huntr

Missing Function Level Access Control in openemr/openemr

0

✓ Valid Reported on Mar 28th 2022

Vulnerability Type

Missing Function Level Access Control

Affected URL

62 vulnerable instances as listed in Table 1

Authentication Required?

Yes

Issue Summary

Web applications usually only show functionality that a user has the need for and right to use in the UI. However, this is not the case for the OpenEMR. Non-privilege users (Accounting, Front-Office, Physician & Clinician) can directly browse to the administrator modules to compromise the confidentiality and integrity of the application. Additionally, the promiscuous privileges of user roles (Accounting, Front-Office, Physician & Clinician) allow users to access each other modules without restriction as listed in Table 1.

Recommendation

Disallow access to all functions in the application by default, then review the user roles matrix of the OpenEMR and apply access only to those users and other parts of the application that are permitted to use it. Don’t rely on the security by obscurity such as hiding buttons and links to functionality within the UI.

Credits

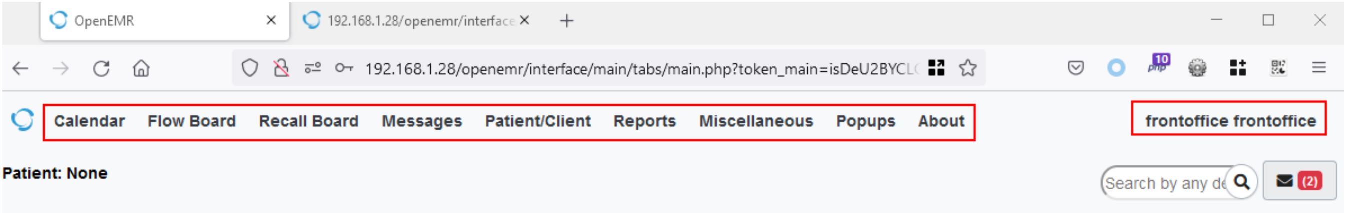
Aden Yap Chuen Zhen (chuenzhen.yap2@baesystems.com)
Rizan, Sheikh (rizan.sheikhmohdfauzi@baesystems.com)

Chat with us

Ali Radzali (muhammadali.radzali@baesystems.com)

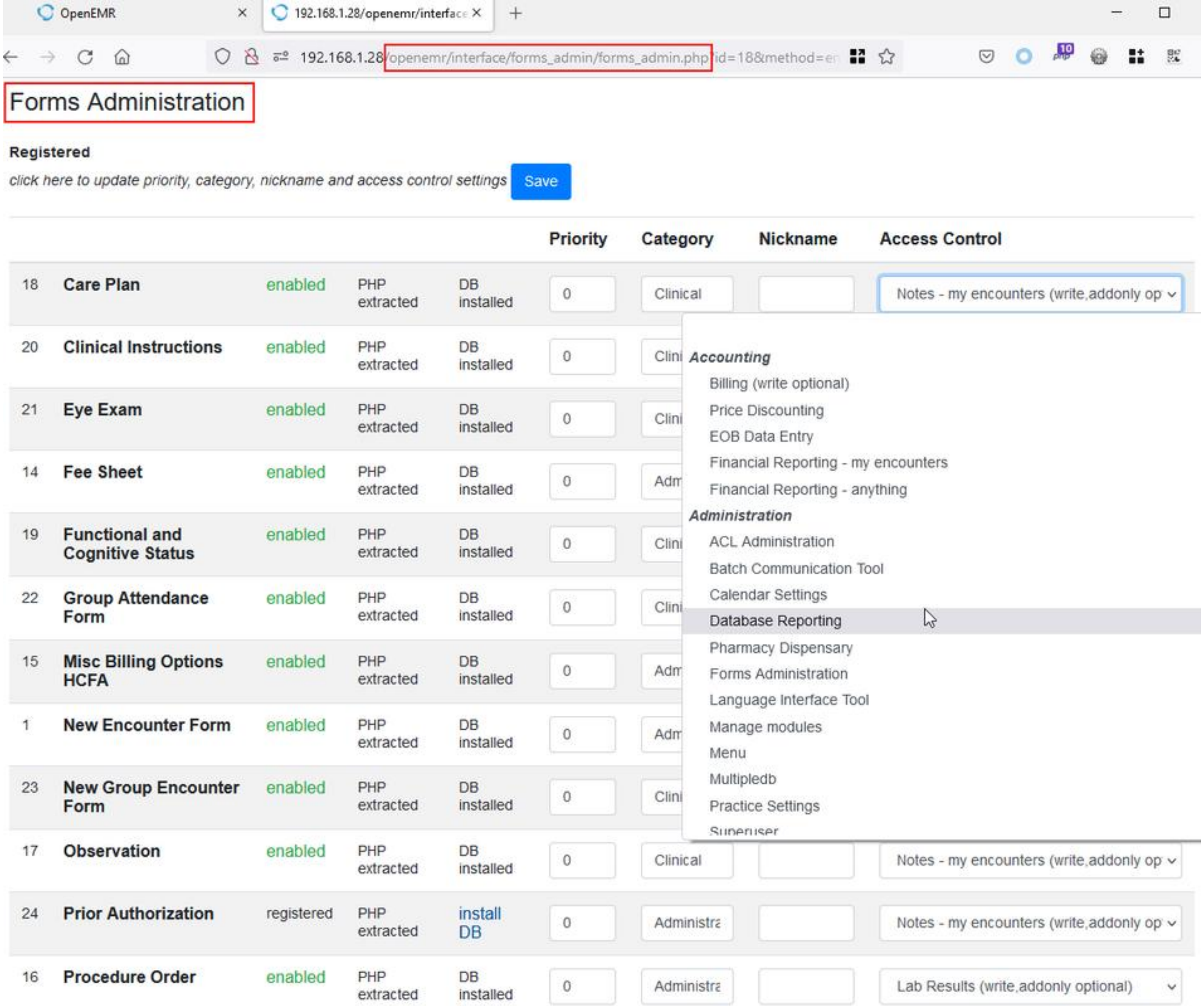
Issue Reproduction

Login as a user (e.g., Front Office). Choose and browse any of the URL that appear “Vulnerable” belong to user (e.g., Front Office) shown in the Error! Reference source not found.. Below are several examples of the affected instances:



Patient: None

Figure 1: The Modules belong to Front Office user


OpenEMR
192.168.1.28/openemr/interface
192.168.1.28/openemr/interface/forms_admin/forms_admin.php?id=18&method=er

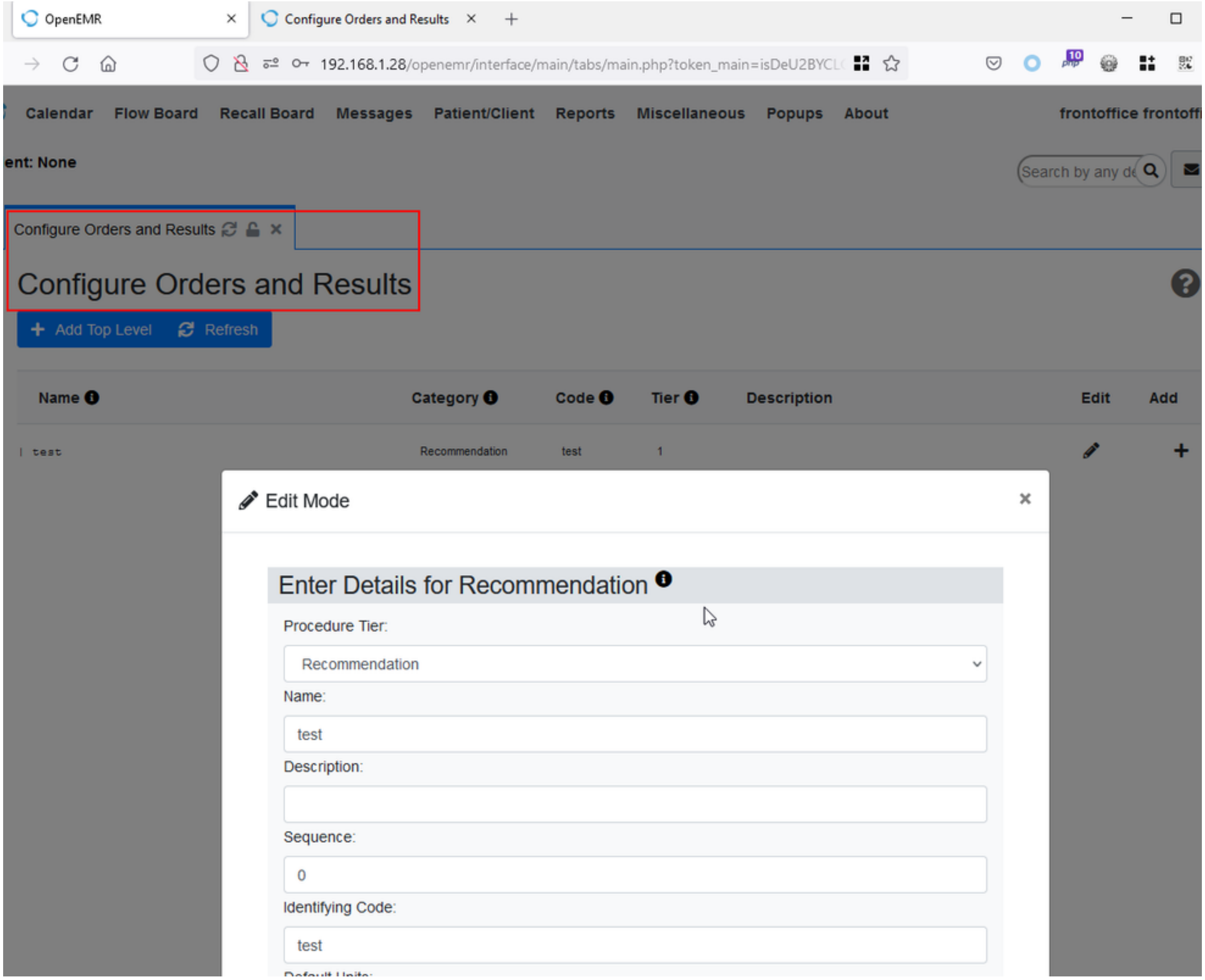
Forms Administration

Registered

click here to update priority, category, nickname and access control settings

					Priority	Category	Nickname	Access Control
18	**Care Plan**	enabled	PHP extracted	DB installed	0	Clinical		Notes - my encounters (write,addonly op
20	**Clinical Instructions**	enabled	PHP extracted	DB installed	0	Clini		
21	**Eye Exam**	enabled	PHP extracted	DB installed	0	Clini		
14	**Fee Sheet**	enabled	PHP extracted	DB installed	0	Adm		
19	**Functional and Cognitive Status**	enabled	PHP extracted	DB installed	0	Clini		
22	**Group Attendance Form**	enabled	PHP extracted	DB installed	0	Clini		
15	**Misc Billing Options HCFA**	enabled	PHP extracted	DB installed	0	Adm		
1	**New Encounter Form**	enabled	PHP extracted	DB installed	0	Adm		
23	**New Group Encounter Form**	enabled	PHP extracted	DB installed	0	Clini		
17	**Observation**	enabled	PHP extracted	DB installed	0	Clinical		Notes - my encounters (write,addonly op
24	**Prior Authorization**	registered	PHP extracted	install DB	0	Administra		Notes - my encounters (write,addonly op
16	**Procedure Order**	enabled	PHP extracted	DB installed	0	Administra		Lab Results (write,addonly optional)

Figure 2: Front Office gained unauthorised access to “Administrator -> Forms -> Forms Administrator”: http://localhost/openemr/interface/forms_admin/forms_admin.php



192.168.1.28/openemr/interface/main/tabs/main.php?token_main=isDeU2BYCL

ent: None

Configure Orders and Results

Configure Orders and Results

Name	Category	Code	Tier	Description	Edit	Add
test	Recommendation	test	1		✎	+

Enter Details for Recommendation

Procedure Tier: Recommendation

Name: test

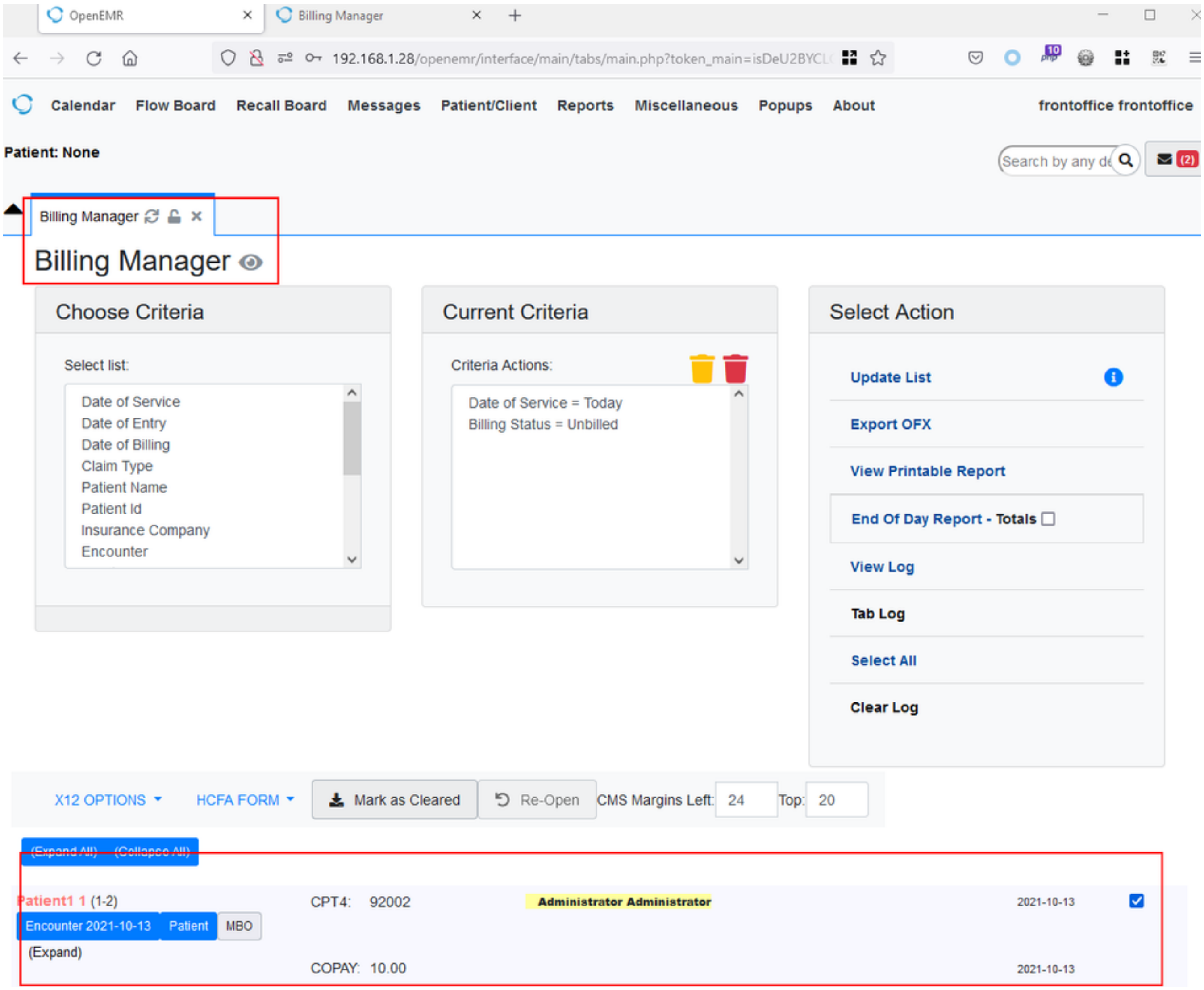
Description:

Sequence: 0

Identifying Code: test

Default Units:

Figure 3: Accessed to Admin Module “Procedure -> Configuration”: http://localhost/openemr/interface/orders/types.php via window load module after tampered the endpoint using BurpSuite



Patient: None

Billing Manager

Select list:

Date of Service
Date of Entry
Date of Billing
Claim Type
Patient Name
Patient Id
Insurance Company
Encounter

Criteria Actions:

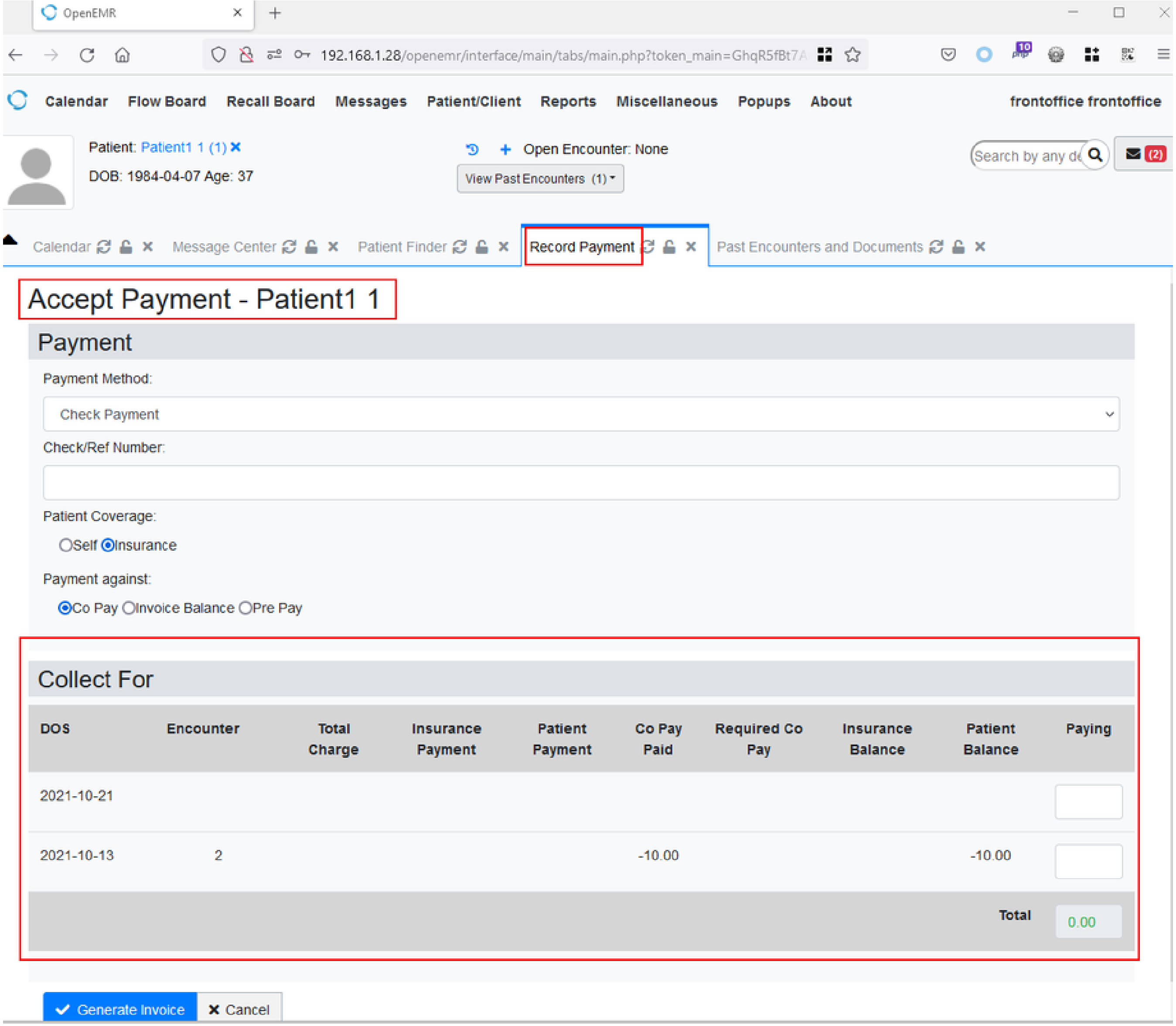
Date of Service = Today
Billing Status = Unbilled

CMS Margins Left: 24 Top: 20

Patient1 1 (1-2) CPT4: 92002 Administrator Administrator 2021-10-13 ☑

COPAY: 10.00 2021-10-13

Figure 4: Front Office gained unauthorised access to Accounting module “Fees -> Billing Manager”: http://localhost/openemr/interface/billing/billing_report.php



Patient: Patient1 1 (1)
DOB: 1984-04-07 Age: 37

Open Encounter: None

View Past Encounters (1)

Accept Payment - Patient1 1

Payment

Payment Method:

Check Payment

Check/Ref Number:

Patient Coverage:

○Self ●Insurance

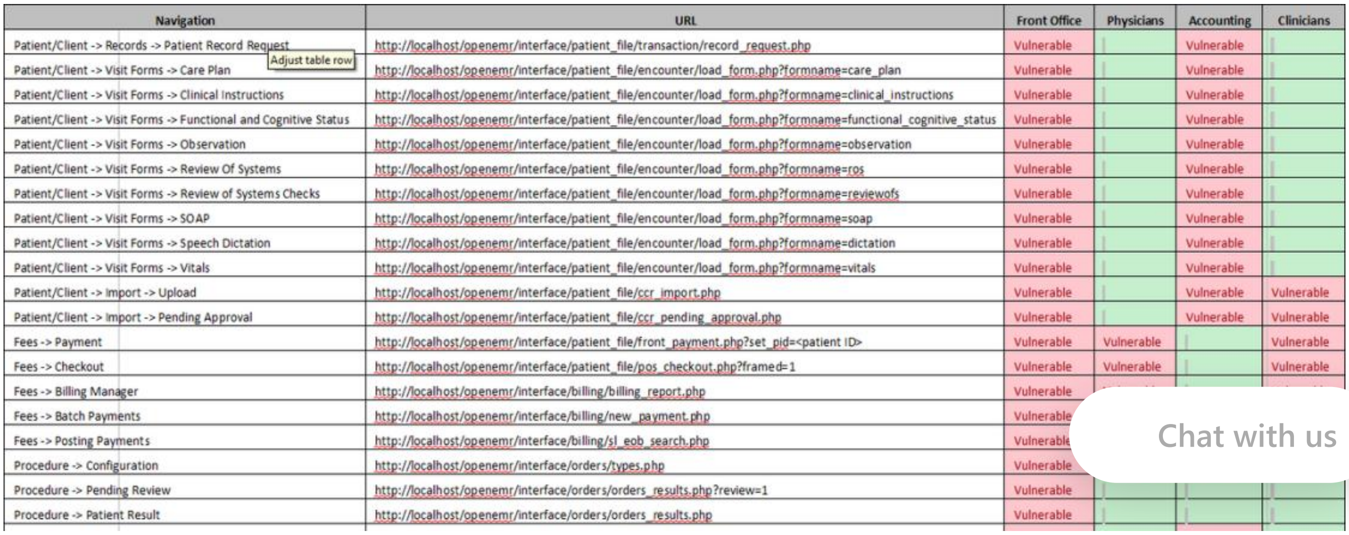
Payment against:

●Co Pay ○Invoice Balance ○Pre Pay

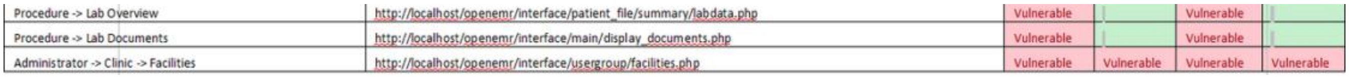
Collect For

DOS	Encounter	Total Charge	Insurance Payment	Patient Payment	Co Pay Paid	Required Co Pay	Insurance Balance	Patient Balance	Paying
2021-10-21									
2021-10-13	2				-10.00			-10.00	
								Total	0.00

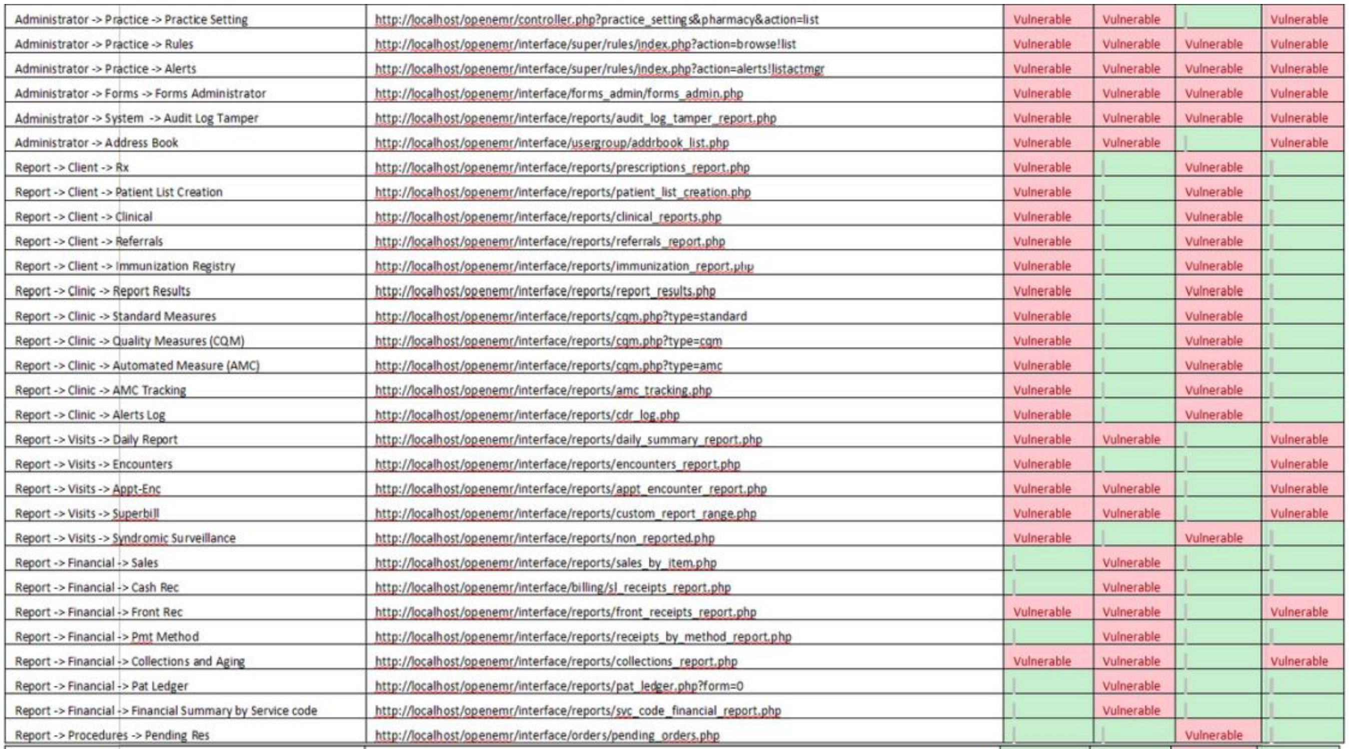
Figure 5: Front Office gained unauthorised access to Accounting module “Fees -> Payment”: http://localhost/openemr/interface/billing/billing_report.php

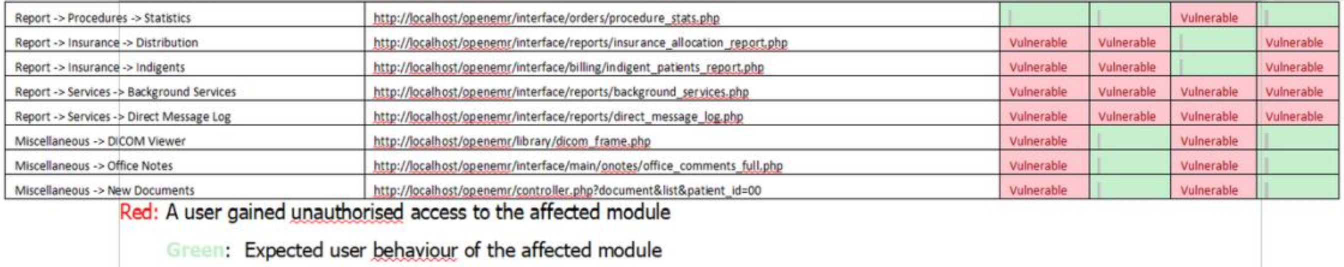

Adjust table row

Navigation	URL	Front Office	Physicians	Accounting	Clinicians
Patient/Client -> Records -> Patient Record Request	http://localhost/openemr/interface/patient_file/transaction/record_request.php	Vulnerable		Vulnerable	
Patient/Client -> Visit Forms -> Care Plan	http://localhost/openemr/interface/patient_file/encounter/load_form.php?formname=care_plan	Vulnerable		Vulnerable	
Patient/Client -> Visit Forms -> Clinical Instructions	http://localhost/openemr/interface/patient_file/encounter/load_form.php?formname=clinical_instructions	Vulnerable		Vulnerable	
Patient/Client -> Visit Forms -> Functional and Cognitive Status	http://localhost/openemr/interface/patient_file/encounter/load_form.php?formname=functional_cognitive_status	Vulnerable		Vulnerable	
Patient/Client -> Visit Forms -> Observation	http://localhost/openemr/interface/patient_file/encounter/load_form.php?formname=observation	Vulnerable		Vulnerable	
Patient/Client -> Visit Forms -> Review Of Systems	http://localhost/openemr/interface/patient_file/encounter/load_form.php?formname=ros	Vulnerable		Vulnerable	
Patient/Client -> Visit Forms -> Review of Systems Checks	http://localhost/openemr/interface/patient_file/encounter/load_form.php?formname=reviewofs	Vulnerable		Vulnerable	
Patient/Client -> Visit Forms -> SOAP	http://localhost/openemr/interface/patient_file/encounter/load_form.php?formname=soap	Vulnerable		Vulnerable	
Patient/Client -> Visit Forms -> Speech Dictation	http://localhost/openemr/interface/patient_file/encounter/load_form.php?formname=dictation	Vulnerable		Vulnerable	
Patient/Client -> Visit Forms -> Vitals	http://localhost/openemr/interface/patient_file/encounter/load_form.php?formname=vitals	Vulnerable		Vulnerable	
Patient/Client -> Import -> Upload	http://localhost/openemr/interface/patient_file/ccr_import.php	Vulnerable		Vulnerable	Vulnerable
Patient/Client -> Import -> Pending Approval	http://localhost/openemr/interface/patient_file/ccr_pending_approval.php	Vulnerable		Vulnerable	Vulnerable
Fees -> Payment	http://localhost/openemr/interface/patient_file/front_payment.php?set_pid=<patient ID>	Vulnerable	Vulnerable		Vulnerable
Fees -> Checkout	http://localhost/openemr/interface/patient_file/pos_checkout.php?framed=1	Vulnerable	Vulnerable		Vulnerable
Fees -> Billing Manager	http://localhost/openemr/interface/billing/billing_report.php	Vulnerable	Vulnerable		Vulnerable
Fees -> Batch Payments	http://localhost/openemr/interface/billing/new_payment.php	Vulnerable	[illegible]	[illegible]	[illegible]
Fees -> Posting Payments	http://localhost/openemr/interface/billing/sl_eob_search.php	Vulnerable	[illegible]	[illegible]	[illegible]
Procedure -> Configuration	http://localhost/openemr/interface/orders/types.php	Vulnerable	[illegible]	[illegible]	[illegible]
Procedure -> Pending Review	http://localhost/openemr/interface/orders/orders_results.php?review=1	Vulnerable			
Procedure -> Patient Result	http://localhost/openemr/interface/orders/orders_results.php	Vulnerable			



Procedure -> Lab Overview	http://localhost/openemr/interface/patient_file/summary/labdata.php	Vulnerable		Vulnerable	
Procedure -> Lab Documents	http://localhost/openemr/interface/main/display_documents.php	Vulnerable		Vulnerable	
Administrator -> Clinic -> Facilities	http://localhost/openemr/interface/usergroup/facilities.php	Vulnerable	Vulnerable	Vulnerable	Vulnerable





Administrator -> Practice -> Practice Setting	http://localhost/openemr/controller.php?practice_settings&pharmacy&action=list	Vulnerable	Vulnerable		Vulnerable
Administrator -> Practice -> Rules	http://localhost/openemr/interface/super/rules/index.php?action=browse!list	Vulnerable	Vulnerable	Vulnerable	Vulnerable
Administrator -> Practice -> Alerts	http://localhost/openemr/interface/super/rules/index.php?action=alerts!listactmgr	Vulnerable	Vulnerable	Vulnerable	Vulnerable
Administrator -> Forms -> Forms Administrator	http://localhost/openemr/interface/forms_admin/forms_admin.php	Vulnerable	Vulnerable	Vulnerable	Vulnerable
Administrator -> System -> Audit Log Tamper	http://localhost/openemr/interface/reports/audit_log_tamper_report.php	Vulnerable	Vulnerable	Vulnerable	Vulnerable
Administrator -> Address Book	http://localhost/openemr/interface/usergroup/addrbook_list.php	Vulnerable	Vulnerable		Vulnerable
Report -> Client -> Rx	http://localhost/openemr/interface/reports/prescriptions_report.php	Vulnerable		Vulnerable	
Report -> Client -> Patient List Creation	http://localhost/openemr/interface/reports/patient_list_creation.php	Vulnerable		Vulnerable	
Report -> Client -> Clinical	http://localhost/openemr/interface/reports/clinical_reports.php	Vulnerable		Vulnerable	
Report -> Client -> Referrals	http://localhost/openemr/interface/reports/referrals_report.php	Vulnerable		Vulnerable	
Report -> Client -> Immunization Registry	http://localhost/openemr/interface/reports/immunization_report.php	Vulnerable		Vulnerable	
Report -> Clinic -> Report Results	http://localhost/openemr/interface/reports/report_results.php	Vulnerable		Vulnerable	
Report -> Clinic -> Standard Measures	http://localhost/openemr/interface/reports/cqm.php?type=standard	Vulnerable		Vulnerable	
Report -> Clinic -> Quality Measures (CQM)	http://localhost/openemr/interface/reports/cqm.php?type=cqm	Vulnerable		Vulnerable	
Report -> Clinic -> Automated Measure (AMC)	http://localhost/openemr/interface/reports/cqm.php?type=amc	Vulnerable		Vulnerable	
Report -> Clinic -> AMC Tracking	http://localhost/openemr/interface/reports/amc_tracking.php	Vulnerable		Vulnerable	
Report -> Clinic -> Alerts Log	http://localhost/openemr/interface/reports/cdr_log.php	Vulnerable		Vulnerable	
Report -> Visits -> Daily Report	http://localhost/openemr/interface/reports/daily_summary_report.php	Vulnerable	Vulnerable		Vulnerable
Report -> Visits -> Encounters	http://localhost/openemr/interface/reports/encounters_report.php	Vulnerable			Vulnerable
Report -> Visits -> Appt-Enc	http://localhost/openemr/interface/reports/appt_encounter_report.php	Vulnerable	Vulnerable		Vulnerable
Report -> Visits -> Superbill	http://localhost/openemr/interface/reports/custom_report_range.php	Vulnerable	Vulnerable		Vulnerable
Report -> Visits -> Syndromic Surveillance	http://localhost/openemr/interface/reports/non_reported.php	Vulnerable		Vulnerable	
Report -> Financial -> Sales	http://localhost/openemr/interface/reports/sales_by_item.php		Vulnerable		
Report -> Financial -> Cash Rec	http://localhost/openemr/interface/billing/sl_receipts_report.php		Vulnerable		
Report -> Financial -> Front Rec	http://localhost/openemr/interface/reports/front_receipts_report.php	Vulnerable	Vulnerable		Vulnerable
Report -> Financial -> Pmt Method	http://localhost/openemr/interface/reports/receipts_by_method_report.php		Vulnerable		
Report -> Financial -> Collections and Aging	http://localhost/openemr/interface/reports/collections_report.php	Vulnerable	Vulnerable		Vulnerable
Report -> Financial -> Pat Ledger	http://localhost/openemr/interface/reports/pat_ledger.php?form=0		Vulnerable		
Report -> Financial -> Financial Summary by Service code	http://localhost/openemr/interface/reports/svc_code_financial_report.php		Vulnerable		
Report -> Procedures -> Pending Res	http://localhost/openemr/interface/orders/pending_orders.php			Vulnerable	
Report -> Procedures -> Statistics	http://localhost/openemr/interface/orders/procedure_stats.php			Vulnerable	
Report -> Insurance -> Distribution	http://localhost/openemr/interface/reports/insurance_allocation_report.php	Vulnerable	Vulnerable		Vulnerable
Report -> Insurance -> Indigents	http://localhost/openemr/interface/billing/indigent_patients_report.php	Vulnerable	Vulnerable		Vulnerable
Report -> Services -> Background Services	http://localhost/openemr/interface/reports/background_services.php	Vulnerable	Vulnerable	Vulnerable	Vulnerable
Report -> Services -> Direct Message Log	http://localhost/openemr/interface/reports/direct_message_log.php	Vulnerable	Vulnerable	Vulnerable	Vulnerable
Miscellaneous -> DICOM Viewer	http://localhost/openemr/library/dicom_frame.php	Vulnerable		Vulnerable	
Miscellaneous -> Office Notes	http://localhost/openemr/interface/main/onotes/office_comments_full.php	Vulnerable		Vulnerable	
Miscellaneous -> New Documents	http://localhost/openemr/controller.php?document&list&patient_id=00	Vulnerable		Vulnerable	

Red: A user gained unauthorised access to the affected module

Green: Expected user behaviour of the affected module

Table 1: Affected Instances

Impact

Non privilege users can view privileged information containing personal records belonging to patients.

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-2022-2493
(Published)

Vulnerability Type
CWE-1083: Data Access from Outside Expected Data Manager Component

Severity
High (8.3)

Registry
Other

Affected Version
below 6.1.0

Visibility
Public

Status
Fixed

Found by

r00t.pgp
@r00tpgp
amateur

This report was seen 520 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

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

r00t.pgp modified the report 8 months ago

We have sent a second follow up to the **openemr** team. We will try again in 10 days. 8 months ago

We have sent a third and final follow up to the **openemr** team. This report is now considered stale. 7 months ago

A **openemr/openemr** maintainer validated this vulnerability 7 months ago

Currently working on fixes for this.

r00t.pgp has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

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

We have sent a second fix follow up to the **openemr** team. We will try again in 10 days. 7 months ago

A openemr/openemr maintainer 7 months ago Maintainer

A preliminary fix for this has been placed in our development codebase at https://github.com/openemr/openemr/commit/871ae5198d8ca18fd17257ae7c5c906a52dca908

The fix will officially be released in the next OpenEMR 6.1.0 patch 2 (6.1.0.2). After we release this patch, I will then mark this item as fixed (probably in about a month).

We have sent a third and final fix follow up to the **openemr** team. This report is now considered stale. 7 months ago

r00t.pgp 4 months ago Researcher

Hi @admin, according to OpenEMR website @ https://www.open-emr.org/wiki/index.php/OpenEMR_Downloads.
The latest version for d/l is 7.0.0. Since this bug is considered fixed, can you kindly issue the CVE for this finding please? Thanks

Jamie Slome 4 months ago Admin

Happy to issue a CVE if the maintainer is happy for one to be assigned and published.

@maintainer - can I proceed with a CVE for this report?

A **openemr/openemr** maintainer marked this as fixed in **7.0.0** with commit **871ae5** 4 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

A **openemr/openemr** maintainer 4 months ago Maintainer

version 7.0.0 was recently released, which fixed this vulnerability.
ok to proceed with CVE

Jamie Slome 4 months ago Admin

Sorted 👍

Sign in to join this conversation