

## HorizontCMS-1.0.0-beta-shell-upload (CVE-2020-28693)

Author: jkana


The vulnerable is in Theme upload function.

- 1.Login as administrator or any users could change themes.
- 2.Create a zip file which have php shell inside. For example `shell.zip` with `shell.php` inside

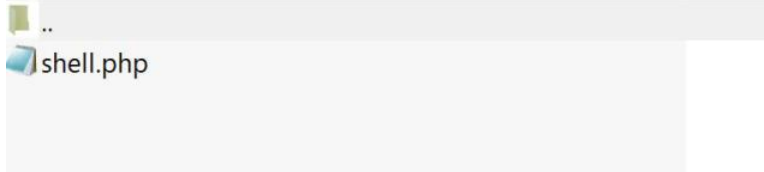
 `shell.zip` (evaluation copy)

File Commands Tools Favorites Options Help

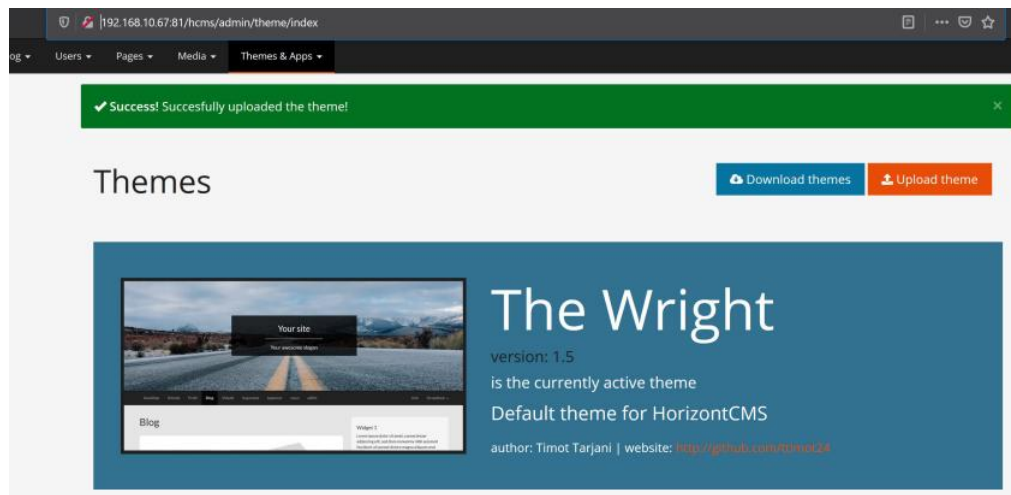


↑  `shell.zip` - ZIP archive, unpacked size 15,744 bytes

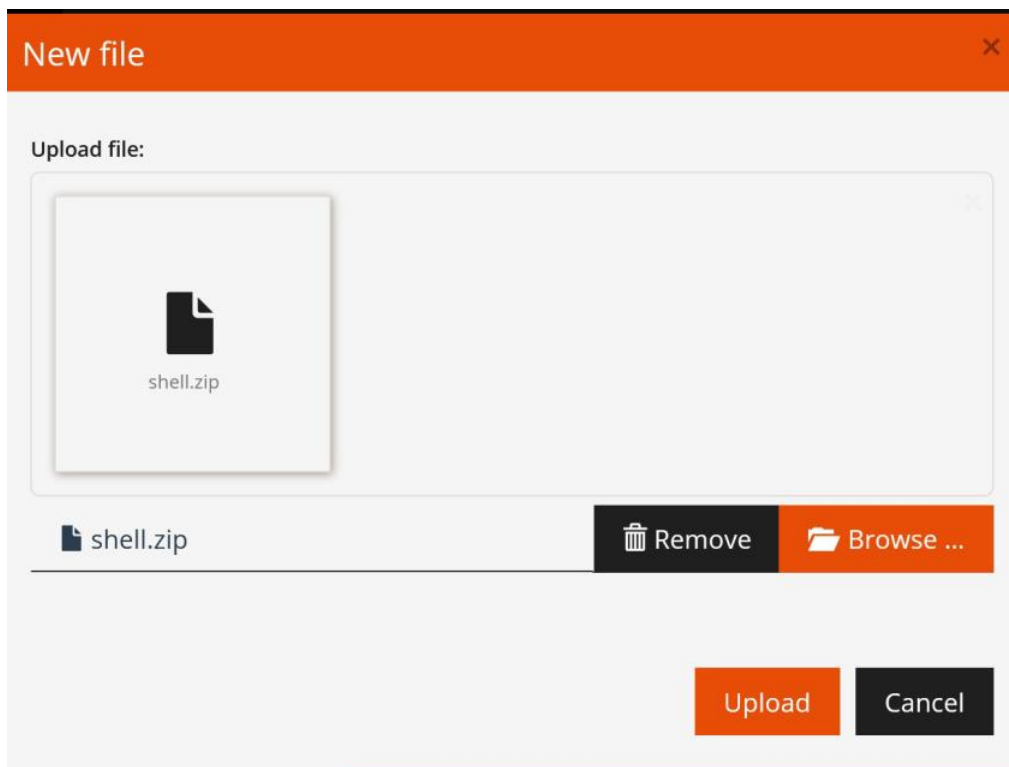
Name



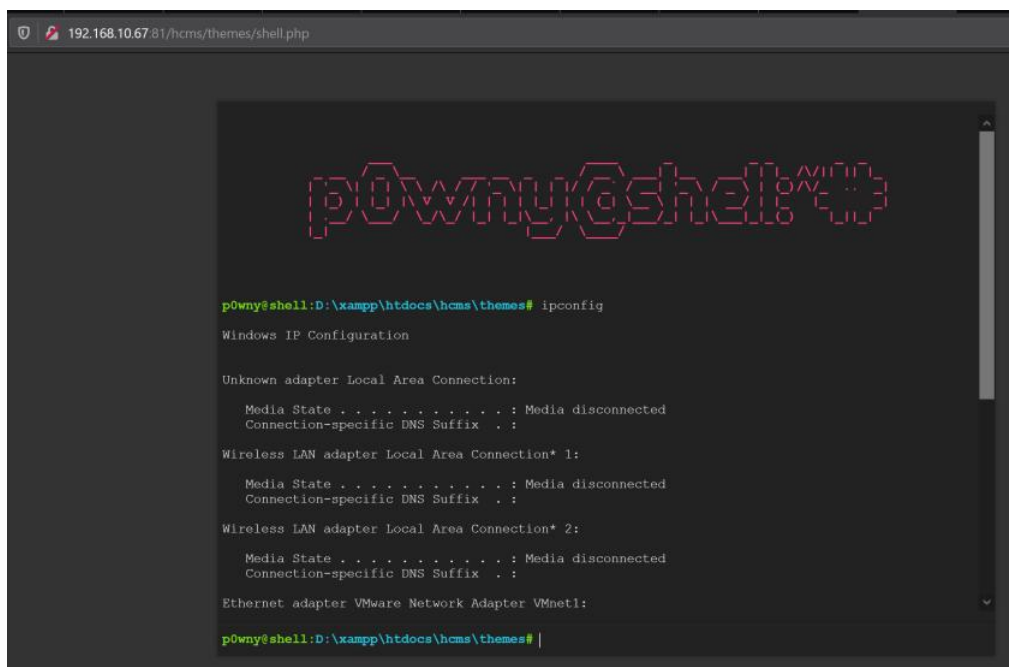
- 2.Access to <http://IP/admin/theme/index> . For example: <http://192.168.10.67:81/hcms/admin/theme/index>



- 3.Upload `shell.zip`



4. Access to shell <http://IP/themes/shell.php>. For example: <http://192.168.10.67:81/hcms/themes/shell.php>



## Releases

No releases published

## Packages

No packages published