

# 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”**.

Custom Fields

### Create New Custom Field

Name:

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

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

Custom field "Vuln Type" was successfully created.  
View your new Custom Field below.

### Settings » Custom Fields

ID	Name	Data Type	Description	Actions
8223	Vuln Type	string		

**Please save this Custom Field ID for later in this process. (Example above: 8223)**  
**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 -

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

Export Vulnerabilities   Link to t

EXPORT VULNERABILITIES

Search...

☐ TRIAGE

☐ TRIAGE END DATE

☒ Vuln Type

☐ Yet another random one

VULNERABILITY FIELDS ▾

☐ Risk Score

☐ CVSS Severity

☐ CVSS Threat

Select All   Deselect All

Continue

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

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