



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

Buddypress Xprofile Custom Fields Type 2.6.3 - Remote Code Execution

EDB-ID:
44432

CVE:
N/A

EDB Verified: ✘

Author:
[LENON LEITE](#)

Type:
[WEBAPPS](#)

Exploit:  

Platform:
[PHP](#)

Date:
2018-04-09

Vulnerable App:





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title: Plugin Buddypress Xprofile Custom Fields Type 2.6.3 RCE – Unlink
# Date: 08/04/2018
# Exploit Author: Lenon Leite
# Vendor Homepage:
# https://wordpress.org/plugins/buddypress-xprofile-custom-fields-type/
# Software Link:
# https://wordpress.org/plugins/buddypress-xprofile-custom-fields-type/
# Contact: http://twitter.com/lenonleite
# Website: http://lenonleite.com.br/
# Category: webapps
# Version: 2.6.3
# Tested on: Ubuntu 16.1
#
#Article:
#http://lenonleite.com.br/publish-exploits/plugin-buddypress-xprofile-custom-fields-type-2-6-3-rce-unlink/
#
#Video:
#https://www.youtube.com/watch?v=By7kT7UbHVk
#

1 - Description
  - Type user access: any user registered used in BuddyPress.
  - $_POST[ 'field_' . $field_id . '_hiddenfile' ] is not escaped.
  - $_POST[ 'field_' . $field_id . '_deleteimg' ] is not escaped.
```

2. Proof of Concept

Login as regular user.

1- Log in with BuddyPress User

2 - Access Edit Profile:

<http://target/members/admin/profile/edit/>

3 - Register data with image:

```
<http://target/wp-content/uploads/2018/01/buddypress-profile.png>4
- Change parameter to delete image in html and save profile:
<http://target/wp-content/uploads/2018/01/buddypress-profile2.png>
<http://target/wp-content/uploads/2018/01/buddypress-profile3-1.png>
```

```
# - -
#*Atenciosamente*
#
#*Lenon Leite*
```

Tags:

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING



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

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