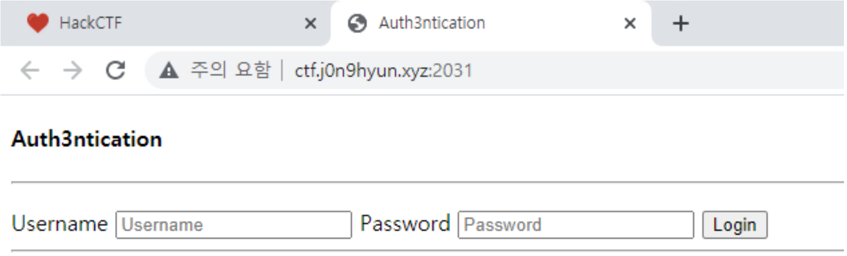
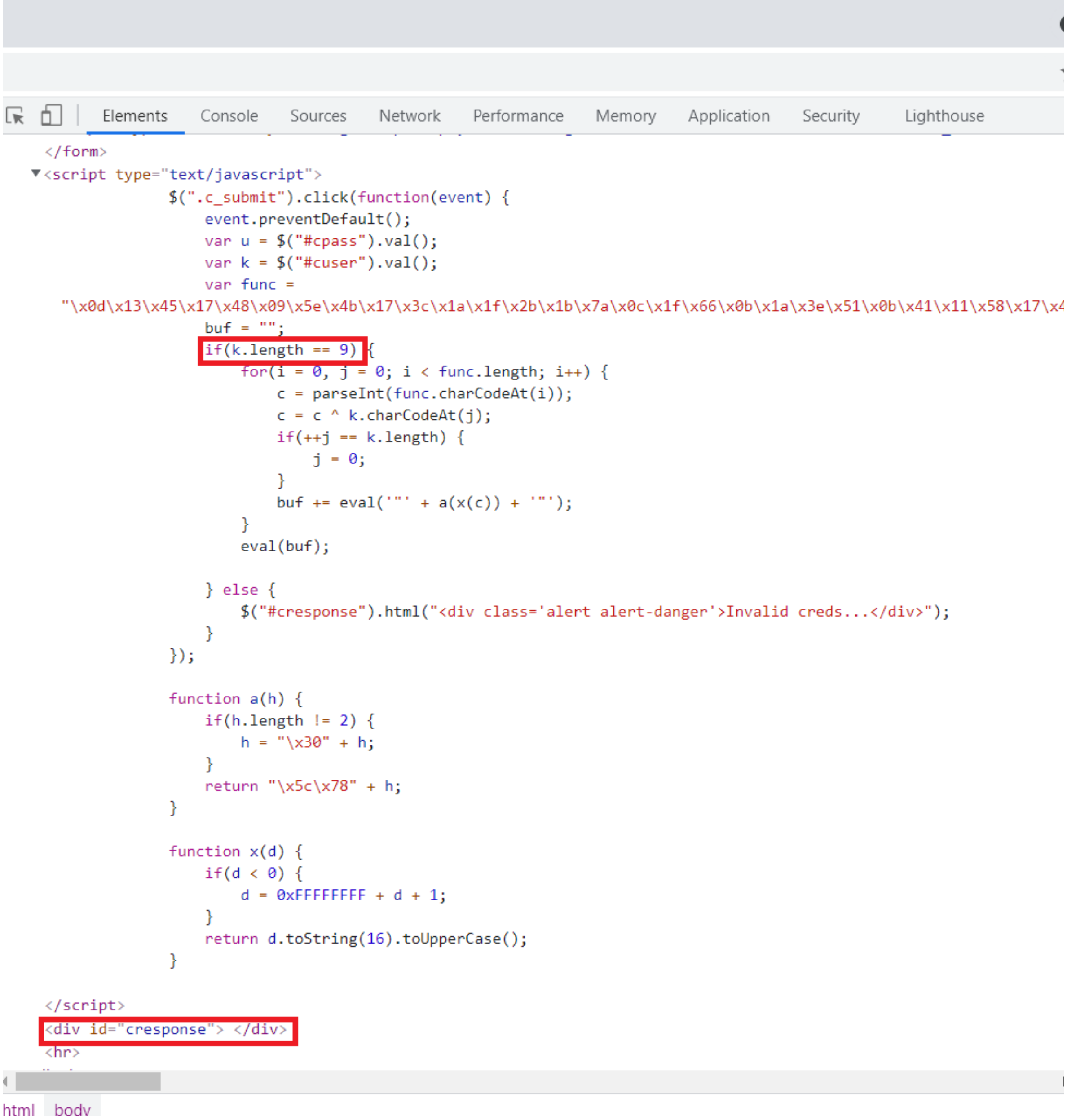
Authenticate



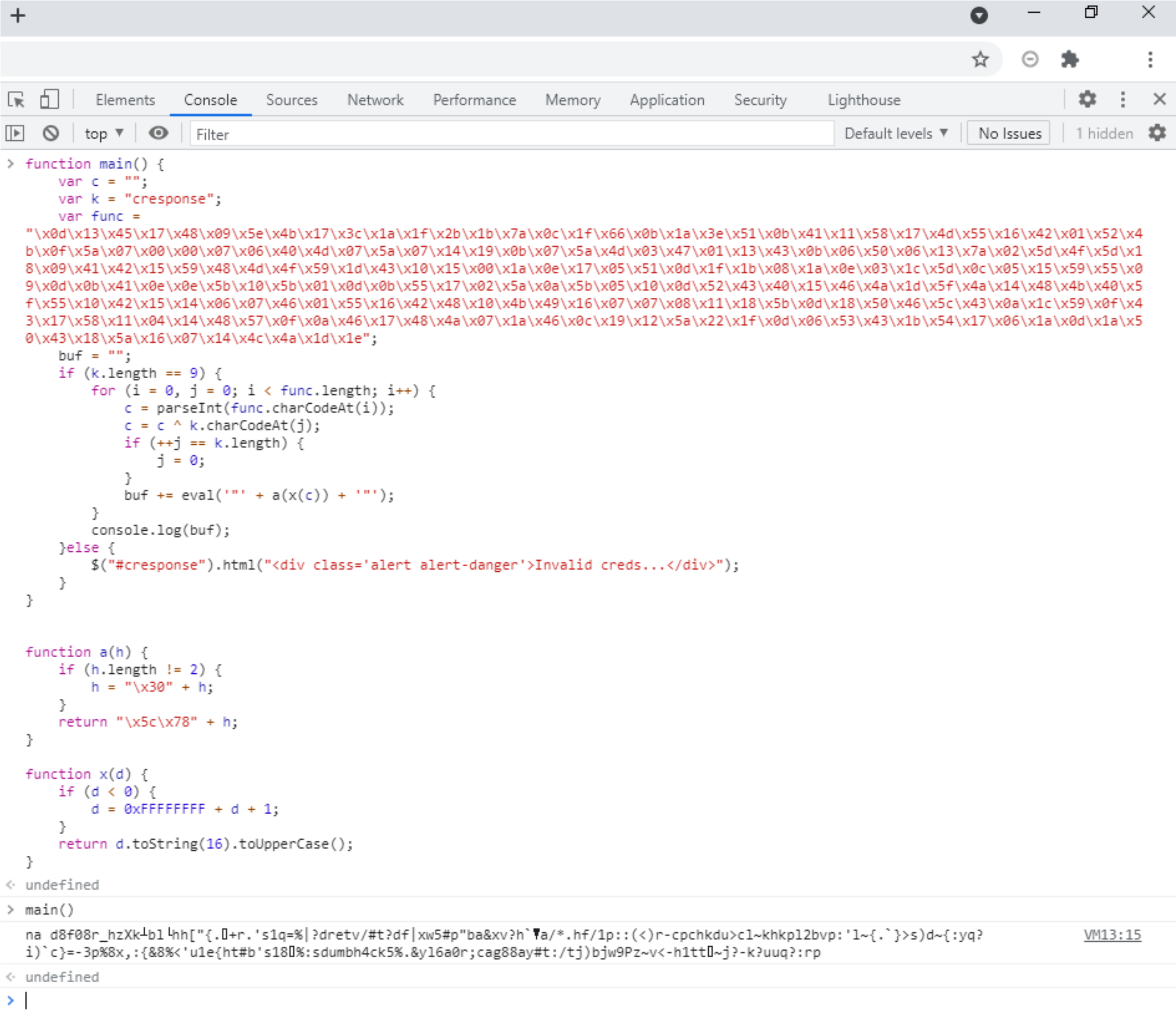
들어가자마자 보이는 것은 로그인 창이다. 그래서 SQL injection인줄 알고 ' OR 1=1 -- 같은 것을 넣어보았으나 아무런 효과가 없었다. 그래서 f12로 살펴보니 자바스크립트가 보인다.



```
  </form>
▼<script type="text/javascript">
            $(".c_submit").click(function(event) {
                event.preventDefault();
                var u = $("#cpass").val();
                var k = $("#cuser").val();
                var func =
"\x0d\x13\x45\x17\x48\x09\x5e\x4b\x17\x3c\x1a\x1f\x2b\x1b\x7a\x0c\x1f\x66\x0b\x1a\x3e\x51\x0b\x41\x11\x58\x17\x4
                buf = "";
                if(k.length == 9) {
                    for(i = 0, j = 0; i < func.length; i++) {
                        c = parseInt(func.charCodeAt(i));
                        c = c ^ k.charCodeAt(j);
                        if(++j == k.length) {
                            j = 0;
                        }
                        buf += eval('"' + a(x(c)) + '"');
                    }
                    eval(buf);

                } else {
                    $("#cresponse").html("<div class='alert alert-danger'>Invalid creds...</div>");
                }
            });

            function a(h) {
                if(h.length != 2) {
                    h = "\x30" + h;
                }
                return "\x5c\x78" + h;
            }

            function x(d) {
                if(d < 0) {
                    d = 0xFFFFFFFF + d + 1;
                }
                return d.toString(16).toUpperCase();
            }

  </script>
  <div id="cresponse"> </div>
  <hr>
```

k(username)의 길이가 9여야하는데 마침 밑에 id라고 9글자인 "cresponse"가 보인다. 구글 콘솔을 이용해 k에 cresponse를 넣고 돌려보니 이상한 문자열이 나온다.

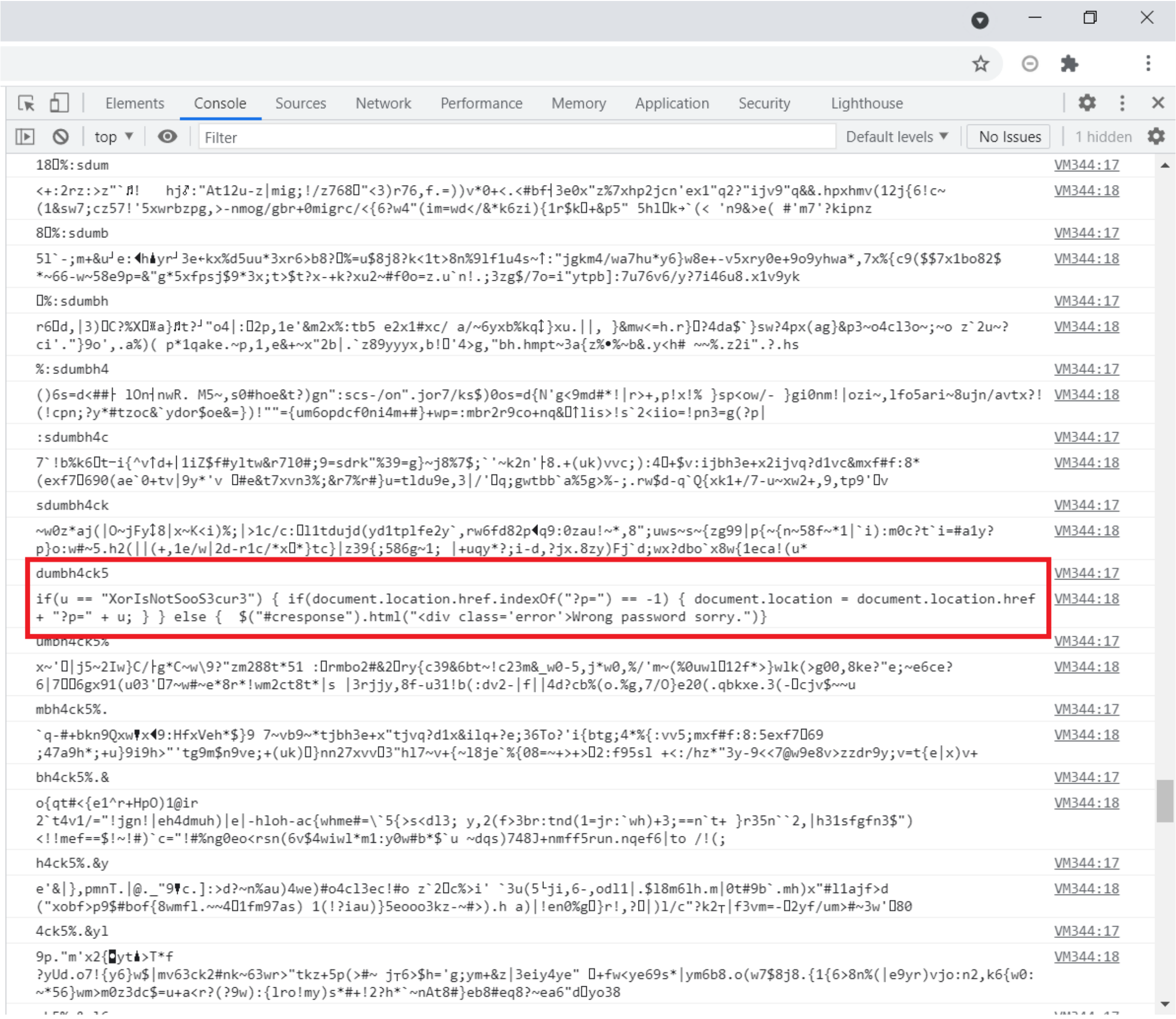
```
function main() {
    var c = "";
    var k = "cresponse";
    var func = "\x0d\x13\x45\x17\x48\x09\x5e\x4b\x17\x3c\x1a\x1f\x2b\x1b\x7a\x0c\x1f\x66\x0b\x1a\x3e\x51\x0b\x41\x11\x58\x17\x4d\x55\x
    buf = "";
    if (k.length == 9) {
        for (i = 0, j = 0; i < func.length; i++) {
            c = parseInt(func.charCodeAt(i));
            c = c ^ k.charCodeAt(j);
            if (++j == k.length) {
                j = 0;
            }
            buf += eval('"' + a(x(c)) + '"');
        }
        console.log(buf);
    }else {
        $("#cresponse").html("<div class='alert alert-danger'>Invalid creds...</div>");
    }
}


function a(h) {
    if (h.length != 2) {
        h = "\x30" + h;
    }
    return "\x5c\x78" + h;
}

function x(d) {
    if (d < 0) {
        d = 0xFFFFFFFF + d + 1;
    }
    return d.toString(16).toUpperCase();
}
```



```
> function main() {
      var c = "";
      var k = "cresponse";
      var func =
  "\x0d\x13\x45\x17\x48\x09\x5e\x4b\x17\x3c\x1a\x1f\x2b\x1b\x7a\x0c\x1f\x66\x0b\x1a\x3e\x51\x0b\x41\x11\x58\x17\x4d\x55\x16\x42\x01\x52\x4
  b\x0f\x5a\x07\x00\x00\x07\x06\x40\x4d\x07\x5a\x07\x14\x19\x0b\x07\x5a\x4d\x03\x47\x01\x13\x43\x0b\x06\x50\x06\x13\x7a\x02\x5d\x4f\x5d\x1
  8\x09\x41\x42\x15\x59\x48\x4d\x4f\x59\x1d\x43\x10\x15\x00\x1a\x0e\x17\x05\x51\x0d\x1f\x1b\x08\x1a\x0e\x03\x1c\x5d\x0c\x05\x15\x59\x55\x0
  9\x0d\x0b\x41\x0e\x0e\x5b\x10\x5b\x01\x0d\x0b\x55\x17\x02\x5a\x0a\x5b\x05\x10\x0d\x52\x43\x40\x15\x46\x4a\x1d\x5f\x4a\x14\x48\x4b\x40\x5
  f\x55\x10\x42\x15\x14\x06\x07\x46\x01\x55\x16\x42\x48\x10\x4b\x49\x16\x07\x07\x08\x11\x18\x5b\x0d\x18\x50\x46\x5c\x43\x0a\x1c\x59\x0f\x4
  3\x17\x58\x11\x04\x14\x48\x57\x0f\x0a\x46\x17\x48\x4a\x07\x1a\x46\x0c\x19\x12\x5a\x22\x1f\x0d\x06\x53\x43\x1b\x54\x17\x06\x1a\x0d\x1a\x5
  0\x43\x18\x5a\x16\x07\x14\x4c\x4a\x1d\x1e";
      buf = "";
      if (k.length == 9) {
          for (i = 0, j = 0; i < func.length; i++) {
              c = parseInt(func.charCodeAt(i));
              c = c ^ k.charCodeAt(j);
              if (++j == k.length) {
                  j = 0;
              }
              buf += eval('"' + a(x(c)) + '"');
          }
          console.log(buf);
      }else {
          $("#cresponse").html("<div class='alert alert-danger'>Invalid creds...</div>");
      }
  }


  function a(h) {
      if (h.length != 2) {
          h = "\x30" + h;
      }
      return "\x5c\x78" + h;
  }

  function x(d) {
      if (d < 0) {
          d = 0xFFFFFFFF + d + 1;
      }
      return d.toString(16).toUpperCase();
  }
<· undefined
> main()
  na d8f08r_hzXk┴bl└hh["{.▯+r.'s1q=%|?dretv/#t?df|xw5#p"ba&xv?h`▼a/*.hf/1p::(<)r-cpchkdu>cl~khkpl2bvp:'l~{.`}>s)d~{:yq?        VM13:15
  i)`c}=-3p%8x,:{&8%<'u1e{ht#b's18▯%:sdumbh4ck5%.&yl6a0r;cag88ay#t:/tj)bjw9Pz~v<-h1tt▯~j?-k?uuq?:rp
<· undefined
> |
```

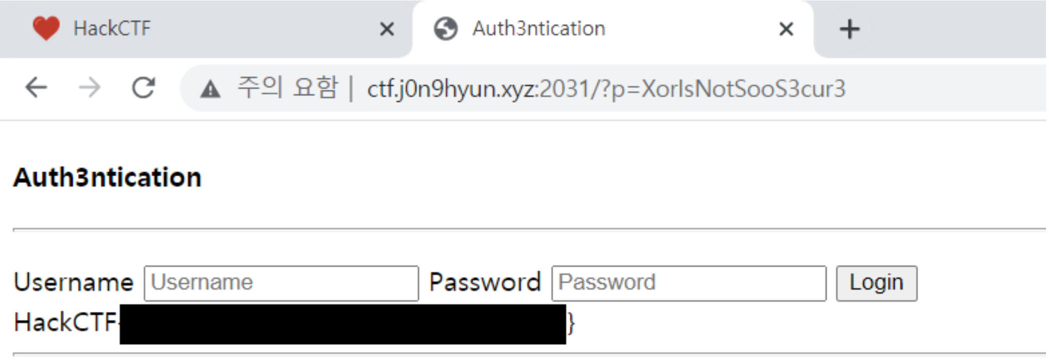
아까전에 username은 9글자였으니까 저 문자열을 9글자씩 나누어서 돌려보자

```
function main() {
    var str = "na d8f08r_hzXkblhh[\"{.+r.'s1q=%|?dretv/#t?df|xw5#p\"ba&xv?h`a/*.hf/1p::(<)r-cpchkdu>cl~khkpl2bvp:\'l~{.`}>s)d~{:yq?i)\
    for(var va=0; va < str.length; va++){
        var c = "";
        var k = str.substr(va, 9);
        var func = "\x0d\x13\x45\x17\x48\x09\x5e\x4b\x17\x3c\x1a\x1f\x2b\x1b\x7a\x0c\x1f\x66\x0b\x1a\x3e\x51\x0b\x41\x11\x58\x17\x4d\x
        buf = "";
        if (k.length == 9) {
            for (i = 0, j = 0; i < func.length; i++) {
                c = parseInt(func.charCodeAt(i));
                c = c ^ k.charCodeAt(j);
                if (++j == k.length) {
                    j = 0;
                }
                buf += eval('"' + a(x(c)) + '"');
            }
            console.log(k);
            console.log(buf);
        }else {
            $("#cresponse").html("<div class='alert alert-danger'>Invalid creds...</div>");
        }
    }
}
```



```
18□%:sdum                                                                                     VM344:17
<+:2rz:>z"`♬!   hj♪:"At12u-z|mig;!/z768□"<3)r76,f.=))v*0+<.<#bf┤3e0x"z%7xhp2jcn'ex1"q2?"ijv9"q&&.hpxhmv(12j{6!c~   VM344:18
(1&sw7;cz57!'5xwrbzpg,>-nmog/gbr+0migrc/<{6?w4"(im=wd</&*k6zi){1r$k□+&p5" 5hl□k+`(< 'n9&>e( #'m7'?kipnz
8□%:sdumb                                                                                     VM344:17
51`-;m+&u┘e:◀h♝yr┘3e←kx%d5uu*3xr6>b8?□%=u$8j8?k<1t>8n%91f1u4s~↑:"jgkm4/wa7hu*y6}w8e+-v5xry0e+9o9yhwa*,7x%{c9($$7x1bo82$   VM344:18
*~66-w~58e9p=&"g*5xfpsj$9*3x;t>$t?x-+k?xu2~#f0o=z.u`n!.;3zg$/7o=i"ytpb]:7u76v6/y?7i46u8.x1v9yk
□%:sdumbh                                                                                     VM344:17
r6□d,|3)□C?%X□※a}♬t?┘"o4|:□2p,1e'&m2x%:tb5 e2x1#xc/ a/~6yxb%kq↕}xu.||, }&mw<=h.r}□?4da$`}sw?4px(ag}&p3~o4cl3o~;~o z`2u~?   VM344:18
ci'."}9o',.a%)( p*1qake.~p,1,e&+~x"2b|.`z89yyyx,b!□'4>g,"bh.hmpt~3a{z%•%~b&.y<h# ~~%.z2i".?.hs
%:sdumbh4                                                                                     VM344:17
()6s=d<##├ 1On┤nwR. M5~,s0#hoe&t?)gn":scs-/on".jor7/ks$)0os=d{N'g<9md#*!|r>+,p!x!% }sp<ow/- }gi0nm!|ozi~,1fo5ari~8ujn/avtx?!   VM344:18
(!cpn;?y*#tzoc&`ydor$oe&=})!""={um6opdcf0ni4m+#}+wp=:mbr2r9co+nq&□↑lis>!s`2<iio=!pn3=g(?p|
:sdumbh4c                                                                                     VM344:17
7`!b%k6□t-i{^v↑d+|1iZ$f#yltw&r710#;9=sdrk"%39=g}~j8%7$;`'~k2n'├8.+(uk)vvc;):4□+$v:ijbh3e+x2ijvq?d1vc&mxf#f:8*   VM344:18
(exf7□690(ae`0+tv|9y*'v □#e&t7xvn3%;&r7%r#}u=tldu9e,3|/'□q;gwtbb`a%5g>%-;.rw$d-q`Q{xk1+/7-u~xw2+,9,tp9'□v
sdumbh4ck                                                                                     VM344:17
~w0z*aj(|O~jFy↕8|x~K<i)%;|>1c/c:□l1tdujd(yd1tplfe2y`,rw6fd82p◀q9:0zau!~*,8";uws~s~{zg99|p{~{n~58f~*1|`i):m0c?t`i=#a1y?   VM344:18
p}o:w#~5.h2(||(+,1e/w|2d-r1c/*x□*}tc}|z39{;586g~1; |+uqy*?;i-d,?jx.8zy)Fj`d;wx?dbo`x8w{1eca!(u*
dumbh4ck5                                                                                     VM344:17
if(u == "XorIsNotSooS3cur3") { if(document.location.href.indexOf("?p=") == -1) { document.location = document.location.href   VM344:18
+ "?p=" + u; } } else {  $("#cresponse").html("<div class='error'>Wrong password sorry.")}
umbh4ck5%                                                                                     VM344:17
x~'□|j5~2Iw}C/├g*C~w\9?"zm288t*51 :□rmbo2#&2□ry{c39&6bt~!c23m&_w0-5,j*w0,%/'m~(%0uwl□12f*>}wlk(>g00,8ke?"e;~e6ce?   VM344:18
6|7□□6gx91(u03'□7~w#~e*8r*!wm2ct8t*|s |3rjjy,8f-u31!b(:dv2-|f||4d?cb%(o.%g,7/O}e20(.qbkxe.3(-□cjv$~~u
mbh4ck5%.                                                                                     VM344:17
`q-#+bkn9Qxw❢x◀9:HfxVeh*$}9 7~vb9~*tjbh3e+x"tjvq?d1x&ilq+?e;36To?'i{btg;4*%{:vv5;mxf#f:8:5exf7□69   VM344:18
;47a9h*;+u}9i9h>"'tg9m$n9ve;+(uk)□}nn27xvv□3"hl7~v+{~l8je`%{08=~+>+>□2:f95sl +<:/hz*"3y-9<<7@w9e8v>zzdr9y;v=t{e|x)v+
bh4ck5%.&                                                                                     VM344:17
o{qt#<{e1^r+HpO)1@ir                                                                          VM344:18
2`t4v1/="!jgn!|eh4dmuh)|e|-hloh-ac{whme#=\`5{>s<dl3; y,2(f>3br:tnd(1=jr:`wh)+3;==n`t+ }r35n``2,|h31sfgfn3$")
<!!mef==$!~!#)`c="!#%ng0eo<rsn(6v$4wiwl*m1:y0w#b*$`u ~dqs)748J+nmff5run.nqef6|to /!(;
h4ck5%.&y                                                                                     VM344:17
e'&|},pmnT.|@._"9❢c.]:>d?~n%au)4we)#o4cl3ec!#o z`2□c%>i' `3u(5└ji,6-,odl1|.$l8m6lh.m|0t#9b`.mh)x"#l1ajf>d   VM344:18
("xobf>p9$#bof{8wmfl.~~4□1fm97as) 1(!?iau)}5eooo3kz-~#>).h a)|!en0%g□}r!,?□|)l/c"?k2┬|f3vm=-□2yf/um>#~3w'□80
4ck5%.&yl                                                                                     VM344:17
9p."m'x2{□yt♝>T*f                                                                             VM344:18
?yUd.o7!{y6}w$|mv63ck2#nk~63wr>"tkz+5p(>#~ j┬6>$h='g;ym+&z|3eiy4ye" □+fw<ye69s*|ym6b8.o(w7$8j8.{1{6>8n%(|e9yr)vjo:n2,k6{w0:
~*56}wm>m0z3dc$=u+a<r?(?9w):{1ro!my)s*#+!2?h*`~nAt8#}eb8#eq8?~ea6"d□yo38
```

k = dumbh4ck5일때 제대로 된 내용이 나오는 것이 보인다. 해석해보면 u(password)가 XorIsNotSooS3cur3여야 하는 것 같다. 그래서 username에 dumbh4ck5을, password에 XorIsNotSooS3cur3 넣고 제출하니 답이 뜬다



Auth3ntication

Username Username Password Password Login

HackCTF[redacted]}