```
import pandas as pd
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns
```

```
data_cve = pd.read_csv('/content/cve.csv')
data_product = pd.read_csv('/content/products.csv')
data_vendorProduct = pd.read_csv('/content/vendor_product.csv')
data_vendors = pd.read_csv('/content/vendors.csv')
```

```
data_cve.columns
```

```
Index(['Unnamed: 0', 'mod_date', 'pub_date', 'cvss', 'cwe_code', 'cwe_name',
       'summary', 'access_authentication', 'access_complexity',
       'access_vector', 'impact_availability', 'impact_confidentiality',
       'impact_integrity'],
      dtype='object')
```

```
data_product.columns
```

```
Index(['cve_id', 'vulnerable_product'], dtype='object')
```

```
data_vendorProduct.columns
```

```
Index(['Unnamed: 0', 'vendor', 'product'], dtype='object')
```

```
data_vendors.columns
```

```
Index(['Unnamed: 0', 'vendor'], dtype='object')
```

```
#data_cve
#data_product
#data_vendorProduct
#data_vendors
```

```
data_cve.head()
```

	Unnamed: 0	mod_date	pub_date	cvss	cwe_code	cwe_name	summary	access_authent
0	CVE-2019-16548	2019-11-21 15:15:00	2019-11-21 15:15:00	6.8	352	Cross-Site Request Forgery (CSRF)	A cross-site request forgery vulnerability in ...	
1	CVE-2019-16547	2019-11-21 15:15:00	2019-11-21 15:15:00	4.0	732	Incorrect Permission Assignment for Critical ...	Missing permission checks in various API endpo...	
2	CVE-2019-16546	2019-11-21 15:15:00	2019-11-21 15:15:00	4.3	639	Authorization Bypass Through User-Controlled Key	Jenkins Google Compute Engine Plugin 4.1.1 and...	
3	CVE-2013-2092	2019-11-20 21:22:00	2019-11-20 21:15:00	4.3	79	Improper Neutralization of Input During Web P...	Cross-site Scripting (XSS) in Dolibarr ERP/CRM...	
4	CVE-2013-2091	2019-11-20 20:15:00	2019-11-20 20:15:00	7.5	89	Improper Neutralization of Special Elements u...	SQL injection vulnerability in Dolibarr ERP/CR...	

Next steps: View recommended plots

```
data_product.head()
```

	cve_id	vulnerable_product
0	CVE-2019-16548	google_compute_engine
1	CVE-2019-16547	google_compute_engine
2	CVE-2019-16546	google_compute_engine
3	CVE-2013-2092	dolibarr
4	CVE-2013-2091	dolibarr

```
data_product.tail()
```

	cve_id	vulnerable_product
180580	CVE-2007-6444	NaN
180581	CVE-2007-6443	NaN
180582	CVE-2007-6442	NaN
180583	CVE-2007-6370	NaN
180584	CVE-2007-3004	NaN

```
data_cve.tail()
```

	Unnamed: 0	mod_date	pub_date	cvss	cwe_code	cwe_name	summary	access_auth
89655	CVE-2007-6444	2008-01-10 05:00:00	2007-12-19 22:46:00	5.0	20	Improper Input Validation	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER...	
89656	CVE-2007-6443	2008-01-10 05:00:00	2007-12-19 22:46:00	5.0	119	Improper Restriction of Operations within the...	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER...	
89657	CVE-2007-6442	2008-01-10 05:00:00	2007-12-19 22:46:00	5.0	119	Improper Restriction of Operations within the...	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER...	
89658	CVE-2007-6370	2008-01-10 05:00:00	2007-12-15 01:46:00	5.0	119	Improper Restriction of Operations within the...	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER...	
89659	CVE-2007-3004	2008-01-10 05:00:00	2007-06-04 17:30:00	5.0	119	Improper Restriction of Operations within the...	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER...	

```
data_vendorProduct.head()
```

	Unnamed: 0	vendor	product
0	0	jenkins	google_compute_engine
1	1	dolibarr	dolibarr
2	2	mediawiki	mediawiki
3	3	debian	debian_linux
4	4	redhat	enterprise_linux

Next steps: View recommended plots

```
data_vendorProduct.tail()
```

	Unnamed: 0	vendor	product
43076	43076	coxco_support	midicart_asp
43077	43077	coxco_support	midicart_asp_maxi
43078	43078	coxco_support	midicart_asp_plus
43079	43079	coxco_support	salescart-pro
43080	43080	coxco_support	salescart-std

```
data_vendors.head()
```

	Unnamed: 0	vendor
0	CVE-2019-16548	jenkins
1	CVE-2019-16547	jenkins
2	CVE-2019-16546	jenkins
3	CVE-2013-2092	dolibarr
4	CVE-2013-2091	dolibarr

```
data_vendors.tail()
```

	Unnamed: 0	vendor
101653	CVE-2007-6444	NaN
101654	CVE-2007-6443	NaN
101655	CVE-2007-6442	NaN
101656	CVE-2007-6370	NaN
101657	CVE-2007-3004	NaN

```
#data_cve
#data_product
#data_vendorProduct
#data_vendors
```

```
data_cve.isnull().sum()
```

```
Unnamed: 0                0
mod_date                  0
pub_date                  0
cvss                      0
cwe_code                  0
cwe_name                  0
summary                   0
access_authentication   884
access_complexity       884
access_vector           884
impact_availability     884
impact_confidentiality  884
impact_integrity        884
dtype: int64
```

```
data_cve = data_cve.dropna()
```

```
data_cve = data_cve.dropna()
```

```
data_cve.isnull().sum()
```

```
Unnamed: 0              0
mod_date                0
pub_date                0
cvss                    0
```

```
cwe_code                  0
cwe_name                  0
summary                   0
access_authentication     0
access_complexity         0
access_vector             0
impact_availability       0
impact_confidentiality    0
impact_integrity          0
dtype: int64
```

```
data_product.isnull().sum()
```

```
cve_id                 0
vulnerable_product    42
dtype: int64
```

```
data_product.shape
```

```
(180585, 2)
```

```
data_product = data_product.dropna()
```

```
data_product.isnull().sum()
```

```
cve_id                0
vulnerable_product    0
dtype: int64
```

```
data_vendorProduct.isnull().sum()
```

```
Unnamed: 0    0
vendor        0
product       0
dtype: int64
```

```
data_vendors.isnull().sum()
```

```
Unnamed: 0     0
vendor        42
dtype: int64
```

```
data_vendors = data_vendors.dropna()
```

```
data_vendors.isnull().sum()
```

```
Unnamed: 0    0
vendor        0
dtype: int64
```

```
data_cve['Unnamed: 0']
```

```
138       CVE-2019-2211
139       CVE-2019-2212
140       CVE-2019-2213
149       CVE-2019-2214
150      CVE-2019-18793
              ...
89639     CVE-2004-2182
89640     CVE-2003-1562
89641     CVE-2002-2230
89642     CVE-2002-1991
89643     CVE-2002-1432
Name: Unnamed: 0, Length: 88776, dtype: object
```

```
data_cve.rename(columns={'Unnamed: 0': 'cve_id'}, inplace=True)
```

```
data_vendorProduct.rename(columns={'Unnamed: 0': 'index_VP'}, inplace=True)
```

```
data_vendors.rename(columns={'Unnamed: 0': 'index_V'}, inplace=True)
```

```
data_cve.columns
```

```
Index(['cve_id', 'mod_date', 'pub_date', 'cvss', 'cwe_code', 'cwe_name',
       'summary', 'access_authentication', 'access_complexity',
       'access_vector', 'impact_availability', 'impact_confidentiality',
       'impact_integrity'],
      dtype='object')
```

```
data_cve['access_authentication'].unique()
```

```
array(['NONE', 'SINGLE', 'MULTIPLE'], dtype=object)
```

```
data_cve['access_complexity'].unique()
```

```
array(['LOW', 'MEDIUM', 'HIGH'], dtype=object)
```

```
data_cve['access_vector'].unique()
```

```
array(['NETWORK', 'LOCAL', 'ADJACENT_NETWORK'], dtype=object)
```

```
data_cve['impact_availability'].unique()
```

```
array(['NONE', 'COMPLETE', 'PARTIAL'], dtype=object)
```

```
data_cve['impact_integrity'].unique()
```

```
array(['NONE', 'COMPLETE', 'PARTIAL'], dtype=object)
```

```
data_cve['cvss'].unique()
```

```
array([ 7.8,  4.9,  6.9,  7.2,  4.3,  6.5,  9. ,  3.5,  5. ,  5.8,  7.5,
        6.8,  4. ,  6. ,  6.4,  2.1,  9.3,  8.5,  7.1,  6.3, 10. ,  2.7,
        2.6,  7.7,  5.5,  3.6,  1.9,  4.6,  1.2,  5.2,  4.4,  3.3,  8.3,
        7.9,  2.9,  6.1,  5.1,  6.6,  4.7,  5.4,  7.6,  5.6,  4.1,  6.2,
        4.8,  5.7,  3.8,  1.7,  1.5,  9.4,  2.3,  3.7,  9.7,  8.7,  8.8,
        6.7,  8. ,  7. ,  3.2,  7.4,  5.9,  7.3,  1.8,  0. ,  3. ,  8.2,
        5.3,  2.4,  1.3,  2.8])
```

```
data_cve.describe()
```

	cvss	cwe_code
count	88776.000000	88776.000000
mean	6.027253	198.775716
std	1.994037	174.976212
min	0.000000	1.000000
25%	4.300000	79.000000
50%	5.800000	119.000000
75%	7.500000	284.000000
max	10.000000	1188.000000

```
#df['Category'].value_counts()
impact_integrity = data_cve['impact_integrity'].value_counts()
```

```
categoricalData_cve = ['access_authentication', 'access_complexity', 'access_vector' , 'impact_availability' , 'impact_confidentiality',
```

```
for x in categoricalData_cve:
  print(data_cve[x].value_counts())
  print(";"*10)
```

```
access_authentication
NONE        76777
SINGLE      11976
MULTIPLE       23
Name: count, dtype: int64
;;;;;;;;;;
access_complexity
LOW       45746
```

```
MEDIUM    40565
HIGH       2465
Name: count, dtype: int64
;;;;;;;;;;
access_vector
NETWORK             76104
LOCAL               10053
ADJACENT_NETWORK     2619
Name: count, dtype: int64
;;;;;;;;;;
impact_availability
PARTIAL     35991
NONE        32491
COMPLETE    20294
Name: count, dtype: int64
;;;;;;;;;;
impact_confidentiality
PARTIAL     42039
NONE        29319
COMPLETE    17418
Name: count, dtype: int64
;;;;;;;;;;
impact_integrity
PARTIAL     46357
NONE        25556
COMPLETE    16863
Name: count, dtype: int64
;;;;;;;;;;
```

```
data_cve
```

	cve_id	mod_date	pub_date	cvss	cwe_code	cwe_name	summar
138	CVE-2019-2211	2019-11-14 21:36:00	2019-11-13 18:15:00	7.8	89	Improper Neutralization of Special Elements u...	createProjectionMapForQue of TvProvider.j
139	CVE-2019-2212	2019-11-14 21:30:00	2019-11-13 18:15:00	4.9	200	Information Exposure	In poisson_distribution random, there is an
140	CVE-2019-2213	2019-11-14 21:24:00	2019-11-13 18:15:00	6.9	416	Use After Free	In binder_free_transaction binder.c, there
149	CVE-2019-2214	2019-11-14 21:19:00	2019-11-13 18:15:00	7.2	269	Improper Privilege Management	In binder_transaction binder.c, there is a
150	CVE-2019-18793	2019-11-14 21:14:00	2019-11-13 20:15:00	4.3	79	Improper Neutralization of Input During Web P...	Parallels Plesk Panel 9 allows XSS in target
...	...	...	...	...	...	...	
89639	CVE-2004-2182	2008-09-05 04:00:00	2004-12-31 05:00:00	7.5	287	Improper Authentication	Session fixation vulnerabili in Macromedia J
89640	CVE-2003-1562	2008-09-05 04:00:00	2003-12-31 05:00:00	7.6	362	Concurrent Execution using Shared Resource wi...	sshd in OpenSSH 3.6.1p and earlier, when Perm
89641	CVE-2002-2230	2008-09-05 04:00:00	2002-12-31 05:00:00	4.3	79	Improper Neutralization of Input During Web P...	Cross-site scripting (XS vulnerability in Ik
89642	CVE-2002-1991	2008-09-05 04:00:00	2002-12-31 05:00:00	7.5	94	Improper Control of Generation of Code ('Code...	PHP file inclusion vulnerabili in osCommerce
89643	CVE-2002-1432	2008-09-05 04:00:00	2003-04-11 04:00:00	5.0	200	Information Exposure	MidiCart stores th midicart.mdb database file

88776 rows × 13 columns

```
data_product
```

	cve_id	vulnerable_product
0	CVE-2019-16548	google_compute_engine
1	CVE-2019-16547	google_compute_engine
2	CVE-2019-16546	google_compute_engine
3	CVE-2013-2092	dolibarr
4	CVE-2013-2091	dolibarr
...	...	...
180564	CVE-2002-1432	midicart_asp
180565	CVE-2002-1432	midicart_asp_maxi
180566	CVE-2002-1432	midicart_asp_plus
180567	CVE-2002-1432	salescart-pro
180568	CVE-2002-1432	salescart-std

180543 rows × 2 columns

```
data_vendorProduct
```

	index_VP	vendor	product
0	0	jenkins	google_compute_engine
1	1	dolibarr	dolibarr
2	2	mediawiki	mediawiki
3	3	debian	debian_linux
4	4	redhat	enterprise_linux
...	...	...	...
43076	43076	coxco_support	midicart_asp
43077	43077	coxco_support	midicart_asp_maxi
43078	43078	coxco_support	midicart_asp_plus
43079	43079	coxco_support	salescart-pro
43080	43080	coxco_support	salescart-std

43081 rows × 3 columns

Next steps: View recommended plots

```
data_vendors
```

	index_V	vendor
0	CVE-2019-16548	jenkins
1	CVE-2019-16547	jenkins
2	CVE-2019-16546	jenkins
3	CVE-2013-2092	dolibarr
4	CVE-2013-2091	dolibarr
...	...	...
101637	CVE-2004-2182	macromedia
101638	CVE-2003-1562	openbsd
101639	CVE-2002-2230	ikonboard
101640	CVE-2002-1991	oscommerce
101641	CVE-2002-1432	coxco_support

101616 rows × 2 columns

```
#merged_df = df1.merge(df2, on='id').merge(df3, on='id').merge(df4, on='id')
#data_product data_cve
```

```
cveId = data_product[data_product['cve_id'].duplicated()]
```

```
cveId
```

	cve_id	vulnerable_product
6	CVE-2013-1817	debian_linux
7	CVE-2013-1817	enterprise_linux
8	CVE-2013-1817	fedora
10	CVE-2013-1816	debian_linux
11	CVE-2013-1816	enterprise_linux
...	...	...
180564	CVE-2002-1432	midicart_asp
180565	CVE-2002-1432	midicart_asp_maxi
180566	CVE-2002-1432	midicart_asp_plus
180567	CVE-2002-1432	salescart-pro
180568	CVE-2002-1432	salescart-std

90925 rows × 2 columns

Next steps: View recommended plots

```
#foreign key is in the data_product , primary key is in data_cve
```

```
mergeData_cve_product = data_cve.merge(data_product, on='cve_id')
```

```
mergeData_cve_product.head(10)
```

	cve_id	mod_date	pub_date	cvss	cwe_code	cwe_name	summary	a
0	CVE-2019-2211	2019-11-14 21:36:00	2019-11-13 18:15:00	7.8	89	Improper Neutralization of Special Elements u...	In createProjectionMapForQuery of TvProvider.j...	
1	CVE-2019-2212	2019-11-14 21:30:00	2019-11-13 18:15:00	4.9	200	Information Exposure	In poisson_distribution of random, there is an...	
2	CVE-2019-2213	2019-11-14 21:24:00	2019-11-13 18:15:00	6.9	416	Use After Free	In binder_free_transaction of binder.c, there ...	
3	CVE-2019-2214	2019-11-14 21:19:00	2019-11-13 18:15:00	7.2	269	Improper Privilege Management	In binder_transaction of binder.c, there is a ...	
4	CVE-2019-18793	2019-11-14 21:14:00	2019-11-13 20:15:00	4.3	79	Improper Neutralization of Input During Web P...	Parallels Plesk Panel 9.5 allows XSS in target...	
5	CVE-2019-18646	2019-11-14 20:57:00	2019-11-14 15:15:00	6.5	89	Improper Neutralization of Special Elements u...	The Untangle NG firewall 14.2.0 is vulnerable ...	
6	CVE-2019-16950	2019-11-14 20:45:00	2019-11-13 19:15:00	4.3	79	Improper Neutralization of Input During Web P...	An XSS issue was discovered in Enghouse Web Ch...	
7	CVE-2019-18647	2019-11-14 20:37:00	2019-11-14 15:15:00	9.0	74	Neutralization of Special Elements in Output ...	The Untangle NG firewall 14.2.0 is vulnerable ...	
8	CVE-2019-18649	2019-11-14 20:23:00	2019-11-14 15:15:00	3.5	79	Improper Neutralization of Input During Web P...	When logged in as an admin user, the Title inp...	
9	CVE-2019-18648	2019-11-14 20:19:00	2019-11-14 15:15:00	3.5	79	Improper Neutralization of Input During Web P...	When logged in as an admin user, the Untangle ...	

```
mergeData_cve_product.columns
```

```
Index(['cve_id', 'mod_date', 'pub_date', 'cvss', 'cwe_code', 'cwe_name',
       'summary', 'access_authentication', 'access_complexity',
       'access_vector', 'impact_availability', 'impact_confidentiality',
       'impact_integrity', 'vulnerable_product'],
      dtype='object')
```

```
searchTest = data_product[data_product['cve_id'] == "CVE-2019-2211"]
```

```
searchTest
```

	cve_id	vulnerable_product
233	CVE-2019-2211	android

```
mergeData_cve_product.shape
```

```
(173246, 14)
```

```
data_vendorProduct
```

	index_VP	vendor	product
0	0	jenkins	google_compute_engine
1	1	dolibarr	dolibarr
2	2	mediawiki	mediawiki
3	3	debian	debian_linux
4	4	redhat	enterprise_linux
...	...	...	...
43076	43076	coxco_support	midicart_asp
43077	43077	coxco_support	midicart_asp_maxi
43078	43078	coxco_support	midicart_asp_plus
43079	43079	coxco_support	salescart-pro
43080	43080	coxco_support	salescart-std

43081 rows × 3 columns

Next steps: View recommended plots

```
data_vendors
```

	index_V	vendor
0	CVE-2019-16548	jenkins
1	CVE-2019-16547	jenkins
2	CVE-2019-16546	jenkins
3	CVE-2013-2092	dolibarr
4	CVE-2013-2091	dolibarr
...	...	...
101637	CVE-2004-2182	macromedia
101638	CVE-2003-1562	openbsd
101639	CVE-2002-2230	ikonboard
101640	CVE-2002-1991	oscommerce
101641	CVE-2002-1432	coxco_support

101616 rows × 2 columns

```
searchTest = data_vendors[data_vendors['index_V'] == "CVE-2019-2211"]
```

```
searchTest
```

	index_V	vendor
160	CVE-2019-2211	google

```
data_vendors.rename(columns={'index_V': 'cve_id'}, inplace=True)
```

```
mergeData_cve_product = mergeData_cve_product.merge(data_vendors, on='cve_id')
```

```
searchTest = mergeData_cve_product[mergeData_cve_product['cve_id'] == "CVE-2019-2211"]
```

```
searchTest
```

	cve_id	mod_date	pub_date	cvss	cwe_code	cwe_name	summary	a
0	CVE-2019-2211	2019-11-14 21:36:00	2019-11-13 18:15:00	7.8	89	Improper Neutralization of Special Elements u...	In createProjectionMapForQuery of TvProvider.j...	

```
data_vendorProduct
```

	index_VP	vendor	product
0	0	jenkins	google_compute_engine
1	1	dolibarr	dolibarr
2	2	mediawiki	mediawiki
3	3	debian	debian_linux
4	4	redhat	enterprise_linux
...	...	...	...
43076	43076	coxco_support	midicart_asp
43077	43077	coxco_support	midicart_asp_maxi
43078	43078	coxco_support	midicart_asp_plus
43079	43079	coxco_support	salescart-pro
43080	43080	coxco_support	salescart-std

43081 rows × 3 columns

Next steps: View recommended plots

```
c = data_vendorProduct['product'].value_counts()
```

```
c
```

```
product
cms                                                                    18
internet_security                                                      13
guestbook                                                              11
gallery                                                                11
antivirus                                                              11
                                                                       ..
electronic_reception_and_examination_of_application_for_radio_licenses  1
photo_sharing_plus                                                      1
glassfish_server                                                        1
elabftw                                                                 1
salescart-std                                                           1
Name: count, Length: 40553, dtype: int64
```

```
mergeData_cve_product
```

	cve_id	mod_date	pub_date	cvss	cwe_code	cwe_name	summa
0	CVE-2019-2211	2019-11-14 21:36:00	2019-11-13 18:15:00	7.8	89	Improper Neutralization of Special Elements u...	createProjectionMapForQu of TvProvider
1	CVE-2019-2212	2019-11-14 21:30:00	2019-11-13 18:15:00	4.9	200	Information Exposure	In poisson_distribution random, there is a
2	CVE-2019-2213	2019-11-14 21:24:00	2019-11-13 18:15:00	6.9	416	Use After Free	In binder_free_transaction binder.c, there
3	CVE-2019-2214	2019-11-14 21:19:00	2019-11-13 18:15:00	7.2	269	Improper Privilege Management	In binder_transaction binder.c, there is a
4	CVE-2019-18793	2019-11-14 21:14:00	2019-11-13 20:15:00	4.3	79	Improper Neutralization of Input During Web P...	Parallels Plesk Panel allows XSS in targe
...	...	...	...	...	...	...	
241974	CVE-2002-1432	2008-09-05 04:00:00	2003-04-11 04:00:00	5.0	200	Information Exposure	MidiCart stores midicart.mdb database fil
241975	CVE-2002-1432	2008-09-05 04:00:00	2003-04-11 04:00:00	5.0	200	Information Exposure	MidiCart stores midicart.mdb database fil
241976	CVE-2002-1432	2008-09-05 04:00:00	2003-04-11 04:00:00	5.0	200	Information Exposure	MidiCart stores midicart.mdb database fil
241977	CVE-2002-1432	2008-09-05 04:00:00	2003-04-11 04:00:00	5.0	200	Information Exposure	MidiCart stores midicart.mdb database fil
241978	CVE-2002-1432	2008-09-05 04:00:00	2003-04-11 04:00:00	5.0	200	Information Exposure	MidiCart stores midicart.mdb database fil

241979 rows × 15 columns

```
mergeData_cve_product.columns
```

```
Index(['cve_id', 'mod_date', 'pub_date', 'cvss', 'cwe_code', 'cwe_name',
       'summary', 'access_authentication', 'access_complexity',
       'access_vector', 'impact_availability', 'impact_confidentiality',
       'impact_integrity', 'vulnerable_product', 'vendor'],
      dtype='object')
```

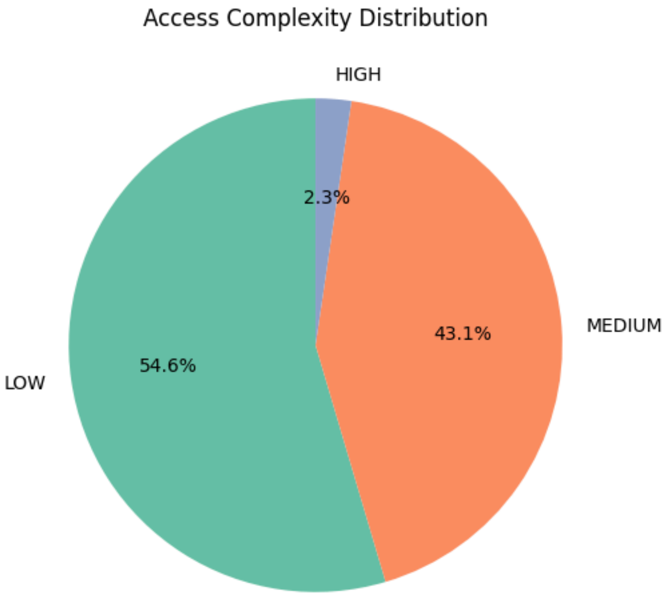
```
mergeData_cve_product['access_complexity'].unique()
```

```
array(['LOW', 'MEDIUM', 'HIGH'], dtype=object)
```

```
# Pie Chart
print(mergeData_cve_product['access_complexity'].value_counts())
access_complexity_counts = mergeData_cve_product['access_complexity'].value_counts()
plt.figure(figsize=(8, 6))
access_complexity_counts.plot.pie(autopct='%1.1f%%', startangle=90, colors=['#66c2a5', '#fc8d62', '#8da0cb'])
plt.title('Access Complexity Distribution')
plt.ylabel('')
plt.show()

```

```
access_complexity
LOW       132077
MEDIUM    104282
HIGH        5620
Name: count, dtype: int64
```



```
# Bar Plot
plt.figure(figsize=(8, 6))
sns.countplot(data=mergeData_cve_product, x='access_complexity', order=['LOW', 'MEDIUM', 'HIGH'], palette='viridis')
plt.title('Access Complexity Distribution')
plt.xlabel('Access Complexity')
plt.ylabel('Count')
plt.show()

```

```
<ipython-input-123-9b2a35ff54c6>:3: FutureWarning:
```

```


# Bar Plots
plt.figure(figsize=(18, 6))

# Bar plot for access_complexity
plt.subplot(1, 3, 1)
sns.countplot(data=mergeData_cve_product, x='access_complexity', order=['LOW', 'MEDIUM', 'HIGH'], palette='viridis')
plt.title('Access Complexity Distribution')
plt.xlabel('Access Complexity')
plt.ylabel('Count')

# Bar plot for impact_confidentiality
plt.subplot(1, 3, 2)
sns.countplot(data=mergeData_cve_product, x='impact_confidentiality', order=['NONE', 'PARTIAL', 'COMPLETE'], palette='viridis')
plt.title('Impact Confidentiality Distribution')
plt.xlabel('Impact Confidentiality')
plt.ylabel('Count')

# Bar plot for impact_integrity
plt.subplot(1, 3, 3)
sns.countplot(data=mergeData_cve_product, x='impact_integrity', order=['NONE', 'PARTIAL', 'COMPLETE'], palette='viridis')
plt.title('Impact Integrity Distribution')
plt.xlabel('Impact Integrity')
plt.ylabel('Count')

# Display the plots
plt.tight_layout()
plt.show()

# Pie Charts
fig, axes = plt.subplots(1, 3, figsize=(18, 6))

# Pie chart for access_complexity
access_complexity_counts = mergeData_cve_product['access_complexity'].value_counts()
access_complexity_counts.plot.pie(ax=axes[0], autopct='%1.1f%%', startangle=90, colors=['#66c2a5', '#fc8d62', '#8da0cb'])
axes[0].set_title('Access Complexity Distribution')
axes[0].set_ylabel('')

# Pie chart for impact_confidentiality
impact_confidentiality_counts = mergeData_cve_product['impact_confidentiality'].value_counts()
impact_confidentiality_counts.plot.pie(ax=axes[1], autopct='%1.1f%%', startangle=90, colors=['#66c2a5', '#fc8d62', '#8da0cb'])
axes[1].set_title('Impact Confidentiality Distribution')
axes[1].set_ylabel('')

# Pie chart for impact_integrity
impact_integrity_counts = mergeData_cve_product['impact_integrity'].value_counts()
impact_integrity_counts.plot.pie(ax=axes[2], autopct='%1.1f%%', startangle=90, colors=['#66c2a5', '#fc8d62', '#8da0cb'])
axes[2].set_title('Impact Integrity Distribution')
axes[2].set_ylabel('')

# Display the plots
plt.tight_layout()
plt.show()

```

```
<ipython-input-124-009fac00649a>:6: FutureWarning:

Passing `palette` without assigning `hue` is deprecated and will be removed in v0.14.0.

  sns.countplot(data=mergeData_cve_product, x='access_complexity', order=['LOW', 'MEDIU
<ipython-input-124-009fac00649a>:13: FutureWarning:

Passing `palette` without assigning `hue` is deprecated and will be removed in v0.14.0.
```