The Obscure Underground

Once we open the homepage we discover an input field along with today's date. The page also mentions a line which says "Encode what ye shall seek~!" which is actually quite important in this challenge.

If we check the source code of the page we will see that a javascript file is connected to this page called index.js which once visited leads us to this page:


```
var _0x2f20=
["","\x6A\x6F\x69\x6E","\x4D\x54\x4D\x7A\x4E\x77\x3D\x3D","\x30","\x70\x61\x64\x53\x74\x61\x72\x74","\x67\x65\x74\x44\x61\x74\x65","\x67\x65\x74\x4D\x6F\x6E\x74\x68","\x67\
x65\x74\x46\x75\x6C\x6C\x59\x65\x61\x72","\x2F","\x72\x65\x70\x6C\x61\x63\x65","\x6C\x65\x6E\x67\x74\x68","\x73\x75\x62\x73\x74\x72","\x30\x30","\x66\x72\x6F\x6D\x43\x68\x6
1\x72\x43\x6F\x64\x65","\x63\x68\x61\x72\x43\x6F\x64\x65\x41\x74","\x70\x75\x73\x68","\x3C\x63\x65\x6E\x74\x65\x72\x3E\x4C\x6F\x67\x69\x6E\x20\x55\x6E\x73\x75\x63\x63\x65\x
73\x73\x66\x75\x6C\x6C\x21\x3C\x2F\x63\x65\x6E\x74\x65\x72\x3E","\x77\x72\x69\x74\x65","\x3C\x63\x65\x6E\x74\x65\x72\x3E\x4C\x6F\x67\x69\x6E\x20\x53\x75\x63\x63\x65\x73\x73
\x66\x75\x6C\x6C\x21\x3C\x2F\x63\x65\x6E\x74\x65\x72\x3E","\x63\x6F\x6F\x6B\x69\x65","\x6A\x75\x73\x74\x61\x63\x6F\x6F\x6B\x69\x65","\x3D","\x3C\x63\x65\x6E\x74\x65\x72\x3E
","\x3C\x2F\x63\x65\x6E\x74\x65\x72\x3E","\x30\x38\x31\x35\x31\x39\x34\x37"];let [uno,dos,tres,cuatro,cinco,seis,siete,ocho,nueve,diez]=[1,2,3,4,5,6,7,8,9,10];var flex=
[uno,dos,tres,cuatro,cinco,seis,siete,ocho,nueve,diez];var leet=[flex[0],flex[2],flex[2],flex[6]];var remc=(leet[_0x2f20[1]](_0x2f20[0]));var added=flex[0]+ flex[2]+
flex[2]+ flex[6];var leetn=1337;var b1=btoa(added);var b2=btoa(remc);var b3=btoa(leetn);var b4=atob(_0x2f20[2]);var b5=atob(b2);var code;var todaysdate;function date(){var
_0x83baxe= new Date();var _0x83baxf=String(_0x83baxe[_0x2f20[5]]())[_0x2f20[4]](2,_0x2f20[3]);var _0x83bax10=String(_0x83baxe[_0x2f20[6]]()+ 1)[_0x2f20[4]]
(2,_0x2f20[3]);var _0x83bax11=_0x83baxe[_0x2f20[7]]();_0x83baxe= _0x83bax10+ _0x2f20[8]+ _0x83baxf+ _0x2f20[8]+ _0x83bax11;_0x83baxe= _0x83baxe[_0x2f20[9]]
(_0x2f20[8],_0x2f20[0]);_0x83baxe= _0x83baxe[_0x2f20[9]](_0x2f20[8],_0x2f20[0]);todaysdate= _0x83baxe}function hex2a(_0x83bax13){var _0x83bax14= _0x83bax13.toString();var
_0x83bax15= _0x2f20[0];for(var _0x83bax16=0;(_0x83bax16< _0x83bax14[_0x2f20[10]]&& _0x83bax14[_0x2f20[11]](_0x83bax16,2)!== _0x2f20[12]);_0x83bax16+= 2){_0x83bax15+=
String[_0x2f20[13]](parseInt(_0x83bax14[_0x2f20[11]](_0x83bax16,2),16))};return _0x83bax15}function a2hex(_0x83bax15){var _0x83bax18=[];for(var
_0x83bax19=0,_0x83bax1a=_0x83bax15[_0x2f20[10]];_0x83bax19<_0x83bax1a;_0x83bax19++){var _0x83bax14=Number(_0x83bax15[_0x2f20[14]]
(_0x83bax19)).toString(16);_0x83bax18[_0x2f20[15]](_0x83bax14)};return _0x83bax18[_0x2f20[1]](_0x2f20[0])}function comparingfunc(){if(b5== b4){document[_0x2f20[17]]
(_0x2f20[16]);code= 0}else {document[_0x2f20[17]](_0x2f20[18]);code= 1}}function processfunc(){comparingfunc();if(code== 0){date();var
_0x83bax1d=btoa(todaysdate);document[_0x2f20[19]]= _0x2f20[20]+ _0x2f20[21]+ _0x83bax1d;_0x83bax1d= a2hex(_0x83bax1d);var _0x83bax1e=hex2a(_0x83bax1d);_0x83bax1e=
atob(_0x83bax1e);document[_0x2f20[17]](_0x2f20[22]+ _0x83bax1e+ _0x2f20[23])}else {if(code== 1){date();var _0x83bax1d=btoa(_0x2f20[24]);document[_0x2f20[19]]= _0x2f20[20]+
_0x2f20[21]+ _0x83bax1d;var _0x83bax1f=atob(_0x83bax1d);_0x83bax1f= hex2a(3038313531393437);document[_0x2f20[17]](_0x2f20[22]+ _0x83bax1f+ _0x2f20[23])}}}processfunc()
```

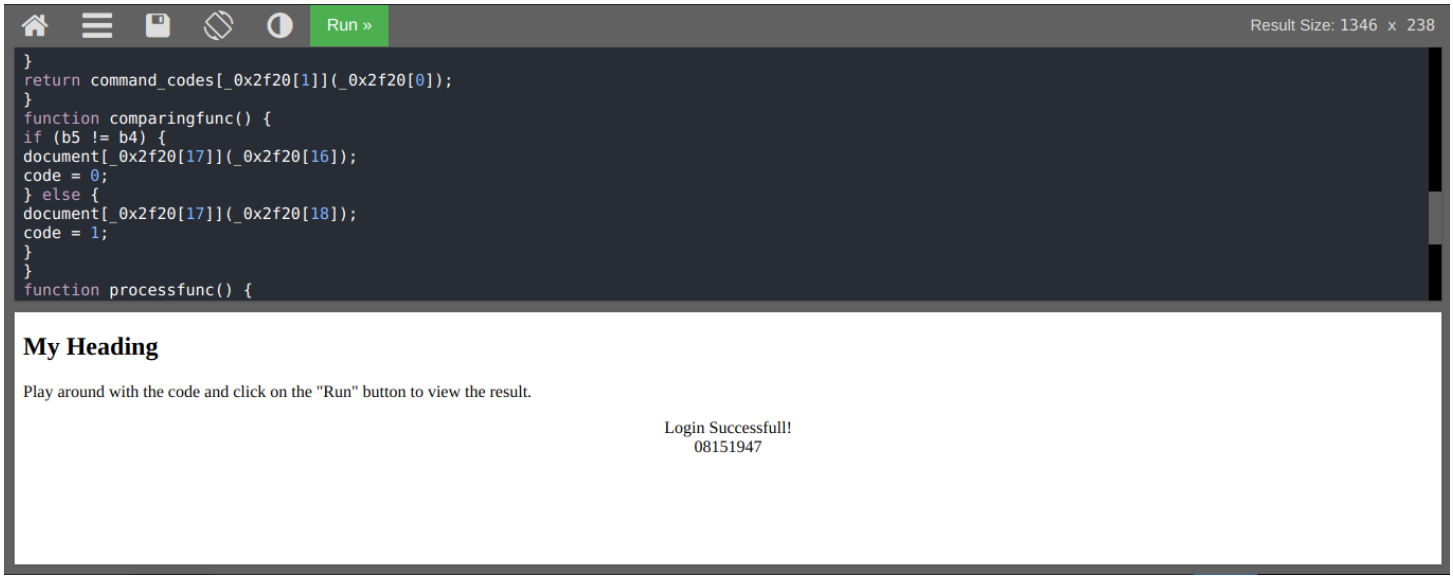

This is actually obfuscated javascript which we can make readable /native using **https://www.dcode.fr/javascript-unobfuscator**

```
'use strict';
var _0x2f20 = ["", "join", "MTMzNw==", "0",
"padStart", "getDate", "getMonth",
"getFullYear", "/", "replace", "length",
"substr", "00", "fromCharCode",
"charCodeAt", "push", "<center>Login
Unsuccessfull!</center>", "write", "
<center>Login Successfull!</center>",
"cookie", "justacookie", "=", "<center>", "
</center>", "08151947"];
var uno = 1;
var dos = 2;
var tres = 3;
var cuatro = 4;
var cinco = 5;
var seis = 6;
var siete = 7;
var ocho = 8;
var nueve = 9;
var diez = 10;
var flex = [uno, dos, tres, cuatro, cinco,
seis, siete, ocho, nueve, diez];
var leet = [flex[0], flex[2], flex[2],
flex[6]];
var remc = leet[_0x2f20[1]](_0x2f20[0]);
var added = flex[0] + flex[2] + flex[2] +
flex[6];
var leetn = 1337;
var b1 = btoa(added);
var b2 = btoa(remc);
var b3 = btoa(leetn);
var b4 = atob(_0x2f20[2]);
var b5 = atob(b2);
var code;
```

The code will then basically look like this, the main objective of this challenge is to go through the whole source code and understand it.

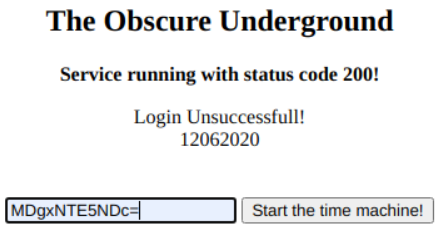
```
function comparingfunc() {
if (b5 == b4) {
document[_0x2f20[17]](_0x2f20[16]);
code = 0;
} else {
document[_0x2f20[17]](_0x2f20[18]);
code = 1;
}
}
```

With just a minor change in this code by changing b5==b4 to b5!=b4



Like we can see in the above code we changed that if condition and ran it on a editor of our choice. I tried the https://www.w3schools.com/js/tryit.asp?filename=tryjs_editor for completing this challenge in less time.

This gives us a string with a previous date "08151947", the base64 encoded value for this date can be found in the cookies. We just need to pass the base64 encoded string to the home page



And there we have our flag:
vulncon{0bfu@73d_javascript_1s_l0b}