# CVE Detail – CVE-2020-11053

In OAuth2 Proxy before 5.1.1, there is an open redirect vulnerability. Users can provide a redirect address for the proxy to send the authenticated user to at the end of the authentication flow. This is expected to be the original URL that the user was trying to access. This redirect URL is checked within the proxy and validated before redirecting the user to prevent malicious actors providing redirects to potentially harmful sites. However, by crafting a redirect URL with HTML encoded whitespace characters the validation could be bypassed and allow a redirect to any URL provided. This has been patched in 5.1.1.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.45792

## CVSS Scoring

CVSS v3.1 Score: 7.1

Severity: HIGH

## Mapped CWE(s)

* CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

## CAPEC(s)

* CAPEC-178: Cross-Site Flashing

## Affected Products

* cpe:2.3:a:oauth2\_proxy\_project:oauth2\_proxy:\*:\*:\*:\*:\*:\*:\*:\*