Risk Assessment and Mitigation

Your Trusted Shield is **Us**

The main findings

1- Basic user with no access authority, can duplicate any pre-built dashboard

4/7
Threat rate

7/7
Misuse rate

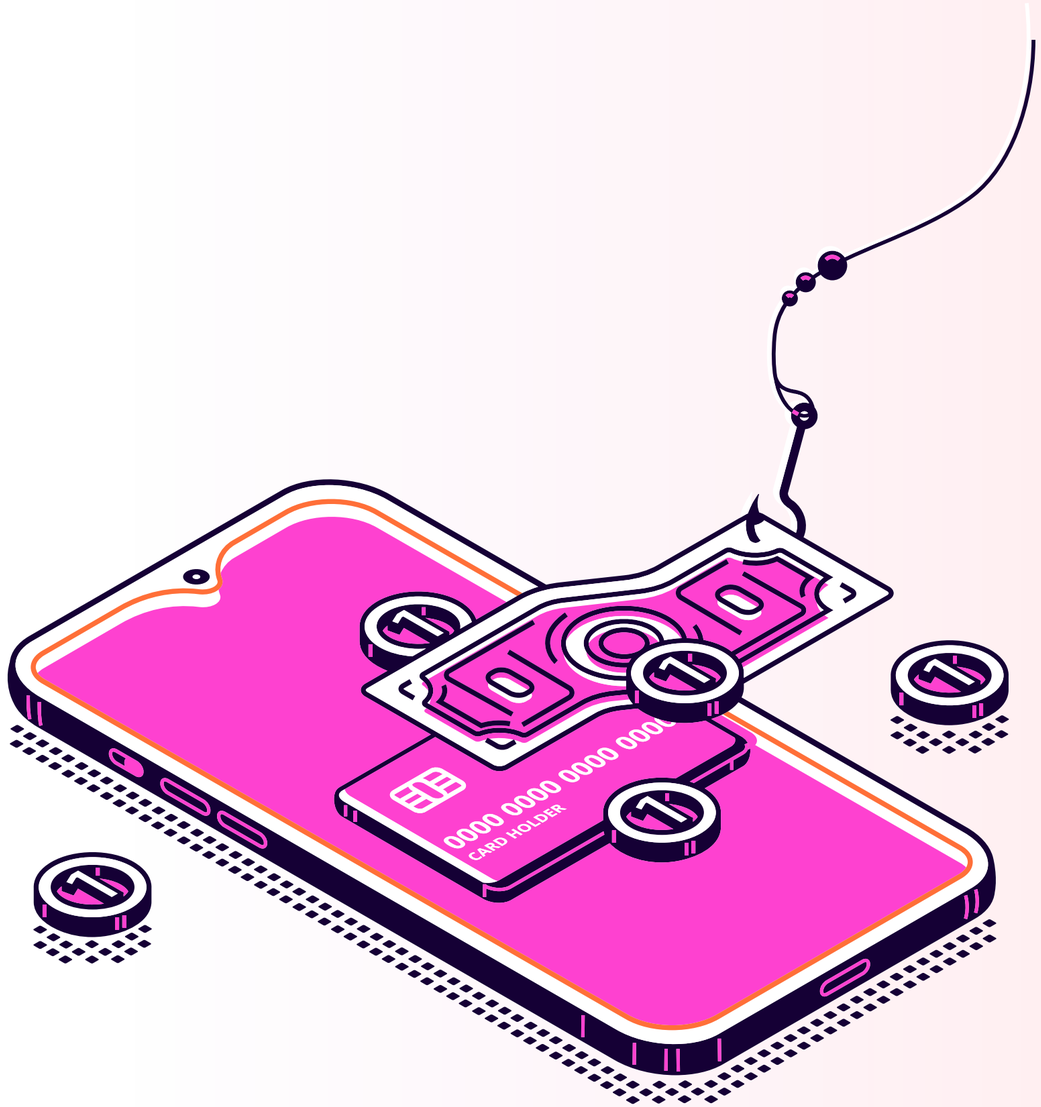
5/7
Consequences

2- Basic user with lowest privileges can duplicate any Private dashboard

6/7
Threat rate

7/7
Misuse rate

7/7
Consequences



Some impacts

How could a malicious user exploit this?

Network Security

malicious user could be able to access private data

Data Protection

breaking the confidentiality and edit the private data as desired without supervision

Potential Threat

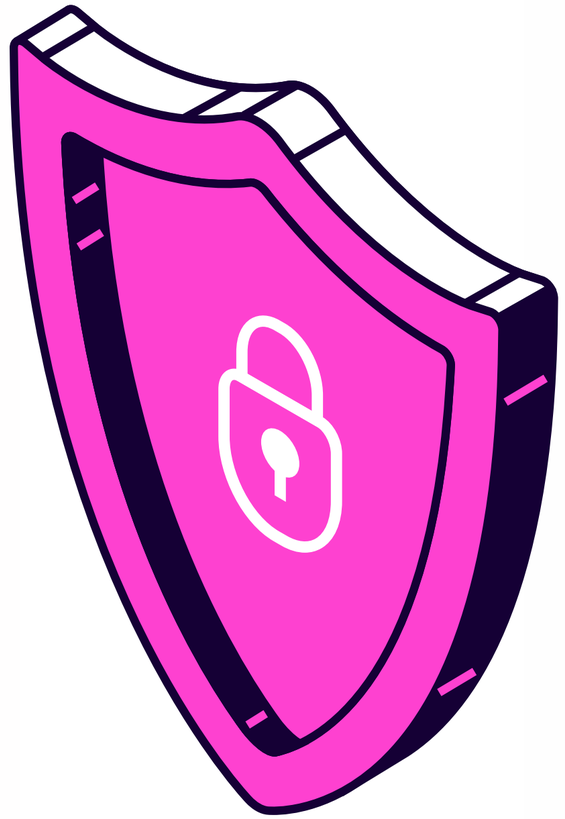
this misconfiguration may lead to data breach for potitional competitors

Loss trust

Customers may lose trust in the platform if unauthorized access to their resources is discovered

Safeguard your data

Protect your valuable data from being exposed, corrupted and misused



01.

Prevention

Always prevent the access by default

02.

avoidance

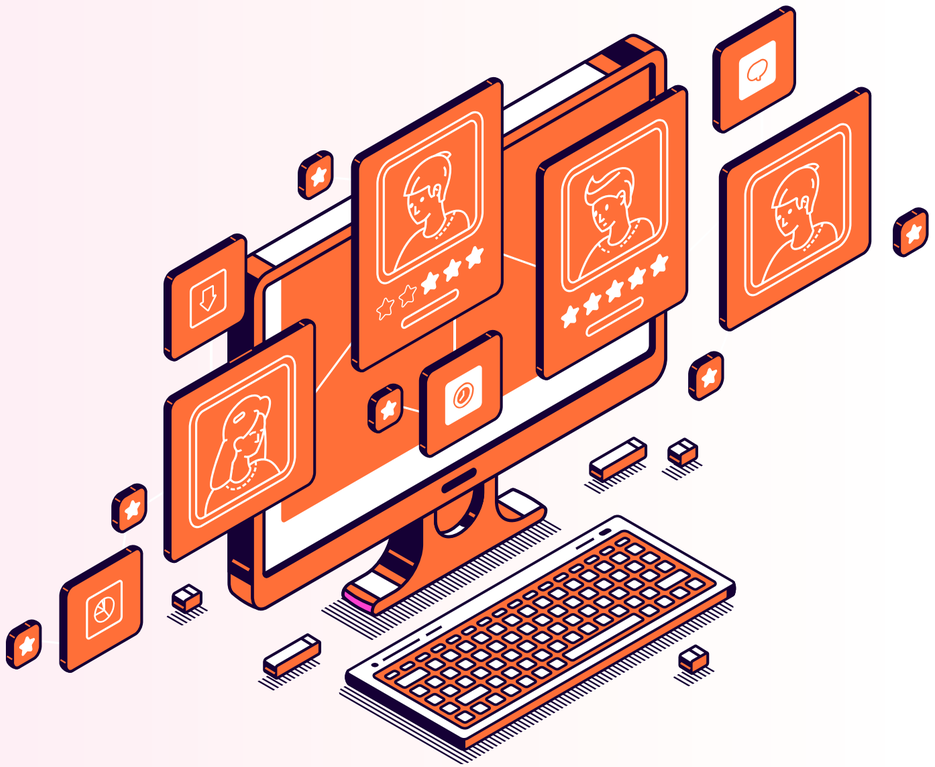
avoid using sequential numeric IDs in URLs

03.

Role-Based Access Control

Implement strict RBAC policies to ensure users only have access to resources necessary for their role.

Essential steps should be taken



Provide training for developers on secure coding practices, particularly regarding access controls. Make sure that your team is aware with the latest attack scenarios, vulnerabilities and weakness in the different technologies

- **24/7 threat monitoring must applied**
- **implementation of Regular Updates and Patch Management**
- **Code Reviews and Security Testing must always be applied**
- **Always enforce access controls on the server side.**

Get protected today and everday!

Created by

- **The Penetration testing team of the future**

Mohamed Ali

Mohamed abdaziz

Nada Elhadad

Farida Talaat

Eman Ahmed

- The detailed report