Open Redirect on nopCommerce 4.50.1

Date: 19/03/2022

Exploit Author: Tin Pham aka TF1T of VietSunshine Cyber Security Services

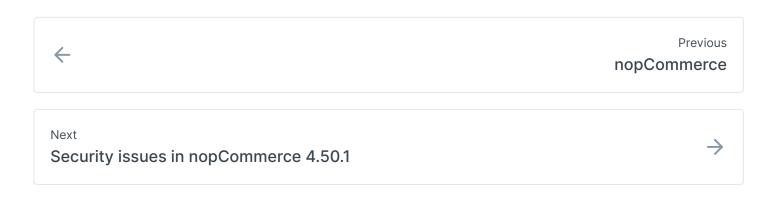
Vendor Homepage: https://www.nopcommerce.com/

Version: nopCommerce 4.50.1 (and prior)

CVE: CVE-2022-27461

Description: In nopCommerce 4.50.1, an open redirect vulnerability can be triggered by luring user to authenticate to nopCommerce page by clicking on a crafted link.

Steps to reproduce: After a successful login of victim, the user will be redirected to https://example.com when the following link is being clicked: https://\$IP/login?returnurl=https://example.com



Last modified 6mo ago