New issue

Jump to bottom

Stored XSS Vulnerability In /admin/pages/new (release/1.2.9) #28

Closed leerina opened this issue on Jan 12, 2021 · 8 comments

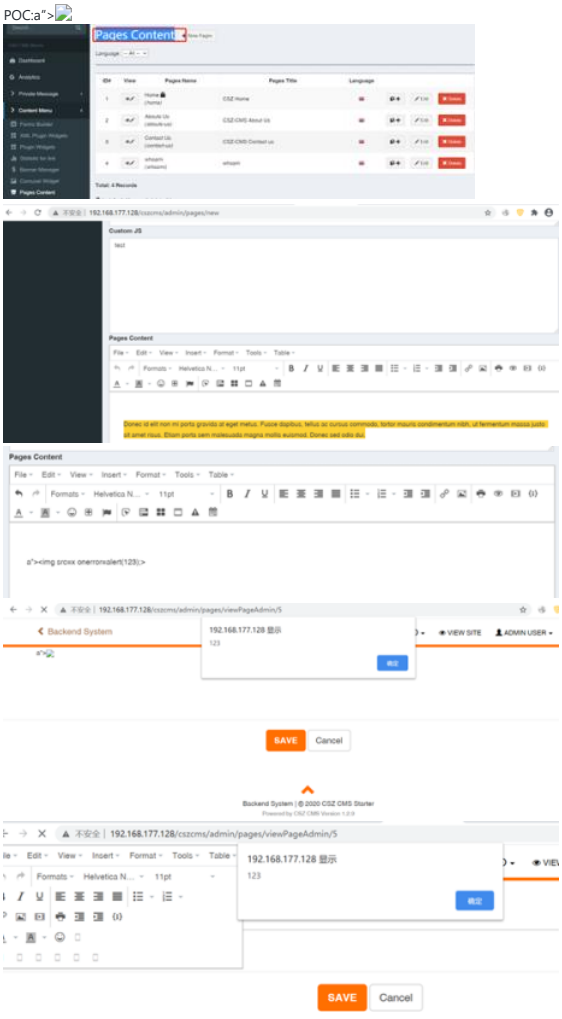
leerina commented on Jan 12, 2021

Hi, **@cskaza**
I found a Stored XSS Vulnerability In /admin/pages/new (release/1.2.9)
In content page ,The content Parameter are not filtered：

```
public function viewPageSaved() {
        admin_helper::is_logged_in($this->session->userdata('admin_email'));
        admin_helper::is_allowchk('pages content');
        admin_helper::is_allowchk('save');
        if($this->uri->segment(4)){
            if($this->input->post('content', FALSE)){
                $this->Csz_admin_model->updatePageView($this->uri->segment(4));
                //Return to last session
                $this->db->cache_delete_all();
                $this->session->set_flashdata('error_message','<div class="alert
                    alert-success" role="alert"><button type="button" class="close"
                    data-dismiss="alert" aria-label="Close"><span
                    aria-hidden="true">&times;</span></button>' .$this->lang->line('
                    success_message_alert') .'</div>');
                redirect($this->Csz_model->base_link() .'/admin/pages/viewPageAdmin/'
                    .$this->uri->segment(4), 'refresh');
            }else{
```

```
if($page !== FALSE){
    $data = array(
        'page_name' => $this->Csz_model->findNameAsCopy('pages', 'pages_id',
            $page->page_name),
        'page_url' => $this->Csz_model->findNameAsCopy('pages', 'pages_id', $
            page->page_url, TRUE),
        'lang_iso' => $page->lang_iso,
        'page_title' => $page->page_title,
        'page_keywords' => $page->page_keywords,
        'page_desc' => $page->page_desc,
        'content' => $page->content,
        'more_metatag' => $page->more_metatag,
        'custom_css' => $page->custom_css,
        'custom_js' => $page->custom_js,
        'active' => 0,
```

POC:a">



Author:leerina

OS-WS commented on Apr 26, 2021

This issue was assigned with CVE-2021-3224
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3224
was it ever addressed?

leerina commented on Apr 26, 2021 Author

> This issue was assigned with CVE-2021-3224
> https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3224
> was it ever addressed?

yes,I Requested a CVE numbers.

OS-WS commented on Apr 27, 2021

@leerina great!
Will it be fixed?

leerina commented on Apr 27, 2021 Author

> **@leerina** great!
> Will it be fixed?

yes,it was fixed!

OS-WS commented on Apr 27, 2021

@leerina
Can you please point me to the fixing commit?

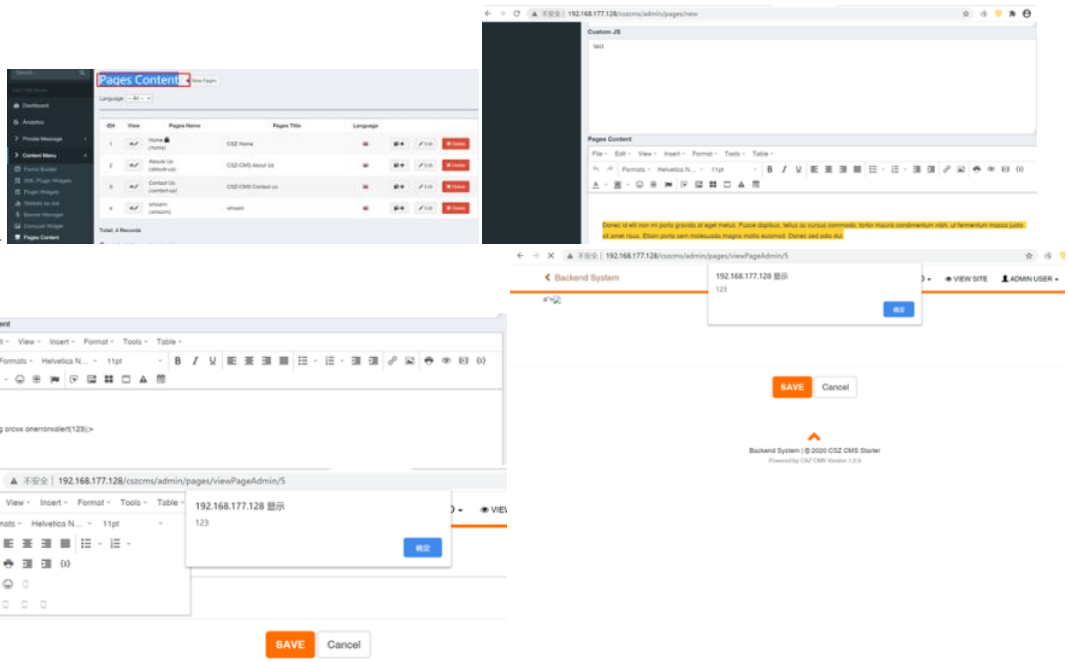
cskaza commented on Nov 9, 2021 Owner

resolved done on next version.

cskaza closed this as completed on Nov 9, 2021

TwoDean commented on Dec 4, 2021

Hi, **@cskaza** I found a Stored XSS Vulnerability In /admin/pages/new (release/1.2.9) In content page ,The content Parameter are not filtered:

POC:a"> 

Author:leerina
"> 

TwoDean commented on Dec 4, 2021 • edited

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants