

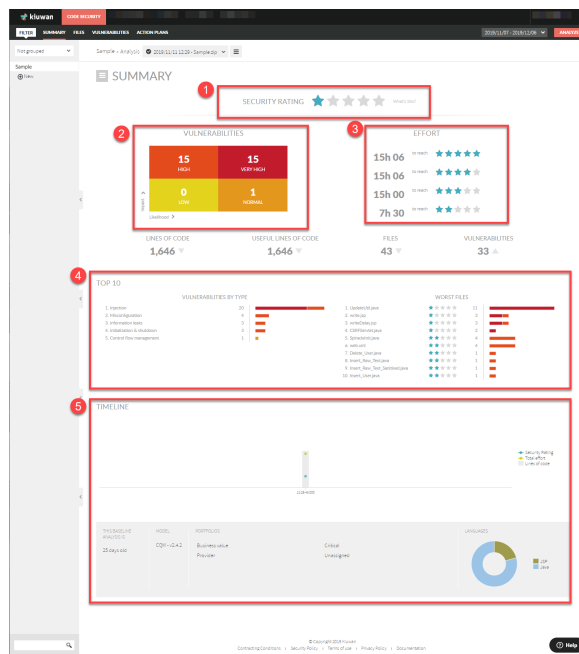
# Security Summary

This section guides you through the **summary** dashboard of Kiuwan Code Security.

The **Code Security Summary** page provides a comprehensive dashboard showcasing a high level overview of the security of your application.

This dashboard shows the following:

- 1 [Security Rating](#)
- 2 [Security Vulnerabilities](#)
- 3 [Effort](#)
- 4 [Top 10 Vulnerabilities and Worst Files](#)
- 5 [Timeline](#)



## Security Rating

The Kiuwan **Security Rating** is a discrete 5-star rating that tells you how secure your application is in terms of the likelihood and impact of the found vulnerabilities.

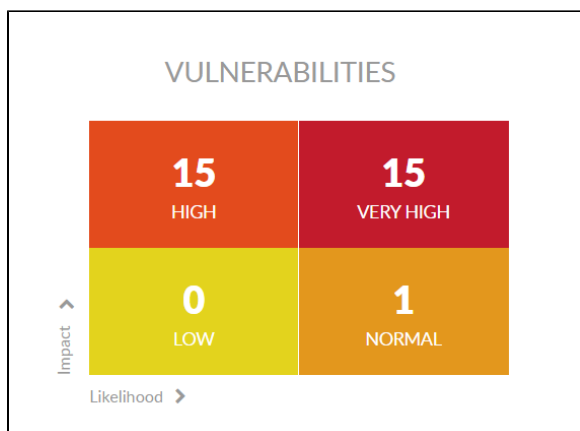
This rating concentrates all the security evidences found in the source.



5 stars = secure

1 star = very insecure

## Security Vulnerabilities



Security vulnerabilities are grouped in a **quadrant** according to two major axes:

- **Impact** of the vulnerability, according to the severity of the associated security risk
- **Likelihood** of the event that could cause the associated security breach

These two axes produce **4 quadrants**. Kiuwan summarizes found vulnerabilities for each quadrant in the following way:

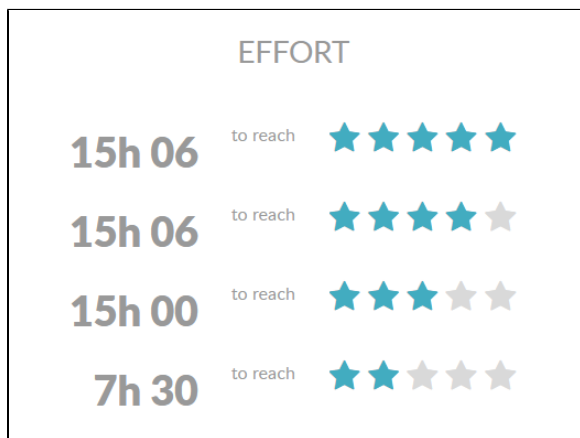
- **Very High**: both likelihood and impact are high
- **High**: likelihood is low but impact is high
- **Low**: likelihood and impact are both low
- **Normal**: likelihood is high and impact is low

This impacts the security rating mentioned above:

- **1-star** = at least 1 Very-High vulnerability (high impact, high likelihood)
- **2-star** = at least 1 High vulnerability (high impact, low likelihood) and none of higher priority
- **3-star** = at least 1 Normal vulnerability (high likelihood, low impact) and none of higher priority
- **4-star** = at least 1 Low vulnerability (low likelihood, low impact) and none of higher priority
- **5-star** = no vulnerabilities in terms of likelihood and impact for your application security

## Effort

Based on the analysis' results, Kiuwan also calculates the **Effort** you need to invest to reach different rating levels according to the remediation effort associated to fix each vulnerability.



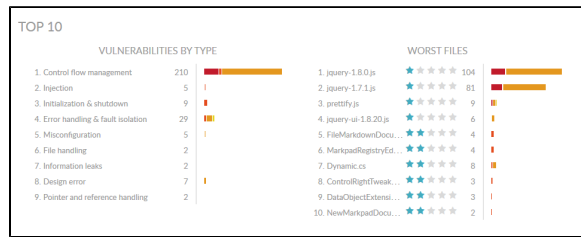
Please note that **Very Low vulnerabilities are discarded in the Security Rating algorithm** and are not included in 4-quadrant image.

That's the reason you could find that the total number of vulnerabilities in the 4-quadrant image is lower than the total vulnerabilities figure.

## Top 10 Vulnerabilities and Worst Files

The summary dashboard also provides a **Top-10 ranking of vulnerability types** and **worst files**.

This way, you can easily concentrate on major contributors to current security rating.



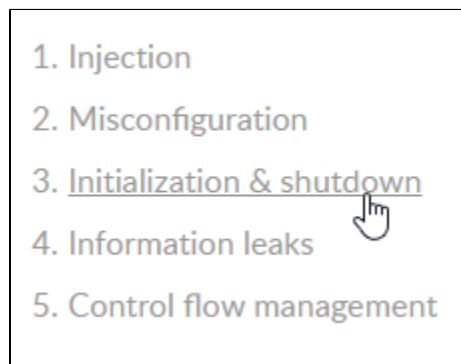
## Vulnerability Types

Kiuwan Code Security considers a vulnerability any defect that could produce a potential security issue, regardless of whether that defect could belong to a software characteristic other than Security.

The **Top-10 Vulnerabilities By Type** graphic lets you to view which ones are the most frequent in your application, showing the total number of vulnerabilities for every type.

To view detailed info on all the vulnerabilities, please go to [Vulnerabilities](#) page.

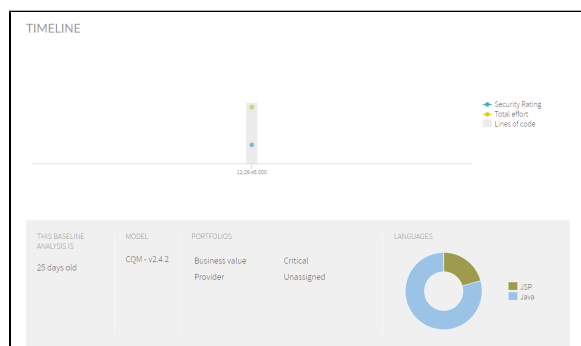
Click on the vulnerability type to see associated defects in a new page.



The **Top-10 Worst Files** graphic displays a ranking of the worst (low-rated) files of your application, showing the security rating and the number of vulnerabilities found.

## Timeline

The **Timeline** section displays a historical evolution of your Security Rating and Total Effort (to reach 5-star rating) as well as the total LOC size of your application.



This section also displays information on:

- When a baseline analysis was performed (only applicable if you are using Life Cycle). If you are not using Life Cycle, that date will be current date of the analysis.
- Model used for the current analysis
- Portfolios this analysis belongs to
- Graphical distribution of LOCs in different languages