Stored Cross Site Scripting in openemr/openemr

0

Valid Reported on Mar 21st 2022

Vulnerability Type

Stored Cross Site-Scripting (XSS)

Affected URL

https://localhost/openemr-6.0.0/interface/new/new_comprehensive_save.php

Affected Parameters

“form_fname” “form_lname”
###Authentication Required? Yes

Issue Summary

A stored XSS vulnerability found in “/interface/new/new_comprehensive_save.php” that allows authenticated user to inject arbitrary web script in 2 different parameters (form_fname, form_lname). The XSS payload will be fired in the Ledger, History and Transactions tabs from the user’s dashboard if any authenticated user views it.

Recommendation

Ensure to HTML encode before inserting any untrusted data into HTML element content. Ensure all inputs entered by user should be sanitized and validated before processing and storage. Inputs should be filtered by the application, for example removing special characters such as < and > as well as special words such as script.

Credits

Aden Yap Chuen Zhen (chuenzhen.yap2@baesystems.com)
Rizan, Sheikh (rizan.sheikhmohdfauzi@baesystems.com) Ali Radzali (muhammadali.radzali@baesystems.com)

Issue Reproduction

Issue Reproduction

Login as any user that has privileges to create new patient. Clinicians should be able to create new patient too. (Click on Patient/Client > Click on New/Search)

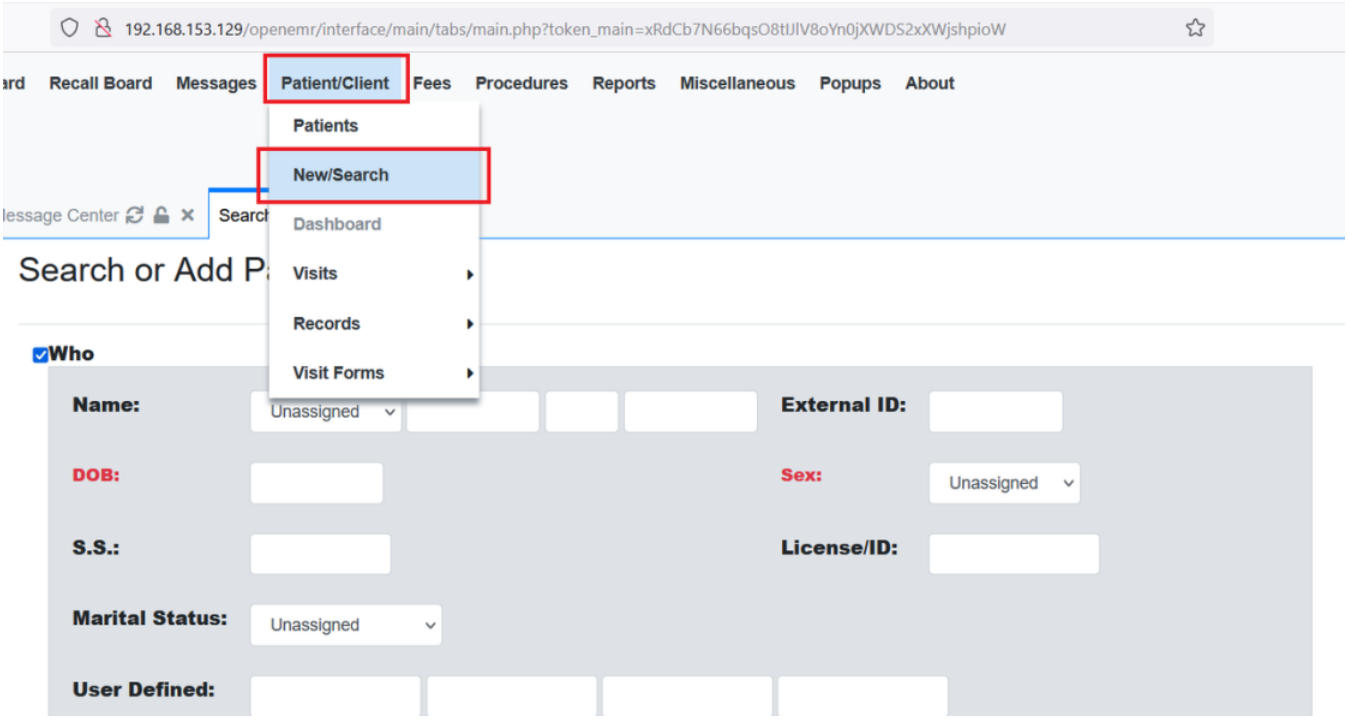
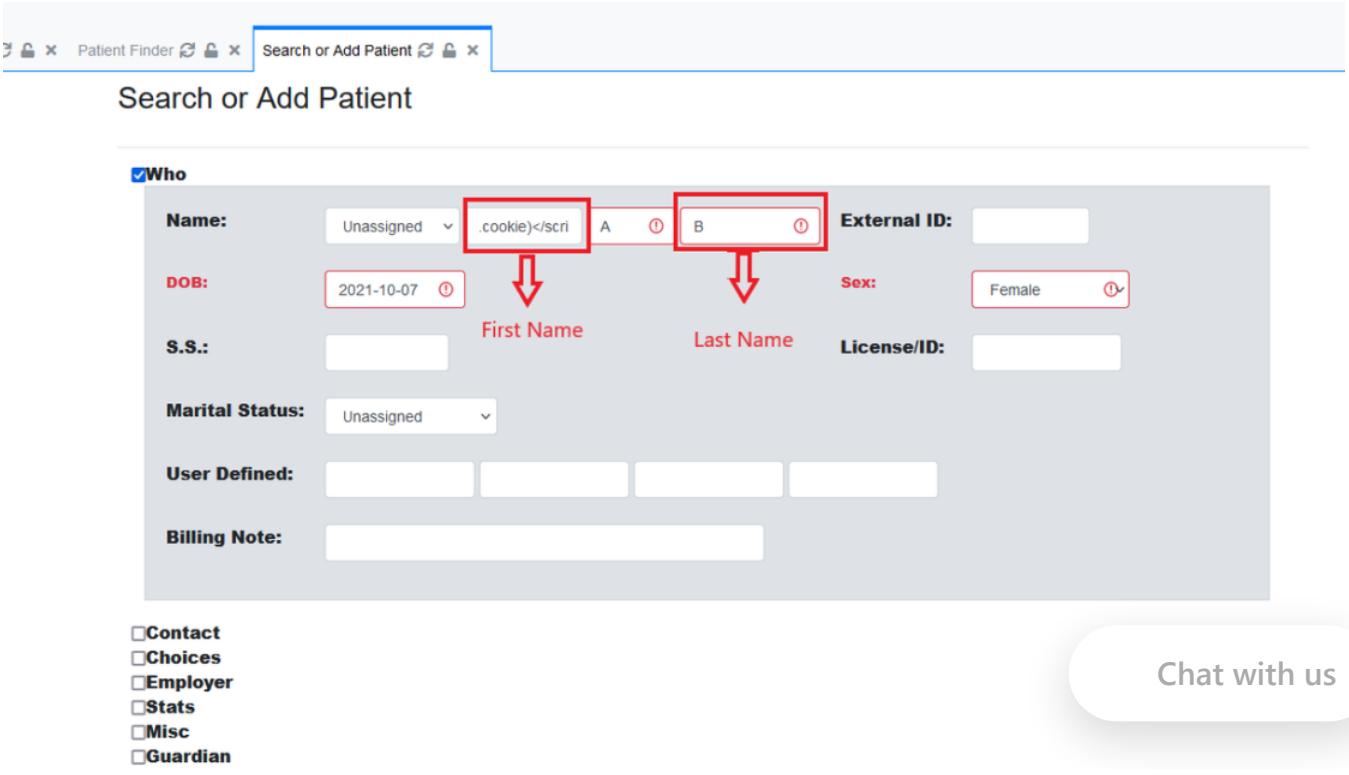


Figure 1: Login as Clinicians and Create New Patient

Insert this payload in either these 2 different input boxes. (First Name, Last Name). Then, click on “Create New Patient” and confirm it.

```
<script>alert(document.cookie)</script>
```



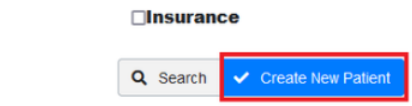


Figure 2: Insert Payload in First Name

We will get into the patient's dashboard now with the XSS payload stated in the Patient's name.

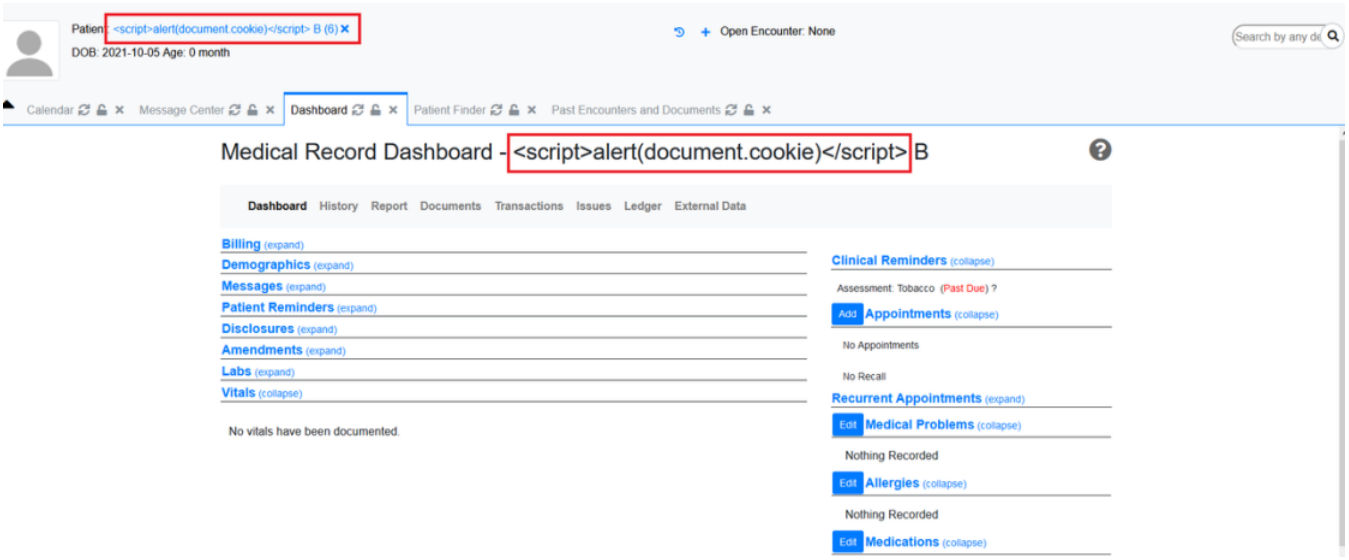


Figure 3: Patient's Dashboard with XSS Payload in Name

The XSS will be fired in the Ledger, History and Transactions tabs but not all roles have the privileges to view it. Login as Administrator or Accounting and click on Ledger tabs of that user. The cookies of the user will be pop out in alert box.

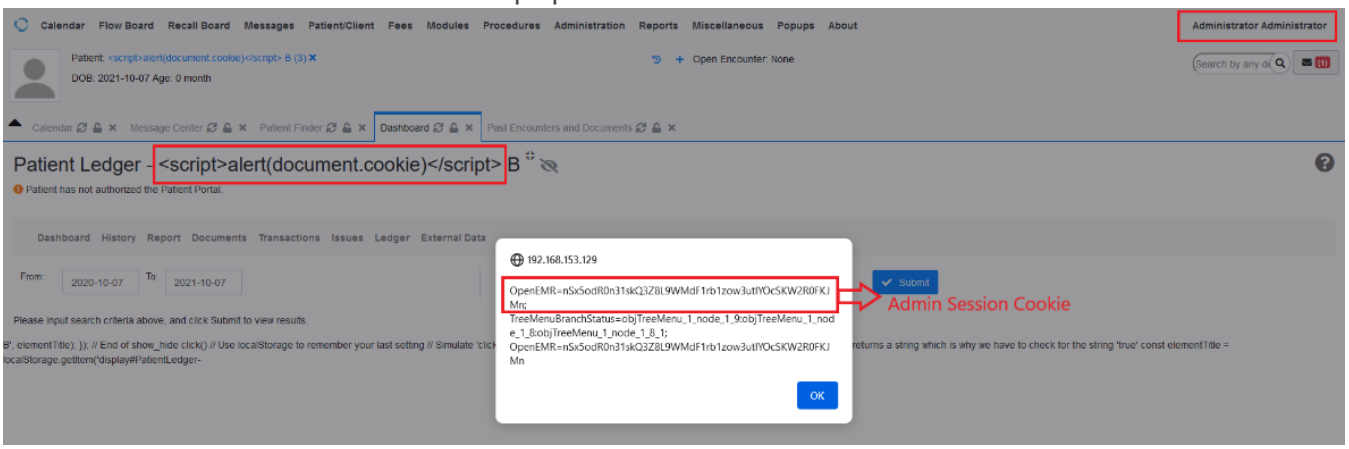
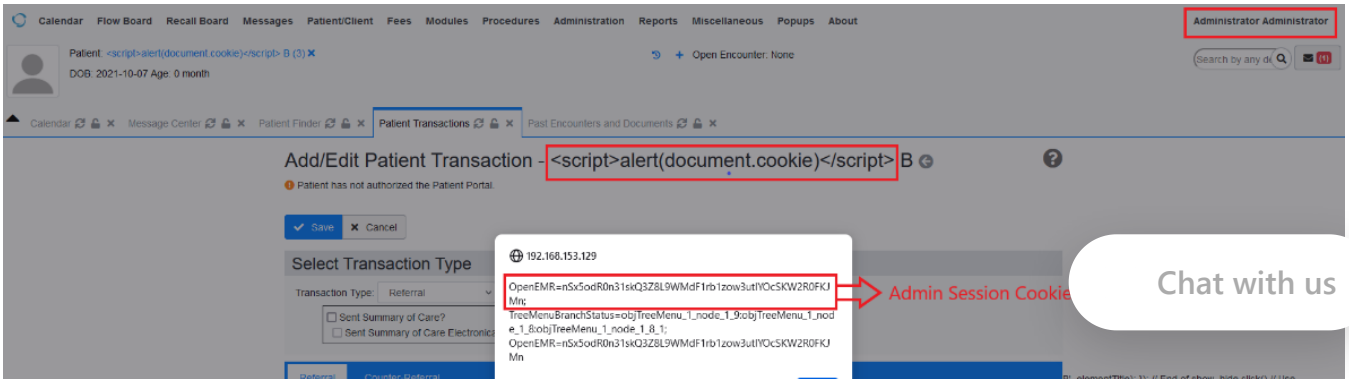


Figure 4: XSS Fired in Ledger Tabs of the User

Click on Transactions tabs of that user. Click on New or Edit any transactions. The cookies of the user will pop out in the alert box.



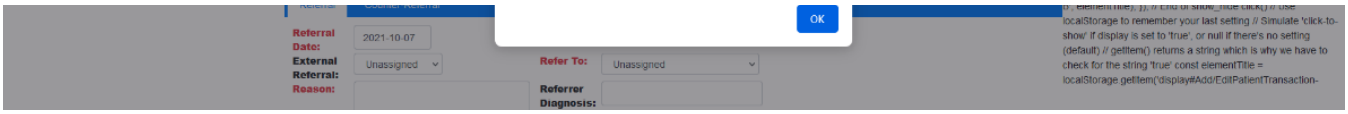


Figure 5: XSS Fired in Transactions Tabs of the User

Click on History tabs of that user. Click on Edit and the cookies of the user will pop out in the alert box.

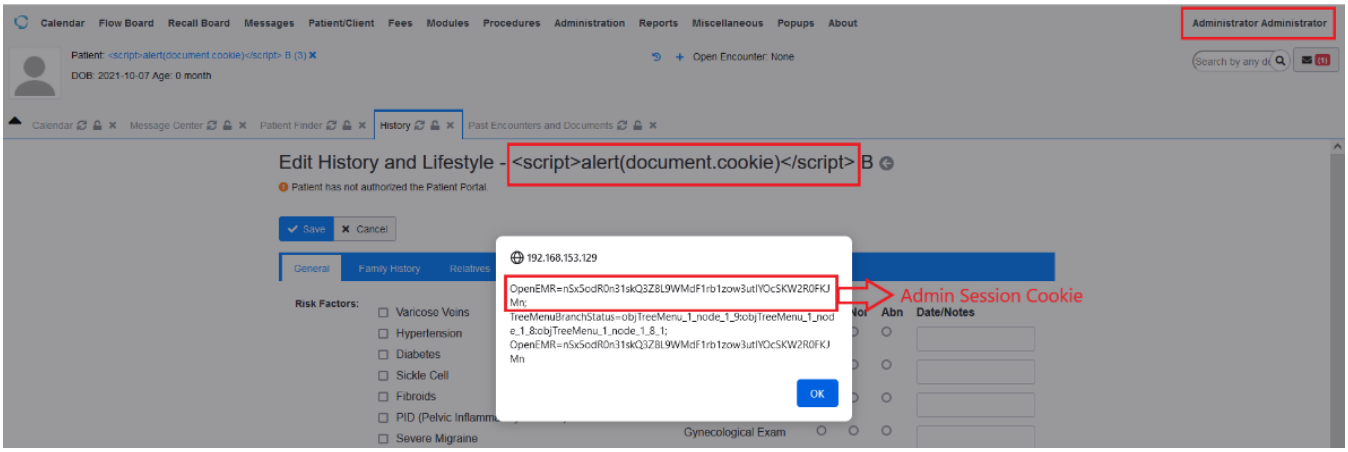


Figure 6: XSS Fired in History Tabs of the User

References

- This bug was already reported and fix by Openemr project team. Kindly reach out to Brad in case of questions. Details of patch at: https://www.open-emr.org/wiki/index.php/OpenEMR_Patches

CVE
CVE-2022-1181
(Published)

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

Severity
High (8)

Visibility
Public

Status
Fixed

Found by

r00t.pgp
@r00tpgp
amateur

This report was seen 754 times.

We are processing your report and will contact the **openemr** team within 24 hours. 8 months ago

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

We have sent a follow up to the **openemr** team. We will try again in 7 days. 8 months ago

A **openemr/openemr** maintainer validated this vulnerability 8 months ago

r00t.pgp has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

A **openemr/openemr** maintainer 8 months ago — Maintainer

This was fixed for 6.0.0 in patch 2 (6.0.0.2). This patch was released about 10 months ago.

A **openemr/openemr** maintainer marked this as fixed in **6.0.0.2** with commit **2835cc** 8 months ago

The fix bounty has been dropped ✘

This vulnerability will not receive a CVE ✘

r00t.pgp 8 months ago — Researcher

Dear @admin I've already ping the maintainer, could you please follow up on the CVE creation? Tq

Dear @maintainer, could you kindly confirm that CVE can be created for this report? Tq

A **openemr/openemr** maintainer 8 months ago — Maintainer

Also note that this fix is also in the recently released 6.1.0 version.

I consent to creation of CVE.

Jamie Slome 8 months ago

Admin

Sorted 👍

> Sign in to join this conversation