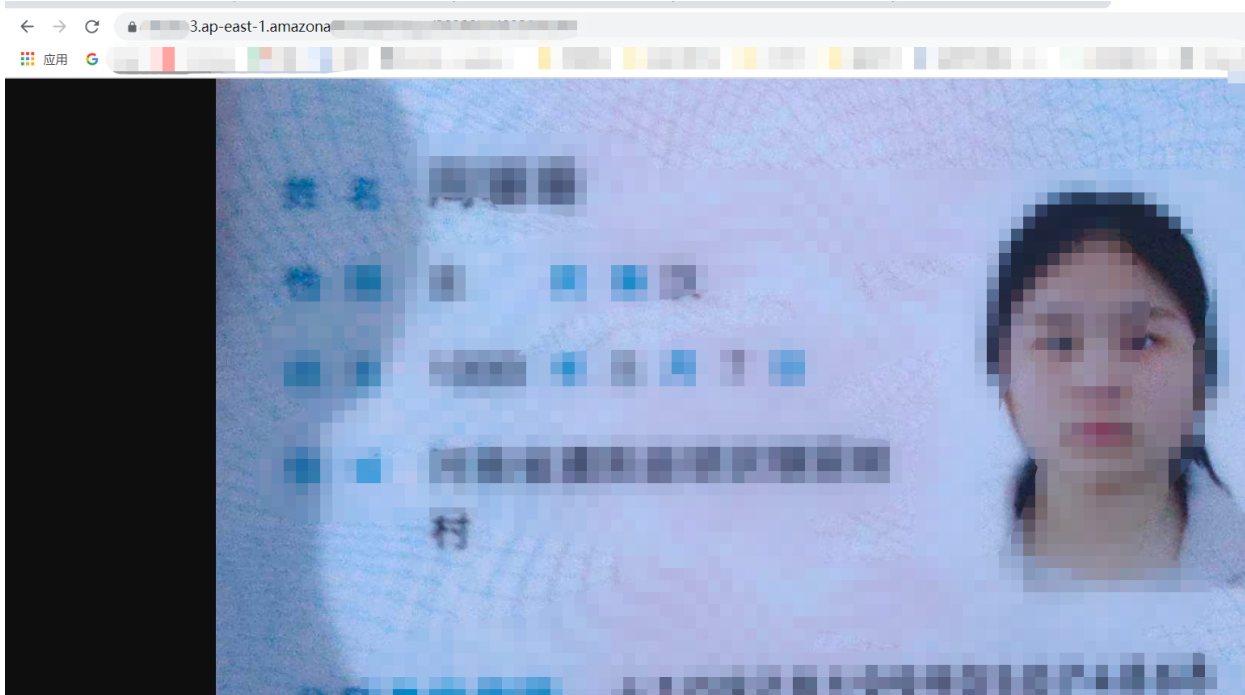


The screenshot shows the output of the AWS CLI command `aws s3 ls`. The output is XML-formatted, showing a directory listing of an S3 bucket. A red box highlights the first three objects, and a red arrow points to the fourth object.

```

<Tag>1a30r00uuec</Tag>
<Size>14387</Size>
<StorageClass>
</Contents>
<Contents>
  <Key>image/202
  <LastModified>
  <ETag>"936rrf69
  <Size>42589</Size>
  <StorageClass>
  </Contents>
  <Contents>
    <Key>image/20
    <LastModified>
    <ETag>"962880e
    <Size>54696</Size>
    <StorageClass>
    </Contents>
    <Contents>
      <Key>image/202
      <LastModified>
      <ETag>"d47c369
      <Size>27180</Size>
      <StorageClass>S
      </Contents>
      <Contents>
        <Key>image/20200
        <LastModified>20
        <ETag>"7c8480944
        <Size>73694</Size>
        <StorageClass>ST
        </Contents>
        <Contents>
          <Key>image/2020
          <LastModified>20
          <ETag>"81421a495
          <Size>104015</Size>
          <StorageClass>ST
          </Contents>
          <Contents>
            <Key>image/202
            <LastModified>
            <ETag>"d54c1b0e
            <Size>23345</Size>
            <StorageClass>S
            </Contents>
            <Contents>
              <Key>image/20
              <LastModified>
              <ETag>"6230284
  
```



**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