WEB: Console

The webpage looks like the following:

	submit

Not much can be done, so the first thing is to try something. Two items are available:
- Box where we can insert text
- Button

We can do a test, like the following:

test	submit

Nope

We can think that by inserting the right password we can get the flag. The first thing to do is to inspect the php.

```html
<!doctype html>
<html>
    <link type="text/css" id="dark-mode" rel="stylesheet" href(unknown)>
    <style type="text/css" id="dark-mode-custom-style"></style>
    ▶<head>…</head>
... ▼<body> == $0
        <!-- It's too easy -->
        <input type="text" id="pass" value>
        <button type="submit" onclick="what()">submit</button>
        <p id="p">Nope</p>
    ▼<script>
```

```javascript
            var foo = document.getElementById("p");

            function what(){
                var input = document.getElementById("pass").value;
                if(md5(input) =="7b1ece53a46f4a5a2995b9cf901bf457"){
                    getThat('Y');
                }else{getThat('N')}
            }
            function getThat(string){
                if(string == 'Y'){
                    $.ajax({
                        type: 'GET',
                        url: '1/key.php',
                        success: function (file_html) {
                            // success
                            foo.innerHTML=(file_html)
                        }
                    });
                }else{
                    foo.innerHTML = "Nope";

                }
            }
            /* this function makes a md5 hash of whatever is passed to it. You DON'T have to understand how it works to solve */
            var md5=function(r){function n(r,n){return r<<n|r>>>32-n}function t(r,n){var t,o,e,u,f;return
e=2147483648&r,u=2147483648&n,t=1073741824&r,o=1073741824&n,f=(1073741823&r)+(1073741823&n),t&o?2147483648^f^e^u:t|o?1073741824&f?
3221225472^f^e^u:1073741824^f^e^u:f^e^u}function o(r,n,t){return r&n|~r&t}function e(r,n,t){return r&t|n&~t}function u(r,n,t){return r^n^t}function
f(r,n,t){return n^(r|~t)}function i(r,e,u,f,i,a,c){return r=t(r,t(t(o(e,u,f),i),c)),t(n(r,a),e)}function a(r,o,u,f,i,a,c){return
r=t(r,t(t(e(o,u,f),i),c)),t(n(r,a),o)}function c(r,o,e,f,i,a,c){return r=t(r,t(t(u(o,e,f),i),c)),t(n(r,a),o)}function C(r,o,e,u,i,a,c){return
r=t(r,t(t(f(o,e,u),i),c)),t(n(r,a),o)}function g(r){for(var n,t=r.length,o=t+8,e=(o-o%64)/64,u=16*(e+1),f=Array(u-1),i=0,a=0;t>a;)n=(a-
a%4)/4,i=a%4*8,f[n]=f[n]|r.charCodeAt(a)<<i,a++;return n=(a-a%4)/4,i=a%4*8,f[n]=f[n]|128<<i,f[u-2]=t<<3,f[u-1]=t>>>29,f}function h(r){var
n,t,o="",e="";for(t=0;3>=t;t++)n=r>>>8*t&255,e="0"+n.toString(16),o+=e.substr(e.length-2,2);return o}function d(r){r=r.replace(/\r\n/g,"\n");for(var
n="",t=0;t<r.length;t++){var o=r.charCodeAt(t);128>o?n+=String.fromCharCode(o):o>127&&2048>o?
(n+=String.fromCharCode(o>>6|192),n+=String.fromCharCode(63&o|128)):
(n+=String.fromCharCode(o>>12|224),n+=String.fromCharCode(o>>6&63|128),n+=String.fromCharCode(63&o|128))}return n}var
v,S,m,l,A,s,y,b,p,w=Array(),D=7,L=12,M=17,j=22,k=5,q=9,x=14,z=20,B=4,E=11,F=16,G=23,H=6,I=10,J=15,K=21;for(r=d(r),w=g(r),s=1732584193,y=4023233417,b=256238
3102,p=271733878,v=0;v<w.length;v+=16)S=s,m=y,l=b,A=p,s=i(s,y,b,p,w[v+0],D,3614090360),p=i(p,s,y,b,w[v+1],L,3905402710),b=i(b,p,s,y,w[v+2],M,606105819),y=i
(y,b,p,s,w[v+3],j,3250441966),s=i(s,y,b,p,w[v+4],D,4118548399),p=i(p,s,y,b,w[v+5],L,1200080426),b=i(b,p,s,y,w[v+6],M,2821735955),y=i(y,b,p,s,w[v+7],j,42492
61313),s=i(s,y,b,p,w[v+8],D,1770035416),p=i(p,s,y,b,w[v+9],L,2336552879),b=i(b,p,s,y,w[v+10],M,4294925233),y=i(y,b,p,s,w[v+11],j,2304563134),s=i(s,y,b,p,w[
v+12],D,1804603682),p=i(p,s,y,b,w[v+13],L,4254626195),b=i(b,p,s,y,w[v+14],M,2792965006),y=i(y,b,p,s,w[v+15],j,1236535329),s=a(s,y,b,p,w[v+1],k,4129170786),
p=a(p,s,y,b,w[v+6],q,3225465664),b=a(b,p,s,y,w[v+11],x,643717713),y=a(y,b,p,s,w[v+0],z,3921069994),s=a(s,y,b,p,w[v+5],k,3593408605),p=a(p,s,y,b,w[v+10],q,3
8016083),b=a(b,p,s,y,w[v+15],x,3634488961),y=a(y,b,p,s,w[v+4],z,3889429448),s=a(s,y,b,p,w[v+9],k,568446438),p=a(p,s,y,b,w[v+14],q,3275163606),b=a(b,p,s,y,w
[v+3],x,4107603335),y=a(y,b,p,s,w[v+8],z,1163531501),s=a(s,y,b,p,w[v+13],k,2850285829),p=a(p,s,y,b,w[v+2],q,4243563512),b=a(b,p,s,y,w[v+7],x,1735328473),y=
a(y,b,p,s,w[v+12],z,2368359562),s=c(s,y,b,p,w[v+5],B,4294588738),p=c(p,s,y,b,w[v+8],E,2272392833),b=c(b,p,s,y,w[v+11],F,1839030562),y=c(y,b,p,s,w[v+14],G,4
259657740),s=c(s,y,b,p,w[v+1],B,2763975236),p=c(p,s,y,b,w[v+4],E,1272893353),b=c(b,p,s,y,w[v+7],F,4139469664),y=c(y,b,p,s,w[v+10],G,3200236656),s=c(s,y,b,p
,w[v+13],B,681279174),p=c(p,s,y,b,w[v+0],E,3936430074),b=c(b,p,s,y,w[v+3],F,3572445317),y=c(y,b,p,s,w[v+6],G,76029189),s=c(s,y,b,p,w[v+9],B,3654602809),p=c
(p,s,y,b,w[v+12],E,3873151461),b=c(b,p,s,y,w[v+15],F,530742520),y=c(y,b,p,s,w[v+2],G,3299628645),s=C(s,y,b,p,w[v+0],H,4096336452),p=C(p,s,y,b,w[v+7],I,1126
891415),b=C(b,p,s,y,w[v+14],J,2878612391),y=C(y,b,p,s,w[v+5],K,4237533241),s=C(s,y,b,p,w[v+12],H,1700485571),p=C(p,s,y,b,w[v+3],I,2399980690),b=C(b,p,s,y,w
[v+10],J,4293915773),y=C(y,b,p,s,w[v+1],K,2240044497),s=C(s,y,b,p,w[v+8],H,1873313359),p=C(p,s,y,b,w[v+15],I,4264355552),b=C(b,p,s,y,w[v+6],J,2734768916),y
=C(y,b,p,s,w[v+13],K,1309151649),s=C(s,y,b,p,w[v+4],H,4149444226),p=C(p,s,y,b,w[v+11],I,3174756917),b=C(b,p,s,y,w[v+2],J,718787259),y=C(y,b,p,s,w[v+9],K,39
51481745),s=t(s,S),y=t(y,m),b=t(b,l),p=t(p,A);var N=h(s)+h(y)+h(b)+h(p);return N.toLowerCase()};
```
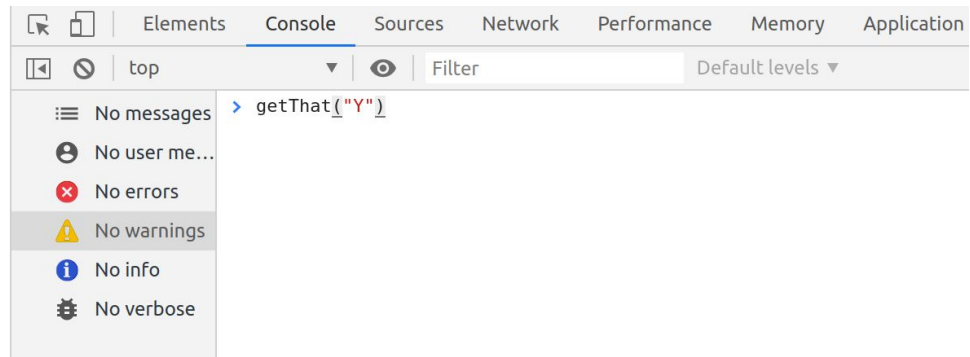
```html
    </script>
```

We can notice javascript. From the flow, we can see that first see that the value that we insert is controlled with the *md5* function and, if there is a match, a function *getThat("Y")* is called, otherwise *getThat("N")*.

When the argument is *"Y"*, the function *getThat* takes something from an external page and it prints its content; otherwise, we can see the default message "Nope".

The main clue is to notice that in order to get the flag, we need to be in a situation like *getThat("Y")*. However, this is just a js function, so in our browser we can go in the console section and call it. The flag is revealed.

Elements   Console   Sources   Network   Performance   Memory   Application

top   ▼   Filter   Default levels ▼

No messages
No user me...
No errors
No warnings
No info
No verbose

> getThat("Y")

test   submit

Password: flag{console_controls_js}