白帽子昵称：Xenc米斯特安全

漏洞URL：如果是Web就填写此项

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

简要描述：漏洞说明、利用条件、危害等

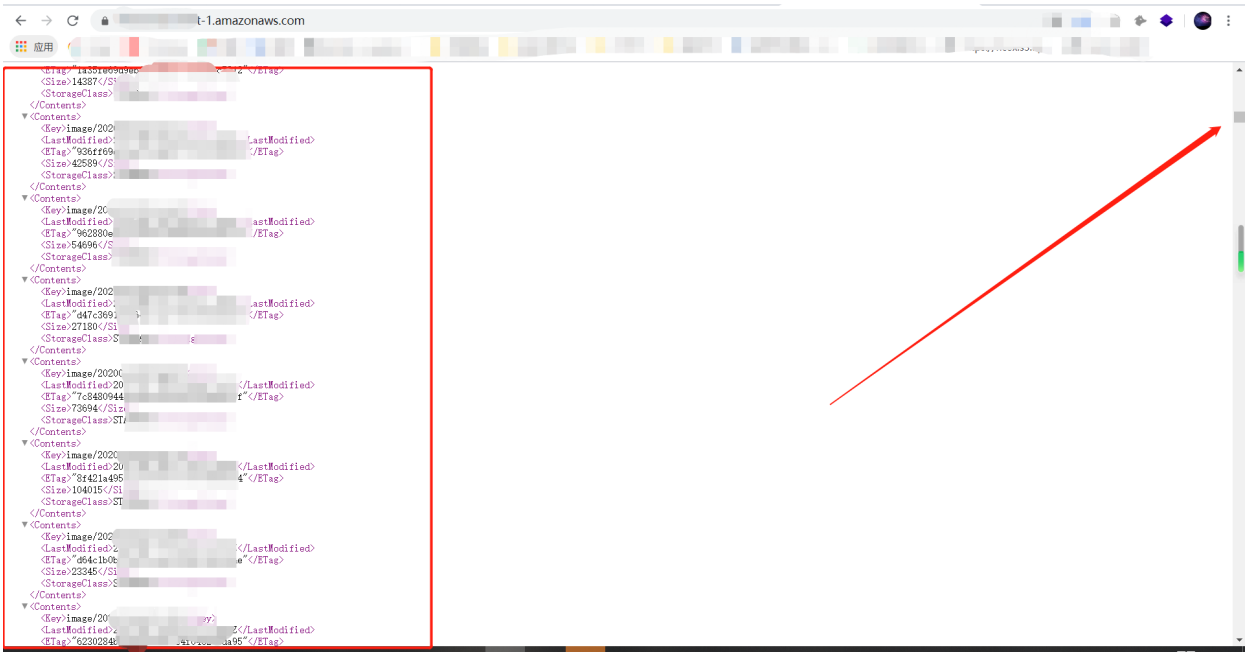
在上传身份证的时候会返回一个数据包时上传图片的地址：

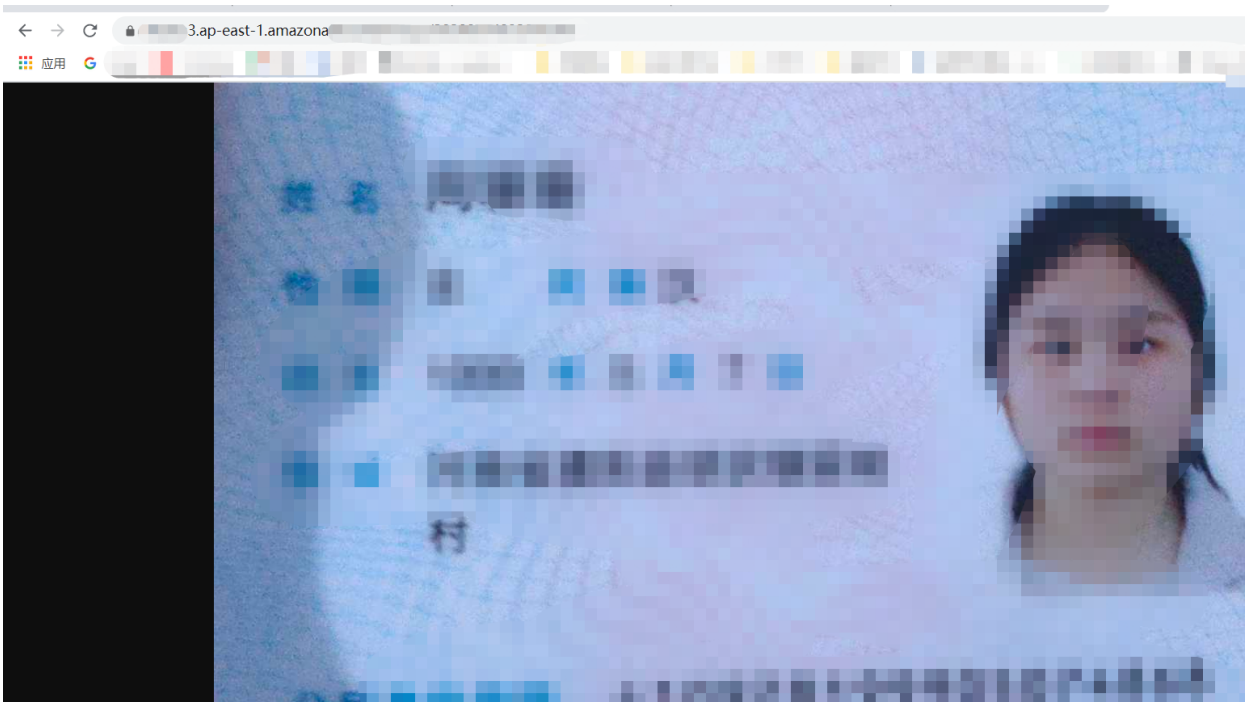
如：https://****.s3.ap-east-1.amazonaws.com/image/*****************90

打开https://****s3.ap-east-1.amazonaws.com/

即可查看到全站用户身份证照片等交易所图片信息： 全部上传的身份证照片都会在这里显示路径

漏洞证明：





漏洞利用代码：

如上

修复方案：

不要将所有的文件显示出来

漏洞总结

AWS中S3的Bucket桶访问策略如果没有严格限制，可能导致严重的信息泄漏事件，运维人员应正确的配置S3访问策略，遵循最小权限原则：

1.存储桶禁止开启公共访问权限（包括列出、写入、ACL的读写等）

2.敏感对象（如kyc认证照片等信息）禁止开启公共访问权限

3.通过控制台定期检查是否存在公共访问的S3 Bucket