# CWE Detail – CWE-183

## Description

The product implements a protection mechanism that relies on a list of inputs (or properties of inputs) that are explicitly allowed by policy because the inputs are assumed to be safe, but the list is too permissive - that is, it allows an input that is unsafe, leading to resultant weaknesses.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2019-12799: chain: bypass of untrusted deserialization issue (CWE-502) by using an assumed-trusted class (CWE-183)

**•** CVE-2019-10458: sandbox bypass using a method that is on an allowlist

**•** CVE-2017-1000095: sandbox bypass using unsafe methods that are on an allowlist

**•** CVE-2019-10458: CI/CD pipeline feature has unsafe elements in allowlist, allowing bypass of script restrictions

**•** CVE-2017-1000095: Default allowlist includes unsafe methods, allowing bypass of sandbox

## Related Attack Patterns (CAPEC)

* CAPEC-120
* CAPEC-3
* CAPEC-43
* CAPEC-71

## Modes of Introduction

**•** Implementation: N/A

## Common Consequences

**•** Impact: Bypass Protection Mechanism — Notes:

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)