

SansecReport Guide

12-2021

Guide version V1.0.2



Description

Your company is under attack. Customers have reported blocked credit cards. Google has blocked your advertisements. You have found suspicious code in the checkout. What else has been tampered with? And how did they get in?

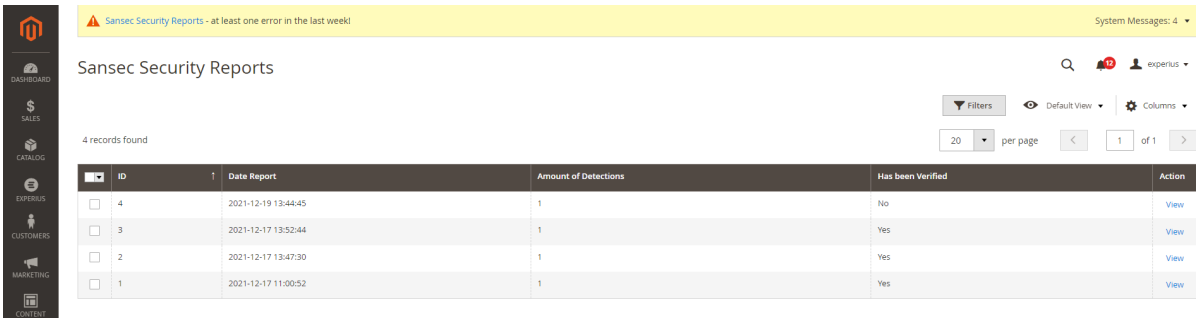
Sansec's flagship product eComscan quickly examines a store for malware, vulnerabilities and unauthorized accounts. Will scan files, databases and 3rd party modules. On average, eComscan saves a technical team 8 to 20 hours of work during the critical incident response stage.

This module creates an administrator interface for eComscan's report. This way, administrators can easily see potential vulnerabilities, malware and miscellaneous risks and quickly respond to it.

Find out more at <https://sansec.io/ecomscan>.

Grid in Administrator Panel

Under the 'System' tab, merchants can now find the 'Tools' -> 'Sansec Security Reports' page. This page shows a grid with all reports generated by the eComscan software - the amount of detections, the date and whether it has already been verified by an administrator.




ID	Date Report	Amount of Detections	Has been Verified	Action
4	2021-12-19 13:44:45	1	No	View
3	2021-12-17 13:52:44	1	Yes	View
2	2021-12-17 13:47:30	1	Yes	View
1	2021-12-17 11:00:52	1	Yes	View

View Report in Administrator Panel

When clicking on the 'View' Action in the grid, a merchant can view more information about the report. This way, all technical details about the vulnerabilities and other risks reported by eComscan can be accessed:

View Sansec Security Report #4 🔍 🔔 👤 experius ▾

← Back Verify



target [redacted]
scan_date 2021-12-19 13:36:39 UTC
scan_path [redacted]
scan_issues 1
scan_version 1.4.21
scan_min_confidence 50
scan_interactive false
scan_tag false
scan_state_file false
email_rcpts [redacted]

[Find out more information about scanning results in the support section of Sansec.io](#)

Detections

Detection

class vulnerability

source file/ [redacted] /vendor/magento/module-security/Model/AdminSessionsManager.php

description

snippet \$this->currentSession->load(\$this->authSession->getSessionId(), 'session_id')

confidence 100

path


moreinfo <https://sansec.io/kb/checks/magento-core-vulnerabilities>

timestamp 2021-12-19T13:40:36.789040Z

meta { "file_ctime": "2021-09-21T12:35:02Z", "file_mtime": "2021-07-13T21:08:00Z", "pathfilter": "Model/AdminSessionsManager.php" }

Verify Report

By using the 'Verify' button (right upper hand corner), an administrator can 'verify' the report. This way, the report won't show up in the notification messages:

 Sansec Security Reports - at least one error in the last week! System Messages: 4 ▾

Installation Guide

* = in production please use the `--keep-generated` option

Type 1: Zip file

- Unzip the zip file in `app/code/Experius`
- Enable the module by running `php bin/magento module:enable Experius_SansecReport`
- Apply database updates by running `php bin/magento setup:upgrade*`
- Flush the cache by running `php bin/magento cache:flush`

Type 2: Composer

- Make the module available in a composer repository for example:
 - private repository `repo.magento.com`
 - public repository `packagist.org`
 - public github repository as `vcs`
- Add the composer repository to the configuration by running `composer config repositories.repo.magento.com composer https://repo.magento.com/`
- Install the module composer by running `composer require experius/module-sansecreport`
- enable the module by running `php bin/magento module:enable Experius_SansecReport`
- apply database updates by running `php bin/magento setup:upgrade*`
- Flush the cache by running `php bin/magento cache:flush`

Configuration

In order to configure eComscan to publish reports to your Magento installation, two steps are required:

- Create a new Integration Bearer token via Magento:
 - System->Extension->Integrations
 - Add New Integration
 - Fill in the name as sansec and fill in your current Administrator password in the lowest field on the page
 - Under the API tab, choose Resource Access Custom. Check the field SansecReports
 - Save And Activate
 - Copy the Access Token
- Change your Sansec Cron to add the POST call (change EXAMPLEBEARERTOKEN to your copied Access Token and change the domain to your Magento store)
 - Add `--format=json | ifne curl -k -H 'Content-Type: application/json' -H 'Authorization: Bearer <bearerToken>' -d@- -X POST <magentowebshopdomain>/rest/V1/experius-sansecreport/sansecreports`
 - Example full Cron: `~/bin/ecomscan -k <key> --report <your_email> --new-only --format=json --slack <webhookurl> <store_path> | ifne curl -k -H 'Content-Type: application/json' -H 'Authorization: Bearer <bearerToken>' -d@- -X POST <magentowebshopdomain>/rest/V1/experius-sansecreport/sansecreports`

Find out more about eComscan's 5-minute installation process:

<https://sansec.io/kb/about-ecomscan/usage>