

New issue

Jump to bottom

Prevent XSS attack using /auth/enable_cookies #1455

Merged

jonpulsifer merged 3 commits into Shopify:master from seamusabshere:prevent-xss-on-enable-cookies on May 23, 2020

Conversation 8 Commits 3 Checks 0 Files changed 4



seamusabshere commented on May 23, 2020

Contributor

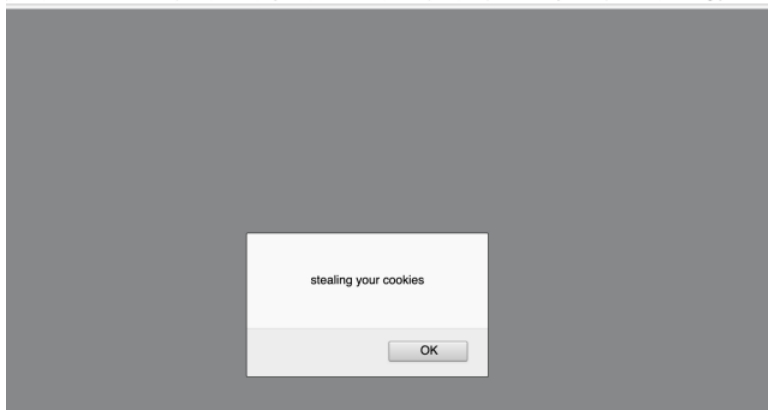
[https://example.com/shopify/auth/enable_cookies?shop=%27%22%3C/title%3E%3C/style%3E%3C/textarea%3E%3C/noscript%3E%3C/script%3E--%3E%3Cdtfy%3E%3Cscript%3Ealert\(%27hello%20world%27\)%3C/script%3E](https://example.com/shopify/auth/enable_cookies?shop=%27%22%3C/title%3E%3C/style%3E%3C/textarea%3E%3C/noscript%3E%3C/script%3E--%3E%3Cdtfy%3E%3Cscript%3Ealert(%27hello%20world%27)%3C/script%3E)

Thanks to @nhusher

Description

Fixes #1453

/auth/enable_cookies?shop=""</title></style></textarea></noscript></script>--><dtfy><script>alert('stealing your co



Prevent XSS attack using /auth/enable_cookies ...

114ce1b

ghost added the cla-needed label on May 23, 2020

2 more spots

4b7179e

ghost removed the cla-needed label on May 23, 2020



ricardotealdi reviewed on May 23, 2020

View changes

packages/koa-shopify-auth/src/auth/create-enable-cookies.ts

```
...    @@ -40,7 +40,7 @@ export default function createEnableCookies({
40    40
41    41    <script>
42    42    window.apiKey = `${apiKey}`;
43    43    window.shopOrigin = "https://${shop}";
43    43    window.shopOrigin = "https://${encodeURIComponent(shop)}";
```



ricardotealdi on May 23, 2020

Should the https:// be part of the encodeURIComponent call as well?



seamusabshere on May 23, 2020

Contributor

Author

i'm pretty sure "shop" always comes back as foo.myshopify.com

a couple years ago, @ragalie did this

[3284be1 #diff-a15b7c0928331371cc40785dd637c644R16](#)

which is a different way of fixing this, in a different place



theodoretan on May 23, 2020

Member


👉 I think it's okay since we only want to encode the value coming from the user



ricardotealdi on May 23, 2020

That makes sense 👍

```
packages/koa-shopify-auth/src/auth/create-request-storage-access.ts
...      ...      @@ -39,7 +39,7 @@ export default function createRequestStorageAccess({
39      39
40      40      <script>
41      41      window.apiKey = "${apiKey}";
42      42      - window.shopOrigin = "https://${shop}";
42      42      + window.shopOrigin = "https://${encodeURIComponent(shop)}";
```

 **ricardotealdi** on May 23, 2020
Same thing here.

seamusabshere commented on May 23, 2020

Contributor **Author**

In general, I have a feeling that this PR is wrong.
The `shop` parameter should be checked as soon as it's received from the user, not every single time it's used.

 2

ricardotealdi commented on May 23, 2020

The `shop` parameter should be checked as soon as it's received from the user, not every single time it's used.
Good point and I agree with you!

  found another one

 8cce0f8

jonpulsifer commented on May 23, 2020 • edited

Contributor

FYI @nhusher @seamusabshere we have a bug bounty program over at <https://hackerone.com/shopify> 🏆 and there are rules for participation!
I am thinking of two rules in particular:

- Rules for reporting must be followed.
- Do not disclose any issues publicly before they have been resolved.





theodoretan approved these changes on May 23, 2020
[View changes](#)



✓ **jonpulsifer** approved these changes on May 23, 2020
[View changes](#)

 **jonpulsifer** merged commit **dec3640** into **Shopify:master** on May 23, 2020
1 check failed

[View details](#)

  **ragalie** mentioned this pull request on May 25, 2020

Update koa changelog #1458




 **Closed**

 2 tasks

  **alexandcote** temporarily deployed to production 2 years ago **Inactive**

  **michenly** temporarily deployed to gem 2 years ago **Inactive**

Reviewers

 **ricardotealdi**
 **jonpulsifer**
 **theodoretan**


✓
✓

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.



6 participants

