

Finding Name: Broken access control

Name	Team	Role	Project	Quality Assurance	Is this a re-tested Finding?
ABDULMAJEED HUSSAIN A ALZAHIRANI	PT	Senior	Gopher Guardian		

Was this Finding Successful?
Yes

Finding Description

The application does not enforce proper role verification for sensitive actions and resources. This allows unauthorized users to perform actions or access areas of application that should be restricted to higher-privileged roles (e.g., administrators)

Risk Rating

Impact: Major

Likelihood: High

Impact values				
Very Minor	Minor	Significant	Major	Severe
Risk that holds little to no impact. Will not cause damage and regular activity can continue.	Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity.	Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally.	Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally.	Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run.

Likelihood				
Rare	Unlikely	Moderate	High	Certain
Event may occur and/or if it did, it happens in specific circumstances.	Event could occur occasionally and/or could happen (at some point)	Event may occur and/or happens.	Event occurs at times and/or probably happens a lot.	Event is occurring now and/or happens frequently.

Business Impact

- Data Breaches: Unauthorized access to sensitive or confidential information.

- Privilege Escalation: Regular users gaining administrative or elevated privileges.
- Service Disruption: Unauthorized modifications to application configurations or data.

Affected Assets


Sensitive Application Data

Administrative Functions

Evidence

Provide a step-by-step guide on how to reproduce vulnerability with screenshots

Step 1. Register to the application using the following data



Full Name
Deakin

Email
Deakin123@Deakin.com

Password
Deakin@123456789

Confirm password
Deakin@123456789

Register as:



Step 2.it redirects us to login page try to login but as administrator

Login as:

- ☐ Caretaker
- ☒ Company Admin
- ☐ Nurse

Email
Deakin123@Deakin.com

Password
Deakin@123456789

Login

Register



Step 3. From my previous report I could bypass otp verification by enter these values

Enter PIN code

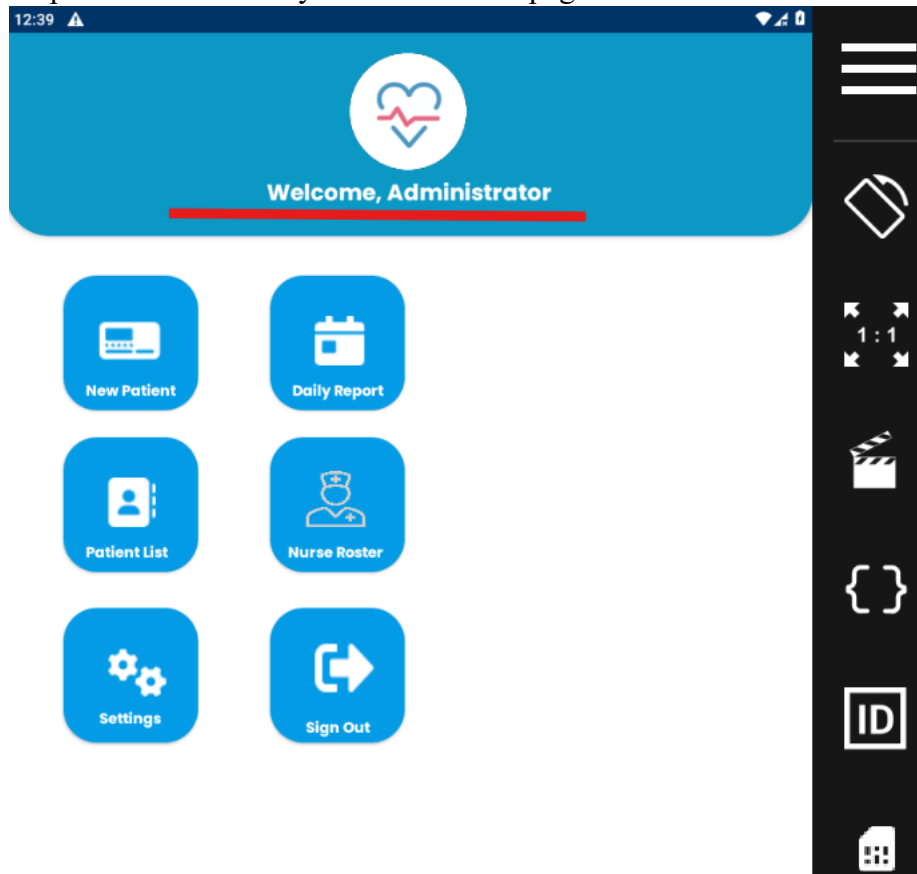
Please check your email for the code.

This code is valid for the next 15 minutes.

Submit

[Resend](#)

Step 4. We successfully enter the admin page



Remediation Advice

- Verify Roles for All Sensitive Operations.
- Secure API Endpoints.
- Verify role of user during login.

References

[OWASP Broken Access Control](#)

[NIST Role-Based Access Control \(RBAC\) Model](#)

Abdulmajeed Hussain A AlZahrani

s223844731@deakin.edu.au

Pentest Leader Feedback.

The lead will provide feedback to enact on