Nickname：Xenc米斯特安全

Vulnerability URL: Fill out this field if it's Web

https://www.*********.net/#/*****

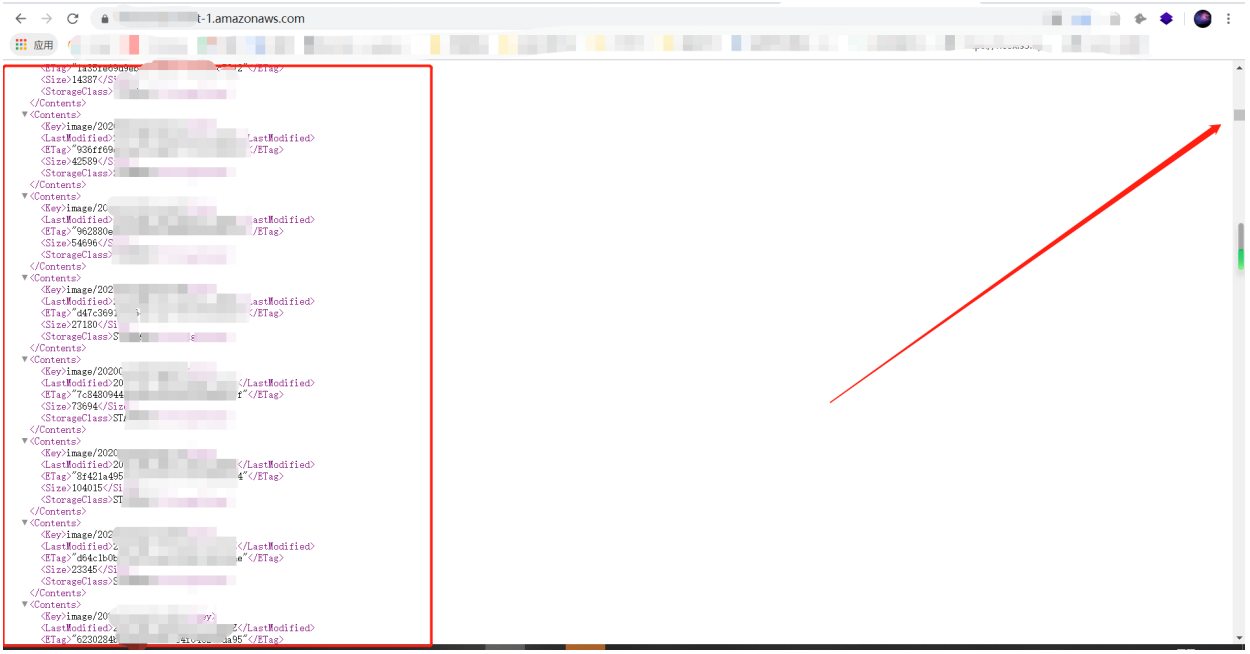
Short Description: Vulnerability Description, Utilization Condition, Hazard, etc.

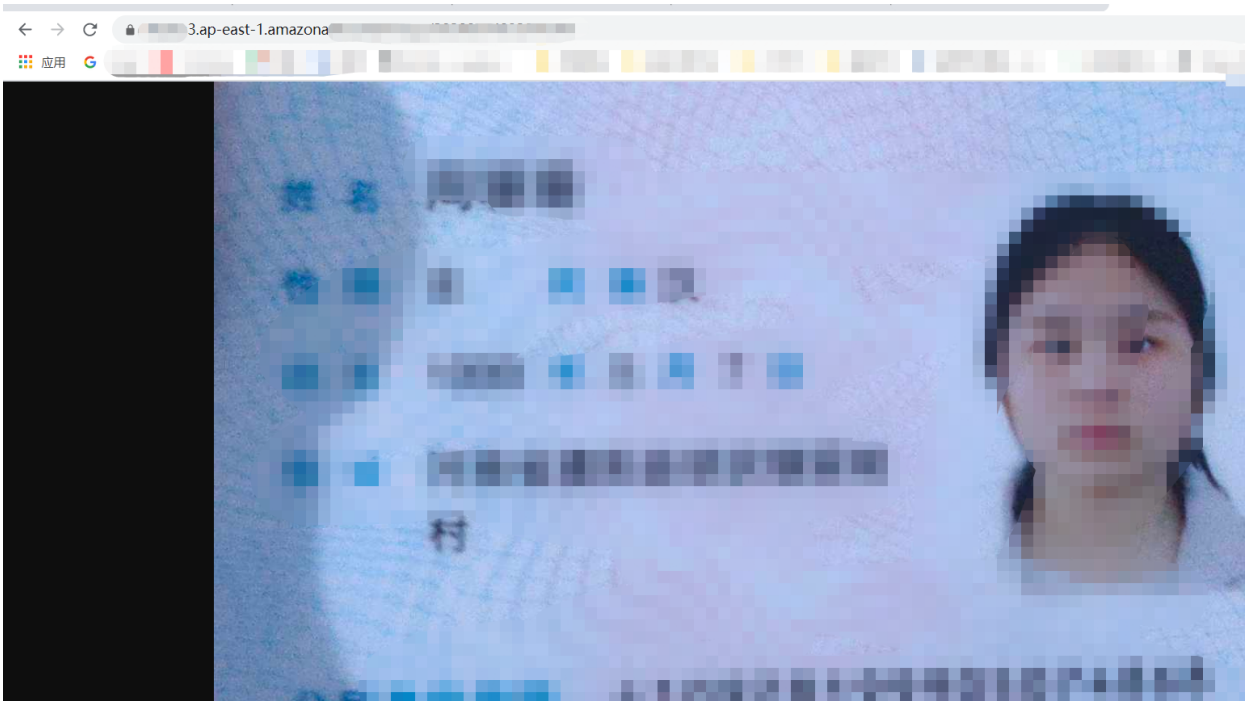
The interface returns an url of picture after User uploads ID information:

e.g. https://****.s3.ap-east-1.amazonaws.com/image/*****************90

Pictures on the exchange database, such as copies of users' ID, can be viewed by clicking https://****s3.ap-east-1.amazonaws.com/ - paths of all uploaded ID copies are shown here.

Proof of the Vulnerability:





Codes used by the Vulnerability:

As Above

Remediation Plan:

Do not display all files

Summary

If the AWS S3 bucket permission is not strictly restricted, serious data breaches may be caused. Ops should correctly set the S3 access policy under the Principle of Least Privilege:
1. Block the public access to the storage bucket (including list, write and ACL read/write)
2. Do not allow public access permissions to all Sensitive objects (such as KYC photos, etc.)
3. Regularly check whether there is a publicly accessible S3 Bucket through the console