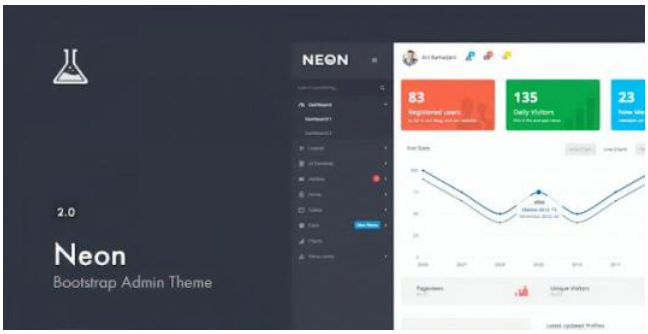
Neon Dashboard XSS

June 03, 2020



What is Neon Dashboard?

Neon is Feature packed & powerful Admin dashboard with UI Kit. It is built on Latest Bootstrap version, Latest Laravel version, PHP, HTML5 , CSS3 and jQuery. All elements are handcrafted full precision as well customizable as per requirements. The Admin Dashboard is Fully Responsive and gives full flexibility to developer to customize it. It consists of 3 Unique Dashboard Layouts, 80+ Inner Pages and 7+ Modern Icon Sets. We are very supportive of our client base.

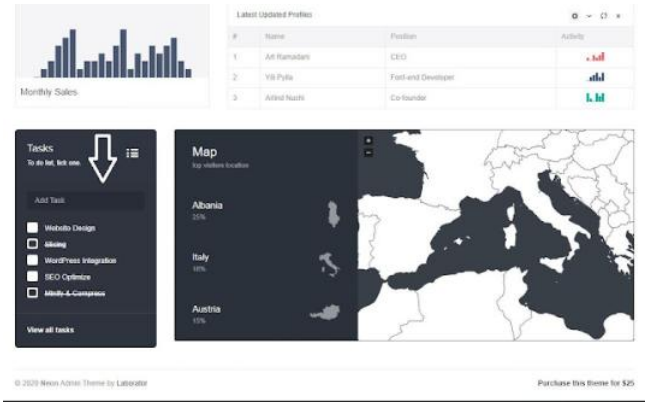
Please, Feel free to contact us in case of any query.

What is XSS?

XSS is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.

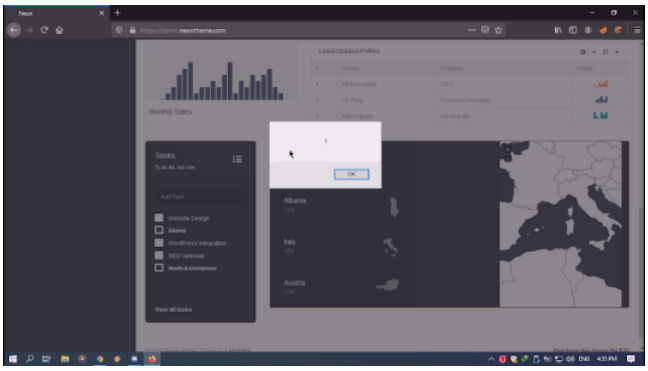
Full PoC :

after installing neon theme on your localhost or just visiting https://demo.neontheme.com/ you'll find the taskes section and add task input like this :



when adding this payload **<script>alert(1)</script>** it will excute the javascript code and showing the (1) popup that means there's an xss here

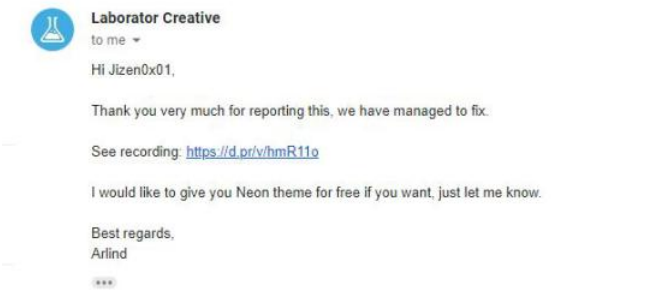
like this :



and BOOOM it worked :)

and here's another PoC video : **PoC**

My Report :



Laborator Creative
to me

Hi Jizen0x01,

Thank you very much for reporting this, we have managed to fix.

See recording: https://d.pr/v/hmR11o

I would like to give you Neon theme for free if you want, just let me know.

Best regards,
Arlind

My links :

Facebook

Github

Email

LABELS: WEB SECURITY

SHARE

Comments

Khaled Nassar · June 21, 2020 at 8:34 AM

This comment has been removed by the author.

REPLY

To leave a comment, click the button below to sign in with Google.

About Me

jizen0x01

VISIT PROFILE

Archive

Labels

Report Abuse

Powered by Blogger