Multiple Stored Cross-site Scripting (XSS) Vulnerabilities in Shop's Other Settings, Shop's Autorespond E-mail Settings and Shops' Payments Methods in microweber/microweber

0

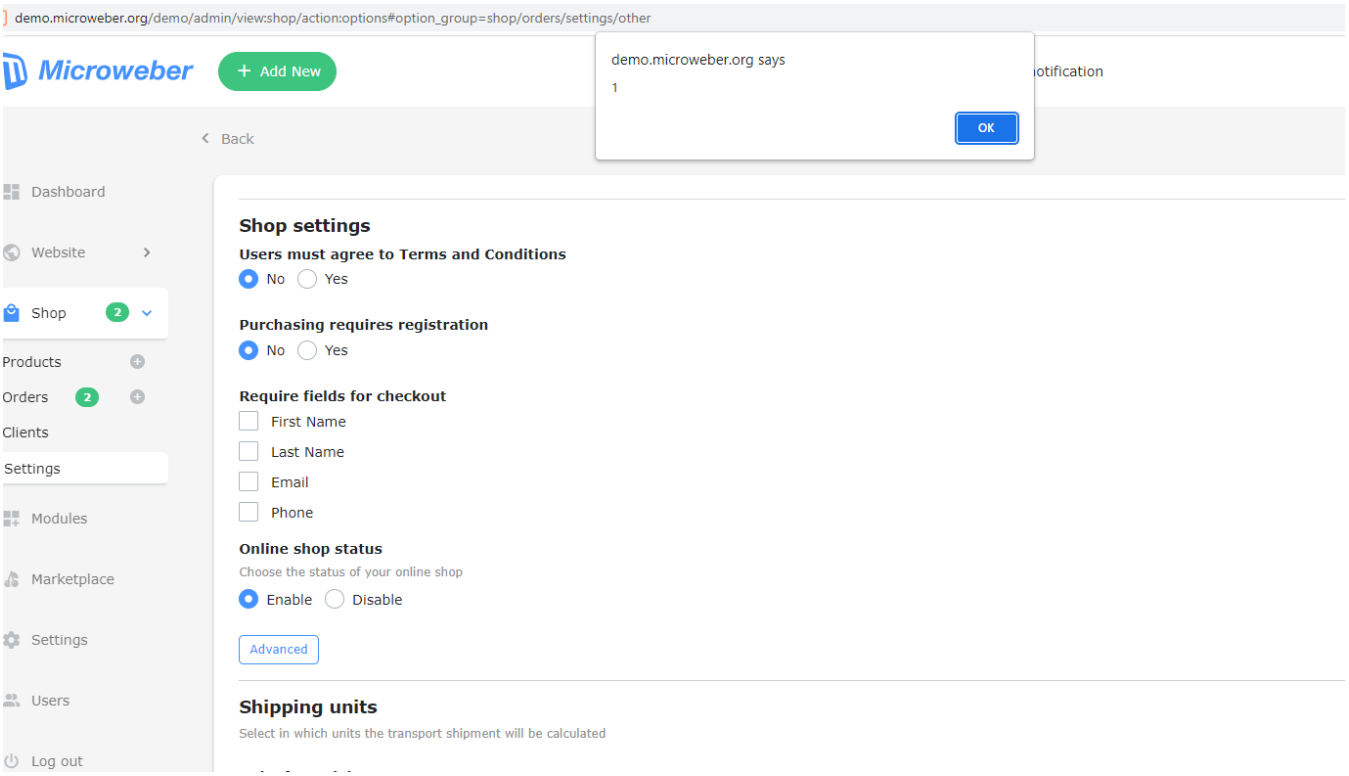
Valid Reported on Mar 11th 2022

Description

(1) Checkout URL and Custom order id parameters are vulnerable to stored XSS, which are located in Shop > Settings > other settings > Advanced
(2) From e-mail address and From name parameters are vulnerable to stored XSS, which are located in Shop Settings > Autorespond E-mail settings > check your e-mail settings
(3) Template Name, Template type, From Name, From E-mail and Subject parameters are vulnerable to stored XSS, which are located in Shop Settings > Autorespond E-mail settings > Edit Templates / Add new email template
(4) Multiple fields in the settings of Payment method settings are vulnerable to stored XSS, which are located in Shop Settings > Autorespond E-mail settings > check your e-mail settings > Test Mail Sending Method
(5) Send test email to and Test mail subject parameters of Send test email function are vulnerable to stored XSS, which are located in Shop Settings > Payment > Settings of each method

Proof of Concept for (1)

Step (1) : Access https://demo.microweber.org/demo/admin/view:shop/action:options#option_group=shop/orders/settings/other
Step (2): Click Advanced
Step (3): Put payload below in Checkout URL or Custom order id parameter
"><iMg SrC="x" oNeRRor="alert(1);">
Refresh this page, stored XSS will be triggered.



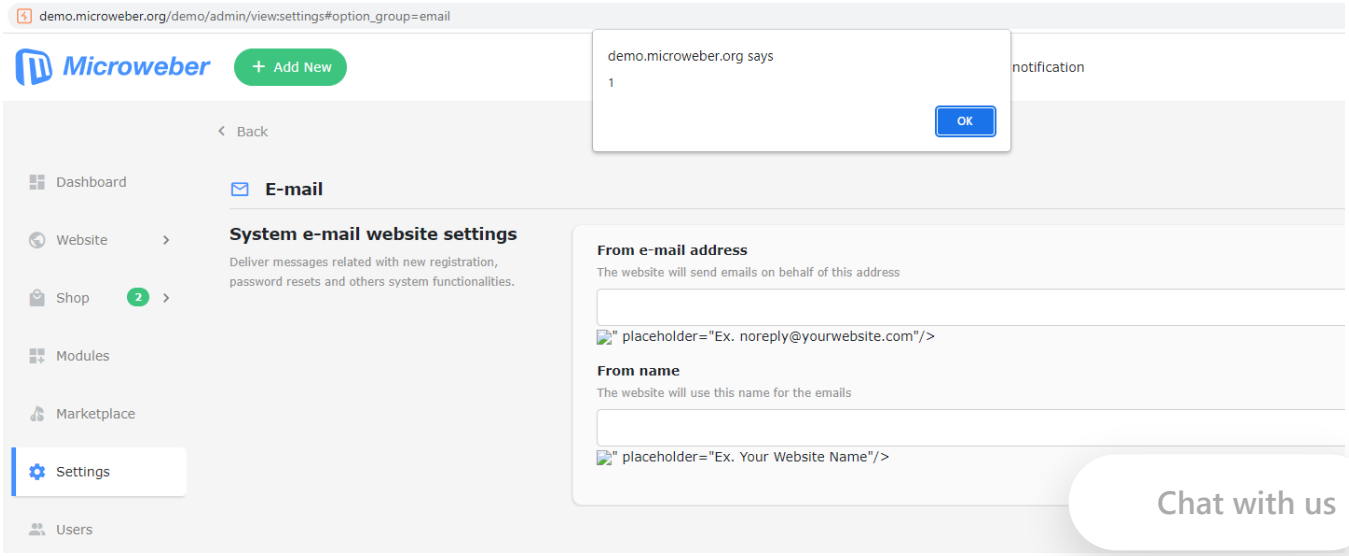
Proof of Concept for (2)

Step (1) : Access https://demo.microweber.org/demo/admin/view:settings#option_group=shop/orders/settings/setup_emails_on_order

Step (2): Click check your e-mail settings

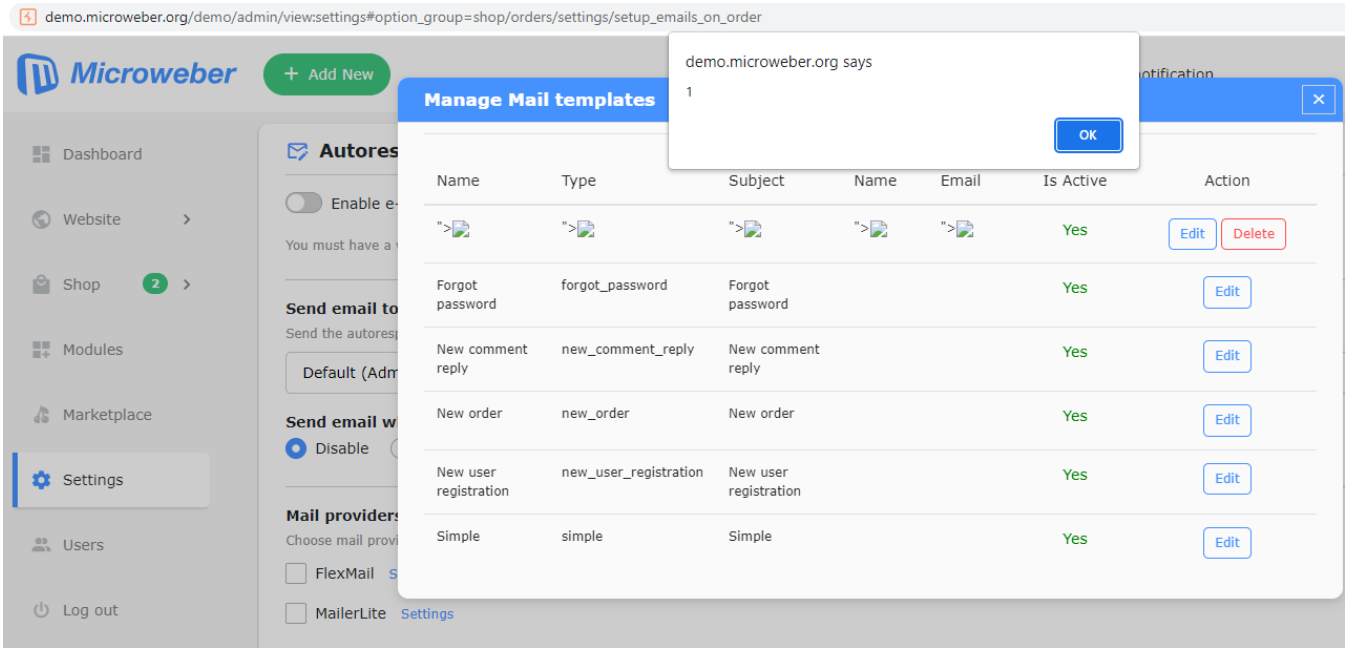
Step (3): Put payload below in From e-mail address or From name parameter

"><iMg SrC="x" oNeRRor="alert(1);">



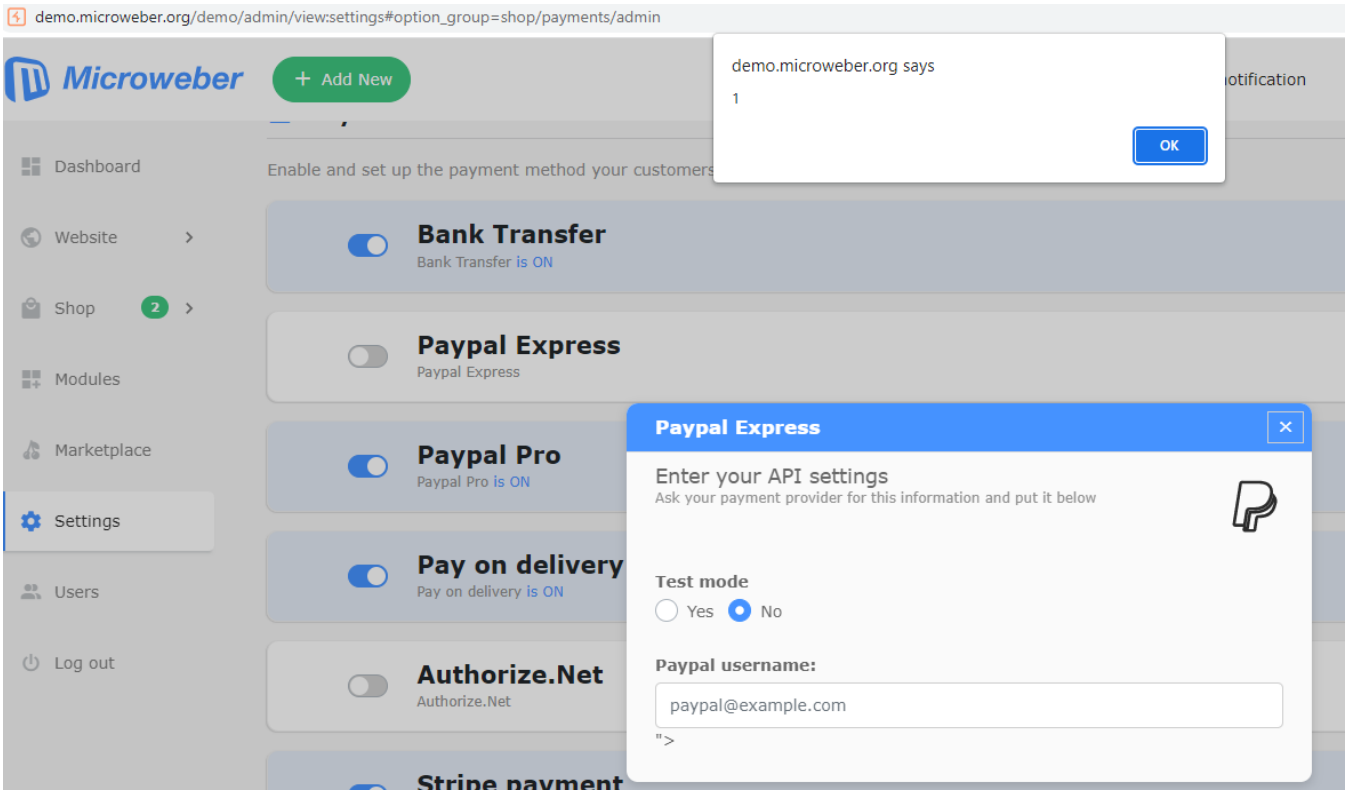
Proof of Concept for (3)

Step (1) : Access https://demo.microweber.org/demo/admin/view:settings#option_group=shop/orders/settings/setup_emails_on_order
Step (2): Click Add new email template or Edit Templates
Step (3): Put payload below in Template Name, Template type, From Name, From E-mail or Subject parameters (*for type parameter, need to change in request)
"><iMg SrC="x" oNeRRor="alert(1);">



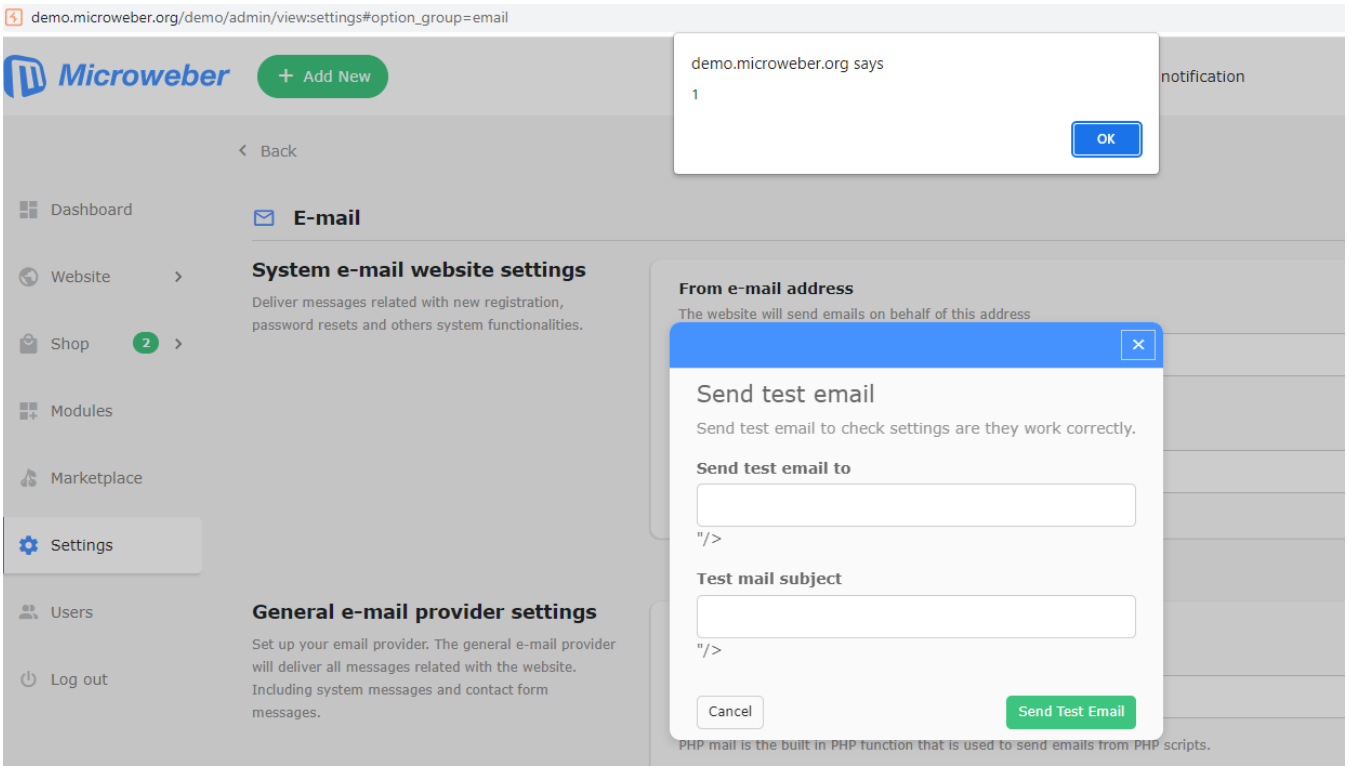
Proof of Concept for (4)

Step (1) : Access https://demo.microweber.org/demo/admin/view:settings#option_group=shop/payments/admin
Step (2): Click Settings of Paypal Express
Step (3): Put payload below in Paypal username
"><iMg SrC="x" oNeRRor="alert(1);">



Proof of Concept for (5)

Step (1) : Access
https://demo.microweber.org/demo/admin/view:settings#option_group=email
Step (2): Click Test Mail Sending Method
Step (3): Put payload below in Send test email to or Test mail subject
"><iMg SrC="x" oNeRRor="alert(1);">
Step (4): Click save email settings



Impact

If an attacker can control a script that is executed in the victim's browser, they might compromise that user, in this case, an admin, by stealing its cookies.

Occurrences

other.php L93-L104

Lack of user input sanitization

CVE
CVE-2022-0954
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (6.8)

Medium (6.8)

Visibility
Public

Status
Fixed

Found by

James Yeung
@scriptidiot
unranked

Fixed by

Bozhidar Slaveykov
@bobimicroweber
maintainer

This report was seen 523 times.

We are processing your report and will contact the **microweber** team within 24 hours.
9 months ago

James Yeung modified the report 9 months ago

James Yeung modified the report 9 months ago

James Yeung modified the report 9 months ago

James Yeung modified the report 9 months ago

James Yeung modified the report 9 months ago

James Yeung modified the report 8 months ago

James Yeung modified the report 8 months ago

James Yeung modified the report 8 months ago

James Yeung modified the report 8 months ago

James Yeung modified the report 8 months ago

We have contacted a member of the microweber team and are waiting to hear back
8 months ago

Bozhidar Slaveykov validated this vulnerability 8 months ago

James Yeung has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Bozhidar Slaveykov marked this as fixed in 1.2.11 with commit 955471 8 months ago

Bozhidar Slaveykov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

other.php#L93-L104 has been validated ✔

Sign in to join this conversation

FAQ

contact us

terms

privacy policy

Chat with us