Reflected XSS on Any.myshopify.com/admin

49

Share:

State	Resolved (Closed)
Disclosed	**November 13, 2018 6:16pm +0800**
Reported To	Shopify
Asset	your-store.myshopify.com (Domain)
Weakness	Cross-site Scripting (XSS) - Reflected
Bounty	$1,500
Severity	High (7 ~ 8.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

dr_dragon submitted a report to **Shopify**. Oct 12th (2 months ago)

Description :

Hi,
I have found a reflected cross site scripting vulnerability in <any>.myshopify.com/admin through return_url parameter .

Step to reproduce :

1-Go to https://<Any>.myshopify.com/admin/authenticate?return_url=javascript:alert(100)//
2-Click on reload this page
3-Xss alert message

Impact

Xss attack in <Any>.myshopify.com/admin

2 attachments:
F359102: 1.PNG
F359103: 2.PNG

dr_dragon posted a comment. Updated Oct 12th (2 months ago)

Another Vulnerable url :

Go to https://<Any>.myshopify.com/admin/authenticate/?return_url=https://<Any>.myshopify.com/admin/authenticate/?return_url=javascript:alert(document.cookie)
and click on reload this page :) .

clayton changed the status to **Triaged**. Oct 12th (2 months ago)
Thank you for your report. We've reproduced the issue, and our engineering team is investigating.

dr_dragon posted a comment. Oct 15th (2 months ago)
It's fixed now
Nice work

jenn-shopify closed the report and changed the status to **Resolved**. Oct 18th (2 months ago)
Hey @dr_dragon!
Thanks again for your report. Great find! As you noted, this issue has been fixed. Our next round of bounty decisions will take place within the next few days, so we'll be in touch with you again soon.

Shopify rewarded dr_dragon with a **$1,500** bounty. Oct 22nd (2 months ago)
Thanks again for this report @dr_dragon!


dr_dragon posted a comment. Oct 22nd (2 months ago)
How can i get $500 bons for this report :) :) :)


clayton posted a comment. Oct 22nd (2 months ago)
@dr_dragon $1,500 is the final, total bounty amount for this report.


dr_dragon posted a comment. Oct 23rd (2 months ago)
ok thanks for the bounty .

shopify-peteryaworski requested to disclose this report. Nov 8th (about 1 month ago)


dr_dragon posted a comment. Nov 8th (about 1 month ago)
not yet .

dr_dragon agreed to disclose this report. Nov 13th (28 days ago)

This report has been disclosed. Nov 13th (28 days ago)