**BlackBox – 3**

1. So, this blackbox start with the secret.rar that should be extracted. The file inside, **secret.exe**, should be run using the cmd command with this command: **>secret.exe**
2. The program printed this:

starting HTTP server at 10.40.40.40:8080

\* Serving Flask app 'secret'

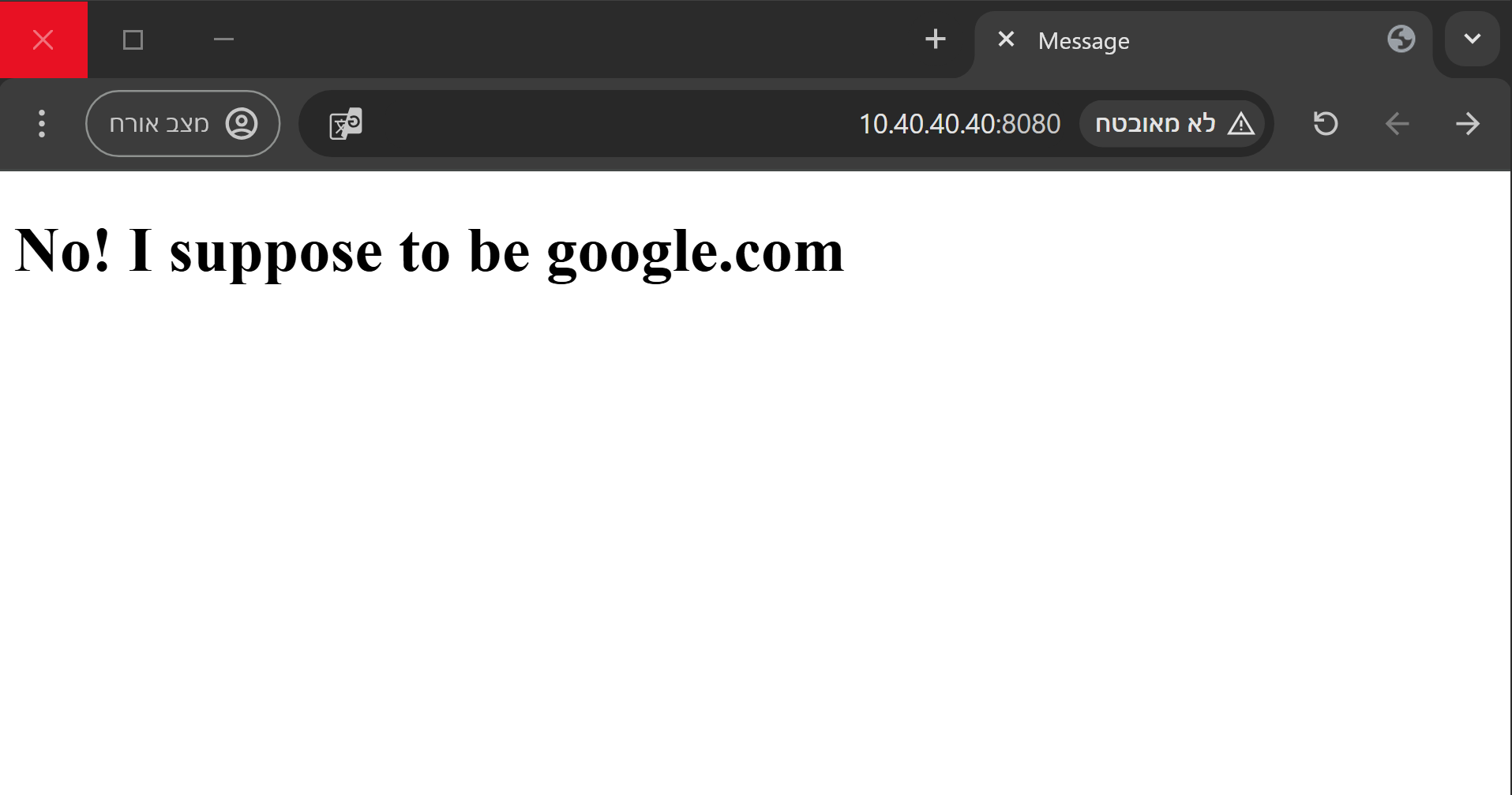
\* Debug mode: off

The requested address is not valid in its context

So, I understood that the server was started(with the ip: **10.40.40.40** and port: **8080**) and therefore I tried to connect to this server, but it failed due to the reason that this ip address is not valid.

1. This led me to change, manually, my local **ipv4** address to **10.40.40.40** which really started the server.

Then I connected the server via my browser(**google.com**) and this is a screenshot from the opening page:



1. When I opened the inspector, I found those 2 **Js** scripts:

The First:

function \_\_fds324f4353fds(\_\_hgffdgx) {

    var fsdv3 = \_\_hgffdgx.\_\_43dfgf3.value;

    console.log(fsdv3);

    if (fsdv3 === "5") {

        alert('Password is correct! Unlocking secret path...');

        // You can redirect or perform further actions here after successful validation

    } else {

        alert('Incorrect password! Access denied.');

    }

    return false;

}

The Second:

$('form').submit(function (event) {

    event.preventDefault(); // Prevents default form submission

    \_\_fds324f4353fds(); // Calls the validation function

});

In addition, I found a cookie named “**isAdmin**” and changed it from false to true.

1. I notice that the label of the page says that the website should be google.com and therefore I set in my hosts file(which located on: **C:\Windows\System32\drivers\etc** ) in my computer so the ip **google.com** domain should direct to the ip: **10.40.40.40**.
2. Then, I entered the website again but with the google.com domain(**google.com:8080**) and it directed me to this new page:

תמונה שמכילה טקסט, צילום מסך, חשמל, מולטימדיה

התיאור נוצר באופן אוטומטי

**\*** Remember to change the **isAdmin** cookie again!