

Vulnerability Typing Use Case

Summary of steps:

1. Create Custom Field within your Kenna (CVM) Vulnerabilities table.
2. Run the **NVD_OS_vs_APP** script on GitHub

1. Create Custom Field within your Kenna (CVM) Vulnerabilities table.

A default feature of CVM (formerly Kenna.VM) is the ability to create and use custom fields. Custom fields allow you track values that are specific to your Kenna Use Case. For this example, we can create a custom field named **“Vuln Type”** with Data Type: String (Long) and Faceted Search option enabled to see the values available as filter option.

Custom Fields

Create New Custom Field

Name

Vuln Type

Description

Product

☒ VM

☐ AppSec

Data Type

☐ Attachment: upload file (.pdf, .jpg, .png, .xlsx)

☐ Date: a calendar date

☐ Dropdown: selection from list

☐ Numeric: a number, with or without decimals up to 6 digits

☐ String (Short): up to 50 characters of text

☒ String (Long): up to 500 characters of text

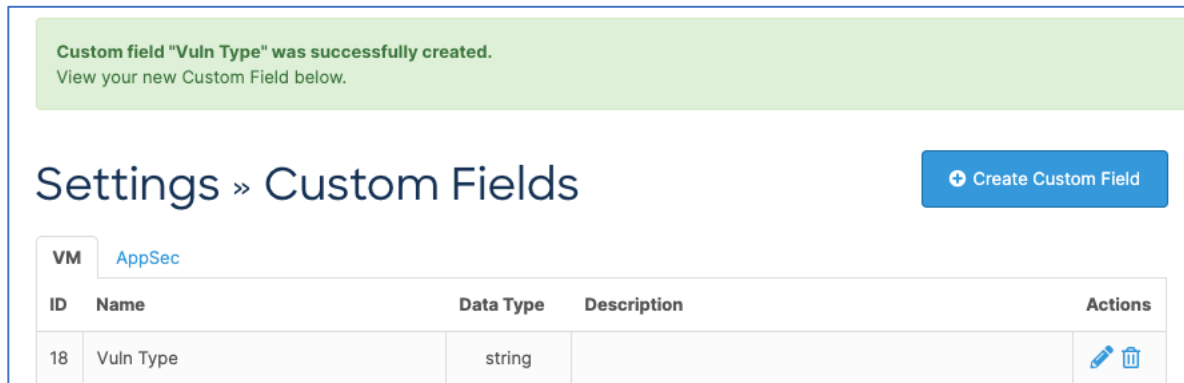
Faceted Search

☒ Generate filter options for vulnerability search

Save

Cancel

Once saved you can see that it was created, as well as the ID for your new custom field.



Please save this Custom Field ID for later in this process. (Example above: 18)
Your actual ID will be different.

Useful links:

- <https://help.kennasecurity.com/hc/en-us/articles/17308899475988-Admin-Settings-Menu-Custom-Fields-Video->
- <https://help.kennasecurity.com/hc/en-us/articles/201921738-Creating-a-Custom-Field>
- <https://help.kennasecurity.com/hc/en-us/articles/201921758-Managing-a-Custom-Field>

2. Run the NVD OS vs APP script

The script taps into the NVD database to get the CVEs classified as OS, Application, Hardware or Network using the CPE information. Also, this script taps into the customer's environment to get the CVEs pertaining to the environment which need to be tagged.

CVE ID	Type	id
CVE-1999-0524	OS	1, 2, 3
CVE-2002-0510	OS	4
CVE-2005-1794	Application	5
CVE-2017-5754	Hardware	6, 7
CVE-2010-3190	Application	8
CVE-2014-7970	OS	9, 10

The script will tag all the CVEs with the 'Type' classification using the custom field created in step#1.

The custom field can be used as a faceted search in UI and then can also be used in the API to export related data

UI -

The image shows two parts of a web application interface. The top part is a form for creating or editing a custom field. It has a 'Name' field with 'Vuln Type' entered, a 'Description' field, a 'Product' section with radio buttons for 'VM' (selected) and 'AppSec', and a 'Data Type' section with radio buttons for various types: 'Attachment: upload file (.pdf, .jpg, .png, .xlsx)', 'Date: a calendar date', 'Dropdown: selection from list', 'Numeric: a number, with or without decimals up to 6 digits', 'String (Short): up to 50 characters of text', and 'String (Long): up to 500 characters of text' (selected). Below these is a 'Faceted Search' section with a checkbox 'Generate filter options for vulnerability search' which is checked and highlighted with a red box. At the bottom are 'Save' and 'Cancel' buttons. The bottom part is a modal dialog titled 'EXPORT VULNERABILITIES'. It has a search bar, a list of checkboxes for fields to export: 'TRIAGE', 'TRIAGE END DATE', 'Vuln Type' (checked), and 'Yet another random one'. Below this is a section 'VULNERABILITY FIELDS' with checkboxes for 'Risk Score', 'CVSS Severity', and 'CVSS Threat'. At the bottom are 'Select All', 'Deselect All', and 'Continue' buttons.

API - <https://apidocs.kennasecurity.com/reference/request-data-export>

```
curl --request POST \
  --url https://api.kennasecurity.com/vulnerabilities/export \
  --header 'X-Risk-Token: [REDACTED]' \
  --header 'accept: application/json' \
  --header 'content-type: application/json' \
  --data '{
  "export_settings": {
    "format": "jsonl",
    "model": "vulnerability",
    "slim": false,
    "fields": [
      "custom_fields:Vuln Type"
    ]
  }
}
```