Self-XSS

Moderate **parabirb** published **GHSA-529v-f2gf-62w9** on Apr 21, 2021

Package

wrongthink (wrongthink.me)

Affected versions	Patched versions
< 2.4.1	2.4.1 (after 4/21/21)

Description

Self-XSS

Impact

All versions before 2.4.1 (and some versions of 2.4.1 made before 4/21/21) are affected.

Abstract

The user could set their fingerprint to something such as `Self-XSS<script>alert(1)</script>` and then check their fingerprint in order to run arbitrary JavaScript on the site. A successful demo is shown below (v2.0.0).

Severity

Moderate 6.6 / 10

CVSS base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	Low
User interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	None

CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N

CVE ID

CVE-2021-29467

Weaknesses

CWE-80