# CVE Detail – CVE-2021-25963

In Shuup, versions 1.6.0 through 2.10.8 are vulnerable to reflected Cross-Site Scripting (XSS) that allows execution of arbitrary javascript code on a victim browser. This vulnerability exists due to the error page contents not escaped.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.59618

## CVSS Scoring

CVSS v3.1 Score: 6.1

Severity: MEDIUM

## Mapped CWE(s)

* CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

## CAPEC(s)

* CAPEC-209: XSS Using MIME Type Mismatch
* CAPEC-588: DOM-Based XSS
* CAPEC-591: Reflected XSS
* CAPEC-592: Stored XSS
* CAPEC-63: Cross-Site Scripting (XSS)
* CAPEC-85: AJAX Footprinting

## Affected Products

* cpe:2.3:a:shuup:shuup:\*:\*:\*:\*:\*:\*:\*:\*