# CWE Detail – CWE-692

## Description

The product uses a denylist-based protection mechanism to defend against XSS attacks, but the denylist is incomplete, allowing XSS variants to succeed.

## Extended Description

While XSS might seem simple to prevent, web browsers vary so widely in how they parse web pages, that a denylist cannot keep track of all the variations. The "XSS Cheat Sheet" [REF-714] contains a large number of attacks that are intended to bypass incomplete denylists.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2007-5727: Denylist only removes <SCRIPT> tag.

**•** CVE-2006-3617: Denylist only removes <SCRIPT> tag.

**•** CVE-2006-4308: Denylist only checks "javascript:" tag

## Related Attack Patterns (CAPEC)

* CAPEC-120
* CAPEC-267
* CAPEC-71
* CAPEC-80
* CAPEC-85

## Attack TTPs

**•** T1027: Obfuscated Files or Information (Tactics: defense-evasion)

## Common Consequences

**•** Impact: Execute Unauthorized Code or Commands — Notes:

## Applicable Platforms

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