# CVE Detail – CVE-2024-3402

A stored Cross-Site Scripting (XSS) vulnerability existed in version (20240121) of gaizhenbiao/chuanhuchatgpt due to inadequate sanitization and validation of model output data. Despite user-input validation efforts, the application fails to properly sanitize or validate the output from the model, allowing for the injection and execution of malicious JavaScript code within the context of a user's browser. This vulnerability can lead to the execution of arbitrary JavaScript code in the context of other users' browsers, potentially resulting in the hijacking of victims' browsers.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.34745

## CVSS Scoring

CVSS v3.1 Score: 5.4

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:gaizhenbiao:chuanhuchatgpt:\*:\*:\*:\*:\*:\*:\*:\*