

New issue

Jump to bottom

XSS issue in the "discountcode" parameter #5322

🔒 Closed
 AndreiMaz opened this issue on Feb 8, 2021 · 1 comment

Assignees



Labels

bug

Milestone

🏠 Version 4.40

AndreiMaz commented on Feb 8, 2021

Member

The vulnerability is a reflected XSS in the discountcode URL parameter. If an invalid discount code is entered, the value is reflected directly in the response without HTML encoding. This was tested on Google Chrome, Firefox and Edge with a fresh install of nopCommerce. I have attached a screenshot of the PoC.

The cause of the issue is the following line:

```

nopCommerce/src/Presentation/Nop.Web.Framework/Mvc/Filters/CheckDiscountCouponAttribute.cs
Line 134 in 879275b

134     _notificationService.WarningNotification(string.Format(InvalidLocale, InvalidCouponCode));

```

which uses the String.format() function without sanitising the user input. The same code exists in the 4.3.0 release tag as well:

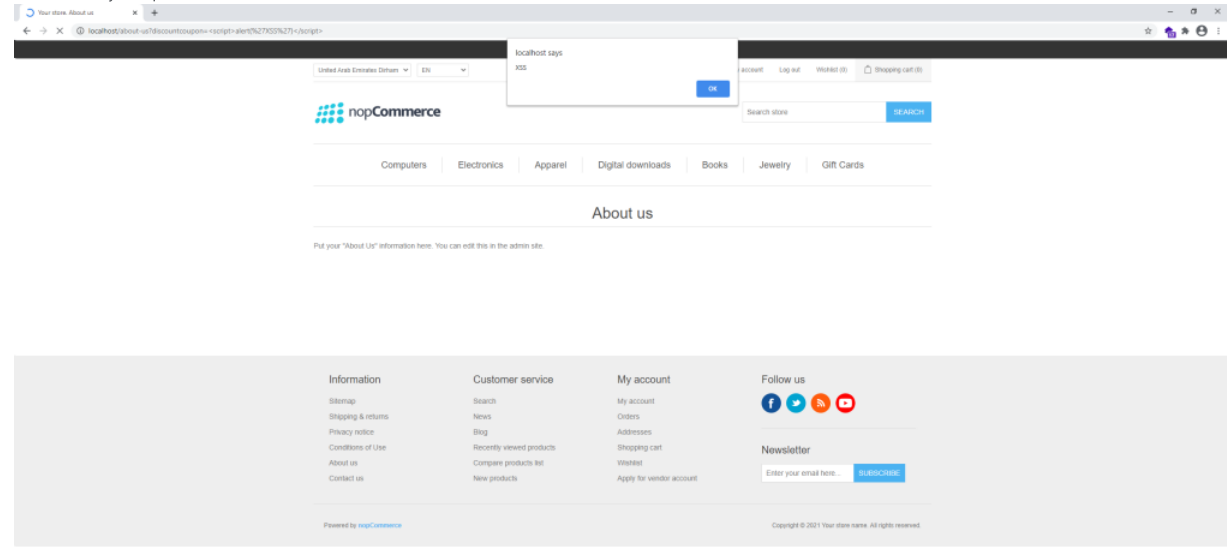
```

nopCommerce/src/Presentation/Nop.Web.Framework/Mvc/Filters/CheckDiscountCouponAttribute.cs
Line 132 in 9f6002d

132     string.Format(_localizationService.GetResource("ShoppingCart.DiscountCouponCode.Invalid"),

```

Let me know if you require additional information.



AndreiMaz added the `bug` label on Feb 8, 2021

AndreiMaz added this to the `Version 4.40` milestone on Feb 8, 2021

AndreiMaz assigned `skoshelev` on Feb 8, 2021

RomanovM assigned `DmitriyKulagin` and unassigned `skoshelev` on Feb 8, 2021

DmitriyKulagin added a commit that referenced this issue on Feb 15, 2021

#5322 Fixed XSS issue in the "discountcode" parameter

f35d311

DmitriyKulagin added a commit that referenced this issue on Feb 15, 2021


#5322 Fixed XSS issue in the "discountcode" parameter

4b3f101

DmitriyKulagin commented on Feb 15, 2021

Contributor

Closed [#5322](#)

 **DmitriyKulagin** closed this as completed on Feb 15, 2021

Assignees

 **DmitriyKulagin**

Labels

bug

Projects

None yet

Milestone

Version 4.40

Development

No branches or pull requests

3 participants

