scanning -

- '**Scan status**' - opens Scan status page.
- '**Pause**' - pauses active scan.
- '**Resume**' - resumes paused scan.
- '**Stop**' - stops active scan; enabled only for active scans expect the 'Starting' and 'Waiting for cloud' statuses.
- '**Cancel**' - cancels active scan; enabled only for scans in 'Starting' and 'Waiting for cloud' statuses.

Delete - shows deletion dialog, enabled if one or more scans are selected; remove the scan.

Upload – opens upload report menu: Standard report/Checkmarx report.

Export all - exports scans data to CSV file (filters are applied).

Defend - button enabled only for defend scas and opens Defend scans page

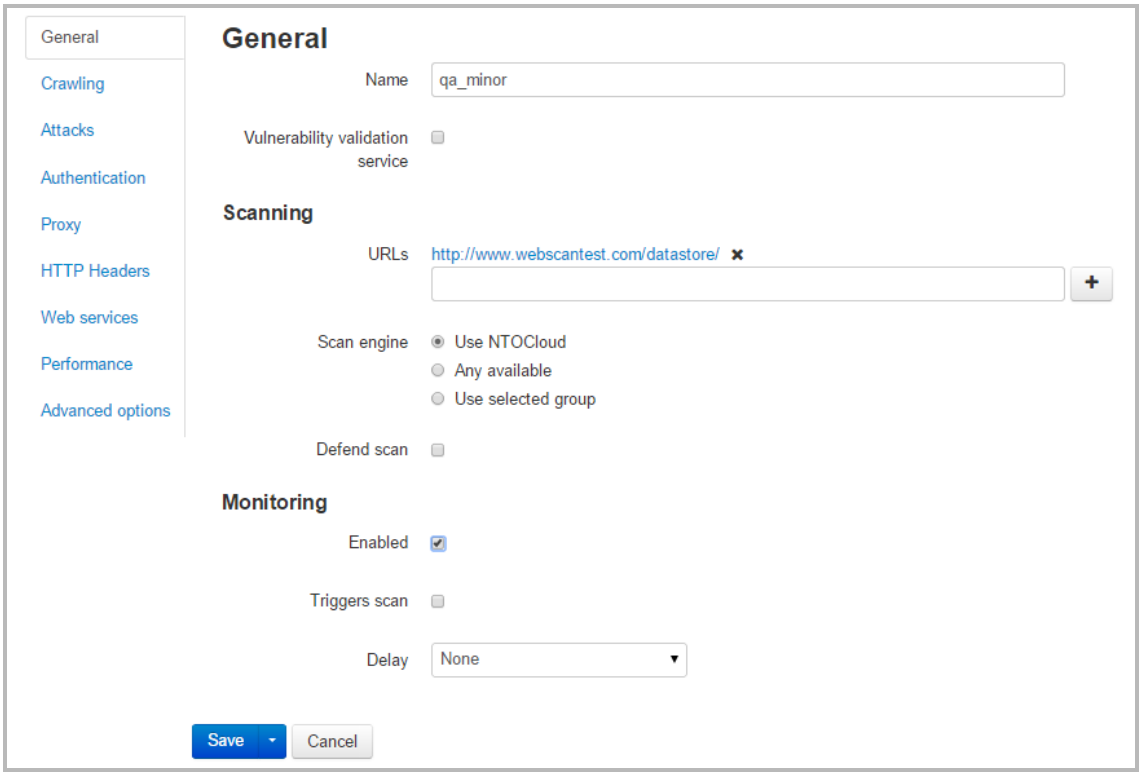
This table has pagination, **Reload / Auto reload** button and **Presets** option.

Monitoring scans

This is a special scans run automatically the system.

For creating this scan, the system admin should create:

- scan engine group with enabled Monitoring status
- a live engine should contained in the monitoring scan engine group;
- scan config with enabled Monitoring option on General tab

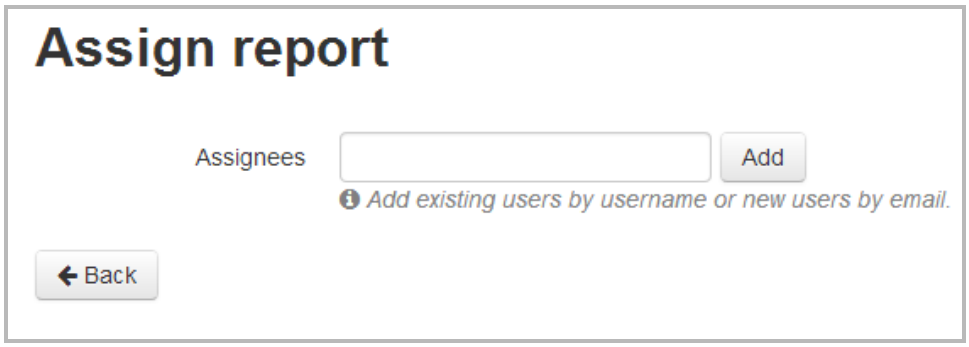


Monitoring option:

- *enabled* - is the scan config is monitoring or not;
- *triggers scan* - if there were changes between the two last monitoring scans a regular scan will be started;
- *delay* - monitoring scan period (none, 1 hour, 1 day, 1 week, 1 month).

Assign report

This page allows the organization to add report viewing permissions to users.



The user is able to add an existing or not existing account as a Report viewer.

Add existing users by username or new users by email. message presented near **Assignees** field.

Add an existing user

User types in username or email to **Assignees** field -

- **Username** (full name, email) is displayed if user was found.
- *System was unable to add assignee (user can't be found).* text is displayed if user was not found

Add button add permissions for user to observe the report

Add an non existing user

User types in email to **Assignees** field.

An eimail will be sent to the user and the user may view the report.

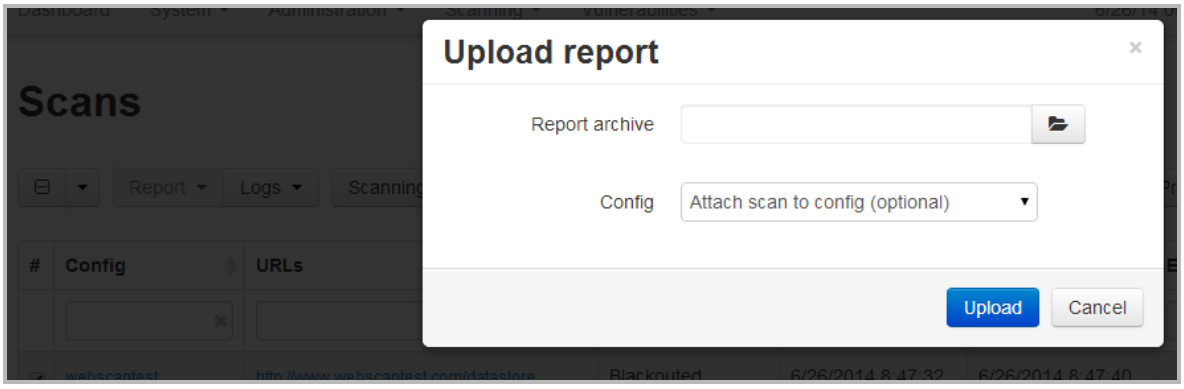
Assign report list contains the following data:

- *User email address* - displays the email address (for existing and non-existing users)
- *Username* - displays username (for existing users)

Remove Rights - action button. Removes permissions to observe the report

Upload standard report

Select Standard report item in Upload menu list. It opens the popup window and allows users to upload scan reports to the portal with max size is 1 Gb.



The popup window contains the following fields:

- **Report archive** - exports ZIP file from web portal
- **Config** - list of all scan configs for current user; *Attach scan to config (optional)* message is displayed in the field.

The portal uploads zipped archives.

If **Upload** is pressed with no file chosen, the *Please select a file* validation message is displayed.

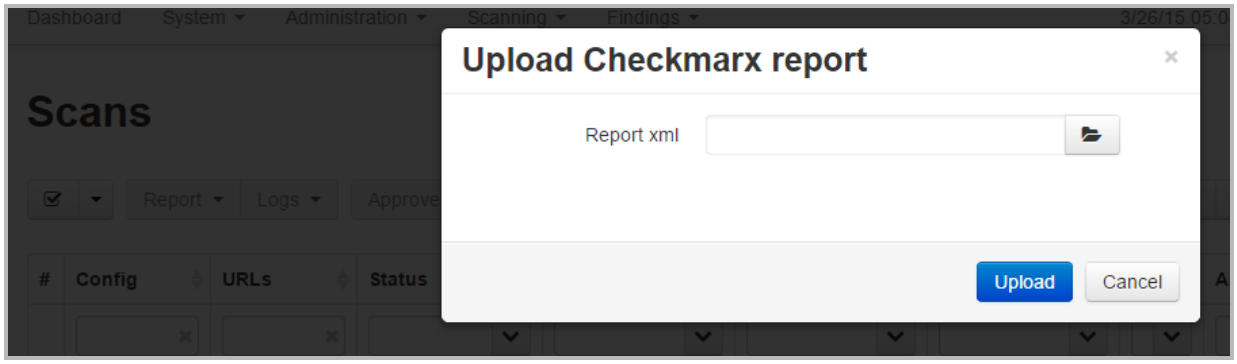
If the **Upload** button is pressed with the correct file chosen, the report is uploaded to the portal and displays in the *Scans* table.

If the base scan config is not chosen in the *Config* list, the report is added to Scans table without the Config name and URL.

Cancel button – closes the popup window.

Upload Checkmarx report

Select Checkmarx report item in Upload menu list. It opens the popup window and allows users to upload Checkmarx reports to the portal.



The popup window contains the following field:

- **Report xml** – exports XML file from web portal. File structure validation is exist.

If **Upload** is pressed with no file chosen, the *File required* validation message is displayed.

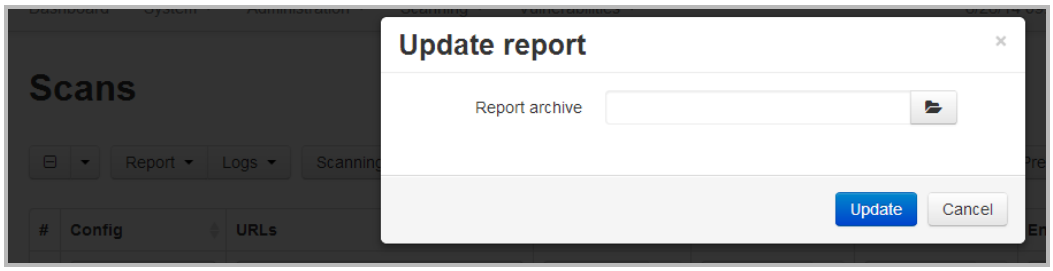
If the **Upload** button is pressed with the correct file chosen, the report is uploaded to the portal and displays in the Scans table.

Cancel button – closes the popup window.

The Checkmarx scan does not have a report. User is able to observe uploaded findings on Discovered grid.

Update report

Update button is enabled only if one scan selected. Update button opens Update report popup window.



The portal uploads the zipped archives with max size is 1 Gb.

Report archive – exports the ZIP file from the web portal.

Update button uploads the new report and replaces the old report with the uploaded one.

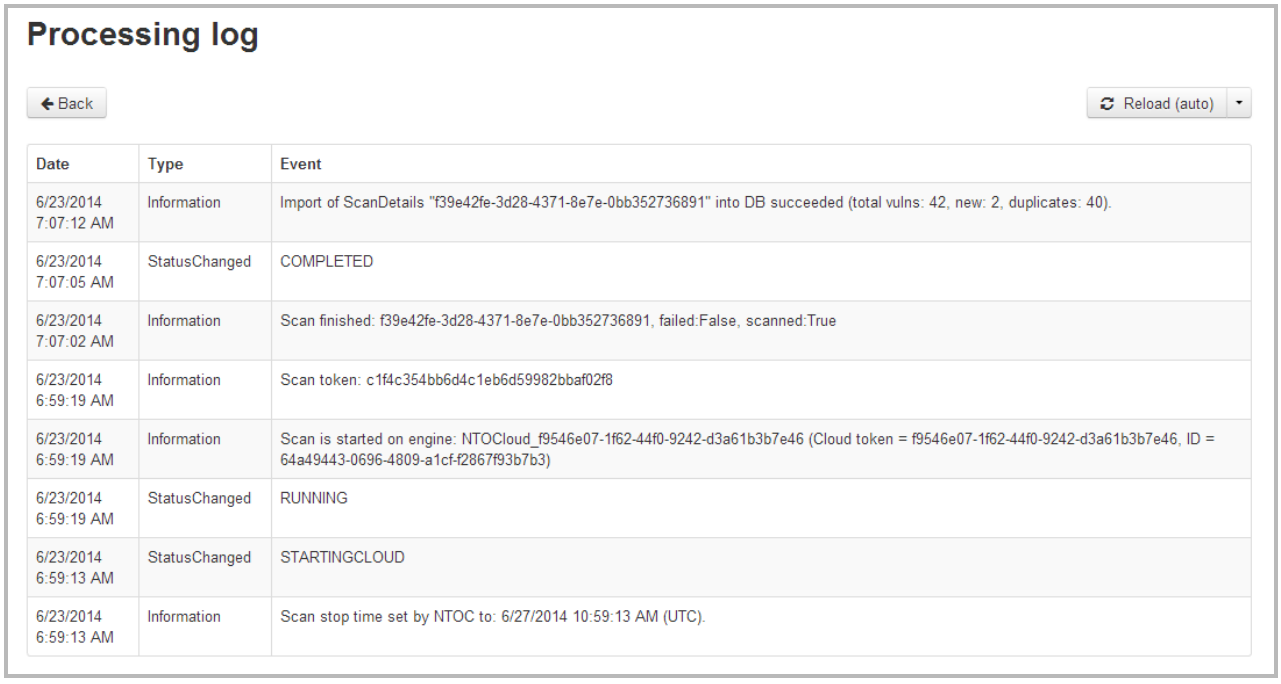
If **Update** is pressed with no file chosen, the Please select a file validation message is displayed.

If **Update** button is pressed with the correct file chosen, the scan report is updated on the portal.

Cancel button – closes the popup window.

Processing log

View processing log button is enabled only if one scan selected. **View processing log** button opens *Processing log* page where users can observes the selected scan events.



Date	Type	Event
6/23/2014 7:07:12 AM	Information	Import of ScanDetails "f39e42fe-3d28-4371-8e7e-0bb352736891" into DB succeeded (total vulns: 42, new: 2, duplicates: 40).
6/23/2014 7:07:05 AM	StatusChanged	COMPLETED
6/23/2014 7:07:02 AM	Information	Scan finished: f39e42fe-3d28-4371-8e7e-0bb352736891, failed:False, scanned:True
6/23/2014 6:59:19 AM	Information	Scan token: c1f4c354bb6d4c1eb6d59982bbaf02f8
6/23/2014 6:59:19 AM	Information	Scan is started on engine: NTOCloud_f9546e07-1f62-44f0-9242-d3a61b3b7e46 (Cloud token = f9546e07-1f62-44f0-9242-d3a61b3b7e46, ID = 64a49443-0696-4809-a1cf-f2867f93b7b3)
6/23/2014 6:59:19 AM	StatusChanged	RUNNING
6/23/2014 6:59:13 AM	StatusChanged	STARTINGCLOUD
6/23/2014 6:59:13 AM	Information	Scan stop time set by NTOC to: 6/27/2014 10:59:13 AM (UTC).

The *Processing log* table contains the following columns:

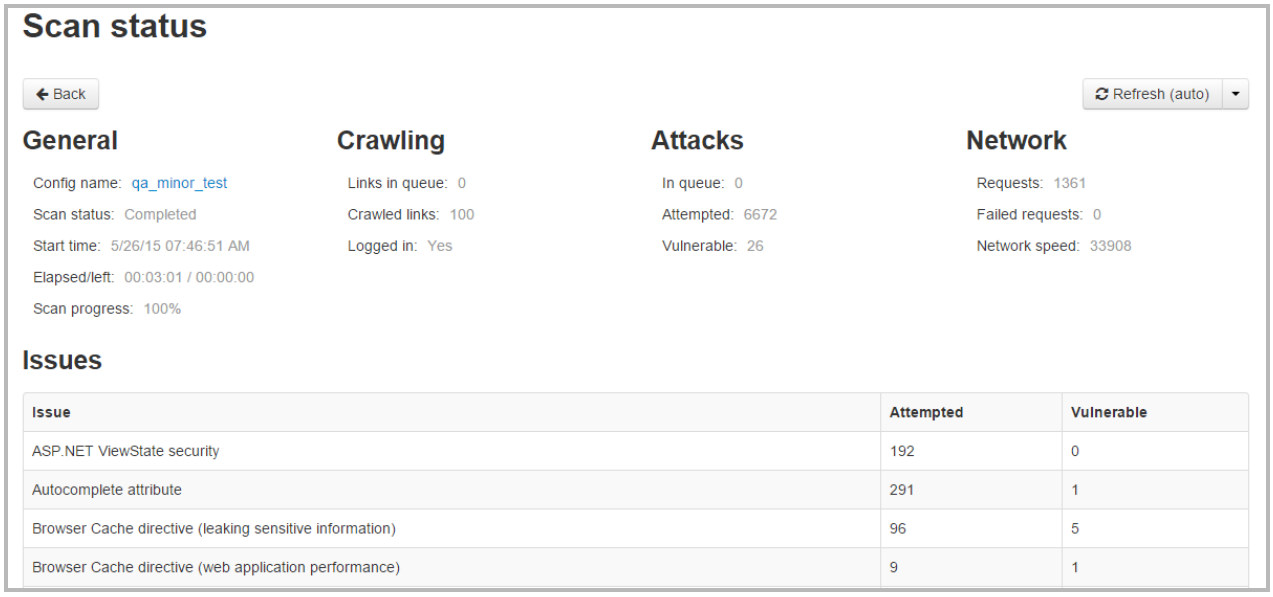
- *Date* - the name of the event;
- *Type* - the type of the event;
- *Event* - the event details.

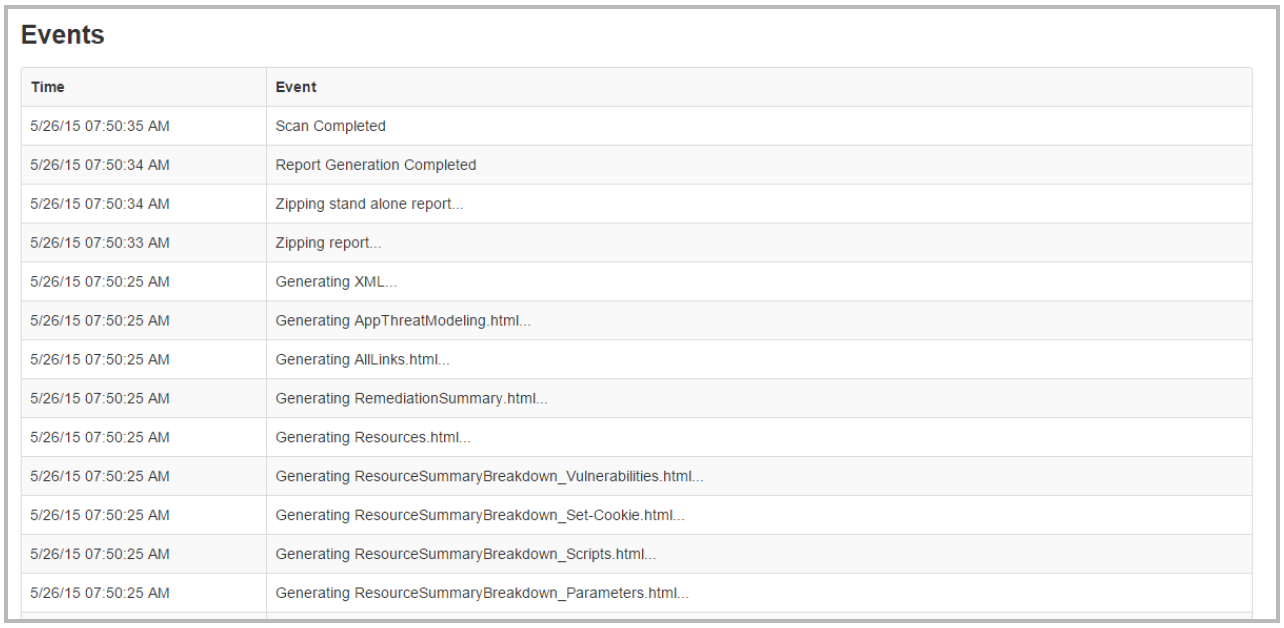
This table has pagination and **Reload / Auto reload** button.

Back button return to Scans page.

Scan *status*

This page details the scan status of scans selected by the user.





Events

Time	Event
5/26/15 07:50:35 AM	Scan Completed
5/26/15 07:50:34 AM	Report Generation Completed
5/26/15 07:50:34 AM	Zipping stand alone report...
5/26/15 07:50:33 AM	Zipping report...
5/26/15 07:50:25 AM	Generating XML...
5/26/15 07:50:25 AM	Generating AppThreatModeling.html...
5/26/15 07:50:25 AM	Generating AllLinks.html...
5/26/15 07:50:25 AM	Generating RemediationSummary.html...
5/26/15 07:50:25 AM	Generating Resources.html...
5/26/15 07:50:25 AM	Generating ResourceSummaryBreakdown_Vulnerabilities.html...
5/26/15 07:50:25 AM	Generating ResourceSummaryBreakdown_Set-Cookie.html...
5/26/15 07:50:25 AM	Generating ResourceSummaryBreakdown_Scripts.html...
5/26/15 07:50:25 AM	Generating ResourceSummaryBreakdown_Parameters.html...

When scan is '*Running*'/'*Resuming*' the **Pause** and **Stop** buttons are presented.

Pause button – pauses/starts the scan.

Stop button – stop the scan (scan will be canceled)

When scan is '*Pausing*' the **Resume** and **Stop** buttons are presented.

Information about the scan is displayed:

General info -

- *Config name*: current scan's config name; has link to edit page of scan config
- *Scan status* - status of scan in current time
- *Start Time* - time of starting the scan
- *Elapsed/left* - elapsed time of current scan
- *Scan progress* - overall scan progress in percents

Crawling info -

- *Links in queue* - number of links are in queue
- *Crawled links* - number of links crawled
- **Logged in** - did the scanner authenticate on the target site?

Attacks info -

- *In queue* - number of attacks are in queue
- *Attempted* - number of attacks attempted
- *Vulnerable* - number of found issues

Network info -

- *Requests* - the main count of requests
- *Failed requests* - number of failed requests
- *Network speed* - network speed

Scan status page has **Back** button leads to *Scans* page.

All the *Issues* and *Events* tables are displayed on Scan status page.

The *Issues* table contains the following columns:

- *Issue* - the issue type
- *Attempted* - number of attacks attempted
- *Vulnerable* - number of found issues

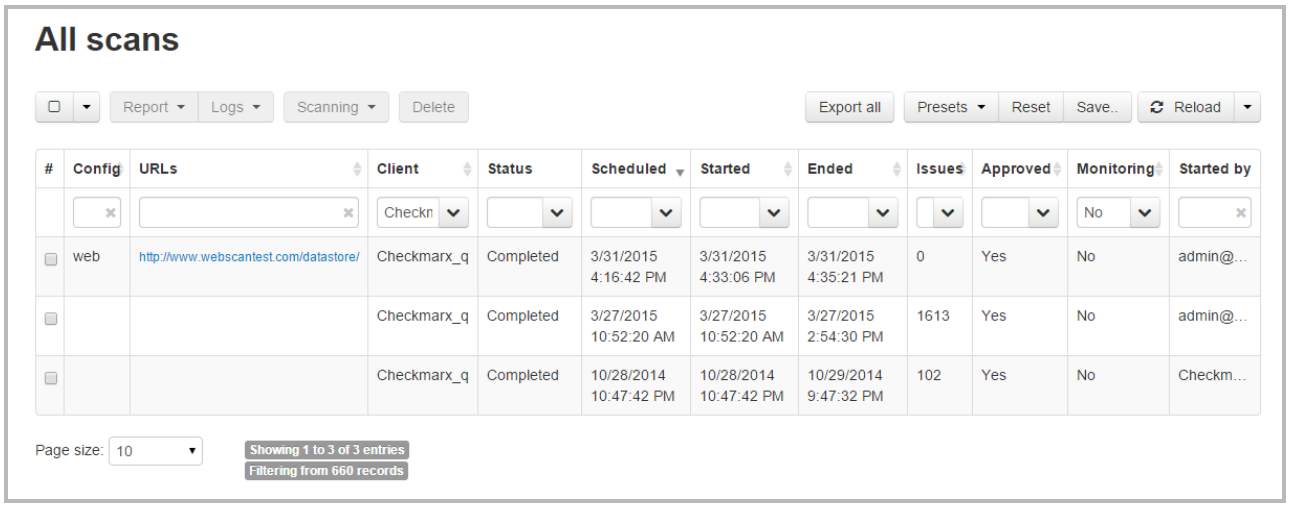
The *Events* table contains the following columns:

- *Date* - the name of the event
- *Event* - the event details

This table has **Reload / Auto reload** button.

All scans (SA)

All scans table consists of all scans for all clients.



This page displays the scans of all clients.

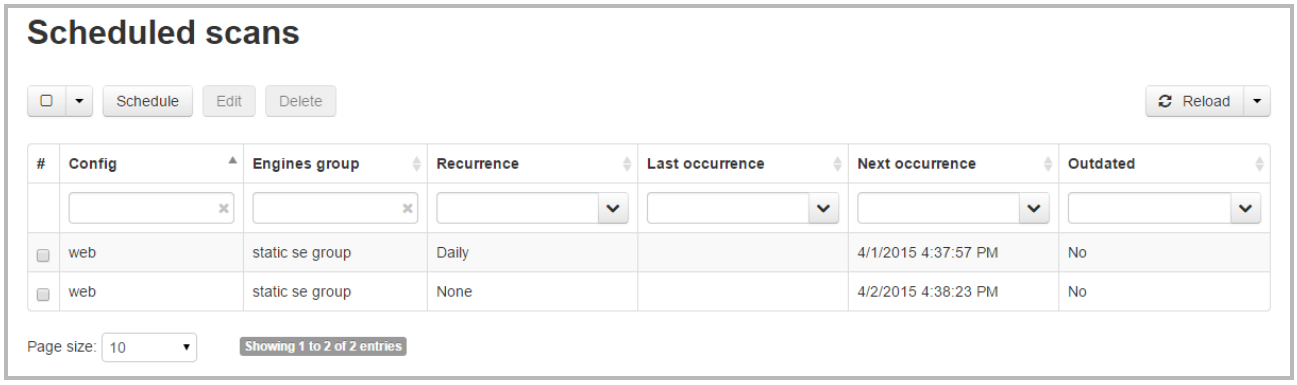
All scans table contains the same columns as Scans table with following delta :

Title is *All scans*.

Column Client is added for filtering scans by client.

Scheduled scans

The *Scheduled scans* table displays all scheduled scans of the current client.



The *Scheduled scans* table contains the following columns:

- *Config* – the scan config name.
- *Engines group* - scan engines group name.
- *Recurrence* - recurrence type (None, Daily, Weekly, Monthly, Yearly); empty if not recurring.
- *Last occurrence* -date and time when scheduled scan last time occurred (null if never occurred).

Last occurrence value is calculated by scheduler when scan is triggered (value is set to current time), if scan of the same scan config is started manually, this value will not change. For newly created scheduled scans the value is null.

- *Next occurrence* - the date and time when the scan is scheduled to start again.

Next occurrence value is calculated when creating/updating scheduled scan or when scan is triggered. When scan occurs for not recurrent scans, the value is set to null.

- *Outdated* - display whether or not the scan is outdated.

Outdated is a scheduled scan that will never be started again. For non-recurring this means that the start time is in the past. For recurring - this means that there will be an occurrence in future.

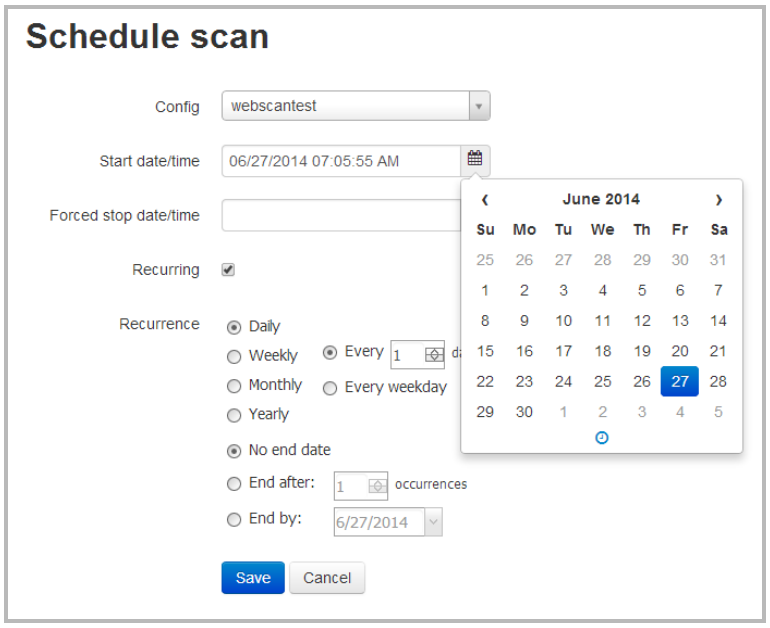
Action buttons are:

- **Add** - opens add schedule scan page, always enabled.
- **Edit** - opens edit schedule scan page, enabled if only one scheduled scan is selected.
- **Delete** - shows deletion dialog, enabled if one or more scheduled scans are selected.

This table has pagination and **Reload / Auto reload** button.

Add scheduled scan

This page allows users to add and edit schedule scan rules.



Config – scan config lookup (required), shows only configs of current client.

Start date/time - date and time when a scan should be started (required), can't be a date/time in the past.

Forced stop date/time (optional) - date and time when a scan should be forcibly stopped if still running, can't be equal or earlier than start date.

Recurring - indicates whether a scheduled scan is recurrent.

Recurrence - recurrence options.

Targets-based security

Action buttons will be disabled for scheduled scans of not approved for current user targets, system admin will have all targets approved.

To restrict actions for scheduled scans instead of checkbox they are grayed out.

Targets wildcards are supported.

Scheduled scans can't be created for configs on not approved targets.

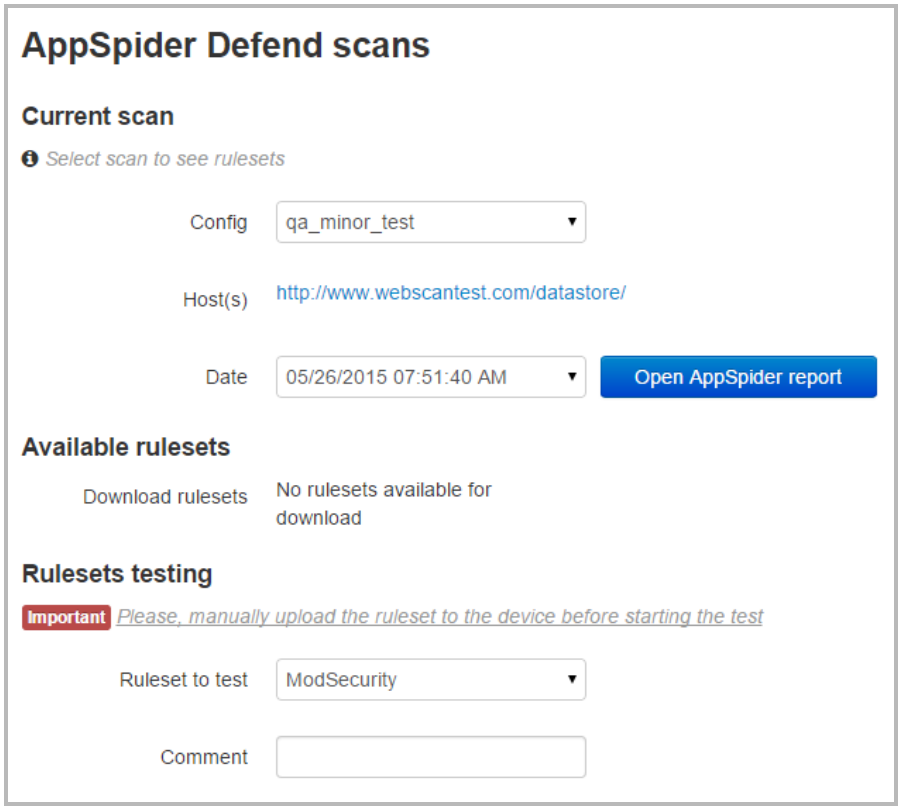
Defend scans

This feature is only available for scan configs scanning targets approved for the current user (user with WAF manager and client admin roles that has all clients approved targets, system admin has all targets approved). System admin is able to manage the defend feature - enable or disable it on the clients edit page.

For create a defend scan, please make sure the following information is entered:

- **Defend** is enabled in scan config.
- Scan result has at least one issue from list: **SQL Injection**, **SQL injection Auth Bypass**, **Blind SQL**, **Blind SQL Injection**, **Reflected Cross-site scripting (XSS)**, **OS Commanding**, **HTTP Response Splitting**, **Remote File Include**, **Remote File Include (RFI)**, **Predictable Resource Location**, **Directory Indexing**;
- The user is a WAF manager or impersonated system admin.
- The scan has **COMPLETED** or **STOPPED** status.
- A scan report exists and is available to download.

The page title is *Appspider Defend scans. Please select scan with findings.* message displays under the title.



Config – list of all scan configs for the current user.

The user selects a scan config and the following scan information is displayed:

Host(s) - the host name (target).

Date - list occurred date and time of selected scan.

The user selects the scans date and the following scan information is displayed:

Open AppSpider report button - opens the html scan report

List of Available rulesets ('*ModSecurity*', '*Sourcefire_Snort*', '*Nitro_Snort*', '*Imperva*', '*Denyall*', '*Secui_Snort*', '*Akamai*', '*Barracuda*').

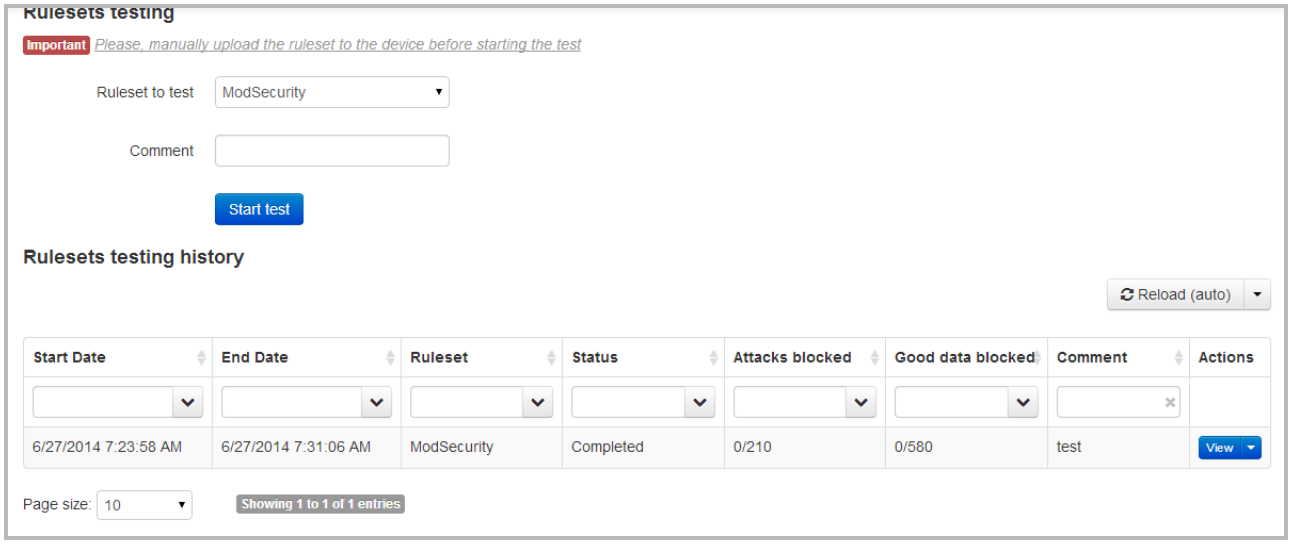
No rulesets available for download message is presented if there are no rulesets.

Important! Please, manually upload the ruleset to the device before starting the test message is presented in *Rulesets* testing block.

Ruleset to test list contains 'ModSecurity' ruleset only.

User types in **Comment** (optional) field and clicks to **Start test**.

'*ModSecurity*' ruleset is started and displays in *Rulesets testing history* table.



The table contains the following columns:

- Start date - start date and time the ruleset
- *End date* - end date and time the ruleset
- *Ruleset* - the ruleset title
- Status - the ruleset status
- *Attacks blocked* - number of blocked attacks
- Good data blocked - *number of blocked good data*
- *Comment* - users comment to the test
- **Actions** - opens menu: **View**, **Download HTML report**, **Download XML report**, **Delete**.

This table has pagination and **Reload / Auto reload** button.

Download HTML report, **Download XML report** actions are enabled only for completed tests.

4. When ruleset completes, the *Ruleset to test* list contains all available rulesets. The user is able to download it.

View button opens *Vulnerabilities scan* page. The title is *NTODefend QuickScan Results*.

Vulnerable URL	Parameter	Vulnerability Type	Traffic	Details	Blocked Good Traffic	Blocked Attack Traffic
http://www.webscantest.com/bjax/servertime.php	msg	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 8
http://www.webscantest.com/business/account.php	accountId	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 4
http://www.webscantest.com/cof	Referer	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 2
http://www.webscantest.com/coffeepits/classes	Unnamed	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 3
http://www.webscantest.com/coffeepits/classes/	Unnamed	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	3 / 3
http://www.webscantest.com/coffeepits/classes/audio	Unnamed	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 3
http://www.webscantest.com/coffeepits/classes/audio/	Unnamed	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	3 / 3
http://www.webscantest.com/coffeepits/classes/images	Unnamed	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 3
http://www.webscantest.com/coffeepits/classes/images/	Unnamed	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	3 / 3
http://www.webscantest.com/coffeepits/classes/images/jon	Unnamed	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 3
http://www.webscantest.com/coffeepits/classes/images/jon/	Unnamed	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	3 / 3
http://www.webscantest.com/crosstraining/aboutyou.php	fname	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 4
http://www.webscantest.com/crosstraining/aboutyou2.php	returnto	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 4
http://www.webscantest.com/crosstraining/aboutyou2.php	fname	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 4
http://www.webscantest.com/crosstraining/aboutyou2.php	nick	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 4
http://www.webscantest.com/crosstraining/blockedbyns.php	Comment	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 4
http://www.webscantest.com/crosstraining/checkitem_lookup.php	q	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 4
http://www.webscantest.com/crosstraining/reservation_submit.php	arrive_date	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 0	0 / 4
http://www.webscantest.com/crosstraining/search.php	q	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	4 / 4
http://www.webscantest.com/crosstraining/sitereviews.php	email	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 4
http://www.webscantest.com/crosstraining/sitereviews.php	description	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 4
http://www.webscantest.com/csrf/csrfpost.php	property	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 4
http://www.webscantest.com/csrf/session.php	jsession	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 4
http://www.webscantest.com/csrf/token.php	property	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 4
http://www.webscantest.com/csrf/token.php	token	Reflected Cross-site scripting (XSS)	Traffic	Details	0 / 10	0 / 4
http://www.webscantest.com/datastore/getimage_by_id.php	id	Blind SQL Injection	Traffic	Details	0 / 10	4 / 4
http://www.webscantest.com/datastore/getimage_by_id.php	id	SQL Injection	Traffic	Details	0 / 10	0 / 4
http://www.webscantest.com/datastore/getimage_by_name.php	name	Blind SQL Injection	Traffic	Details	0 / 10	1 / 1

The table contains the following columns:

- **Vulnerable URL** - link to a vulnerable URL
- **Parameter** - vulnerability parameter
- **Vulnerability Type** - vulnerability type
- **Traffic** - link to Scan files page
- **Details** - link to Vulnerability information page
- **Blocked Good Traffic** - number of blocked good data
- **Blocked Attack Traffic** - number of blocked attacks

Scan files page contains a table with links to scan files (requests, responses txt and html files).

The *Vulnerability information* page contains the vulnerability data (*WEBSITE*, *VULNTYPE*, *VULNURL*, *ATTACKTYPE*, etc.)

Vulnerability Information	
WEBSITE	http://www.webscantest.com:80
VULNTYPE	Reflected Cross-site scripting (XSS)
VULNURL	http://www.webscantest.com/bjax/servertime.php
MATCHEDSTRING	
NORMALIZEDPOSTPARAMS	
VULNPARAM	msg
HTMLENTITYATTACKED	Form-Parameters
ATTACKTYPE	xml with double quote - script tag
ATTACKSCORE	3-Medium
ATTACKVALUE	<abc xmlns:xyz="http://www.w3.org/1999/xhtml" ><xyz:script>alert("xvczit7d")</xyz:script></abc>
METHOD	POST
ROOTCAUSEID	6f330101-cda6-b8d1-e31e-8c41adeebe99
URL	http://www.webscantest.com/bjax/servertime.php
VULNPARAMTYPE	unknown
NTOSPIDER SCANDATE	2014-06-26T08:47:27-04:00
PCREREGEX	'|\"|<|>|\;|\bonchange\s*=|\bon(?:(?:dbl)?click)\s*=|\bon(?:blur|focus)\s*=|\bon(?:submit|reset)\s*=|\bonmouse(?:over|out|down|up)\s*=|\bonkey(?:down|press|up|up)\s*=|\bon(?:(?:un)?load|error|abort|(?:mov|resiz)e|dragdrop)\s*=|\b(?:java|j|vb|live)script\:|<script[^\w]|<iframe[^\w]|<frame[^\w]|<img[^\w]|\-\->|\/*|*\/
MODSECURITY	
SNORT	
IMPERVA	cross-site-scripting

Targets-based security

Action buttons (including defend button) are disabled for scans ran against not approved for current user targets.

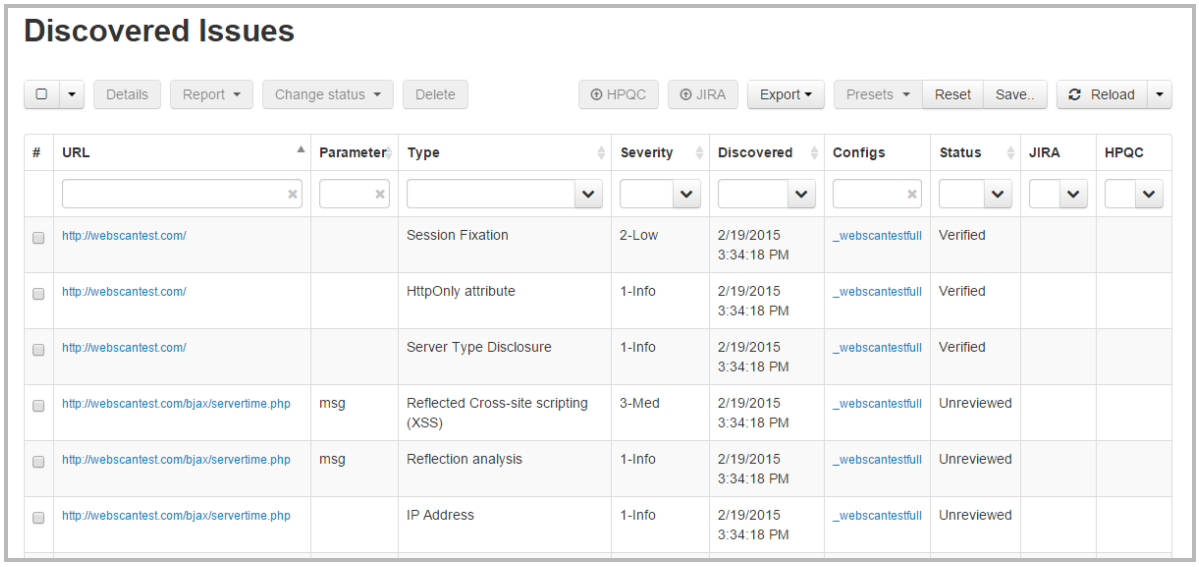
To restrict actions for such scans, instead of checkbox being visible, they are grayed out.

Targets wildcards are supported.

Findings menu

Discovered Issues

The table displays all issues of the current client.



The table contains the following columns:

- *URL*: link to issues URL (filter, sortable)
- *Parameter*: issue parameter (filter, sortable)
- *Type*: issue type (multi-select filter, sortable)
- *Severity*: issue severity (multi-select filter, sortable)
- *Discovered*: discovered date (filter, sortable)
- *Configs*: link to scan config edit page (filter)
- *Status*: issue status (multi-select filter, sortable)
- *JIRA*: displays whether the issue imported to JIRA or not.

The *JIRA* column has a tooltip: *Indicates whether a issue was imported into JIRA or not*. If an issue is imported into JIRA, the column contains an *ok* icon. The column is not sortable and has single-value dropdown filter *(Imported / Not imported*).

The column is visible if at least one JIRA server was added.

- HPQC - displays the issue imported to HPQC or not.

HPQC column has a tooltip: *Indicates whether an issue was imported into HPQC or not.*. If issue is imported into HPQC column contains ok icon. Column is not sortable, has single-value dropdown filter (**Imported** / **Not imported**).

The column is visible if only at least one HPQC server was added.

Action buttons are:

Details - opens Issues details page

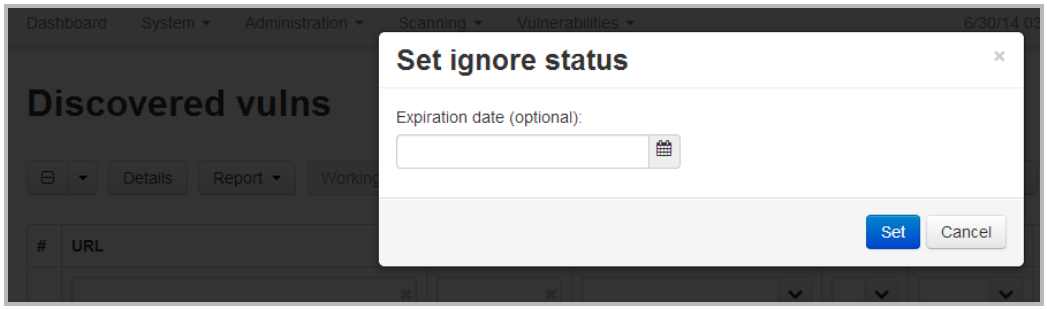
Report:

- **View** - opens the HTML report page.
- **Download** - download the report as ZIP archive.

Change status - changes the issues status. Multi-select filter with the following parameters: Fixed, Ignored, Unreviewed, Verified.

Ignored - opens popup window with **Expiration date (optional)**. User is able to set the date and apply it by clicking on Set button.

Cancel button – closes the popup window.



Delete - shows deletion dialog, enabled if one or more scans are selected; remove the scan.

HPQC - opens import dialog (title is Import into HPQC)

HPQC button is enabled only if at least one not imported issue is selected.

The button is visible if only at least one HPQC server was added.

JIRA - opens import dialog (title is *Import into JIRA*)

JIRA button is enabled only if at least one not imported issue is selected.

The button is visible if only at least one JIRA server was added.

Import findings

Import into JIRA popup window contains:

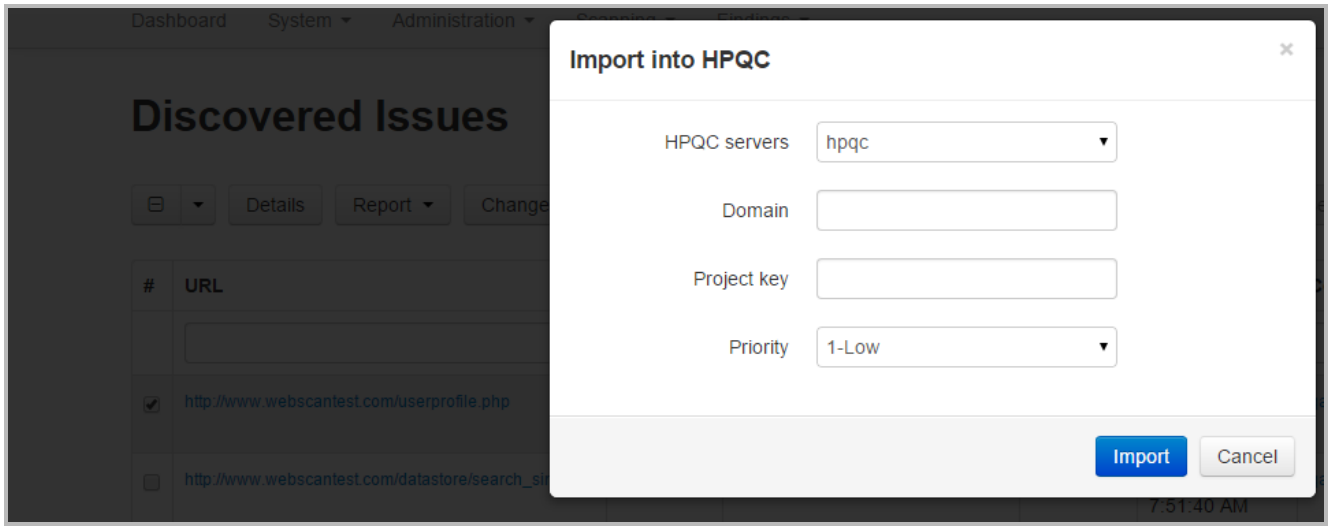
- *JIRA servers* - list of available for user JIRA servers (required);
- *Project key* - the unique key for import doman (required)

Action buttons are:

- **Cancel** - closes the popup window
- **Import** - imported selected issue to JIRA server

Clicking the **Import** button starts the import process for selected issues . While importing, set the **Import** button label to **Working**.. and buttons are disabled. After importing issues marked as imported, the grid is updated.

Import into HPQC - is the same as JIRA import with the following differences listed below.



Dialog contains:

- *HPQC servers* - list of available for user HPQC servers (required);
- *Domain* - HPQC domain (required).
- *Project key* - the unique key for import doman.
- *Priority* - imported issues priority (1-low, 2-Medium, 3-High, 4-Very high).

Export findings

Export menu contains two options: **Export to CSV** and **Export to HTML**.

Export to CSV - exports findings data to CSV file (filters are applied).

Export to HTML - exports findings data to HTML file (filters are applied). Zipped NYSE report downloaded when user select this item.

This table has pagination, **Reload / Auto reload** button and Presets options.

Targets based security

The current user sees only findings found on targets approved for that user. Target wildcards are supported.

Issues details

This page details the issues selected by the user.

The Issues details page contains the following data:

***General* information**

(*Type* - Issue type, *Severity* - issue severity, *Status* - issue status, *First seen of* - first seen date/time, *Last seen of* - last seen date/time, *ID* - issue ID).

Change button changes the status of the issue:

- *Unreviewed* - means the issue was not fixed. After the next scan, the issue status will be revised.
- *Ignore* with date - means the issue was fixed but the fix is not available on the server. Until the date, the issue status remains Ignore. After this date, the status will be revised.
- *Verified* - means the issue was verified but not fixed.
- *Fixed* - means the issue was fixed. The status will be revised after the next scan.

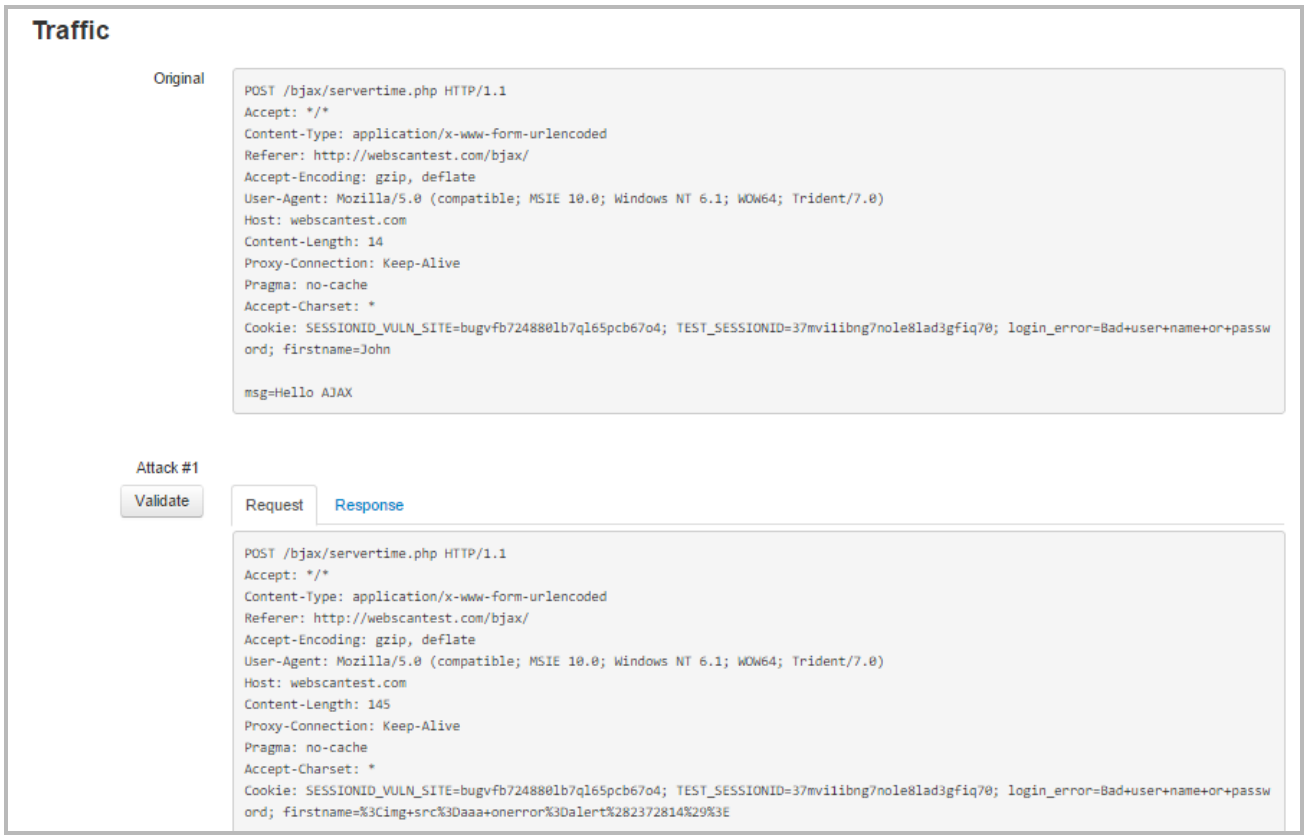
Attack information

(*Attack type* - type of attack, *URL* - vulnerable URL, *Parameter* - attack parameter, *Method* - attack method (*GET/POST*), *Attack value* - value of attack).

Traffic information

Includes original and attack traffics with *Request* and *Response* tabs.

Validate button opens Java applet with options to test the issue against the live server.



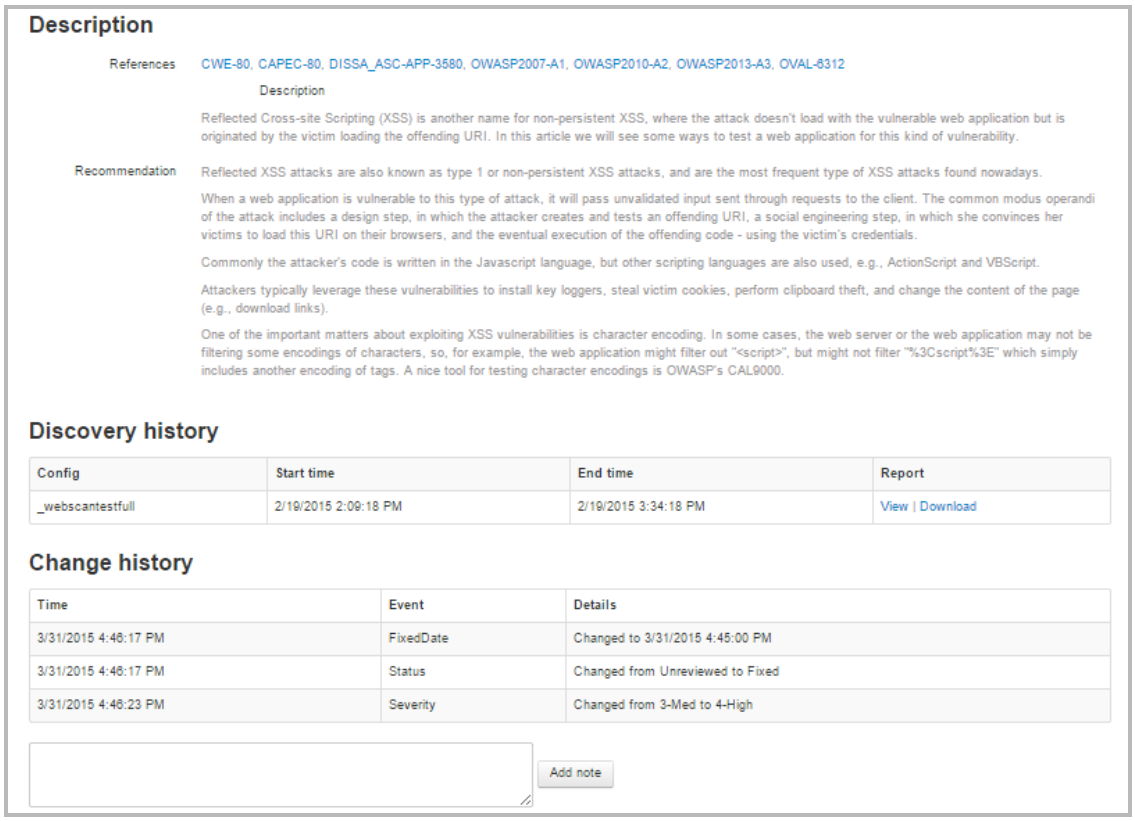
Description

Includes *References* links, attack Description, Recommendation to developers.

Discovery history

Includes a table with following columns:

- *Config* - scan config name
- *Start time* - start date/time of the scan
- *End time* - end date/time of the scan
- *Report* - links to View and Download the scan report
- *Add note* text field.



Description

References CWE-80, CAPEC-80, DISSA_ASC-APP-3580, OWASP2007-A1, OWASP2010-A2, OWASP2013-A3, OVAL-6312

Description

Reflected Cross-site Scripting (XSS) is another name for non-persistent XSS, where the attack doesn't load with the vulnerable web application but is originated by the victim loading the offending URI. In this article we will see some ways to test a web application for this kind of vulnerability.

Recommendation

Reflected XSS attacks are also known as type 1 or non-persistent XSS attacks, and are the most frequent type of XSS attacks found nowadays.

When a web application is vulnerable to this type of attack, it will pass unvalidated input sent through requests to the client. The common modus operandi of the attack includes a design step, in which the attacker creates and tests an offending URI, a social engineering step, in which she convinces her victims to load this URI on their browsers, and the eventual execution of the offending code - using the victim's credentials.

Commonly the attacker's code is written in the Javascript language, but other scripting languages are also used, e.g., ActionScript and VBScript.

Attackers typically leverage these vulnerabilities to install key loggers, steal victim cookies, perform clipboard theft, and change the content of the page (e.g., download links).

One of the important matters about exploiting XSS vulnerabilities is character encoding. In some cases, the web server or the web application may not be filtering some encodings of characters, so, for example, the web application might filter out "<script>", but might not filter "%3Cscript%3E" which simply includes another encoding of tags. A nice tool for testing character encodings is OWASP's CAL9000.

Discovery history

Config	Start time	End time	Report
_webscantestfull	2/19/2015 2:09:18 PM	2/19/2015 3:34:18 PM	View | Download

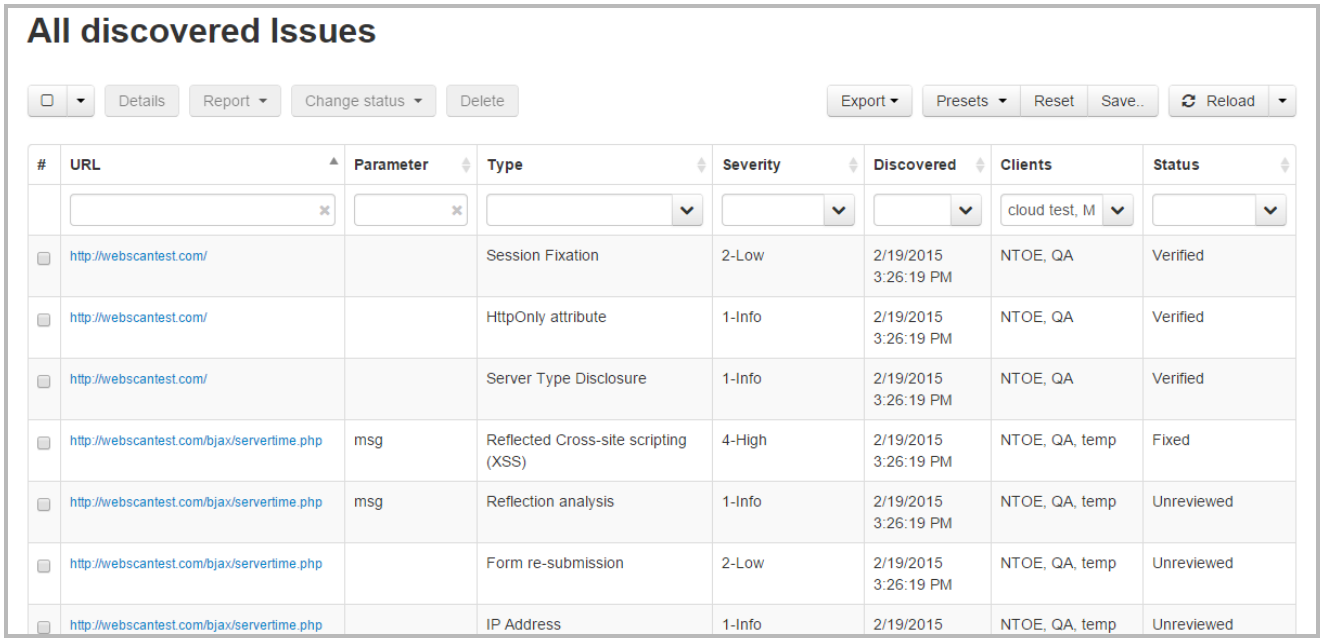
Change history

Time	Event	Details
3/31/2015 4:46:17 PM	FixedDate	Changed to 3/31/2015 4:45:00 PM
3/31/2015 4:46:17 PM	Status	Changed from Unreviewed to Fixed
3/31/2015 4:46:23 PM	Severity	Changed from 3-Med to 4-High

Add note

All discovered Issues (SA)

The table displays all issues of all clients without any restrictions by targets.



All discovered Issues

Details | Report | Change status | Delete | Export | Presets | Reset | Save.. | Reload

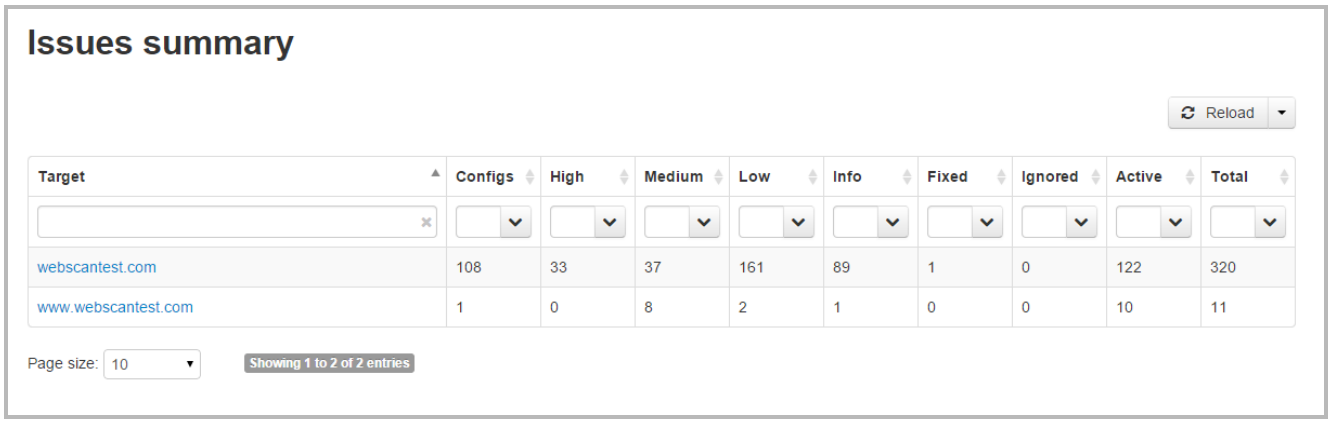
#	URL	Parameter	Type	Severity	Discovered	Clients	Status
						cloud test, M	
	http://webscantest.com/		Session Fixation	2-Low	2/19/2015 3:26:19 PM	NTOE, QA	Verified
	http://webscantest.com/		HttpOnly attribute	1-Info	2/19/2015 3:26:19 PM	NTOE, QA	Verified
	http://webscantest.com/		Server Type Disclosure	1-Info	2/19/2015 3:26:19 PM	NTOE, QA	Verified
	http://webscantest.com/bjax/servertime.php	msg	Reflected Cross-site scripting (XSS)	4-High	2/19/2015 3:26:19 PM	NTOE, QA, temp	Fixed
	http://webscantest.com/bjax/servertime.php	msg	Reflection analysis	1-Info	2/19/2015 3:26:19 PM	NTOE, QA, temp	Unreviewed
	http://webscantest.com/bjax/servertime.php		Form re-submission	2-Low	2/19/2015 3:26:19 PM	NTOE, QA, temp	Unreviewed
	http://webscantest.com/bjax/servertime.php		IP Address	1-Info	2/19/2015	NTOE, QA, temp	Unreviewed

The table displays the same data as in "*Discovered Issues*" with following changes:

- Title is *All discovered Issues*.
- No restrictions based on targets.
- *Clients* column - shows clients having this issue, multi-select filter, sortable.

Issues summary

The table displays the issues summary of the current client grouped by targets.



The table contains the following columns:

- *Target* - link to host approved for current user.
- *Configs* - count of configs related row target.
- *High*, *Medium*, *Low*, *Info* - count of issues related row target with respective severity.
- *Fixed*, *Ignored*, *Active* - count of issues related row target with respective status; *Active* means *Verified* status.
- *Total* - total count of issues related row target. May not be sum of counts by status or severity as Safe severity and Unreviewed status are missing in the grid.

This table has pagination and *Reload / Auto reload* button

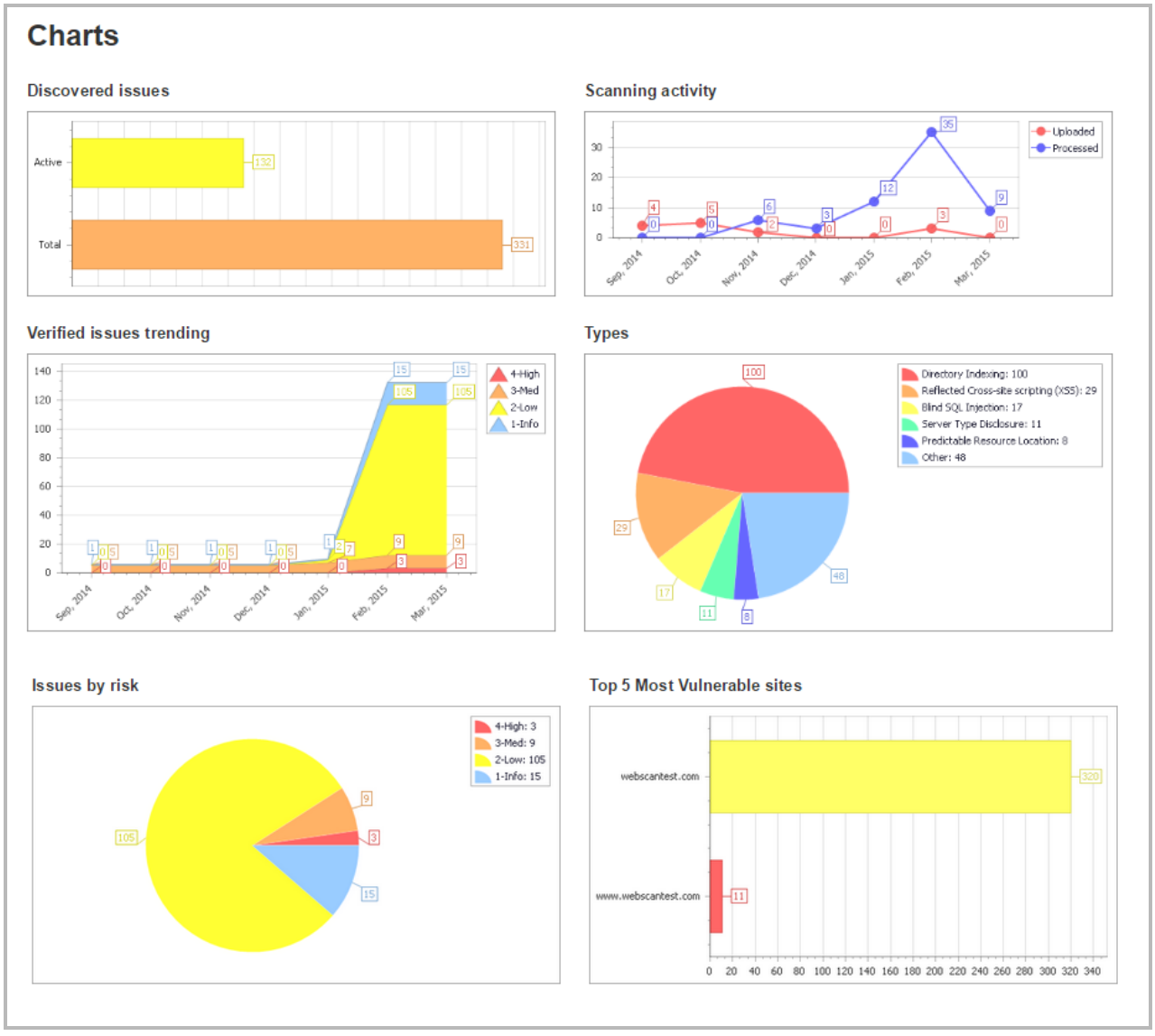
Targets based security

The current user sees only a summary for issues found on targets approved for that user.

The impersonated system admins and client admins sees all client approved targets.

Charts

The page displays issue data of the current client.



The following charts are displayed on the page:

- *Discovered Issues* – number of discovered issues in Active state and total discovered issues.
- *Scanning activity* – number of scans uploaded and processed.
- *Verified issues trending* – number of discovered issues by priority.
- *Types* – issues divided by type.
- *Issues By Risk* – issues divided by risk.
- *Top 5 Most Vulnerable Sites* – a count of discovered issues divided by top 5 most vulnerable sites for current client.

Targets based security

The current user sees only issues found on approved for that user targets. The impersonated system admins and client admins sees all client approved targets. Targets wildcards are supported.

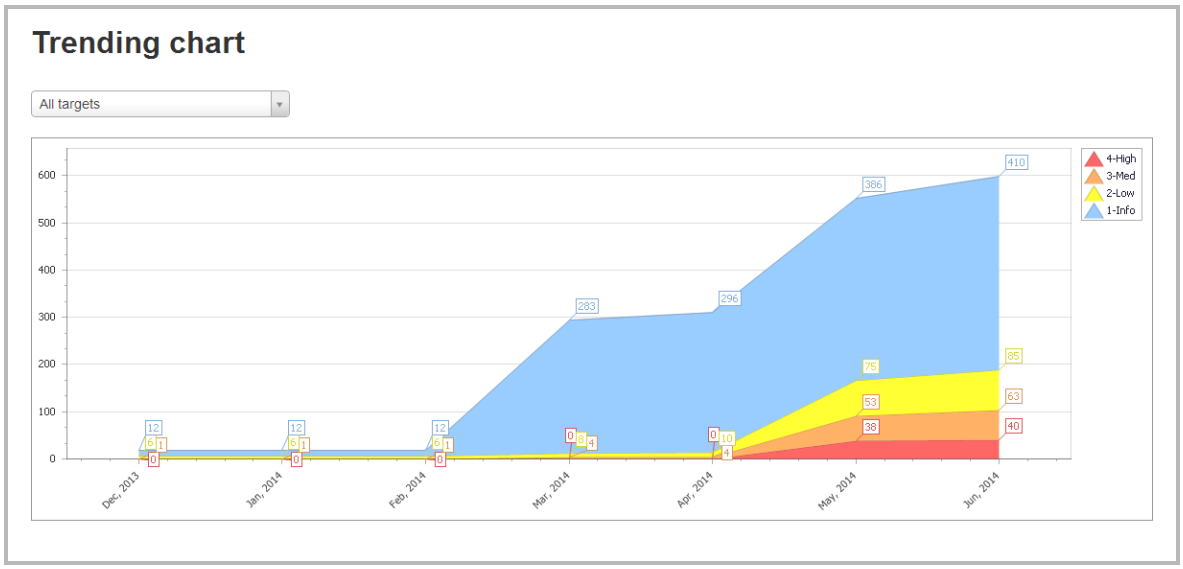
Trending chart

The page displays issues data of current client with the ability to filter by target.

The *Trending* chart displays the number of issues divided by priorities for different dates.

Targets based security

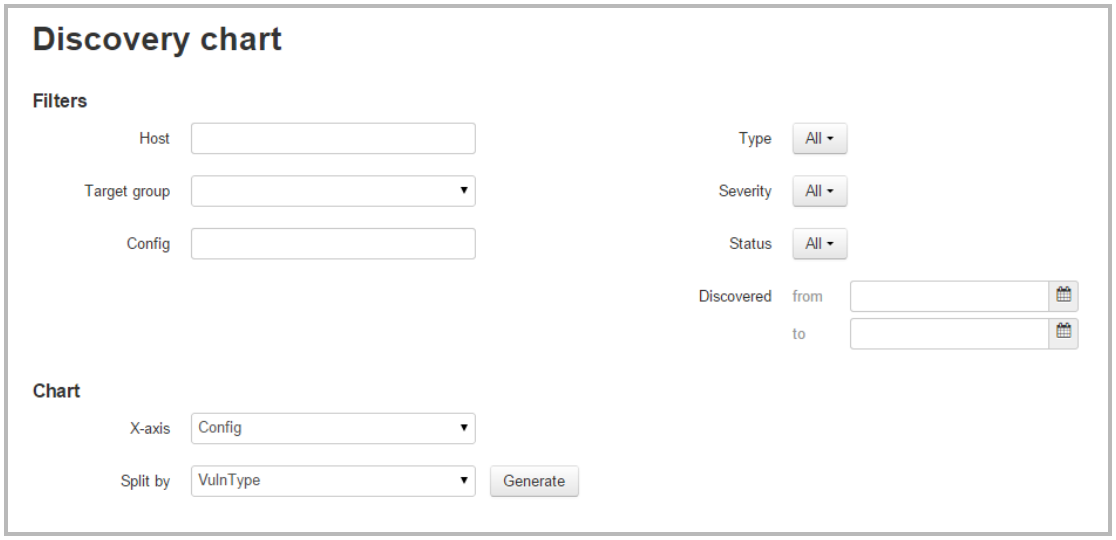
The current user sees only issues found on approved for that user targets. The targets list also contains only approved targets. The impersonated system admin sees data for all targets approved for the current client. Targets wildcards are supported.



Discovery chart

The chart displays aggregated issues data for the current client taking into account target approval statuses.

Target group filter doesn't require client admin permissions.



The discovery chart page contains the following data:

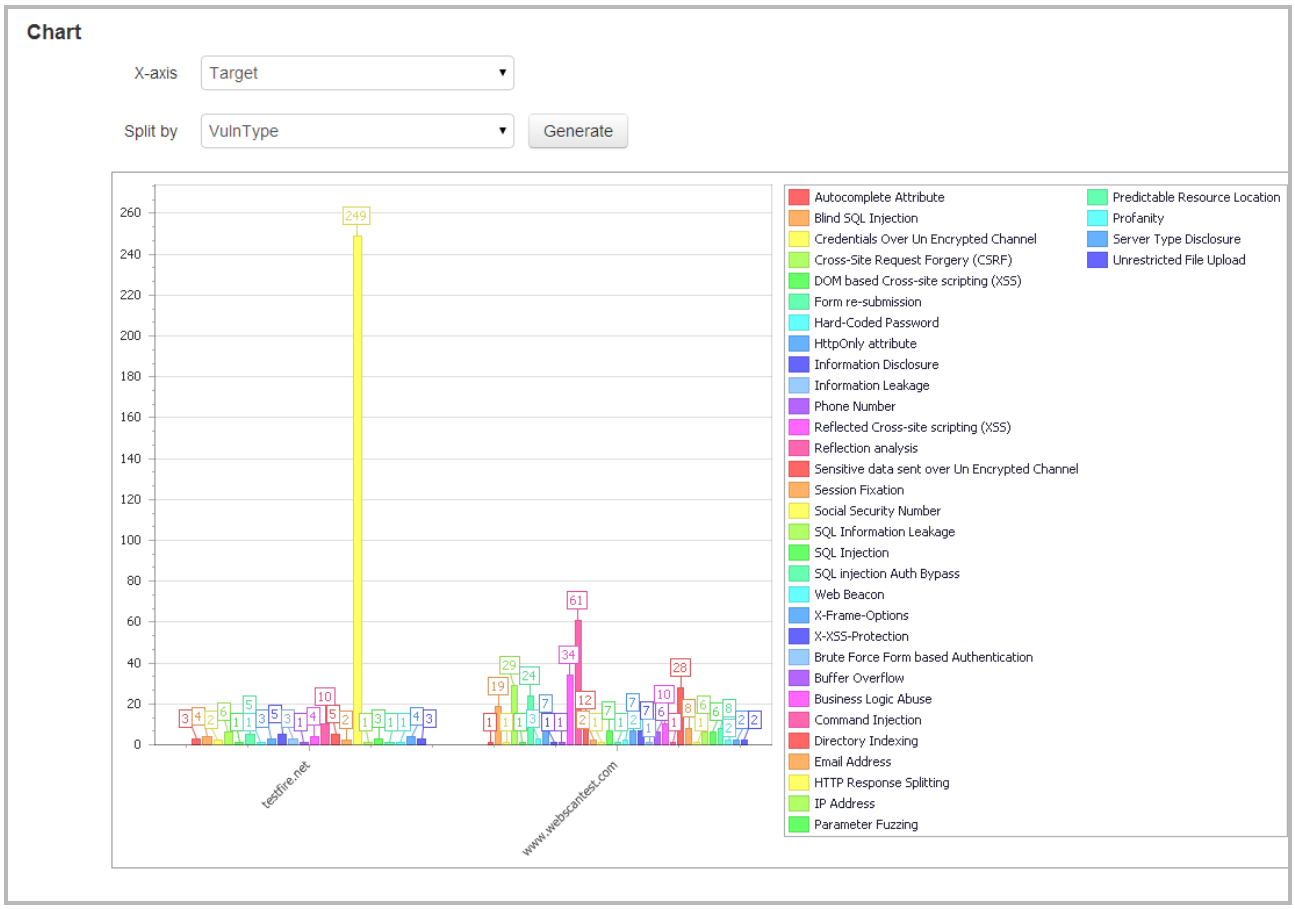
Filters:

- *Host* - to find target by hostname
- *Target group* - list of all user's target groups
- *Config* - scan config name
- *Type* - issue attack type
- *Severity* - issue severity
- *Status* - issue status
- *Discovered from/to* - discovered dates period

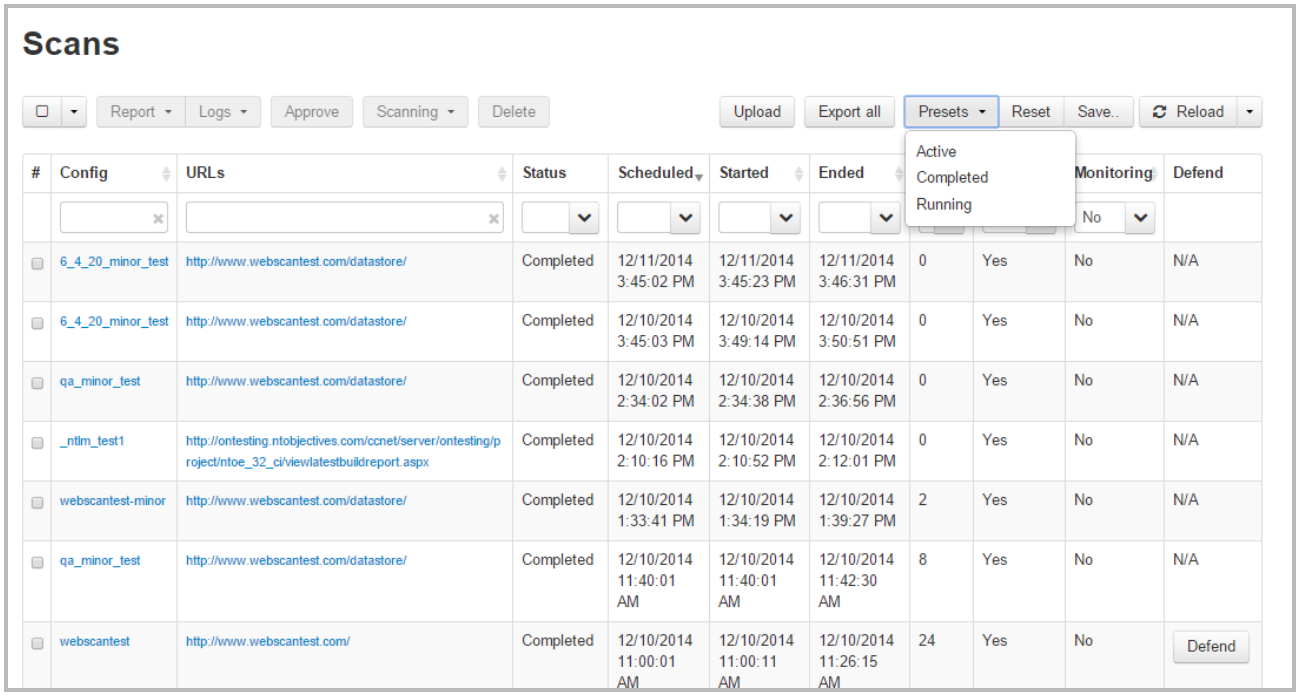
Chart:

- *X-axis* - Split by Config, Target, issue type on x-axis
- *Split by* - split by Config, Target, issue type on y-axis

User fill filters and clicks on **Generate** button. The generated graph is presented:



Presets functionality



This functionality is for saving the filter options and restoring them in one click.

Presets combo box with a list of presets, **Reset** and **Save** buttons are displayed at the top right corner. The combo box contains all presets saved for the current page and the current client.

Predefined preset filters **Active**, **Completed**, **Running** are available on *Scans*, *All scans* and *Scans for config* pages.

Click on any preset in the list loads selected filters in the combo box preset.

Save button saves information for the current page and current client.

Reset button clears all filter information for the current page.

Targets security schema

This chart summarizes the security schema used by the Portal.