Reflected XSS via query parameter injection into HTML attributes

Moderate **harlan-zw** published **GHSA-mg36-wvcr-m75h** last week

Package

nuxt-og-image (npm)

Affected versions	Patched versions
< 6.2.5	6.2.5

Description

Product: Nuxt OG Image
Version: 6.1.2
CWE-ID: CWE-79: Improper Neutralization of Input During Web Page Generation
CVSS vector v.4.0: 6.1 (AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:H/SI:N/SA:N)
Description: Incorrect parsing of GET parameters leads to the possibility of HTML injection and JavaScript code injection.
Impact: Client-Side JavaScript Execution
Exploitation condition: An external user
Mitigation: Correct the logic of parsing GET parameters and their subsequent implementation into the generated page.
Researcher: Dmitry Prokhorov (Positive Technologies)

Research

During the analysis of the nuxt-og-image package, which is shipped with the nuxt-seo package, a zero-day vulnerability was discovered.
This research revealed that the image-generation component by the URI: `/_og/d/` (and, in older versions, `/og-image/`) contains a vulnerability that allows injection of arbitrary attributes into the HTML page body. The vulnerability was reproduced using the standard configuration and the default templates.

Listing 1. The content of the configuration file `nuxt.config.ts`

```
export default defineNuxtConfig({
  modules: ['nuxt-og-image'],
  devServer: {
    host: 'web-test.local',
    port: 3000
  },
  site: {
    url: 'http://web-test.local:3000',
  },
  ogImage: {
    fonts: [
      'Inter:400',
      'Inter:700'
    ],
  }
})
```

Vulnerability reproduction

To demonstrate the proof-of-concept, follow the URI: `/_og/d/og.html?width=1000&height=1000&onmouseover=alert(document.cookie)&autofocus`
The injected parameters `onmouseover=alert(document.cookie)` and `autofocus` are treated as attributes and are inserted directly into the generated HTML page.

Listing 2. HTTP-request example

```
GET /_og/d/og.html?width=1000&height=1000&onmouseover=alert(document.cookie) HTTP/
Host: web-test.local:3000
```

Figure 1. The injected attribute in the HTML body

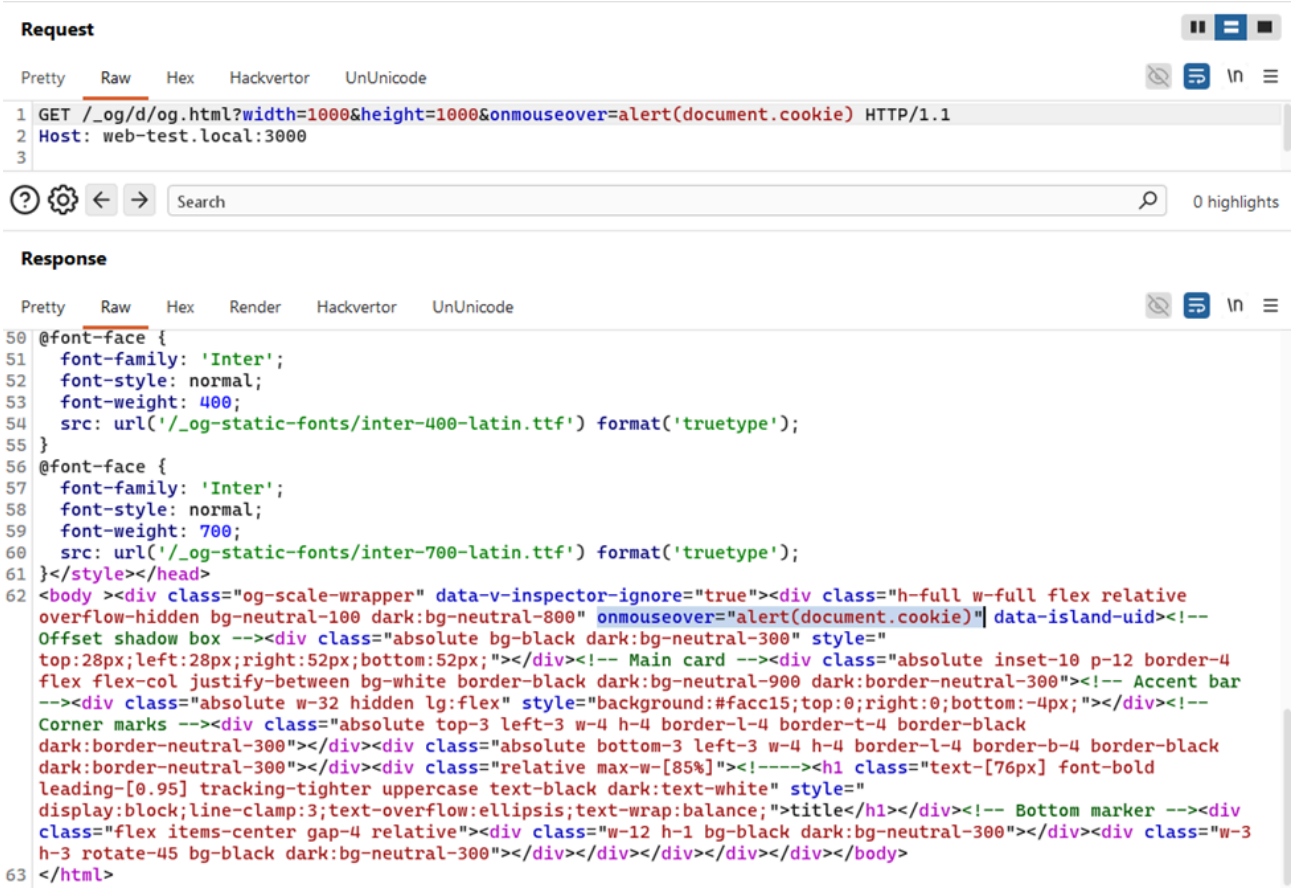

Figure 2. JavaScript code execution

Credits

Researcher: Dmitry Prokhorov (Positive Technologies)

Severity

Moderate 6.1 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	Required
Scope	Changed
Confidentiality	Low
Integrity	Low
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2026-34405

Weaknesses

▶ CWE-79