

Kiuwan and CWE

Kiuwan and its team makes their best effort to keep up to date with the latest **CWE** version. We map every applicable vulnerability found to the correspondent **CWE**. The mapping is clearly accessible from the list of vulnerabilities found with a direct link to the **CWE** mapped with the vulnerability.

18	28	Avoid SQL code formed with non neutralized	0			Security	Injection	Java	14h 00
user input CERT: CERT: CERT:AD0000: CWE: CWE:BP CWASP: CWASP:2020A5: CWASP:2020A5: PCI POC:2020A5: JAVASCRIPT: JAVASCRIPT: JAVASCRIPT is injected									

With every **Kiuwan Code Security** major release, the mappings are reviewed and modified accordingly to keep up to date with **CWE** versions. If there are any changes regarding **CWE** mappings all users are promptly informed with an in-app message.

See al the information about CWE in the [CWE mitre.org site](#)

See also these other Kiuwan's documentation pages to help you understand **CWE** mapping:

[CWE in Models Management > Rules Management](#)

[CWE in Vulnerabilities reports](#)