A stored XSS in dolibarr/htdocs/admin/accountant.php in dolibarr/dolibarr

3

✓ Valid Reported on Jun 11th 2022

Description

I found a stored XSS in the admin/accountant.php, the field `town` , `name` , `Accountant code` can escape the double quote. In the path 'dolibarr/htdocs/main.inc.php' has a WAF, we can not inject any the javascript `onxxx` event. However, in the path `dolibarr/htdocs/core/lib/functions.lib.php` (line 6643), there is a statement:

```
$temp = preg_replace('/<+([a-z]+)/i', '\1', $temp);
```

We can use it to bypass the WAF by adding a `<` in the payload.

Proof of Concept

```
POST /dolibarr/htdocs/admin/accountant.php HTTP/1.1
...
...&town="on<click=alert(/xss/);"
```

The PoC Video

Impact

This vulnerability has the potential to deface websites, result in compromised user accounts, and can run malicious code on web pages, which can lead to a compromise of the user's device.

CVE
CVE-2022-2060
(Published)

Vulnerability Type

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

Severity

High (8.4)

Registry

Other

Affected Version

15.0.2

Visibility

Public

Status

Fixed

Found by

i0hex

@iohehe

legend

Fixed by

Laurent Destailleur

@eldy

maintainer

This report was seen 537 times.

We are processing your report and will contact the **dolibarr** team within 24 hours. 5 months ago

i0hex modified the report 5 months ago

We have contacted a member of the **dolibarr** team and are waiting to hear back 5 months ago

i0hex modified the report 5 months ago

Laurent Destailleur validated this vulnerability 5 months ago

i0hex has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Laurent Destailleur marked this as fixed in **16.0** with commit **2b5b99** 5 months ago

Laurent Destailleur has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us