CVE 2019 -15813 Sentrifugo 3.2 - File Upload Restriction Bypass (Authenticated)

Exploitation:

The exploit has two entrypoints

1. /index.php/mydetails/documents -- Self Service >> My Details >> Documents (any permissions needed i.e Employee login)
2. /index.php/policydocuments/add -- Organization >> Policy Documents (higher permissions needed i.e Super user login)

Credentials used:

Employee

Username: EMPP123

Password: useramyde

SUPER USER

Username : empp0001

Password : 5ee51b484955a

Requirement:

- Burpe suite
- Credentials
- PHP RCE script (I'm using p0wny-shell https://github.com/flozz/p0wny-shell)

POC

1. Self Service >> My Details >> Documents >> add New Document (/sentrifugo/index.php/mydetails/documents)

2. Turn Burp Intercept On

3. Select webshell with valid extension - ex: shell.php.doc

4. Alter request in the upload...

Update 'filename' to desired extension. ex: shell.php

Change content type to 'application/x-httpd-php'

5. note down the new file name

6. Replace the Filename with you file name and enter in the url

1st entry point save location /public/uploads/employeedocs/{FILENAME}

2nd entry point save location /public/uploads/policydocs/{FILENAME}