VishwaCTF

CHALLENGE NAME : [Boot-Failed]

DEV : [Samarth Ghante]

CATEGORY : [Web]

LEVEL : [Hard]

2024

Challenge Name: Boot-Failed

Challenge Description: Fix The System ASAP!

Home Page

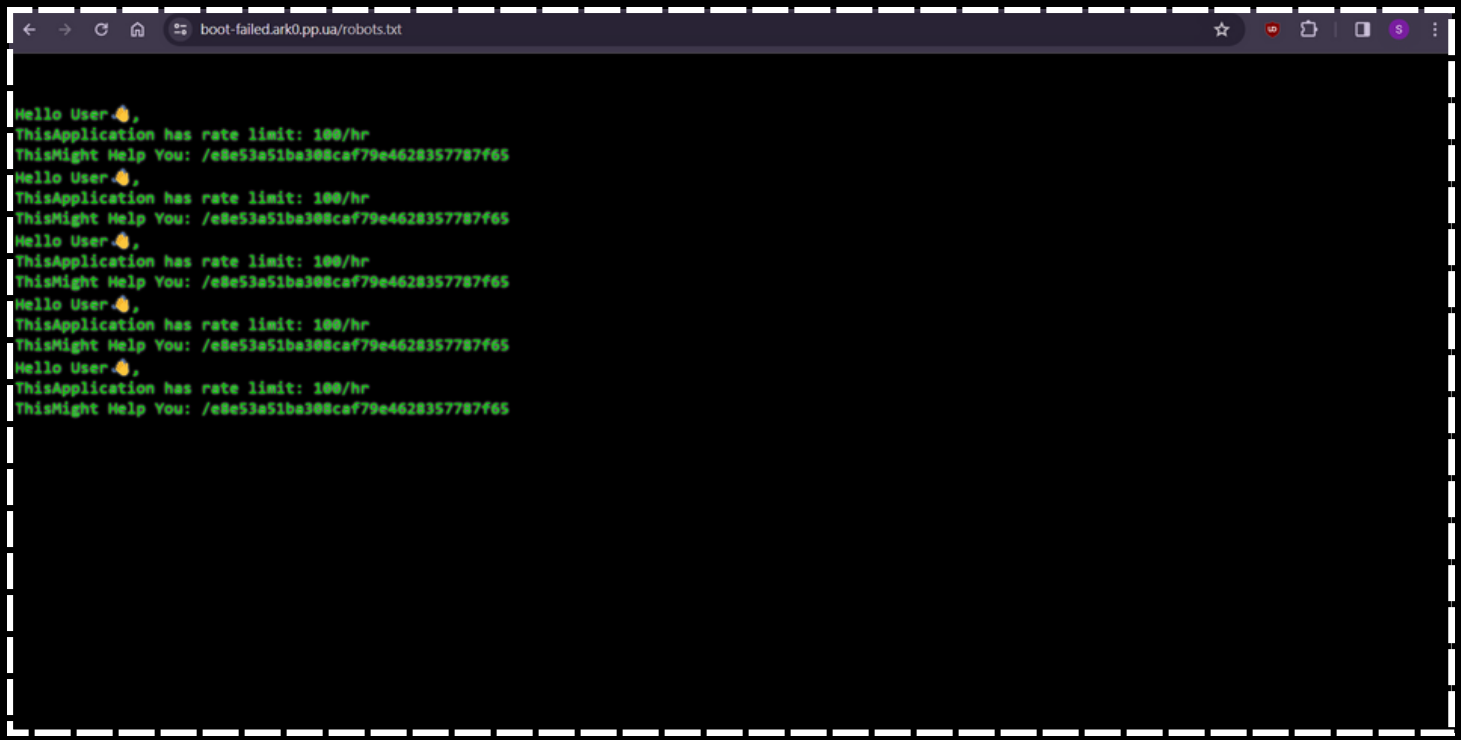
It shows the boot logs of the system!
& There is a error notice highlighted

```
[0.000000] Notice: System is Running out of RAM. Upgrade your memory to 8GB.
```

Remember, We have to upgrade the RAM to 8GB

Now, We know what to solve in this! Lets Begin!!!

Go To /Robots.txt



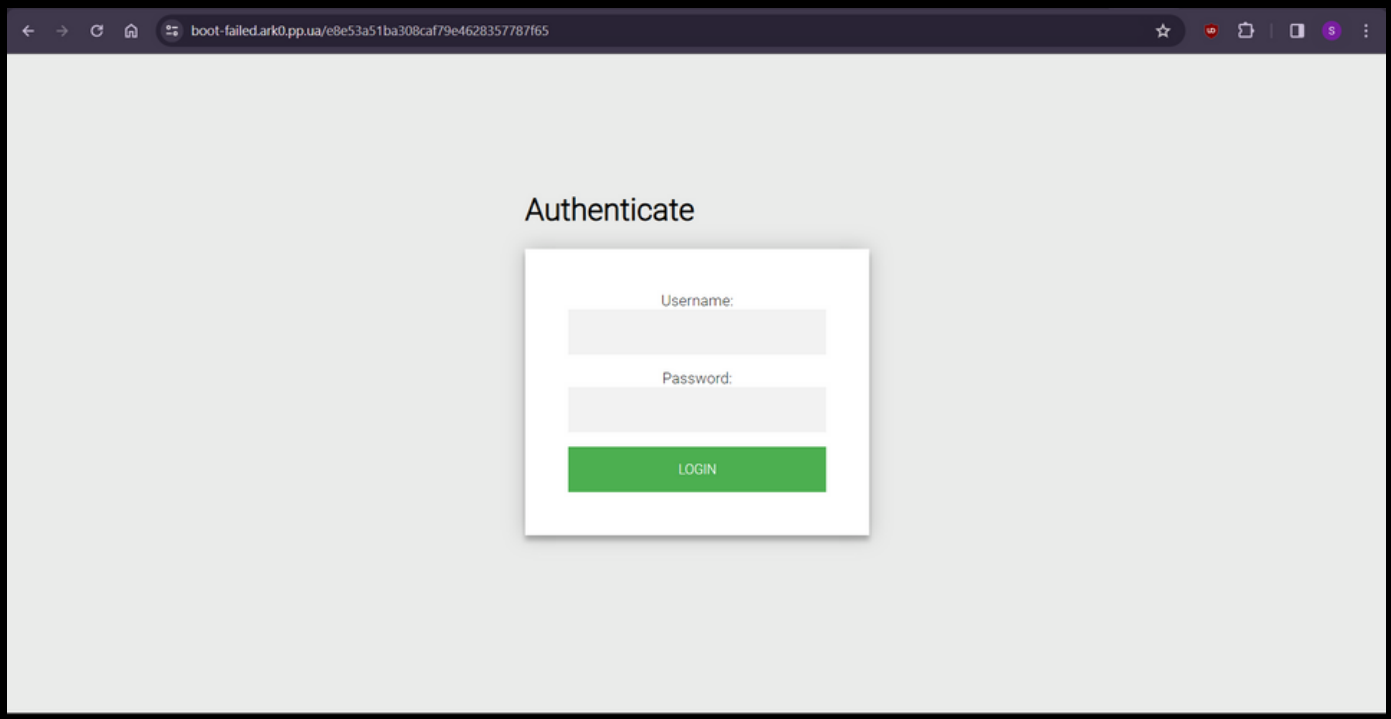
You have press key on keyboards to reveal the msg...

CHALLENGE NAME : [Boot-Failed]

boot-failed.ark0.pp.ua/robots.txt

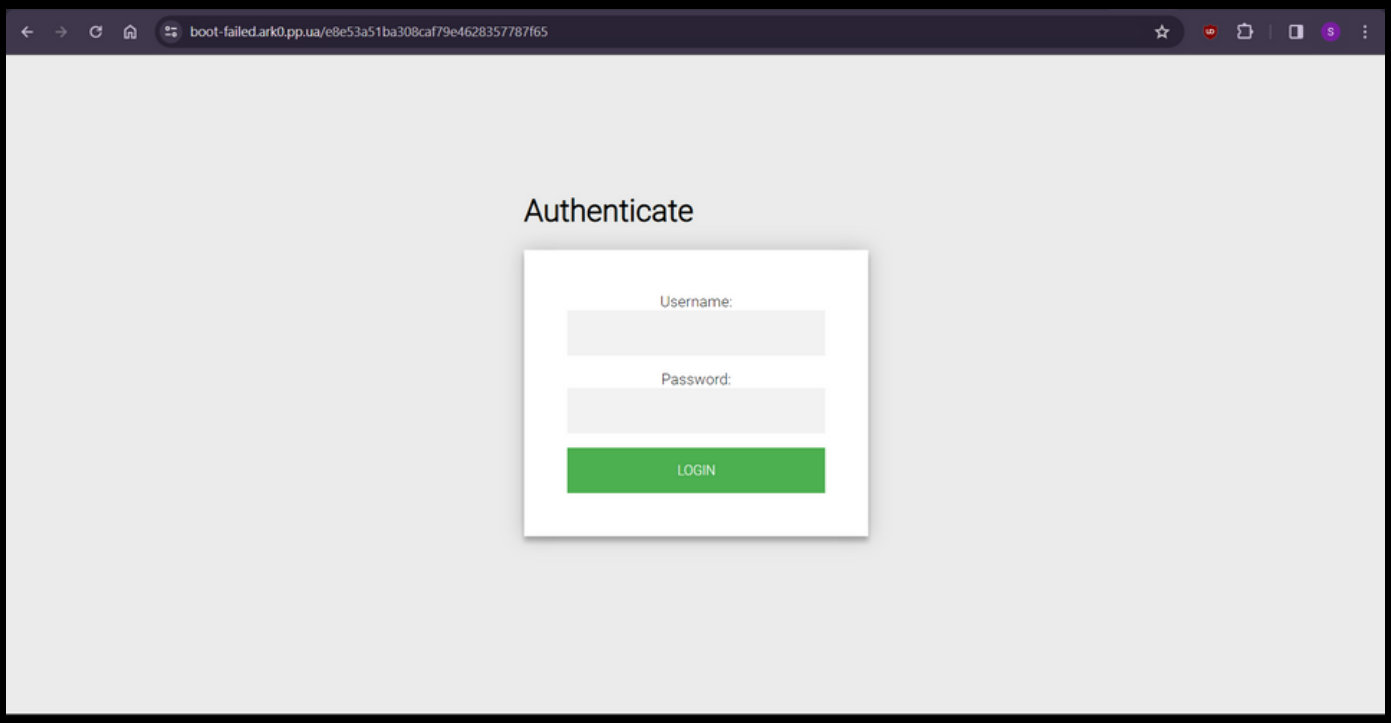
```
Hello User👋,
ThisApplication has rate limit: 100/hr
ThisMight Help You: /e8e53a51ba308caf79e4628357787f65
Hello User👋,
ThisApplication has rate limit: 100/hr
ThisMight Help You: /e8e53a51ba308caf79e4628357787f65
Hello User👋,
ThisApplication has rate limit: 100/hr
ThisMight Help You: /e8e53a51ba308caf79e4628357787f65
Hello User👋,
ThisApplication has rate limit: 100/hr
ThisMight Help You: /e8e53a51ba308caf79e4628357787f65
Hello User👋,
ThisApplication has rate limit: 100/hr
ThisMight Help You: /e8e53a51ba308caf79e4628357787f65
```

Go to /e8e53a51ba308caf79e4628357787f65

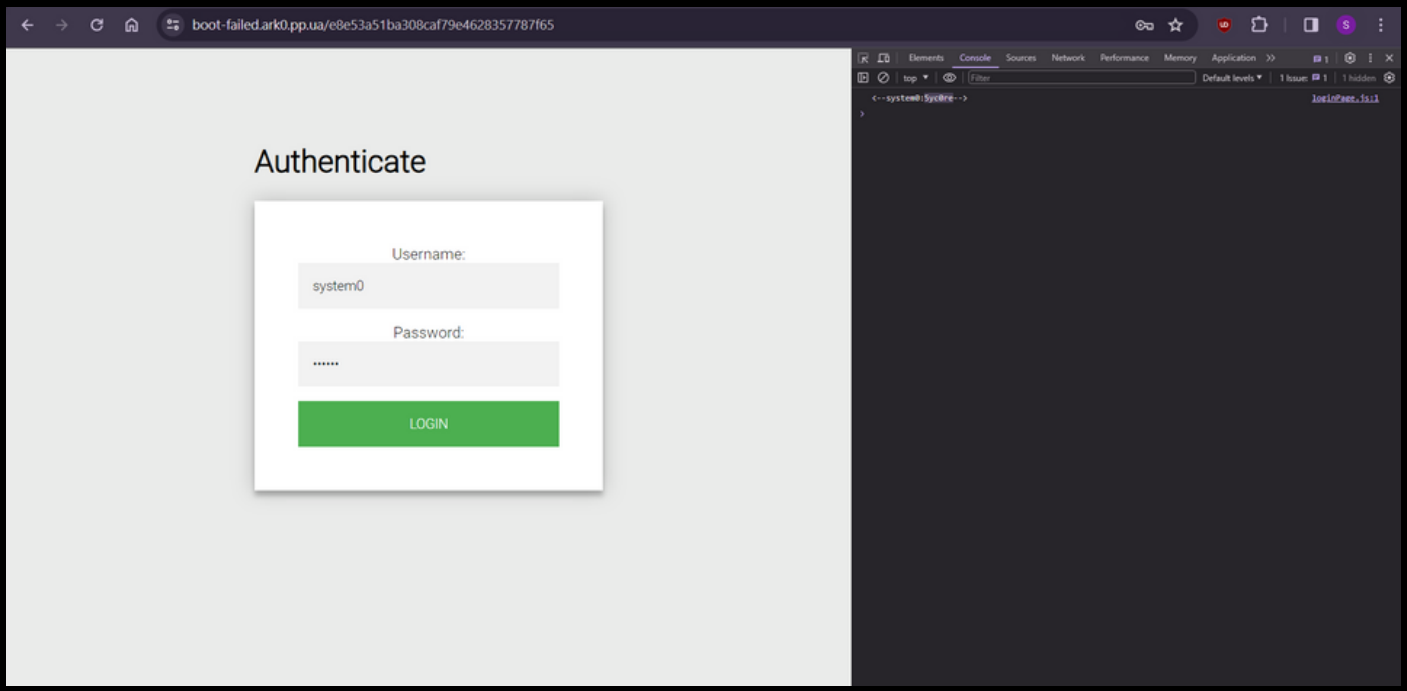


CHALLENGE NAME : [Boot-Failed]

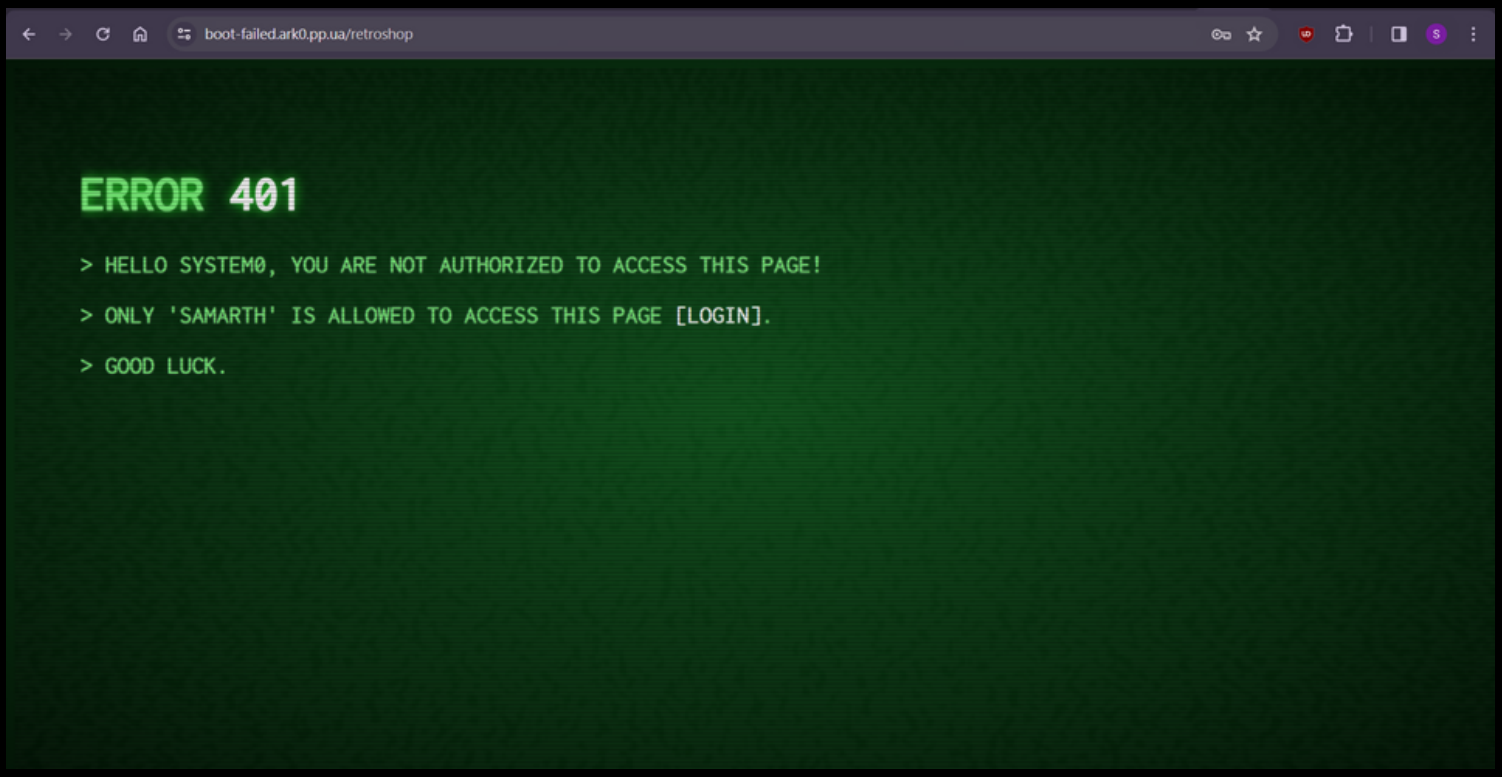
You have to find the login credentials!



login creds are in console log --> system0:5yc0re



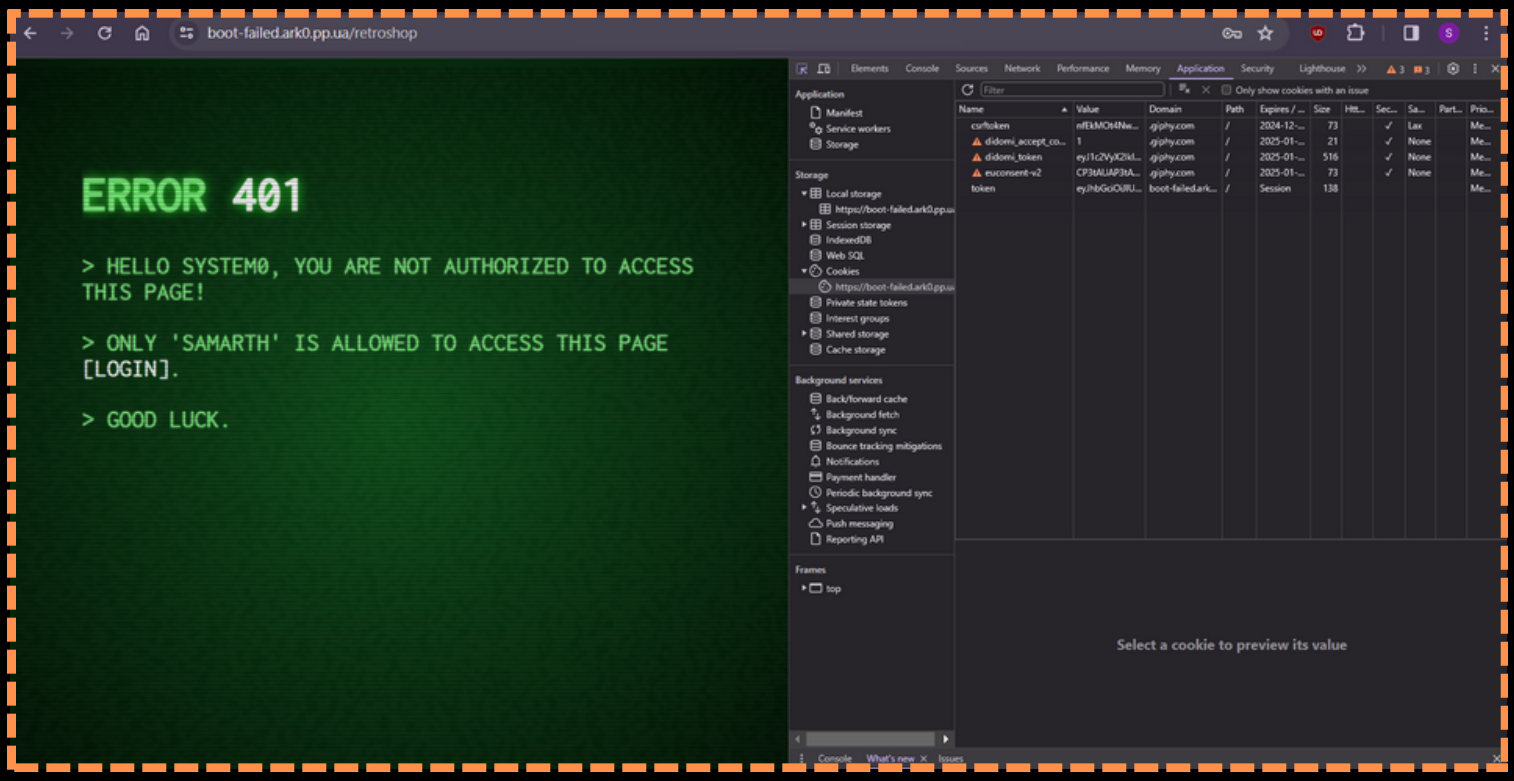
After You Authenticate with the login creds



It shows error, “System0” is not authorized to access the page, only “samarth” is authorized to do so!

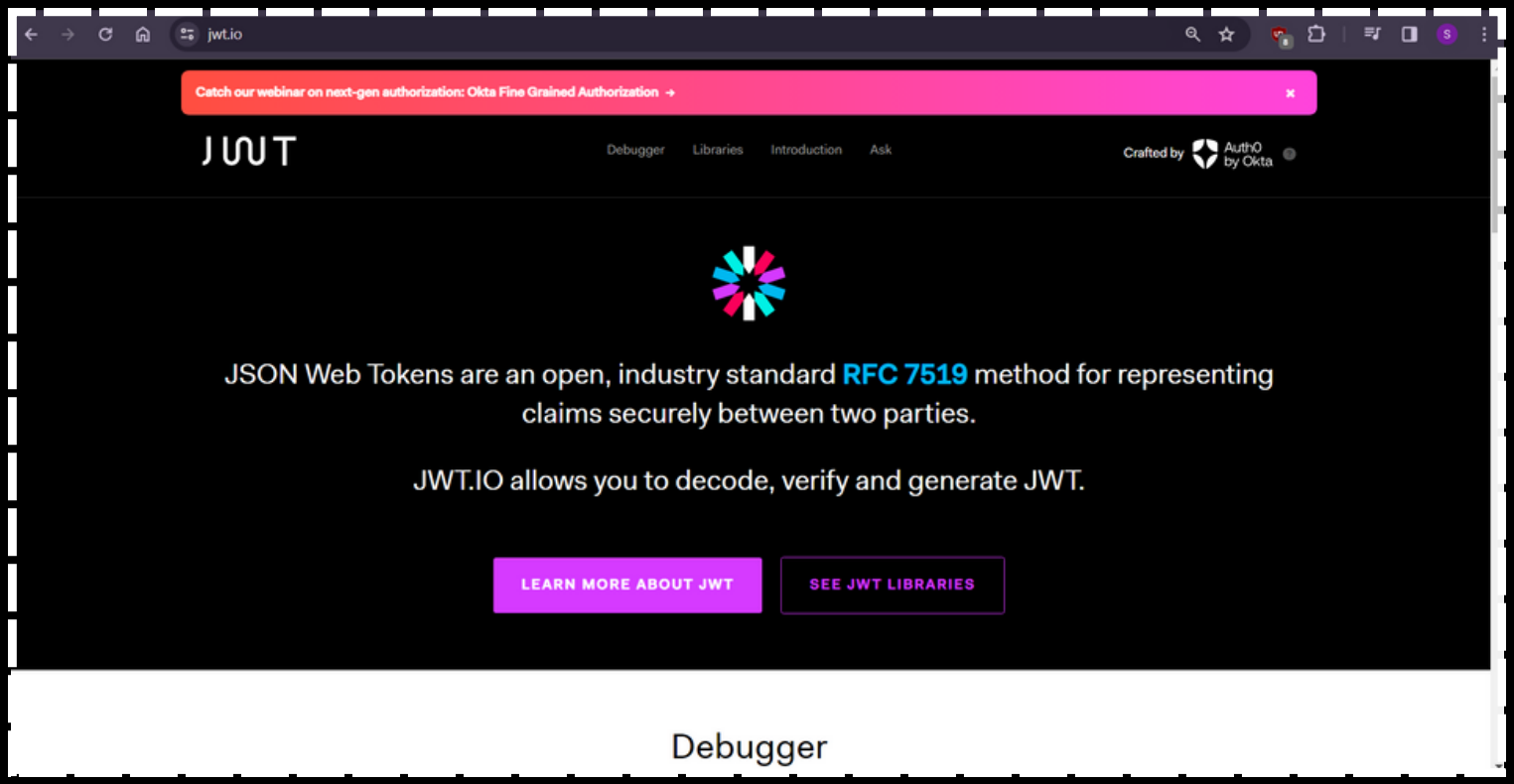
So We have to somehow login as the samarth. Let’s check if this site is using token system for user session. (if its JWT Token, then it could be cracked)

CHALLENGE NAME : [Boot-Failed]

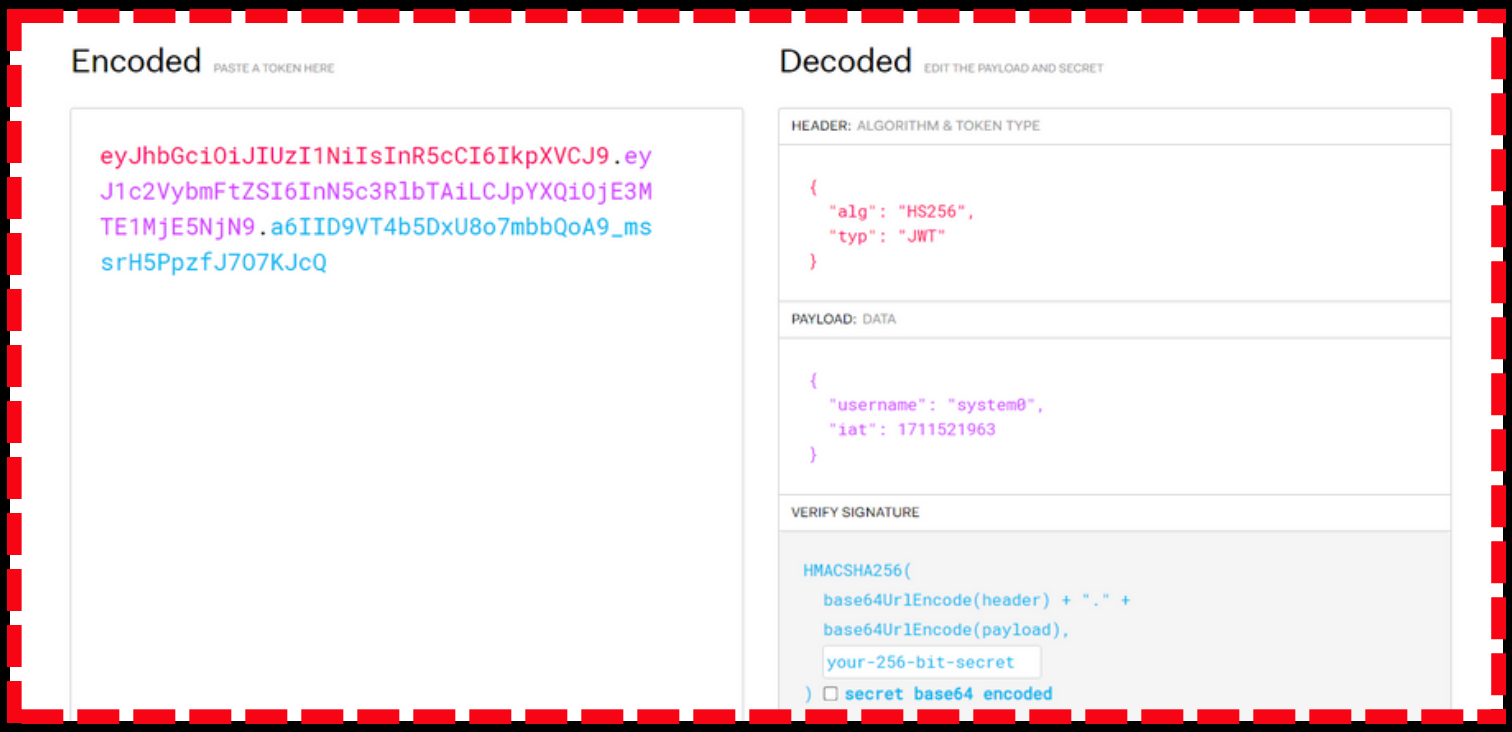


It is having a token key value pair in the cookies!

Let’s Check if it is a JWT (Json Web Token) Token?



vishwaCTF | CHALLENGE NAME : [Boot-Failed]



Yess! It is a JWT Token! It has username -> **system0**

JWT Tokens use a key/secret for encoding, If we get the key we can change the Payload Data, without key, changing the payload will trigger data tempering & It won't work!

DEV: SAMARTH GHANTE

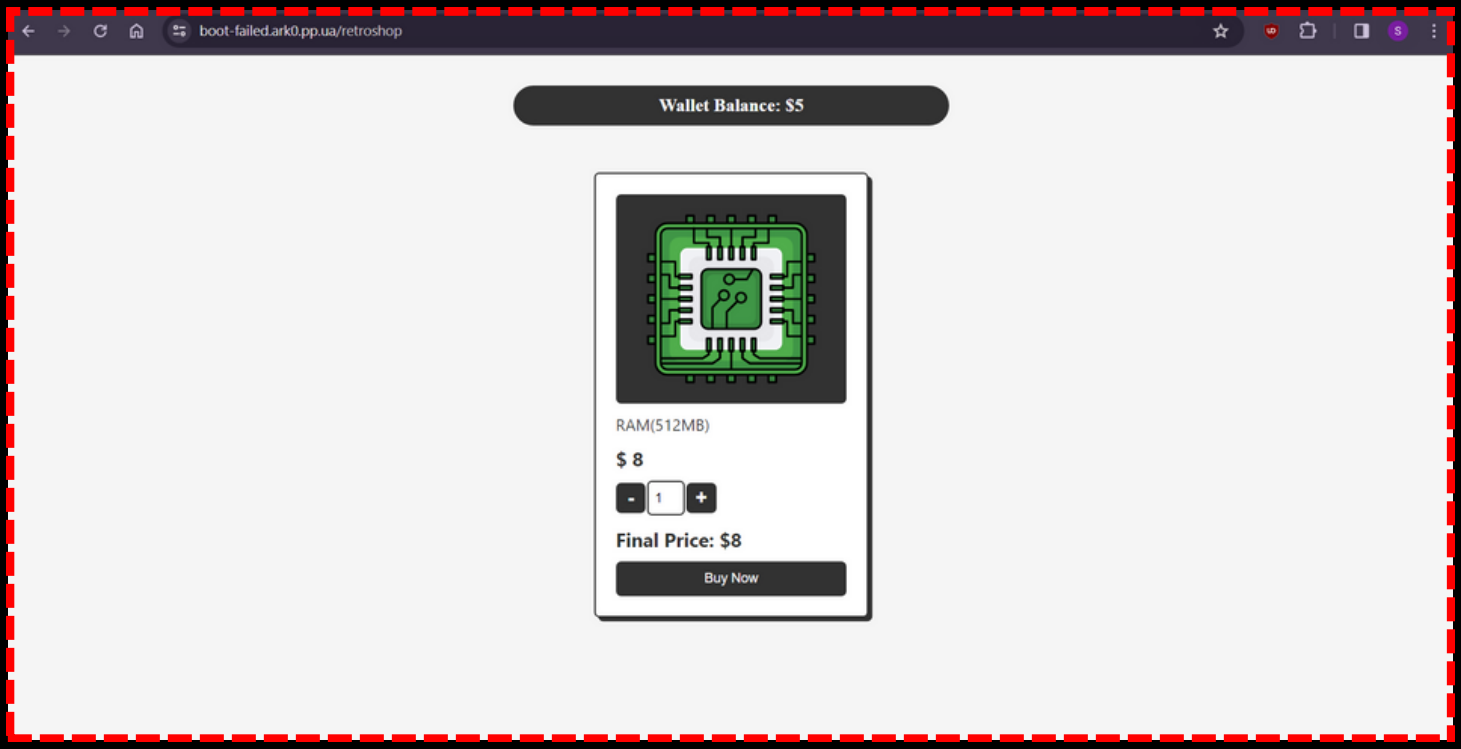
We can use the JWT Tool for Brute Forcing the Token with keys from a wordlist, it is a fantastic tool!

You are right, use this tool and the famous / common “rockyou” wordlist & You will get the key!

key is: winniethepooh

Put The Key In the Signature Field & Change The Payload Data [**System0 ---> samarth**]

Copy The Encoded Token From Left Window and paste in the token value on the website.

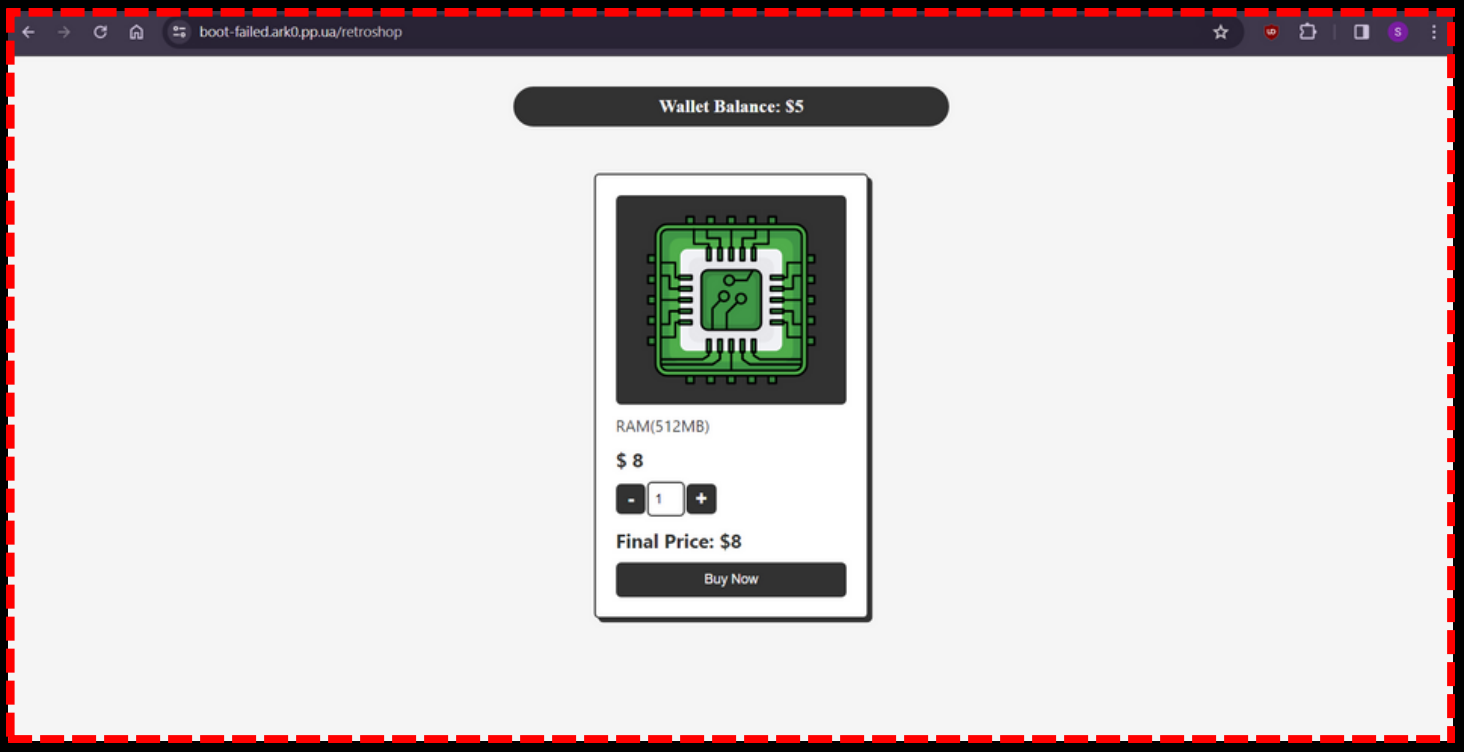


Congrats, You are now logged into the shop!

Now Remeber, You have to upgrade the RAM to total 8GB But If You read the boot logs carefully you will see the system already has 4GB RAM so we will need 4GB More, **Thus 8*512 MB = 4GB!**

```
[0.000000] Notice: System is Running out of RAM. Upgrade your memory to 8GB.
[0.000000] Memory: 4096MB = 4096MB total
```

CHALLENGE NAME : [Boot-Failed]



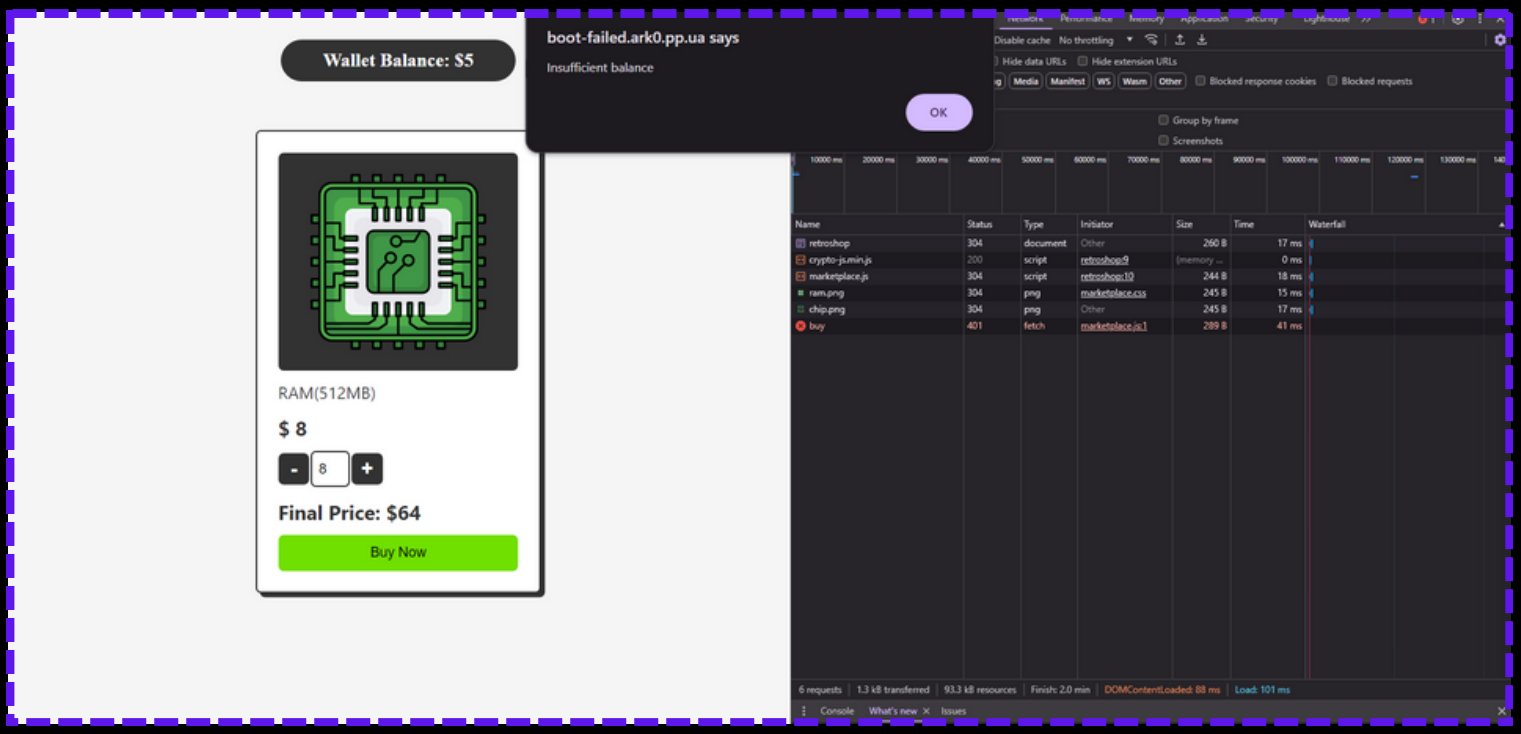
Congrats, You are now logged into the shop!

Now Remeber, You have to upgrade the RAM to total 8GB But If You read the boot logs carefully you will see the system already has 4GB RAM so we will need 4GB More, **Thus 8*512 MB = 4GB!**

```
[0.000000] Notice: System is Running out of RAM. Upgrade your memory to 8GB.
[0.000000] Memory: 4096MB = 4096MB total
```

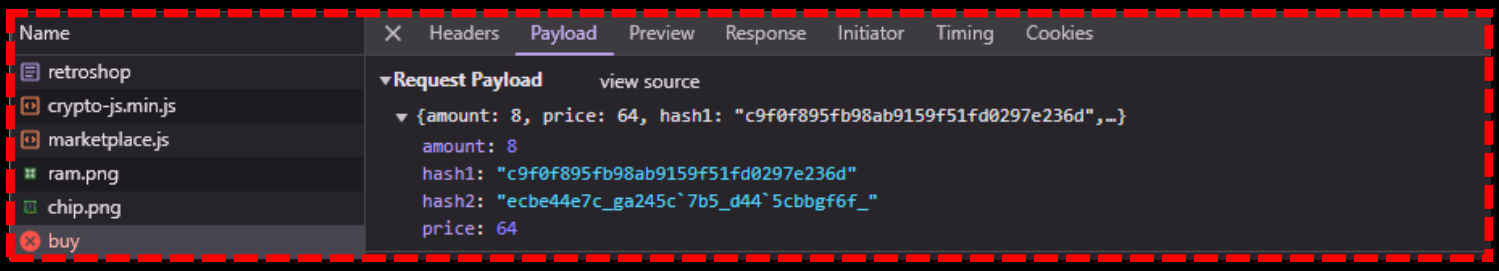
DEV: SAMARTH GHANTE

But There is a catch💀
You have wallet balance of 5$ only!
Thus You will get “insufficient Balance” Error!



You can capture the network packets / activities from network tab in the developer tool.
Here we can see that the application is sending an **Post Request to “/buy” endpoint.**

Payload consist of [amount, price, hash1, hash2]



If we just modify the amount or price field without the respective hashes then we get error “data tempering detected”

So we will need to modify the respective hash to match that value; for that we must know a the hashing type or cipher type.
use any online cipher indentifiers such as dcode.fr

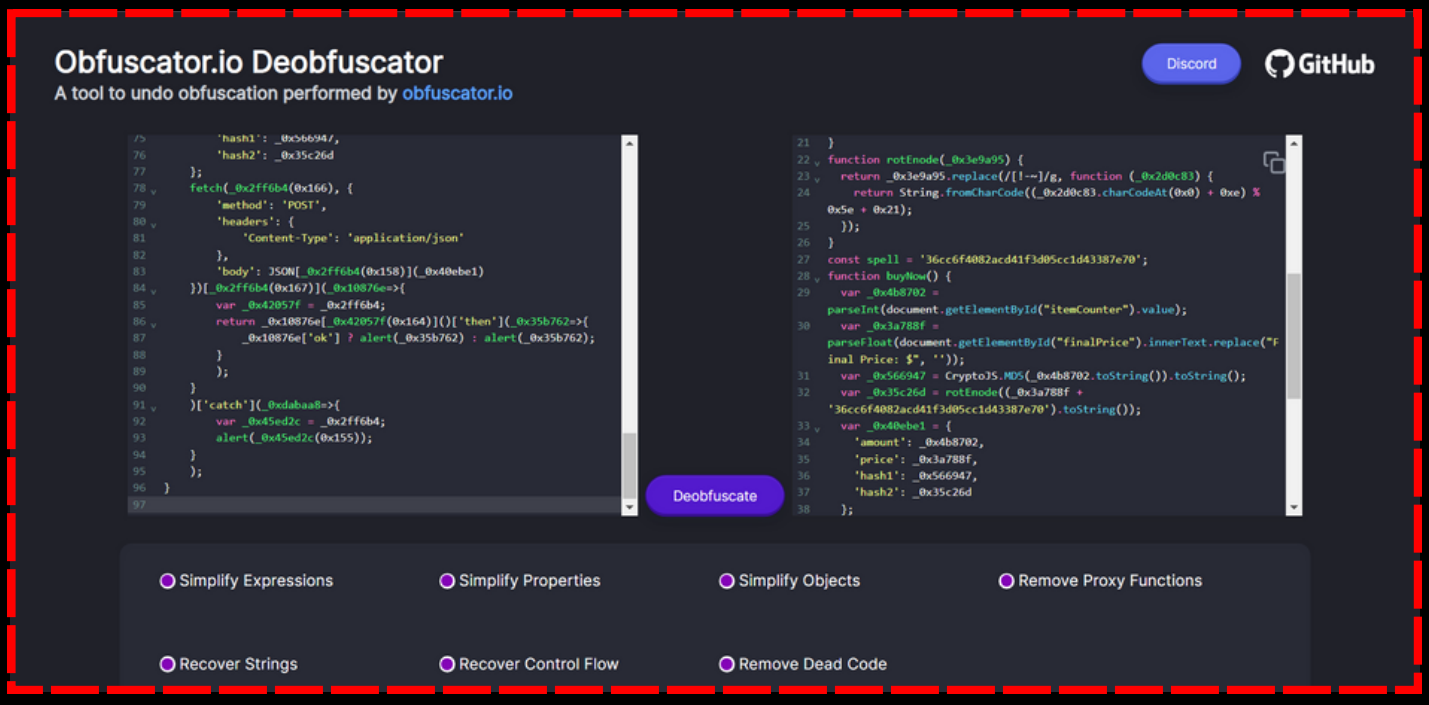
We need to modify only the Price and its hash because we have already selected 8 amount of RAM Chips (512MB Each)

vishwaCTF

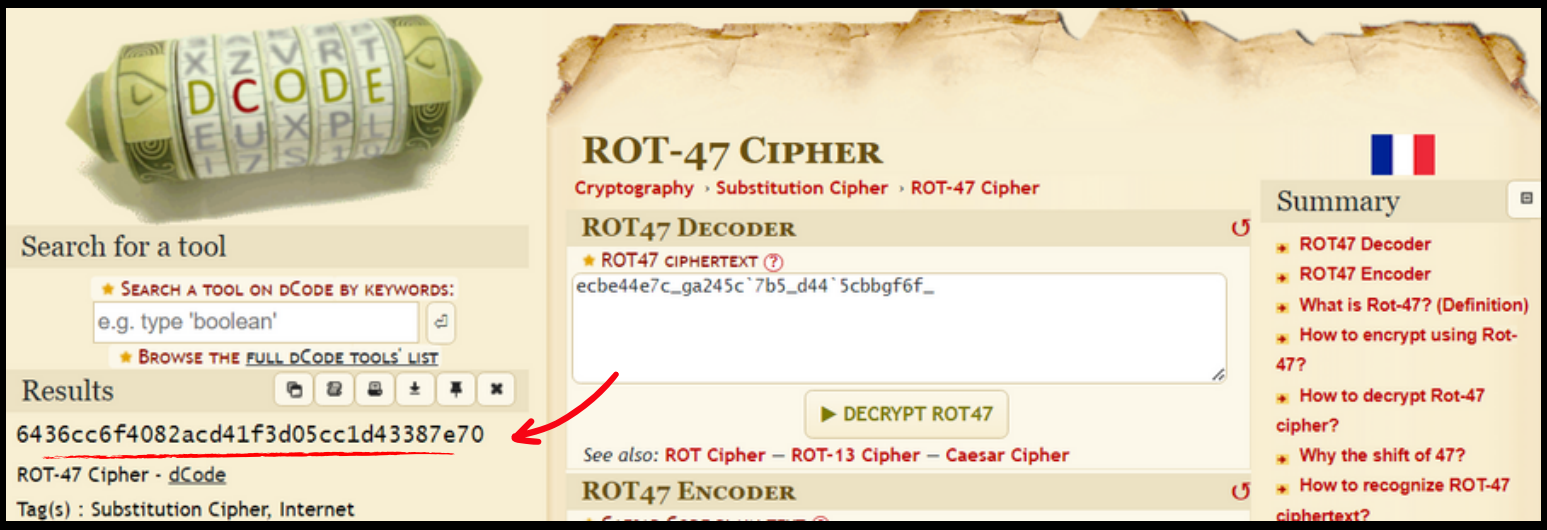
CHALLENGE NAME : [Boot-Failed]

dcode.fr: Indicating hash2 is Rot-47 Cipher

You Can Even Use JavaScript Source File Of The Page Which is simply obfuscated, De-obfucate online using any tool and you get to know how the hashes are made?...



DEV: SAMARTH GHANTE



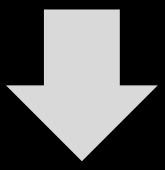
Upon Decoding With Rot-47 Cipher
We Get "6436cc6f4082acd41f3d05cc1d43387e70"
Where 64 is the price and later is something like a salt that is constant, You get to know this by analysing multiple hashes for different different price or simply by looking at the JavaScript Code

```
21  }
22  function rotEnode(_0x3e9a95) {
23    return _0x3e9a95.replace(/[!-~]/g, function (_0x2d0c83) {
24      return String.fromCharCode((_0x2d0c83.charCodeAt(0x0) + 0xe) %
    0x5e + 0x21);
25    });
26  }
27  const spell = '36cc6f4082acd41f3d05cc1d43387e70';
28  function buyNow() {
29    var _0x4b8702 =
    parseInt(document.getElementById("itemCounter").value);
30    var _0x3a788f =
    parseFloat(document.getElementById("finalPrice").innerText.replace("F
    inal Price: $", ''));
31    var _0x566947 = CryptoJS.MD5(_0x4b8702.toString()).toString();
32    var _0x35c26d = rotEnode((_0x3a788f +
    '36cc6f4082acd41f3d05cc1d43387e70').toString());
33    var _0x40ebe1 = {
34      'amount': _0x4b8702,
35      'price': _0x3a788f,
36      'hash1': _0x566947,
37      'hash2': _0x35c26d
38    };
```

Here you can see spell is being appended in the hash2

Even, If You don't know about the later part of that hash, modify the initial part of the hash
i.e price from $64 ---> $1 (anything below 5$)

So the hash2 must be the rot47 encryption of 1 & the spell/constant part as it is!
i.e 136cc6f4082acd41f3d05cc1d43387e70



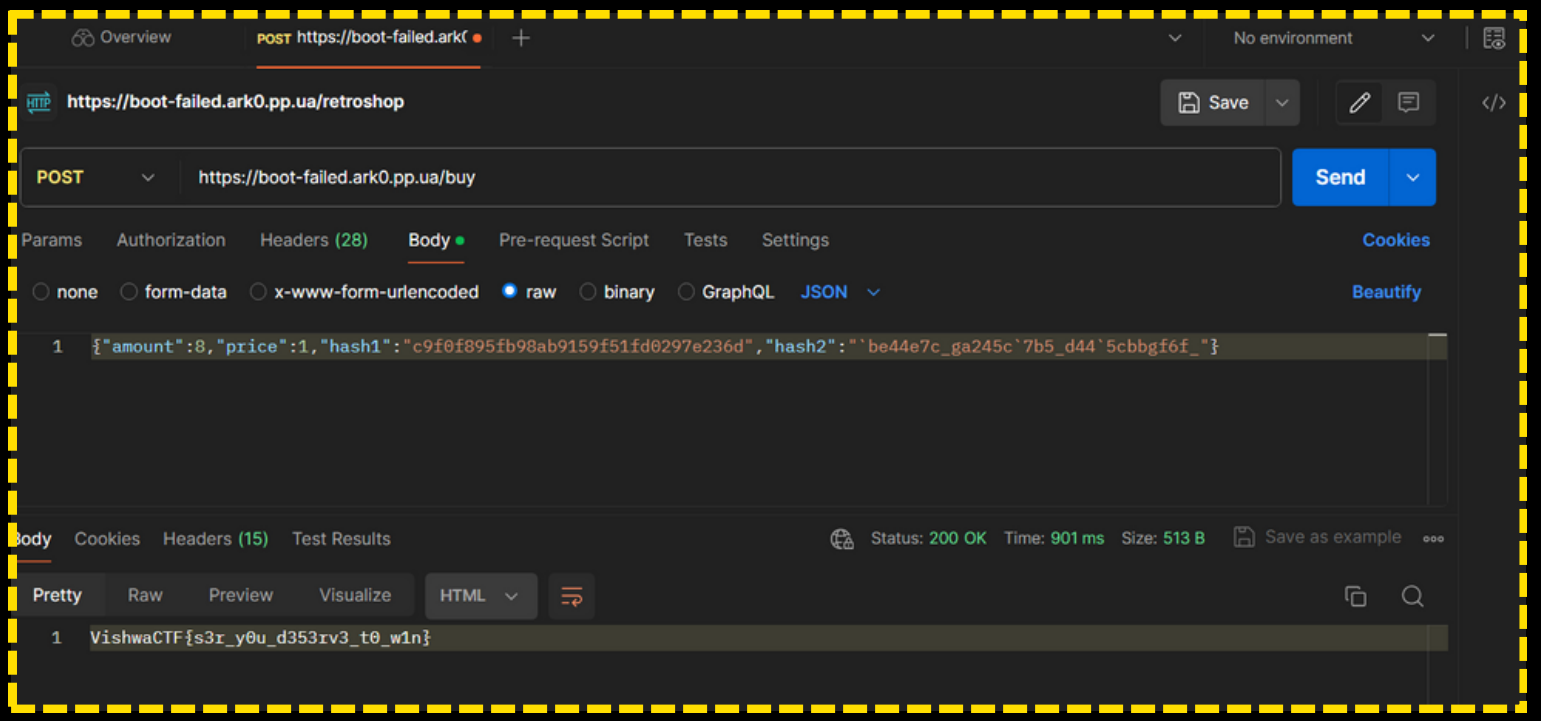
Now Encrypt it again with Rot47 Cipher

Final Hash2: **`be44e7c_ga245c`7b5_d44`5cbbgf6f_**

Now Change The Value of
Price = 1 & The Hash2 =
`be44e7c_ga245c`7b5_d44`5cbbgf6f_
& Submit The Post Request to /buy endpoint

VishwaCTF

CHALLENGE NAME : [Boot-Failed]



You will get the flag!!! 🚩🚩🚩

Flag: VishwaCTF{s3r_y0u_d353rv3_t0_w1n}

I HOPE YOU ENJOY THIS CHALLENGE,
YOU CAN CONNECT WITH ME ON MY
LINKEDIN

THANK YOU🙏

DEV: SAMARTH GHANTE