① Role Based vulnerability
② user registeration process
③ account provisining process
④ account enumeration (disable user account)
⑤ weak or unenforced user name policy.

① Test role Definition:

Application has
↳ two different group → admin, user

admin has access to sensitive functionality in formsense

what if a user can access admin panal and see prohibited content then there is a vulnerability.

* System role to manage users and authorization of system resources.

* How to test ?
① login to admin account (white box testing)
② visit admin page
↳ any.com/admin
③ logout
④ login as normal user
⑤ visit the admin page directory or any page have higher access

* Test user registeration process

① verify that identity requirements for user registeration
② validation the registeration
You will get many vulnerabilities.

① can anyone register for access of this app ?
② are registeration vetted by a human prior to provisioning
③ can the same person or identity register multiple times.
④ can users register for different roles or permissions
⑤ what proof of identity is required for registeration to be seccessful
⑥ are registered identities verified.

* Validation registeration process

You need to focus on :

① can identity information be easily faked or forged

② can the exchange of identity information be manipulated during registeration.

things you should think of while hunting :

① is there any validation of credentials → email id, mobile number ? not? it is usdn.

② can I use anyone email to register ?

if I can use credentials one more time and register, then this is vulnerability.

* Test account provisoning process.

the provisioning of accounts presents an opportunity for an attacker to create a valid account without proper identification and authorization.

Keep in mind :

① is there any verification, authorization presents on provisioning requests.

② is there any verification, authorization presents on de-provisioning requests.

③ can admin provision other administrator or just users.

④ can admin or normal user de-provision themself.

Big Note :

let's say you deleted your account but account data still on the application then there is a vulnerability.

Steps to hunt :

1. sign up
2. go to : profile → upload your image
4. delete your account
3. copy image location.
5. after account deletion just open the image link again.

if you will see image still there, then it is vulnerable.

* testing for account enumeration and guessable user account.

is to verify if its possible to collect as set of valid usernames by interacting with the authentication mechanism of the App