

# Code Injection

## Description

See [CWE-94](#)

## Example

<https://github.com/btarr/node-eval-code-injection>

## Mitigation

- Design your program in such a way that you don't need to dynamically generate code based off of user input
- If you must take in user input, ensure that input is sanitized
  - Use of a whitelist highly recommended
- Run any dynamically generated code with user input in it in a sandbox environment so that the extent a user can maliciously affect your system with this code is managed and contained

## Notes

- Try not to execute code generated based off of user input, there are probably safer ways to do what you're attempting, weather they be other features in the language or a library