New issue

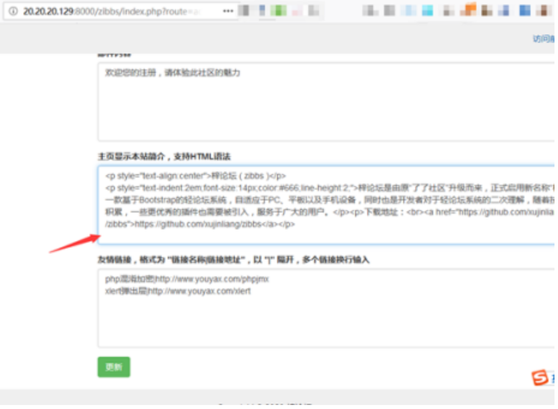
Jump to bottom

Background setting function parameter【bbsmeta】Storage XSS vulnerabilities #5

⊙ Open **Stellarsss** opened this issue on Jun 22, 2020 · 4 comments

Stellarsss commented on Jun 22, 2020

First log in to the background and go to the background Settings，（Compare the storage XSS vulnerabilities of chicken ribs）



20.20.20.129:8000/zibbs/index.php?route=a

欢迎您的注册，请体验此社区的魅力

主页显示本站简介，支持HTML语法

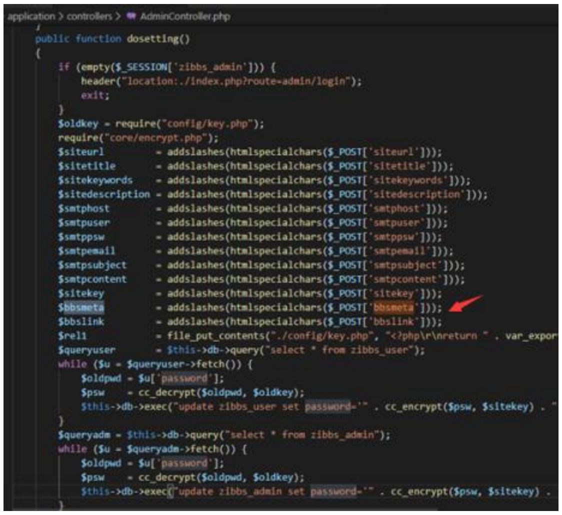
<p style="text-align:center">梓论坛 (zibbs)</p>
<p style="text-indent:2em;font-size:14px;color:#666;line-height:2;">梓论坛是由原"了了社区"升级而来，正式启用新名称
一款基于Bootstrap的轻论坛系统，自适应于PC、平板以及手机设备，同时也是开发者对于轻论坛系统的二次理解，随着
积累，一些更优秀的插件也需要被引入，服务于广大的用户。</p><p>下载地址：
<a href="https://github.com/xujinlia
/zibbs">https://github.com/xujinliang/zibbs</a></p>

友情链接，格式为"链接名称|链接地址"，以"|"隔开，多个链接换行输入

php混淆加密|http://www.youyax.com/phpjmx
xlert弹出层|http://www.youyax.com/xlert

Description here（HTML syntax support），Guess there is an XSS vulnerability，Get the parameter 【bbsmeta】here by grabbing the bag，Trace in the source code

application/controllers/AdminController.php code

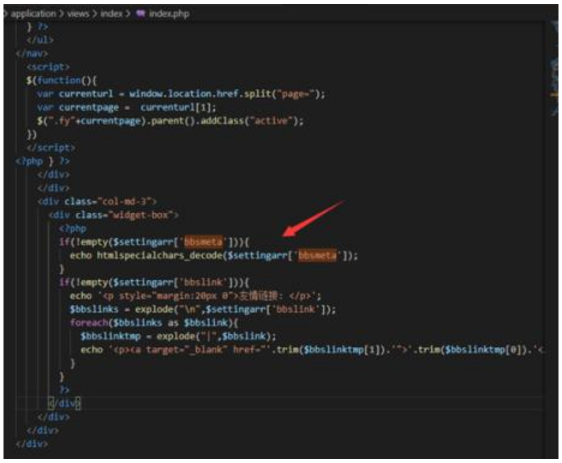


application > controllers > AdminController.php

```
    public function dosetting()
    {
        if (empty($_SESSION['zibbs_admin'])) {
            header("location:./index.php?route=admin/login");
            exit;
        }
        $oldkey = require("config/key.php");
        require("core/encrypt.php");
        $siteurl         = addslashes(htmlspecialchars($_POST['siteurl']));
        $sitetitle       = addslashes(htmlspecialchars($_POST['sitetitle']));
        $sitekeywords    = addslashes(htmlspecialchars($_POST['sitekeywords']));
        $sitedescription = addslashes(htmlspecialchars($_POST['sitedescription']));
        $smtphost        = addslashes(htmlspecialchars($_POST['smtphost']));
        $smtpuser        = addslashes(htmlspecialchars($_POST['smtpuser']));
        $smtppsw         = addslashes(htmlspecialchars($_POST['smtppsw']));
        $smtpemail       = addslashes(htmlspecialchars($_POST['smtpemail']));
        $smtpsubject     = addslashes(htmlspecialchars($_POST['smtpsubject']));
        $smtpcontent     = addslashes(htmlspecialchars($_POST['smtpcontent']));
        $sitekey         = addslashes(htmlspecialchars($_POST['sitekey']));
        $bbsmeta         = addslashes(htmlspecialchars($_POST['bbsmeta']));
        $bbslink         = addslashes(htmlspecialchars($_POST['bbslink']));
        $rel1            = file_put_contents("./config/key.php", "<?php\r\nreturn " . var_expor
        $queryuser       = $this->db->query("select * from zibbs_user");
        while ($u = $queryuser->fetch()) {
            $oldpwd = $u['password'];
            $psw    = cc_decrypt($oldpwd, $oldkey);
            $this->db->exec("update zibbs_user set password='" . cc_encrypt($psw, $sitekey) . "
        }
        $queryadm = $this->db->query("select * from zibbs_admin");
        while ($u = $queryadm->fetch()) {
            $oldpwd = $u['password'];
            $psw    = cc_decrypt($oldpwd, $oldkey);
            $this->db->exec("update zibbs_admin set password='" . cc_encrypt($psw, $sitekey) .
        }
```

This was filtered by addslashes() and htmlspecialchar ()
Obviously when you insert the data into the database you will have a layer of filtering, and then you will continue to track the specific page output location of this parameter to the following

application/views/index/index.php code

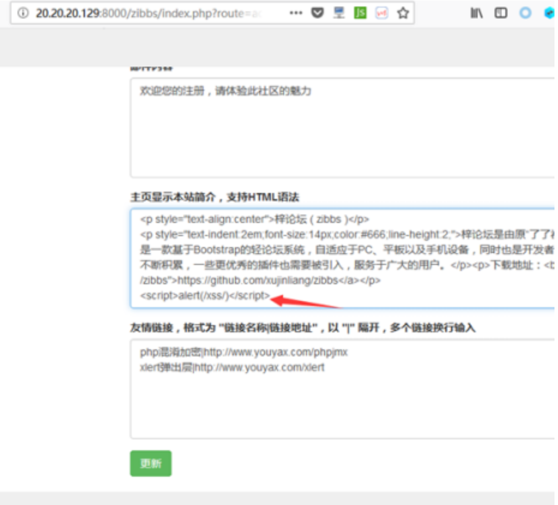


```
application > views > index > index.php
    } ?>
    </ul>
  </nav>
    <script>
    $(function(){
      var currenturl = window.location.href.split("page=");
      var currentpage =  currenturl[1];
      $(".fy"+currentpage).parent().addClass("active");
    })
    </script>
  <?php } ?>
      </div>
      </div>
      <div class="col-md-3">
        <div class="widget-box">
          <?php
          if(!empty($settingarr['bbsmeta'])){
            echo htmlspecialchars_decode($settingarr['bbsmeta']);
          }
          if(!empty($settingarr['bbslink'])){
            echo '<p style="margin:20px 0">友情链接: </p>';
            $bbslinks = explode("\n",$settingarr['bbslink']);
            foreach($bbslinks as $bbslink){
              $bbslinktmp = explode("|",$bbslink);
              echo '<p><a target="_blank" href="'.trim($bbslinktmp[1]).'">'.trim($bbslinktmp[0]).'<
            }
          }
          ?>
        </div>
      </div>
    </div>
  </div>
```

When the page is output here, the following function is made for the parameter 【bbsmeta】to handle htmlspecialchars_decode
The storage XSS here results in the storage XSS due to the use ofhtmlspecialchars_decode() function,
So through the black box to verify
Insert the following test statement in the background and click Update

payload:

<script>alert(/xss/)</script>



20.20.20.129:8000/zibbs/index.php?route=a

欢迎您的注册，请体验此社区的魅力

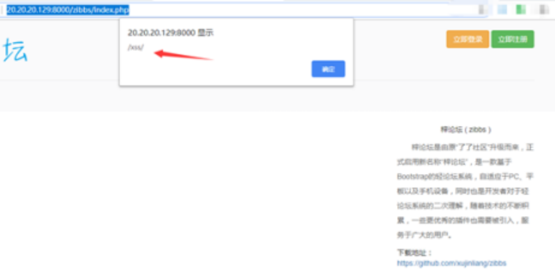
主页显示本站简介，支持HTML语法

```
<p style="text-align:center">梓论坛 ( zibbs )</p>
<p style="text-indent:2em;font-size:14px;color:#666;line-height:2;">梓论坛是由原"了了社
是一款基于Bootstrap的轻论坛系统，自适应于PC、平板以及手机设备，同时也是开发者
不断积累，一些更优秀的插件也需要被引入，服务于广大的用户。</p><p>下载地址：<a
/zibbs">https://github.com/xujinliang/zibbs</a></p>
<script>alert(/xss/)</script>
```

友情链接，格式为 "链接名称|链接地址"，以 "|" 隔开，多个链接换行输入

```
php混淆加密|http://www.youyax.com/phpjmx
xlert弹出层|http://www.youyax.com/xlert
```

The XSS is then accessed directly to the foreground and executed successfully
 http://20.20.20.129:8000/zibbs/index.php



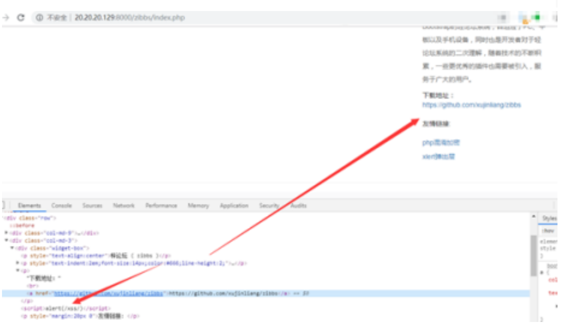
20.20.20.129:8000/zibbs/index.php

20.20.20.129:8000 显示
/xss/

梓论坛 (zibbs)

梓论坛是由原"了了社区"升级而来，正式启用新名称"梓论坛"，是一款基于Bootstrap的轻论坛系统，自适应于PC、平板以及手机设备，同时也是开发者对于轻论坛系统的二次理解，随着技术的不断积累，一些更优秀的插件也需要被引入，服务于广大的用户。

下载地址：
https://github.com/xujinliang/zibbs



不安全 | 20.20.20.129:8000/zibbs/index.php

板以及手机设备，同时也是开发者对于轻论坛系统的二次理解，随着技术的不断积累，一些更优秀的插件也需要被引入，服务于广大的用户。

下载地址：
https://github.com/xujinliang/zibbs

友情链接

php混淆加密
xlert弹出层

```
<div class="row">
  ::before
  ▶<div class="col-md-9">…</div>
  ▼<div class="col-md-3">
    ▼<div class="widget-box">
       <p style="text-align:center">梓论坛 ( zibbs )</p>
      ▶<p style="text-indent:2em;font-size:14px;color:#666;line-height:2;">…</p>
      ▼<p>
         "下载地址："
         <br>
         <a href="https://github.com/xujinliang/zibbs">https://github.com/xujinliang/zibbs</a> == $0
       </p>
       <script>alert(/xss/)</script>
       <p style="margin:20px 0">友情链接: </p>
```

Solution:
filter or encode special characters like this
<

"
'
&
%
… …
and filter some keyword like this

script
javascript

… …
or filter some label function which can run javascript like this
onclick
onerror
onload
… …

xujinliang commented on Jun 22, 2020 Owner

3Q，But i think if a people need to access to the backend,and destroy it,then this is not a bug

Stellarsss commented on Jun 22, 2020 Author

I think it is difficult to exploit the vulnerability，But，it is recommended to filter dangerous characters such as <script>

xujinliang commented on Jun 22, 2020 Owner

i think i can't ignore your kindness, I decided to update to github during the 端午 Festival

Stellarsss commented on Jun 22, 2020 Author

thank you

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants