New issue

Jump to bottom

Fix security issue in order status endpoint #10573

Merged damianlegawiec merged 1 commit into spree:master from upsidelab:fix/order_status_accepting_blank_order_token on Nov 10, 2020

Conversation 1 Commits 1 Checks 0 Files changed 2

kshalot commented on Nov 9, 2020 Contributor

Issue

`ensure_order_token` in `OrderStatusController` (permalink) checks if `order_token` is truthy instead of checking if it's `present?`.

Outcome

Passing an empty string `''` as the token allows to query any complete order without knowing it's token.

Description

Searching for complete orders forms a pipeline where the last step should filter out every order whose token doesn't match the token provided by the client:

spree/core/app/finders/spree/orders/find_complete.rb
Lines 12 to 18 in 4cc2c29

```
12    def execute
13      orders = by_user(scope)
14      orders = by_number(orders)
15      orders = by_token(orders)
16
17      orders
18    end
```

`by_token` first checks whether token is present:

spree/core/app/finders/spree/orders/find_complete.rb
Lines 34 to 36 in 4cc2c29

```
34    def token?
35      token.present?
36    end
```

spree/core/app/finders/spree/orders/find_complete.rb
Lines 50 to 54 in 4cc2c29

```
50    def by_token(orders)
51      return orders unless token?
52
53      orders.where(token: token)
54    end
```

This completely skips filtering by token when the token is blank. In particular, it skips it when the token is an empty string `''`. Since empty string evaluates to `true`, `ensure_order_token` would accept it as valid input. This makes it possible to query for any complete order without knowing it's token.

Steps to reproduce

1. Complete an order `<order_number>`.
2. Set the `X-Spree-Order-Token` header to an empty string `''`.
3. Query `/api/v2/storefront/order_status/<order_number>`.

You should now see the order's details.

Fix 'ensure_order_token' accepting empty string as valid input a20a53c

squash-labs bot commented on Nov 9, 2020

Manage this branch in Squash

Test this branch here: https://upsidelabfixorder-status-accep-8htfj.squash.io

damianlegawiec approved these changes on Nov 10, 2020

View changes

damianlegawiec merged commit bc1b1ad into spree:master on Nov 10, 2020

2 checks passed

View details

Reviewers

damianlegawiec

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

2 participants