Non-Privilege User Can Created New Rule and Lead to Stored Cross Site Scripting in openemr/openemr

0

Valid Reported on Mar 20th 2022

Vulnerability Type

Stored Cross Site-Scripting (XSS)

Affected URL

https://localhost/openemr-6.0.0/ /interface/super/rules/index.php?action=edit!submit_summary

Affected Parameters

“fld_title”
###Authentication Required? Yes

Issue Summary

Non-privilege users (accounting, front-office) can create new rule and allows them to inject arbitrary web script that led to Stored Cross Site Scripting. This vulnerability found in “/interface/super/rules/index.php?action=edit!submit_summary” on one parameter (fid_title). The XSS payload will be fired in the Plan Rules that can only be viewed by privileged users.

Recommendation

nsure 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

Login to EMR using admin and we can see there is a Rules tab in (Administration > Practice > Rules).

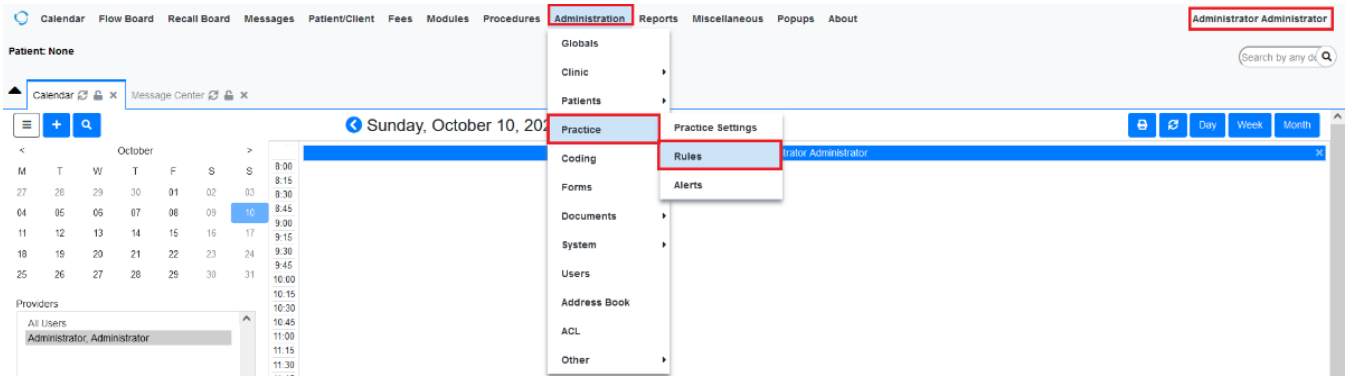

Figure 1: Login as Administrator and Go to Rules tab

Login to EMR using non-privilege users (accountant, front-office) and we can see there is no Rules tab in (Administration > Practice).

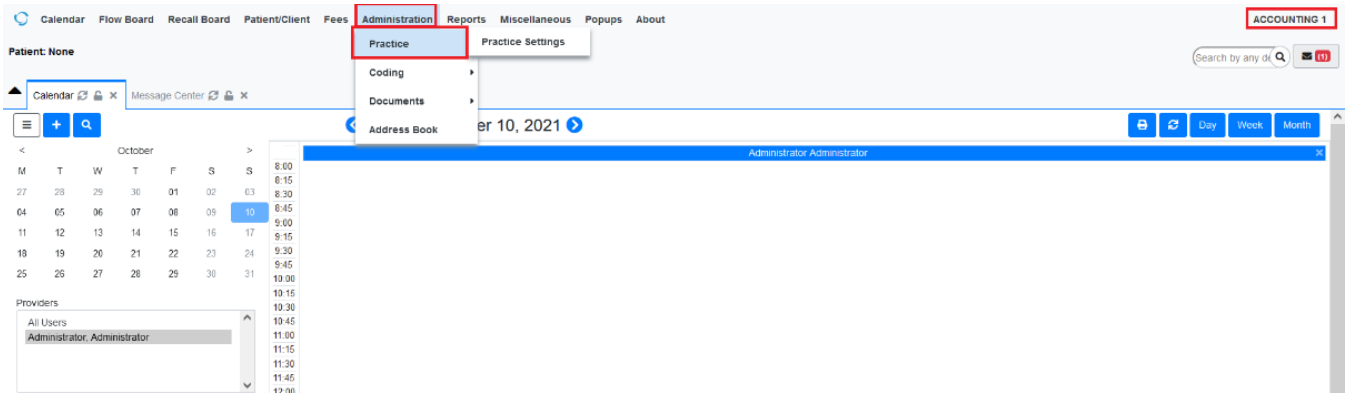

Figure 2: Login as Accountant and Check For Rules tab

Using Burp, we intercept the Admin request to add new rules in Rules tab and swap the "OpenEMR" cookie using an Accountant cookie and we are be able to create new rule that contain our XSS payload.

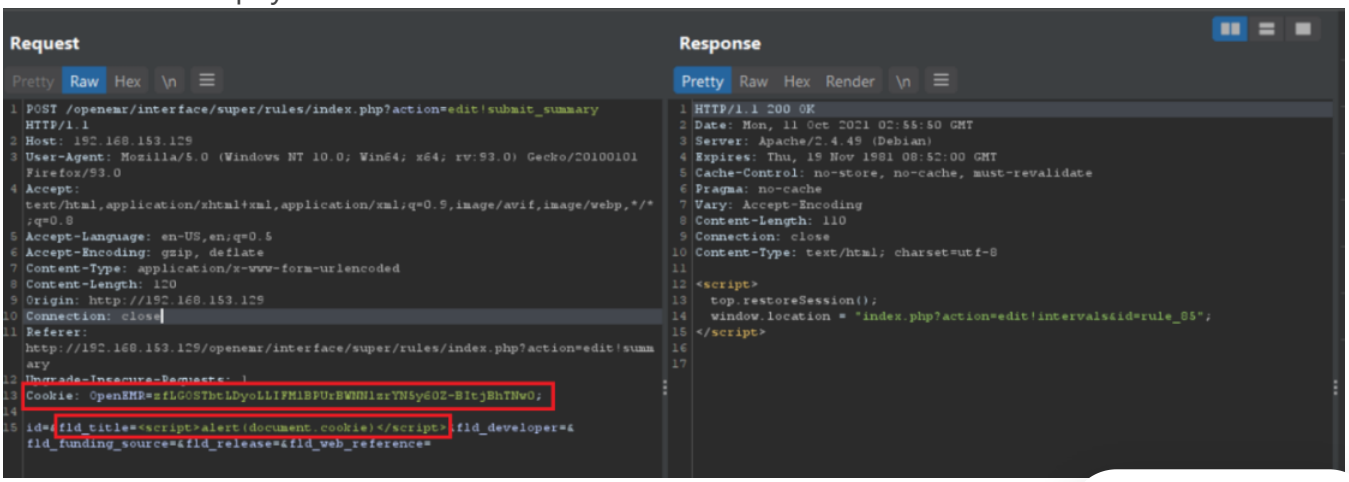

Figure 3: Burp Request Captured Using Accountant Cookie to Create New Ru

The Raw Request looks like:

```
POST /openemr/interface/super/rules/index.php?action=edit!submit_summary HT
Host: 192.168.153.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/201001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 120
Origin: http://192.168.153.129
Connection: close
Referer: http://192.168.153.129/openemr/interface/super/rules/index.php?act
Upgrade-Insecure-Requests: 1
Cookie: OpenEMR=zfLGOSTbtLDyoLLIFMlBPUrBWNNlzrYN5y60Z-BItjBhTNw0;
id=&fld_title=<script>alert(document.cookie)</script>&fld_developer=&fld_fu
```

Go to Rules page (Administration > Practice > Rules) and Click “Go” on Plans Configuration.

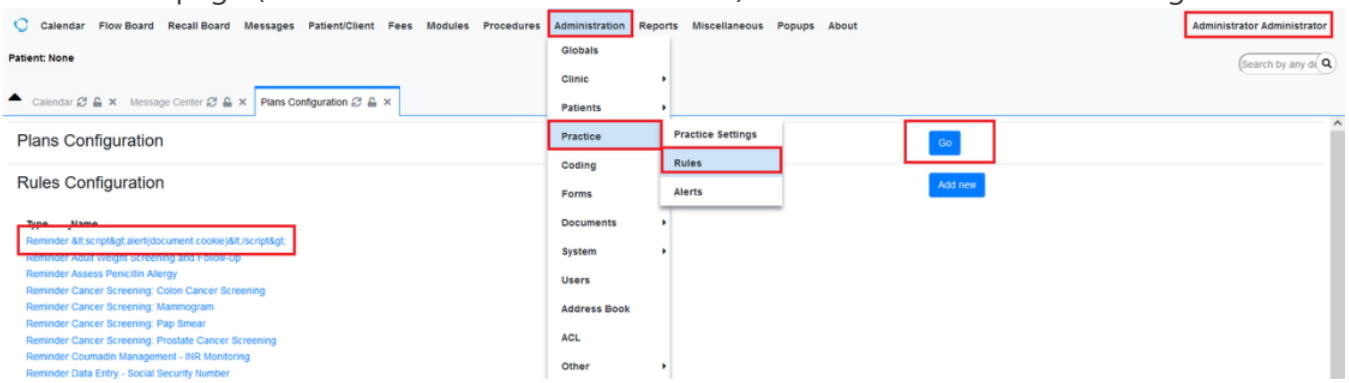

Figure 4: Plans & Rules Configuration Page

The XSS will be fired in any Plans configurations. For example, an Admin can select any plans and the cookies of the admin will be pop out in alert box.

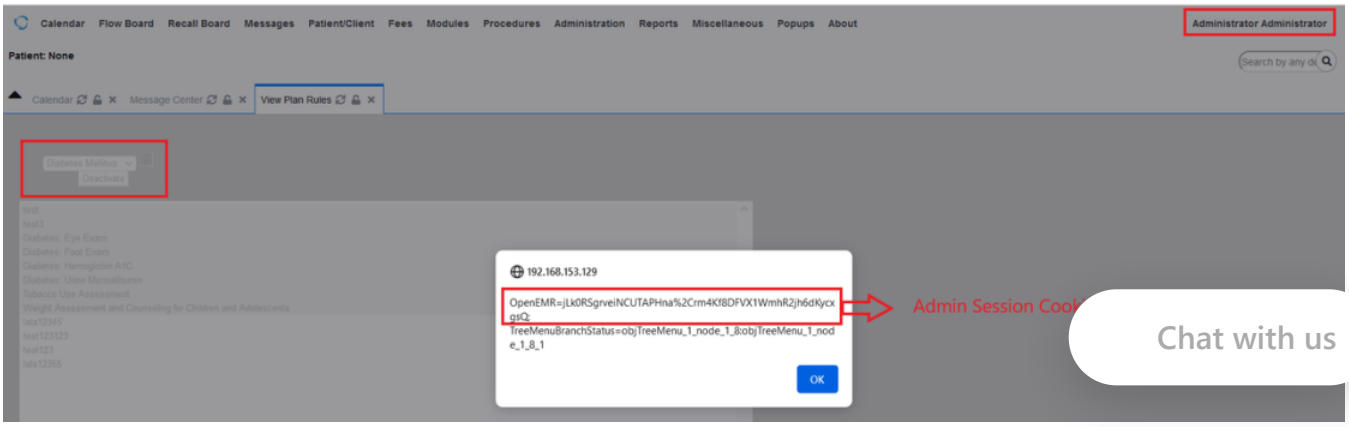

Figure 5: XSS Fired in Any Selected Plans

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-2022-1179
(Published)

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

Severity
Medium (4.6)

Visibility
Public

Status
Fixed

Found by

r00t.pgp
@r00tpgp
amateur

This report was seen 615 times.

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

r00t.pgp modified the report 8 months ago

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

A **openemr/openemr** maintainer has acknowledged this report 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 has been fixed in 6.0.0.4 .

A openemr/openemr maintainer marked this as fixed in 6.0.0.4 with commit 347ad6
8 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

r00t.pgp 8 months ago Researcher

Hi, Kindly issue a CVE for this vulnerability. Tq

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