Data adjustment + enrichment

In [ ]:

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


df = pd.read_csv("./irius_threats_microservice.csv")

df
```

Out[ ]:

	Component	Use Case	Source	Threat	Risk response	Inherent Risk	Current Risk	Countermeasure Progress	Weakness Tests
0	API gateway	Authentication and Authorization	Created by rules engine	Authentication Bypass	Planned Mitigation: 0%. Mitigated: 0%. Unmitig...	High	High	0%	Not tested
1	API gateway	Logging and Monitoring	Created by rules engine	Exploitation of insufficient logging and monit...	Planned Mitigation: 0%. Mitigated: 0%. Unmitig...	High	High	0%	Not tested
2	Catalog DB	Access service	Created by rules engine	Attackers gain access to unauthorised data by ...	Planned Mitigation: 0%. Mitigated: 0%. Unmitig...	Critical	Critical	0%	Not tested
3	Catalog DB	Access service	Created by rules engine	Authentication Bypass	Planned Mitigation: 0%. Mitigated: 0%. Unmitig...	High	High	0%	Not tested
4	Catalog DB	Access service	Created by rules engine	Data leakage or disclosure to unauthorized par...	Planned Mitigation: 0%. Mitigated: 0%. Unmitig...	High	High	0%	Not tested
...	...	...	...	...	...	...	...	...	...
123	Web Client	General	Created by rules engine	An adversary embeds malicious scripts in conte...	Planned Mitigation: 0%. Mitigated: 0%. Unmitig...	High	High	0%	Not tested
124	Web Client	General	Created by rules engine	Application contains security vulnerabilities ...	Planned Mitigation: 0%. Mitigated: 0%. Unmitig...	Critical	Critical	0%	Not tested
125	Web Client	General	Created by rules engine	Attackers gain unauthorised access to data or ...	Planned Mitigation: 0%. Mitigated: 0%. Unmitig...	Critical	Critical	0%	Not tested
126	Web Client	General	Created by rules engine	Attackers gain unauthorised access to the appl...	Planned Mitigation: 0%. Mitigated: 0%. Unmitig...	High	High	0%	Not tested
127	Web Client	Read or Post data	Created by rules engine	Attackers could gain access to sensitive data ...	Planned Mitigation: 0%. Mitigated: 0%. Unmitig...	Critical	Critical	0%	Not tested

128 rows × 12 columns

Print All Threats

In [ ]:

```
threats = df["Threat"]
threats_unique = df["Threat"].unique()

print(threats.tolist())
print(len(threats))
```

```
['Authentication Bypass', 'Exploitation of insufficient logging and monitoring', 'Attackers gain access to unaut
horised data by exploiting vulnerabilities in the service', 'Authentication Bypass', 'Data leakage or disclosure
to unauthorized parties', 'Attackers who compromise the application or application server could directly access
and modify the data store', 'Sensitive data is exposed through weak security configurations', 'Attackers use kno
wn cloud vulnerabilities to access unauthorized data', 'Excessive Allocation', 'Attackers compromise images by m
odifying their content', 'Attackers gain access to the sensitive data through injecting code in the repositories
', 'Availability is compromised through attacks against scalability configuration', 'Sensitive data is compromis
ed by unauthorized access to container volumes', 'Exploitation of insufficient logging and monitoring', 'Sensiti
ve data is compromised through network access', 'Attackers gain unauthorised access to data and/or systems throu
gh SQL Injection attacks', 'Attackers gain access to unauthorised data by exploiting vulnerabilities in the serv
ice', 'Authentication Bypass', 'Data leakage or disclosure to unauthorized parties', 'Attackers who compromise t
he application or application server could directly access and modify the data store', 'Sensitive data is expose
d through weak security configurations', 'Attackers use known cloud vulnerabilities to access unauthorized data'
, 'Excessive Allocation', 'Attackers compromise images by modifying their content', 'Attackers gain access to th
e sensitive data through injecting code in the repositories', 'Availability is compromised through attacks again
st scalability configuration', 'Sensitive data is compromised by unauthorized access to container volumes', 'Exp
loitation of insufficient logging and monitoring', 'Sensitive data is compromised through network access', 'Atta
ckers gain unauthorised access to data and/or systems through SQL Injection attacks', 'An adversary embeds malic
ious scripts in content that will be served to web browsers', 'Application contains security vulnerabilities not
identified during the development process', 'Attackers gain unauthorised access to data by compromising third pa
rty web resources', 'Attackers gain unauthorised access to data or services by accessing a client side secret',
'Attackers gain unauthorised access to the application by the use of deprecated client-side technologies', 'An a
dversary embeds malicious scripts in content that will be served to web browsers', 'Attackers could gain access
to sensitive data through a man in the middle attack', 'Privilege Abuse', 'Attackers cause users to peform arbit
rary clicks on the site through ClickJacking attacks', 'Sensitive data is exposed through weak security configur
ations', 'Attackers use known cloud vulnerabilities to access unauthorized data', 'Excessive Allocation', 'Attac
kers compromise images by modifying their content', 'Attackers gain access to the sensitive data through injecti
ng code in the repositories', 'Availability is compromised through attacks against scalability configuration', '
Sensitive data is compromised by unauthorized access to container volumes', 'Exploitation of insufficient loggin
g and monitoring', 'Sensitive data is compromised through network access', 'Attackers gain access to unauthorise
d data by exploiting vulnerabilities in the service', 'Authentication Bypass', 'Data leakage or disclosure to un
authorized parties', 'Attackers who compromise the application or application server could directly access and m
odify the data store', 'Sensitive data is exposed through weak security configurations', 'Attackers use known cl
oud vulnerabilities to access unauthorized data', 'Excessive Allocation', 'Attackers compromise images by modify
ing their content', 'Attackers gain access to the sensitive data through injecting code in the repositories', 'A
vailability is compromised through attacks against scalability configuration', 'Sensitive data is compromised by
unauthorized access to container volumes', 'Exploitation of insufficient logging and monitoring', 'Sensitive dat
a is compromised through network access', 'Attackers gain unauthorised access to data and/or systems through SQL
Injection attacks', 'An attacker could send malicious push notifications, leading to unauthorized actions, data
breaches, or phishing attacks', 'Attackers could gain access to sensitive data through a man in the middle attac
k', 'Attackers gain unauthorised access to data and/or systems through SQL Injection attacks', 'Attackers gain u
nauthorized access to the control of the environment', 'Attackers gain unauthorized access to the user account d
ue to the lack of configuration of the account', 'Attackers perform a Denial of Service (DoS)', 'Data is intenti
onally or accidentally deleted', 'An attacker attempts to invoke all common switches and options to discover wea
knesses', 'Application contains security vulnerabilities not identified during the development process', "Attack
er gains access to sensitive data by modifying the application's expected behavior", 'Users lose trust in the ap
plication because it requests unnecessary privileges', 'Accessing Functionality Not Properly Constrained by ACLs
', 'Attackers gain access to the data through the WebView functionality', 'Attackers gain unauthorised access to
the application through an error handling flaw', 'Attackers gain unauthorised access to the application through
buffer overflow flaws', 'An adversary embeds malicious scripts in content that will be served to web browsers',
'Application contains security vulnerabilities not identified during the development process', 'Attackers gain u
nauthorised access to data by compromising third party web resources', 'Attackers gain unauthorised access to da
ta or services by accessing a client side secret', 'Attackers gain unauthorised access to the application by the
use of deprecated client-side technologies', 'An adversary embeds malicious scripts in content that will be serv
ed to web browsers', 'Attackers could gain access to sensitive data through a man in the middle attack', 'Privil
ege Abuse', 'Attackers cause users to peform arbitrary clicks on the site through ClickJacking attacks', 'Attack
ers gain access to unauthorised data by exploiting vulnerabilities in the service', 'Authentication Bypass', 'Da
ta leakage or disclosure to unauthorized parties', 'Attackers who compromise the application or application serv
er could directly access and modify the data store', 'Sensitive data is exposed through weak security configurat
ions', 'Attackers use known cloud vulnerabilities to access unauthorized data', 'Excessive Allocation', 'Attacke
rs compromise images by modifying their content', 'Attackers gain access to the sensitive data through injecting
code in the repositories', 'Availability is compromised through attacks against scalability configuration', 'Sen
sitive data is compromised by unauthorized access to container volumes', 'Exploitation of insufficient logging a
nd monitoring', 'Sensitive data is compromised through network access', 'Attackers gain unauthorised access to d
ata and/or systems through SQL Injection attacks', 'Attackers gain access to unauthorised data by exploiting vul
nerabilities in the service', 'Authentication Bypass', 'Data leakage or disclosure to unauthorized parties', 'At
tackers who compromise the application or application server could directly access and modify the data store', '
Sensitive data is exposed through weak security configurations', 'Attackers use known cloud vulnerabilities to a
ccess unauthorized data', 'Excessive Allocation', 'Attackers compromise images by modifying their content', 'Att
ackers gain access to the sensitive data through injecting code in the repositories', 'Availability is compromis
ed through attacks against scalability configuration', 'Sensitive data is compromised by unauthorized access to
container volumes', 'Exploitation of insufficient logging and monitoring', 'Sensitive data is compromised throug
h network access', 'Attackers gain unauthorised access to data and/or systems through SQL Injection attacks', 'S
ensitive data is exposed through weak security configurations', 'Attackers use known cloud vulnerabilities to ac
cess unauthorized data', 'Excessive Allocation', 'Attackers compromise images by modifying their content', 'Atta
ckers gain access to the sensitive data through injecting code in the repositories', 'Availability is compromise
d through attacks against scalability configuration', 'Sensitive data is compromised by unauthorized access to c
ontainer volumes', 'Exploitation of insufficient logging and monitoring', 'Sensitive data is compromised through
network access', 'An adversary embeds malicious scripts in content that will be served to web browsers', 'Applic
ation contains security vulnerabilities not identified during the development process', 'Attackers gain unauthor
ised access to data or services by accessing a client side secret', 'Attackers gain unauthorised access to the a
pplication by the use of deprecated client-side technologies', 'Attackers could gain access to sensitive data th
rough a man in the middle attack']
128
```

Add threats abbrieviations for cleaner plotting + map each threat to STRIDE nomenclature

In [ ]:

```python
threats_gpt = [
    'Authentication Bypass', 'Insufficient Logging', 'Unauthorized Data Access', 'Authentication Bypass',
    'Data Leakage', 'App Data Manipulation', 'Weak Security Config', 'Cloud Vulnerability', 'Excessive Allocati
    'Image Tampering', 'Code Injection', 'Scalability Attack', 'Container Access', 'Insufficient Logging',
    'Network Compromise', 'SQL Injection', 'Unauthorized Data Access', 'Authentication Bypass', 'Data Leakage',
    'App Data Manipulation', 'Weak Security Config', 'Cloud Vulnerability', 'Excessive Allocation', 'Image Tamp
    'Code Injection', 'Scalability Attack', 'Container Access', 'Insufficient Logging', 'Network Compromise',
    'SQL Injection', 'Cross-Site Scripting', 'Security Misconfiguration', 'Third-Party Access', 'Client-Side Se
    'Deprecated Technology', 'Cross-Site Scripting', 'Man-in-the-Middle Attack', 'Privilege Abuse', 'ClickJacki
    'Weak Security Config', 'Cloud Vulnerability', 'Excessive Allocation', 'Image Tampering', 'Code Injection',
    'Scalability Attack', 'Container Access', 'Insufficient Logging', 'Network Compromise', 'Unauthorized Data
    'Authentication Bypass', 'Data Leakage', 'App Data Manipulation', 'Weak Security Config', 'Cloud Vulnerabil
    'Excessive Allocation', 'Image Tampering', 'Code Injection', 'Scalability Attack', 'Container Access',
    'Insufficient Logging', 'Network Compromise', 'SQL Injection', 'Malicious Push Notifications', 'Man-in-the-
    'SQL Injection', 'Environment Control', 'Account Configuration Flaw', 'Denial of Service', 'Data Deletion',
    'Command Injection', 'Security Misconfiguration', 'Behavior Modification', 'Unnecessary Privileges',
    'Improper ACL Configuration', 'WebView Data Access', 'Error Handling Flaw', 'Buffer Overflow', 'Cross-Site
    'Security Misconfiguration', 'Third-Party Access', 'Client-Side Secret', 'Deprecated Technology', 'Cross-Si
    'Man-in-the-Middle Attack', 'Privilege Abuse', 'ClickJacking', 'Unauthorized Data Access', 'Authentication
    'Data Leakage', 'App Data Manipulation', 'Weak Security Config', 'Cloud Vulnerability', 'Excessive Allocati
    'Image Tampering', 'Code Injection', 'Scalability Attack', 'Container Access', 'Insufficient Logging',
    'Network Compromise', 'SQL Injection', 'Unauthorized Data Access', 'Authentication Bypass', 'Data Leakage',
    'App Data Manipulation', 'Weak Security Config', 'Cloud Vulnerability', 'Excessive Allocation', 'Image Tamp
    'Code Injection', 'Scalability Attack', 'Container Access', 'Insufficient Logging', 'Network Compromise', '
    'Weak Security Config', 'Cloud Vulnerability', 'Excessive Allocation', 'Image Tampering', 'Code Injection',
    'Scalability Attack', 'Container Access', 'Insufficient Logging', 'Network Compromise', 'Cross-Site Scripti
    'Security Misconfiguration', 'Client-Side Secret', 'Deprecated Technology', 'Man-in-the-Middle Attack'
]

threat_mapping = dict(zip(df["Threat"].unique(), threats_gpt))
df['Threat abbv'] = threats_gpt
# df['Threat'] = df['Threat'].map(threat_mapping)

# df.to_csv("output_to_check.csv",index=True)

threats_to_stride = {
    'Authentication Bypass': 'Spoofing',
    'Exploitation of insufficient logging and monitoring': 'Repudiation',
    'Attackers gain access to unauthorised data by exploiting vulnerabilities in the service': 'Information Dis
    'Data leakage or disclosure to unauthorized parties': 'Information Disclosure',
    'Attackers who compromise the application or application server could directly access and modify the data s
    'Sensitive data is exposed through weak security configurations': 'Information Disclosure',
    'Attackers use known cloud vulnerabilities to access unauthorized data': 'Information Disclosure',
    'Excessive Allocation': 'Denial of Service',
    'Attackers compromise images by modifying their content': 'Tampering',
    'Attackers gain access to the sensitive data through injecting code in the repositories': 'Information Disc
    'Availability is compromised through attacks against scalability configuration': 'Denial of Service',
    'Sensitive data is compromised by unauthorized access to container volumes': 'Information Disclosure',
    'Sensitive data is compromised through network access': 'Information Disclosure',
    'Attackers gain unauthorised access to data and/or systems through SQL Injection attacks': 'Elevation of Pr
    'An adversary embeds malicious scripts in content that will be served to web browsers': 'Elevation of Privi
    'Application contains security vulnerabilities not identified during the development process': 'Information
    'Attackers gain unauthorised access to data by compromising third party web resources': 'Information Disclo
    'Attackers gain unauthorised access to data or services by accessing a client side secret': 'Information Di
    'Attackers gain unauthorised access to the application by the use of deprecated client-side technologies':
    'Attackers could gain access to sensitive data through a man in the middle attack': 'Information Disclosure
    'Privilege Abuse': 'Elevation of Privilege',
    'Attackers cause users to perform arbitrary clicks on the site through ClickJacking attacks': 'Elevation of
    'An attacker could send malicious push notifications, leading to unauthorized actions, data breaches, or ph
    'Attackers gain unauthorized access to the control of the environment': 'Elevation of Privilege',
    'Attackers gain unauthorized access to the user account due to the lack of configuration of the account': '
    'Attackers perform a Denial of Service (DoS)': 'Denial of Service',
    'Data is intentionally or accidentally deleted': 'Tampering',
    'An attacker attempts to invoke all common switches and options to discover weaknesses': 'Information Discl
    'Attacker gains access to sensitive data by modifying the application\'s expected behavior': 'Tampering',
    'Users lose trust in the application because it requests unnecessary privileges': 'Elevation of Privilege',
    'Accessing Functionality Not Properly Constrained by ACLs': 'Elevation of Privilege',
    'Attackers gain access to the data through the WebView functionality': 'Information Disclosure',
    'Attackers gain unauthorised access to the application through an error handling flaw': 'Elevation of Privi
    'Attackers gain unauthorised access to the application through buffer overflow flaws': 'Elevation of Privil
}

df['STRIDE Category'] = df['Threat'].map(threats_to_stride)

df.head()
```

Out[ ]:

	Component	Use Case	Source	Threat	Risk response	Inherent Risk	Current Risk	Countermeasure Progress	Weakness Tests	Co
0	API gateway	Authentication and Authorization	Created by rules engine	Authentication Bypass	Planned Mitigation: 0%. Mitigated: 0%. Unmitig...	High	High	0%	Not tested	
1	API gateway	Logging and Monitoring	Created by rules engine	Exploitation of insufficient logging and monit...	Planned Mitigation: 0%. Mitigated: 0%. Unmitig...	High	High	0%	Not tested	
2	Catalog DB	Access service	Created by rules engine	Attackers gain access to unauthorised data by ...	Planned Mitigation: 0%. Mitigated: 0%. Unmitig...	Critical	Critical	0%	Not tested	
3	Catalog DB	Access service	Created by rules engine	Authentication Bypass	Planned Mitigation: 0%. Mitigated: 0%. Unmitig...	High	High	0%	Not tested	
4	Catalog DB	Access service	Created by rules engine	Data leakage or disclosure to unauthorized par...	Planned Mitigation: 0%. Mitigated: 0%. Unmitig...	High	High	0%	Not tested	

Most useful data

Tasks:

1. Link Components with Threats [x]
2. Link Components with Inherent Risks [x]
3. Link Components with STRIDE Category [x]
4. Link Use Cases with Threats [x]

In [ ]:

```
useful = df[["Component","Use Case","Threat","Threat abbv","Inherent Risk","STRIDE Category"]]
useful.head()
```

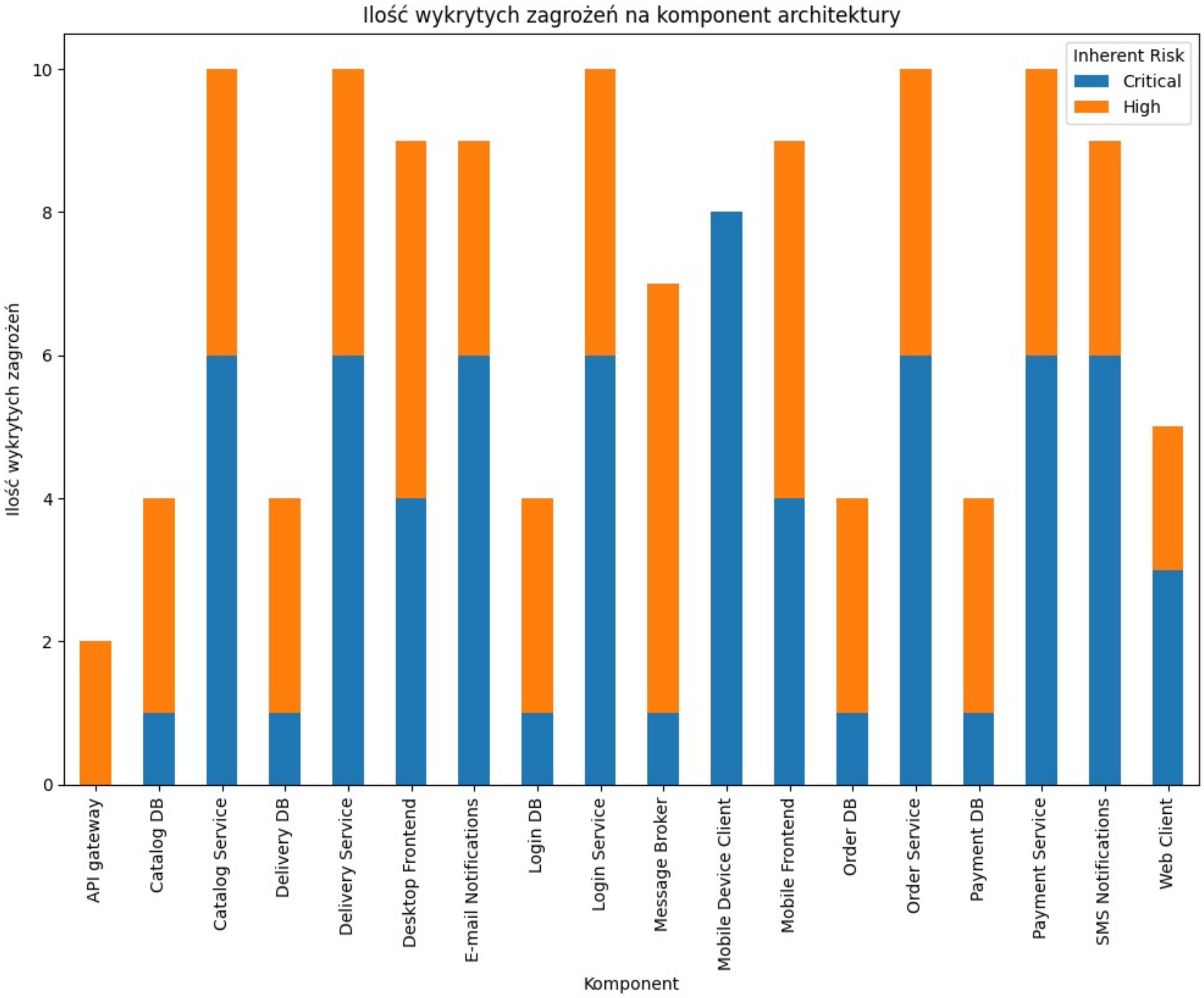
Out[ ]:

	Component	Use Case	Threat	Threat abbv	Inherent Risk	STRIDE Category
0	API gateway	Authentication and Authorization	Authentication Bypass	Authentication Bypass	High	Spoofing
1	API gateway	Logging and Monitoring	Exploitation of insufficient logging and monit...	Insufficient Logging	High	Repudiation
2	Catalog DB	Access service	Attackers gain access to unauthorised data by ...	Unauthorized Data Access	Critical	Information Disclosure
3	Catalog DB	Access service	Authentication Bypass	Authentication Bypass	High	Spoofing
4	Catalog DB	Access service	Data leakage or disclosure to unauthorized par...	Data Leakage	High	Information Disclosure

Threats + risk per component

In [ ]:

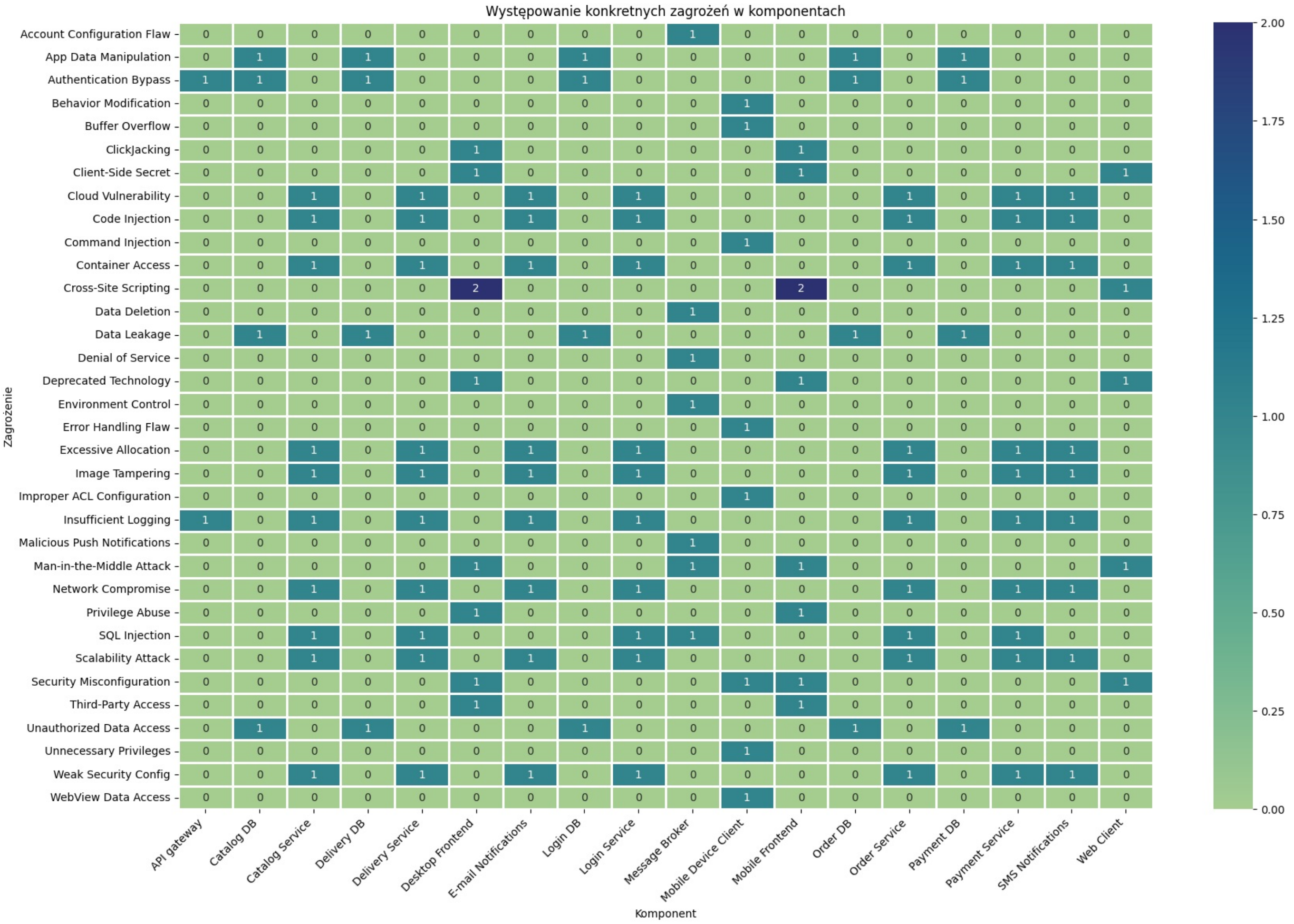
```
grouped_df = df.groupby(['Component', 'Inherent Risk']).size().unstack(fill_value=0)

grouped_df.plot(kind='bar', stacked=True, figsize=(12, 8))
plt.title('Ilość wykrytych zagrożeń na komponent architektury')
plt.xlabel('Komponent')
plt.ylabel('Ilość wykrytych zagrożeń')
plt.legend(title='Inherent Risk')
plt.show()
```



Threats in components

In [ ]:

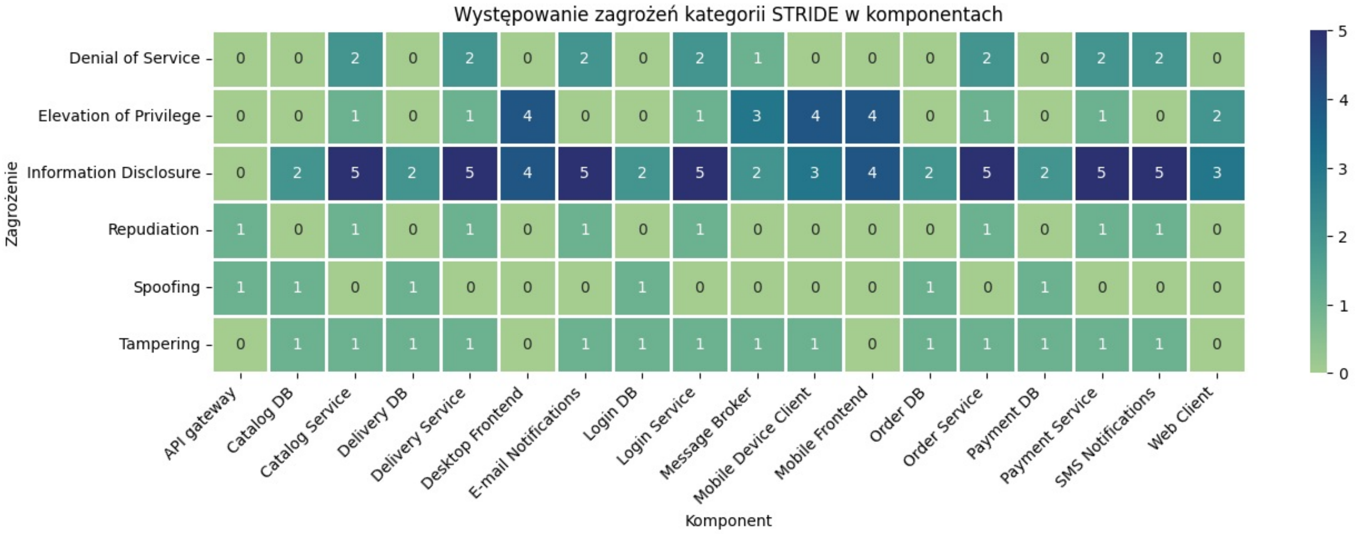
```
heatmap_data = df.groupby(['Threat abbv', 'Component']).size().unstack(fill_value=0)

# Plot the heatmap
plt.figure(figsize=(20, 13))
sns.heatmap(heatmap_data, annot=True, fmt="d",linewidths=1, cmap="crest")
plt.title('Występowanie konkretnych zagrożeń w komponentach')
plt.xlabel('Komponent')
plt.ylabel('Zagrożenie')
plt.xticks(rotation=45,ha="right")
plt.show()
```



STRIDE Categories in Components

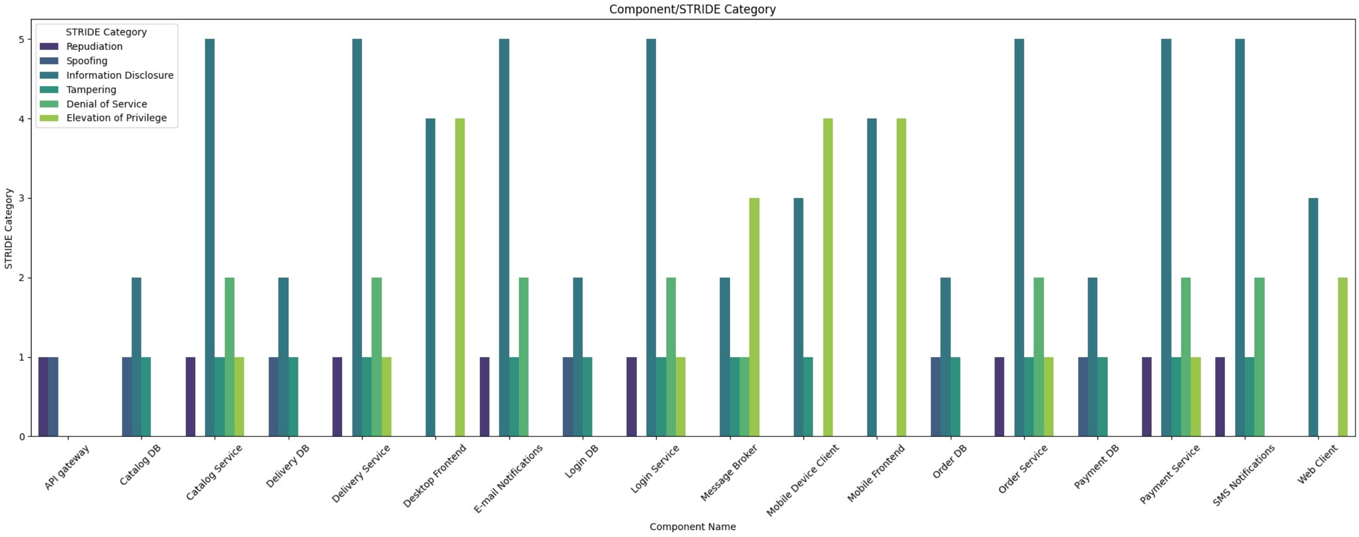
In [ ]:

```
component_category_heatmap = df.groupby(['STRIDE Category','Component']).size().unstack(fill_value=0)
plt.figure(figsize=(15, 4))
sns.heatmap(component_category_heatmap, annot=True,linewidth=1,cmap="crest")
plt.title('Występowanie zagrożeń kategorii STRIDE w komponentach')
plt.xlabel('Komponent')
plt.ylabel('Zagrożenie')
plt.xticks(rotation=45,ha="right")
plt.show()
```



In [ ]:

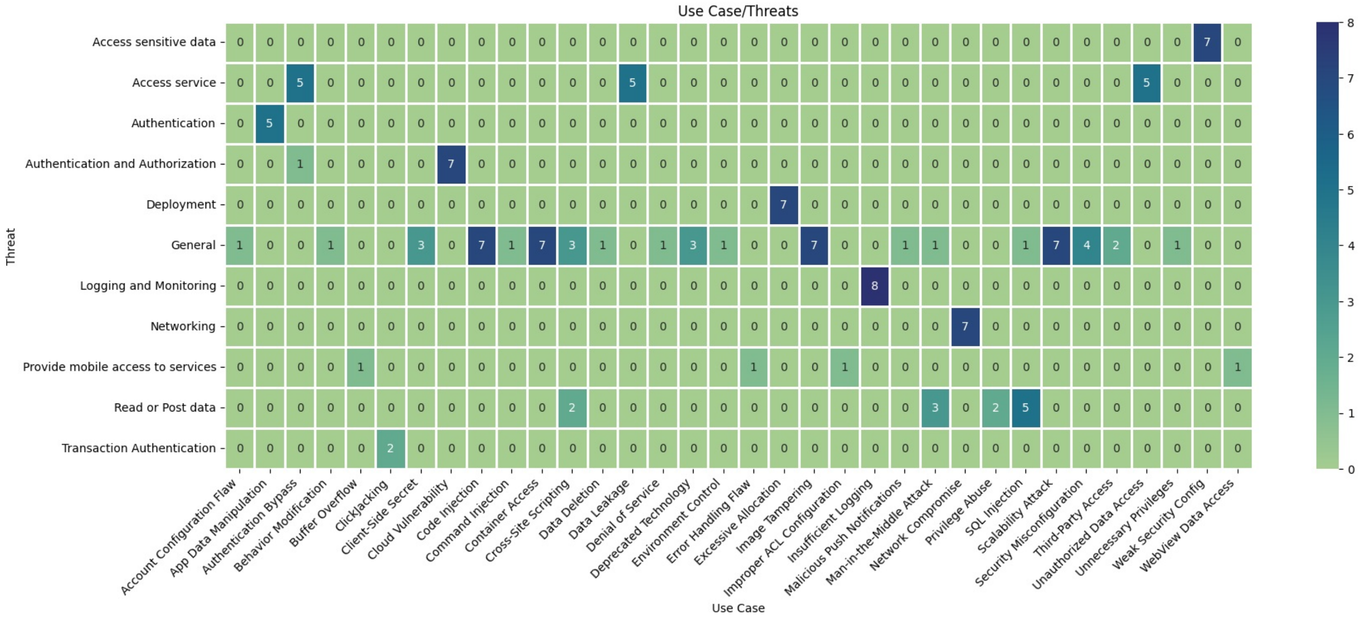
```
component_category_counts = df.groupby(['Component','STRIDE Category']).size().reset_index(name='Count')

# Plotting the data
plt.figure(figsize=(20, 8))
sns.barplot(x='Component', y='Count', hue='STRIDE Category', data=component_category_counts, palette='viridis')
plt.title('Component/STRIDE Category')
plt.xlabel('Component Name')
plt.ylabel('STRIDE Category')
plt.xticks(rotation=45)
plt.legend(title='STRIDE Category')
plt.tight_layout()
plt.show()
```



Threats in use cases

In [ ]:

```
usecase_threat_heatmap = df.groupby(['Use Case','Threat abbv']).size().unstack(fill_value=0)
plt.figure(figsize=(20,7))
sns.heatmap(usecase_threat_heatmap, annot=True,linewidth=1,cmap="crest")
plt.title('Use Case/Threats')
plt.xlabel('Use Case')
plt.ylabel('Threat')
plt.xticks(rotation=45,ha="right")
plt.show()
```



Threat	Account Configuration Flaw	App Data Manipulation	Authentication Bypass	Behavior Modification	Buffer Overflow	Clickjacking	Client-Side Secret	Cloud Vulnerability	Code Injection	Command Injection	Container Access	Cross-Site Scripting	Data Deletion	Data Leakage	Denial of Service	Deprecated Technology	Environment Control	Error Handling Flaw	Excessive Allocation	Image Tampering	Improper ACL Configuration	Insufficient Logging	Malicious Push Notifications	Man-in-the-Middle Attack	Network Compromise	Privilege Abuse	SQL Injection	Scalability Attack	Security Misconfiguration	Third-Party Access	Unauthorized Data Access	Unnecessary Privileges	Weak Security Config	WebView Data Access
Access sensitive data	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0
Access service	0	0	5	0	0	0	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0
Authentication	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Authentication and Authorization	0	0	1	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Deployment	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
General	1	0	0	1	0	0	3	0	7	1	7	3	1	0	1	3	1	0	0	7	0	0	1	1	0	0	1	7	4	2	0	1	0	0
Logging and Monitoring	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0
Networking	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	0	0	0	0	0	0
Provide mobile access to services	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
Read or Post data	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	3	0	2	5	0	0	0	0	0	0	0
Transaction Authentication	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Loading [MathJax]/jax/output/CommonHTML/fonts/TeX/fontdata.js