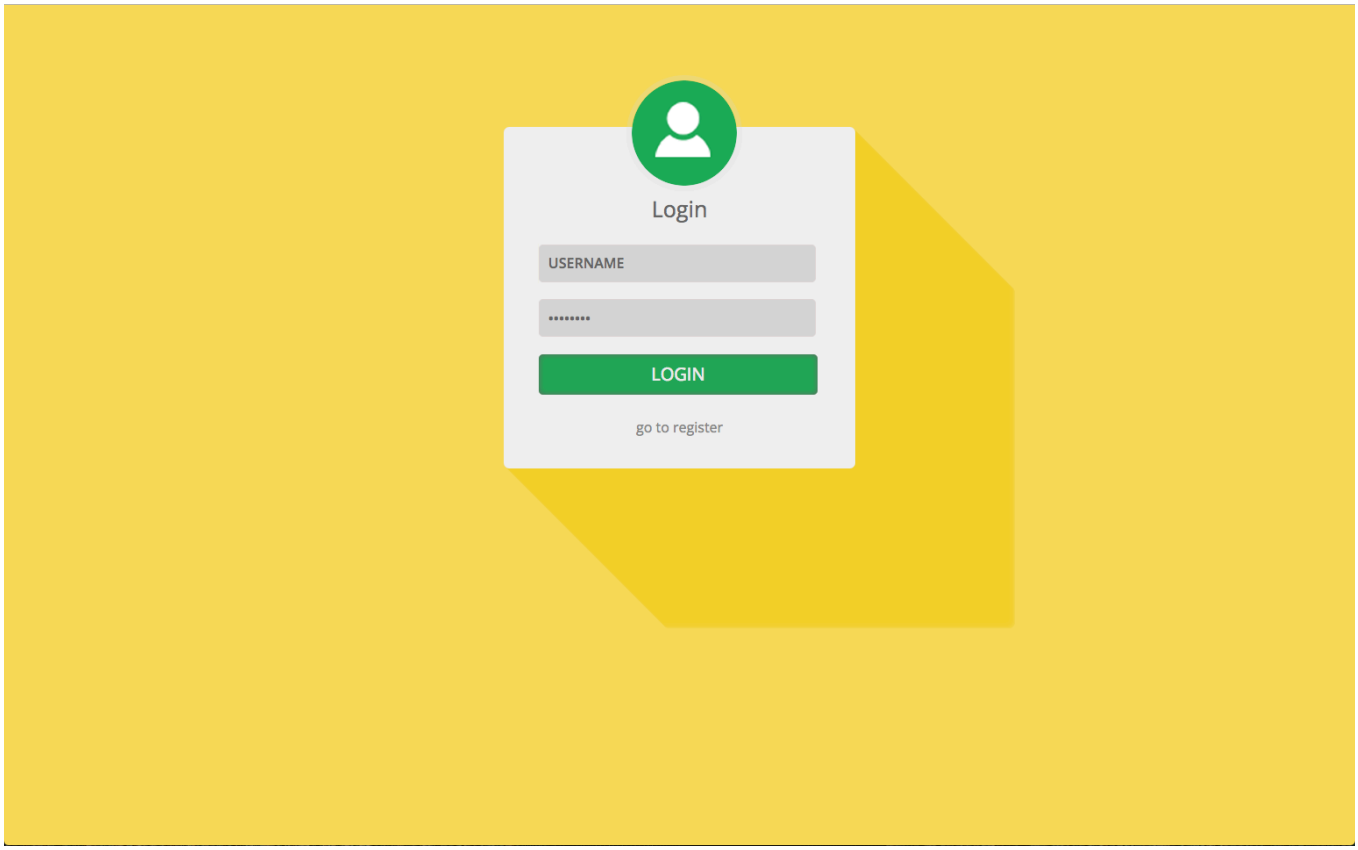
全国大学生信息安全竞赛WP-2018

就做出两题，简单记录一下。

Web

easyweb：

登陆后的界面如下：

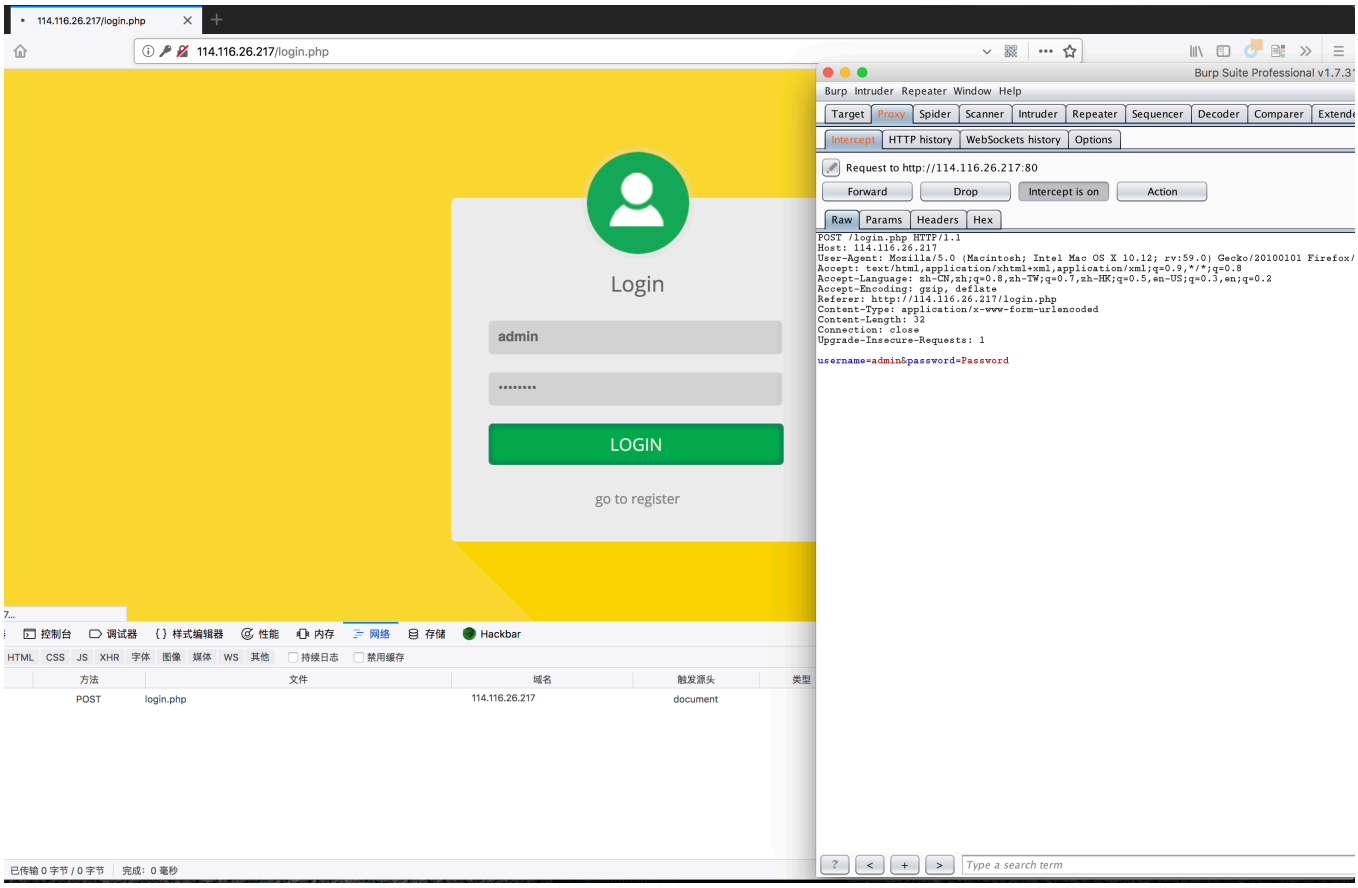


进入注册界面后，发现不论注册什么账号都说**username been used**，说明服务端屏蔽了注册，当作一个伪功能，应该从登陆界面入手。

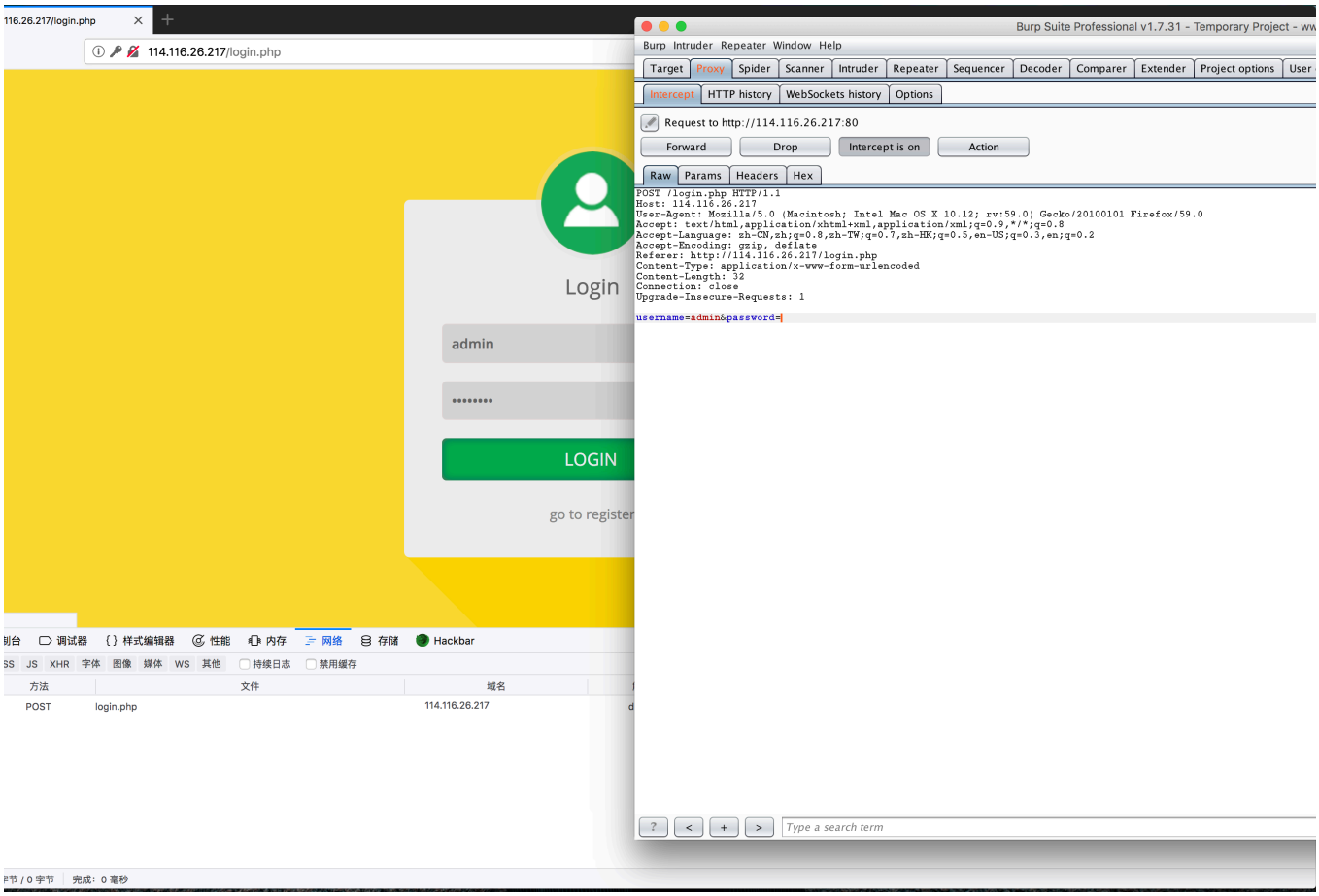
查看源代码发现，登陆界面输入空值时，空值会被填充，说明可能将密码置空值传送到服务端时，服务端会自动帮我们填充正确密码，话不多说开始实战。以下是观测环节：

```
<!DOCTYPE html>
<html>
<head>
<title></title>
<meta charset="utf-8">
<link href="/static/css/style.css" rel='stylesheet' type='text/css' />
<meta name="viewport" content="width=device-width, initial-scale=1">
<link href='http://fonts.googleapis.com/css?family=Open+Sans:600italic,400,300,600,700'
rel='stylesheet' type='text/css'>
<!--//webfonts-->
</head>
<body>
<!-----start-main---->
```

```
<div class="main">
<div class="login-form">
<h1>Login</h1>
<div class="head">
<img src="/static/images/user.png" alt=""/>
</div>
<form method="post" action="login.php">
<input type="text" class="text" name="username" value="USERNAME" onfocus="this.value = '';"
onblur="if (this.value == '') {this.value = 'USERNAME';}" >
<input type="password" name="password" value="PASSWORD" onfocus="this.value = '';"
onblur="if (this.value == '') {this.value = 'Password';}">
<div class="submit">
<input type="submit" value="LOGIN" >
</div>
<p><a href="register.php">go to register</a></p>
</form>
</div>
</div>
</body>
</html>
```



那么我们就用**burpsuite**截包并且修改**Password**为空，发现返回**token**，并且**location**定义到了**index.php**界面，之后的响应返回答案界面。



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
1	http://114.116.26.217	GET	/login.php			200	1324	HTML	php
3	http://fonts.googleapis.com	GET	/css?family=Open+Sans:600italic,40...	✓					
5	http://114.116.26.217	POST	/login.php	✓	✓	302	329	HTML	php
6	http://114.116.26.217	GET	/index.php			200	684	HTML	php

Original request | Edited request | Response

Raw | Headers | Hex

```
HTTP/1.1 302 Found
Date: Sun, 29 Apr 2018 10:36:53 GMT
Server: Apache/2.4.18 (Ubuntu)
Set-Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJzaGEyNTYiLCJraWQiOiIzMSJ9.eyJuYW1lIjoiYWRtaW4ifQ.Jri5vsFutJW7XDdG8g0PBBGAaDPZcgbn6uJp5r5sWzQ
Location: index.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

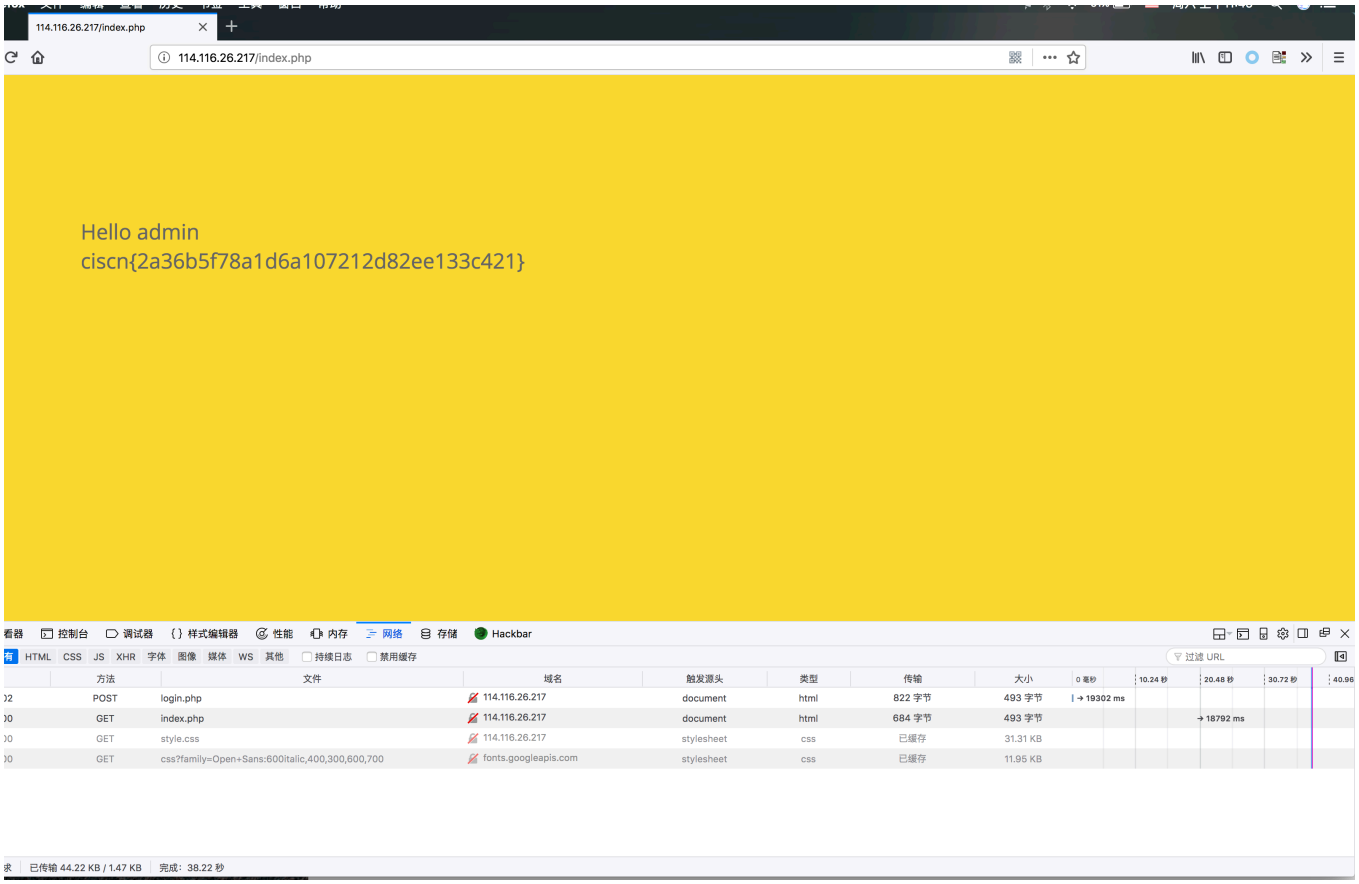
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
1	http://114.116.26.217	GET	/login.php			200	1324	HTML	php
3	http://fonts.googleapis.com	GET	/css?family=Open+Sans:600italic,40...	✓					
5	http://114.116.26.217	POST	/login.php	✓	✓	302	329	HTML	php
6	http://114.116.26.217	GET	/index.php			200	684	HTML	php

Request | Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Date: Sun, 29 Apr 2018 10:37:01 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 493
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
    <title></title>
    <meta charset="utf-8">
    <link href="/static/css/style.css" rel='stylesheet' type='text/css' />
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link href='http://fonts.googleapis.com/css?family=Open+Sans:600italic,400,300,600,700' rel='stylesheet' type='text/css'>
    <!--//webfonts-->
</head>    <body>
        <div class="container">
<p>Hello admin<br/>ciscn{2a36b5f78a1d6a107212d82ee133c421}
```



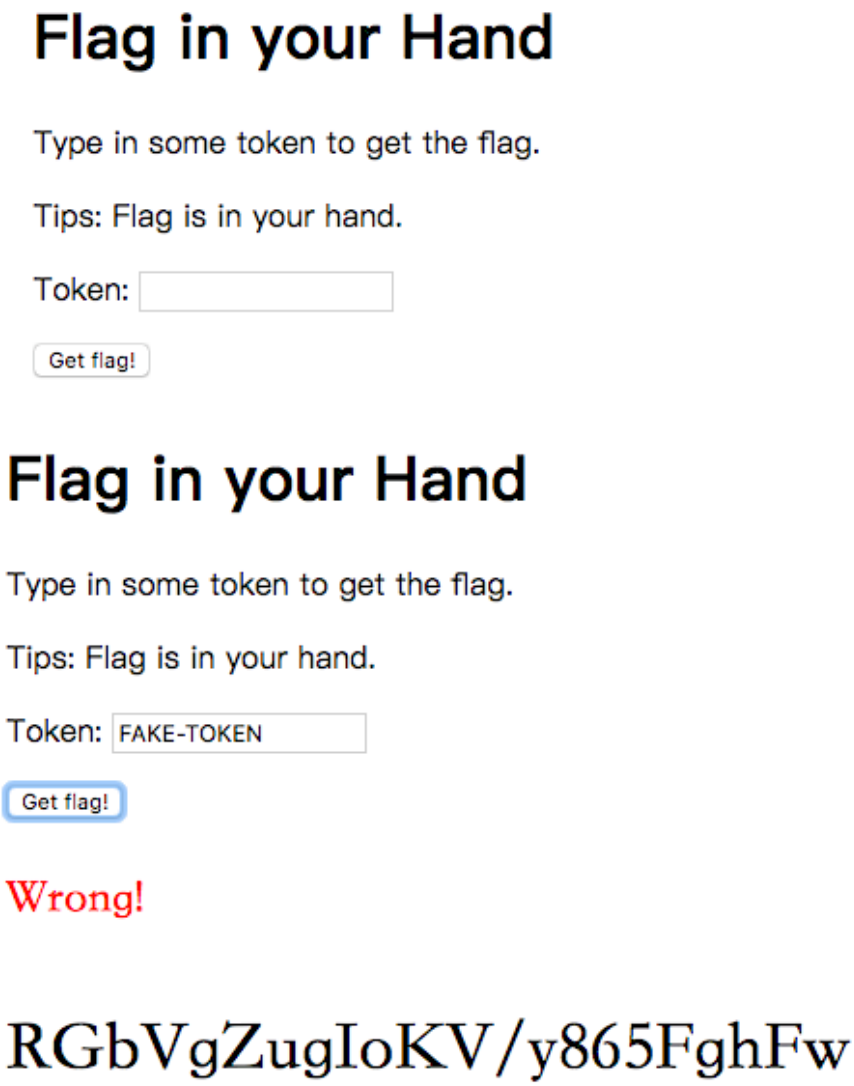
finish.

CRYPTO:

flag_in_your_hand:

这道密码题更加像web题讲道理...

解压出来一个html文件一个javascript文件：



html文件如下：

```
<html>
    <head>
        <title>Flag in your Hand</title>
        <style type="text/css">
            body {
                padding-left: 30%;
            }

            #flag {
                font-family: Garamond, serif;
```

```
            font-size: 36px;
        }

        #flagtitle {
            font-family: Garamond, serif;
            font-size: 24px;
        }

        .rightflag {
            color: green;
        }

        .wrongflag {
            color: red;
        }
    </style>
    <script src="script-min.js"></script>
    <script type="text/javascript">
        var ic = false;
        var fg = "";

        function getFlag() {
            var token = document.getElementById("secToken").value;
            ic = checkToken(token);
            fg = bm(token);
            showFlag()
        }

        function showFlag() {
            var t = document.getElementById("flagTitle");
            var f = document.getElementById("flag");
            t.innerText = !!ic ? "You got the flag below!!" : "Wrong!";
            t.className = !!ic ? "rightflag" : "wrongflag";
            f.innerText = fg;
        }
    </script>
</head>
<body>
    <h1>Flag in your Hand</h1>
    <p>Type in some token to get the flag.</p>
    <p>Tips: Flag is in your hand.</p>
    <div>
        <p>
            <span>Token:</span>
            <span><input type="text" id="secToken"/></span>
        </p>
        <p>
            <input type="button" value="Get flag!" onclick="getFlag()" />
        </p>
    </div>
    <div>
        <p id="flagTitle"></p>
        <p id="flag"></p>
    </div>
</body>
</html>
```

js文件如下：

```
function hm(s) {
    return rh(rstr(str2rstr_utf8(s)));
}
function bm(s) {
    return rb(rstr(str2rstr_utf8(s)));
}
function rstr(s) {
    return binl2rstr(binl(rstr2binl(s), s.length * 8));
}
function checkToken(s) {
    return s === "FAKE-TOKEN";
}
function rh(ip) {
    try {
        hc
    } catch (e) {
        hc = 0;
    }
    var ht = hc ? "0123456789ABCDEF" : "0123456789abcdef";
    var op = "";
    var x;
    for (var i = 0; i < ip.length; i++) {
        x = ip.charCodeAt(i);
        op += ht.charAt((x >>> 4) & 0x0F) + ht.charAt(x & 0x0F);
    }
    return op;
}
function rb(ip) {
    try {
        bp
    } catch (e) {
        bp = '';
    }
    var b = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";
```

```
    var op = "";
    var len = ip.length;
    for (var i = 0; i < len; i += 3) {
        var t = (ip.charCodeAt(i) << 16) | (i + 1 < len ? ip.charCodeAt(i + 1) << 8 : 0) | (i + 2 < len ? ip.charCodeAt(i + 2) : 0);
        for (var j = 0; j < 4; j++) {
            if (i * 8 + j * 6 > ip.length * 8)
                op += bp;
            else
                op += b.charAt((t >>> 6 * (3 - j)) & 0x3F);
        }
    }
    return op;
}
function ck(s) {
    try {
        ic
    } catch (e) {
        return;
    }
    var a = [118, 104, 102, 120, 117, 108, 119, 124, 48, 100, 101, 102];
    if (s.length == a.length) {
        for (i = 0; i < s.length; i++) {
            if (a[i] - s.charCodeAt(i) != 3)
                return ic = false;
        }
        return ic = true;
    }
    return ic = false;
}
function str2rstr_utf8(input) {
    var output = "";
    var i = -1;
    var x, y;
    while (++i < input.length) {
        x = input.charCodeAt(i);
        y = i + 1 < input.length ? input.charCodeAt(i + 1) : 0;
        if (0xD800 <= x && x <= 0xDBFF && 0xDC00 <= y && y <= 0xDFFF) {
            x = 0x10000 + ((x & 0x03FF) << 10) + (y & 0x03FF);
            i++;
        }
        if (x <= 0x7F)
            output += String.fromCharCode(x);
        else if (x <= 0x7FF)
            output += String.fromCharCode(0xC0 | ((x >>> 6) & 0x1F), 0x80 | (x & 0x3F));
        else if (x <= 0xFFFF)
            output += String.fromCharCode(0xE0 | ((x >>> 12) & 0x0F), 0x80 | ((x >>> 6) & 0x3F), 0x80 | (x & 0x3F));
        else if (x <= 0x1FFFFF)
            output += String.fromCharCode(0xF0 | ((x >>> 18) & 0x07), 0x80 | ((x >>> 12) & 0x3F), 0x80 | ((x >>> 6) & 0x3F), 0x80 | (x & 0x3F));
    }
    return output;
}
function rstr2binl(input) {
    var output = Array(input.length >> 2);
```

```
    for (var i = 0; i < output.length; i++)
        output[i] = 0;
    for (var i = 0; i < input.length * 8; i += 8)
        output[i >> 5] |= (input.charCodeAt(i / 8) & 0xFF) << (i % 32);
    return output;
}
function binl2rstr(i) {
    var o = "";
    for (var j = 0; j < i.length * 32; j += 8)
        o += String.fromCharCode((i[j >> 5] >>> (j % 32)) & 0xFF);
    return o;
}
function binl(x, len) {
    s = binl2rstr(x);
    x[len >> 5] |= 0x80 << ((len) % 32);
    x[((((len + 64) >>> 9) << 4) + 14] = len;
    var a = 1732584193;
    var b = -271733879;
    var c = -1732584194;
    var d = 271733878;
    for (var i = 0; i < x.length; i += 16) {
        var olda = a;
        var oldb = b;
        var oldc = c;
        var oldd = d;
        a = ff(a, b, c, d, x[i + 0], 7, -680876936);
        d = ff(d, a, b, c, x[i + 1], 12, -389564586);
        c = ff(c, d, a, b, x[i + 2], 17, 606105819);
        b = ff(b, c, d, a, x[i + 3], 22, -1044525330);
        a = ff(a, b, c, d, x[i + 4], 7, -176418897);
        d = ff(d, a, b, c, x[i + 5], 12, 1200080426);
        c = ff(c, d, a, b, x[i + 6], 17, -1473231341);
        b = ff(b, c, d, a, x[i + 7], 22, -45705983);
        a = ff(a, b, c, d, x[i + 8], 7, 1770035416);
        d = ff(d, a, b, c, x[i + 9], 12, -1958414417);
        c = ff(c, d, a, b, x[i + 10], 17, -42063);
        b = ff(b, c, d, a, x[i + 11], 22, -1990404162);
        a = ff(a, b, c, d, x[i + 12], 7, 1804603682);
        d = ff(d, a, b, c, x[i + 13], 12, -40341101);
        c = ff(c, d, a, b, x[i + 14], 17, -1502002290);
        b = ff(b, c, d, a, x[i + 15], 22, 1236535329);
        ck(s);
        a = gg(a, b, c, d, x[i + 1], 5, -165796510);
        d = gg(d, a, b, c, x[i + 6], 9, -1069501632);
        c = gg(c, d, a, b, x[i + 11], 14, 643717713);
        b = gg(b, c, d, a, x[i + 0], 20, -373897302);
        a = gg(a, b, c, d, x[i + 5], 5, -701558691);
        d = gg(d, a, b, c, x[i + 10], 9, 38016083);
        c = gg(c, d, a, b, x[i + 15], 14, -660478335);
        b = gg(b, c, d, a, x[i + 4], 20, -405537848);
        a = gg(a, b, c, d, x[i + 9], 5, 568446438);
        d = gg(d, a, b, c, x[i + 14], 9, -1019803690);
        c = gg(c, d, a, b, x[i + 3], 14, -187363961);
        b = gg(b, c, d, a, x[i + 8], 20, 1163531501);
        a = gg(a, b, c, d, x[i + 13], 5, -1444681467);
        d = gg(d, a, b, c, x[i + 2], 9, -51403784);
```

```
        c = gg(c, d, a, b, x[i + 7], 14, 1735328473);
        b = gg(b, c, d, a, x[i + 12], 20, -1926607734);
        a = hh(a, b, c, d, x[i + 5], 4, -378558);
        d = hh(d, a, b, c, x[i + 8], 11, -2022574463);
        c = hh(c, d, a, b, x[i + 11], 16, 1839030562);
        b = hh(b, c, d, a, x[i + 14], 23, -35309556);
        a = hh(a, b, c, d, x[i + 1], 4, -1530992060);
        d = hh(d, a, b, c, x[i + 4], 11, 1272893353);
        c = hh(c, d, a, b, x[i + 7], 16, -155497632);
        b = hh(b, c, d, a, x[i + 10], 23, -1094730640);
        a = hh(a, b, c, d, x[i + 13], 4, 681279174);
        d = hh(d, a, b, c, x[i + 0], 11, -358537222);
        c = hh(c, d, a, b, x[i + 3], 16, -722521979);
        b = hh(b, c, d, a, x[i + 6], 23, 76029189);
        a = hh(a, b, c, d, x[i + 9], 4, -640364487);
        d = hh(d, a, b, c, x[i + 12], 11, -421815835);
        c = hh(c, d, a, b, x[i + 15], 16, 530742520);
        b = hh(b, c, d, a, x[i + 2], 23, -995338651);
        a = ii(a, b, c, d, x[i + 0], 6, -198630844);
        d = ii(d, a, b, c, x[i + 7], 10, 1126891415);
        c = ii(c, d, a, b, x[i + 14], 15, -1416354905);
        b = ii(b, c, d, a, x[i + 5], 21, -57434055);
        a = ii(a, b, c, d, x[i + 12], 6, 1700485571);
        d = ii(d, a, b, c, x[i + 3], 10, -1894986606);
        c = ii(c, d, a, b, x[i + 10], 15, -1051523);
        b = ii(b, c, d, a, x[i + 1], 21, -2054922799);
        a = ii(a, b, c, d, x[i + 8], 6, 1873313359);
        d = ii(d, a, b, c, x[i + 15], 10, -30611744);
        c = ii(c, d, a, b, x[i + 6], 15, -1560198380);
        b = ii(b, c, d, a, x[i + 13], 21, 1309151649);
        a = ii(a, b, c, d, x[i + 4], 6, -145523070);
        d = ii(d, a, b, c, x[i + 11], 10, -1120210379);
        c = ii(c, d, a, b, x[i + 2], 15, 718787259);
        b = ii(b, c, d, a, x[i + 9], 21, -343485551);
        a = sa(a, olda);
        b = sa(b, oldb);
        c = sa(c, oldc);
        d = sa(d, oldd);
    }
    return Array(a, b, c, d);
}
function cmn(q, a, b, x, s, t) {
    return sa(br(sa(sa(a, q), sa(x, t)), s), b);
}
function ff(a, b, c, d, x, s, t) {
    return cmn((b & c) | ((~b) & d), a, b, x, s, t);
}
function gg(a, b, c, d, x, s, t) {
    return cmn((b & d) | (c & (~d)), a, b, x, s, t);
}
function hh(a, b, c, d, x, s, t) {
    return cmn(b ^ c ^ d, a, b, x, s, t);
}
function ii(a, b, c, d, x, s, t) {
    return cmn(c ^ (b | (~d)), a, b, x, s, t);
}
```

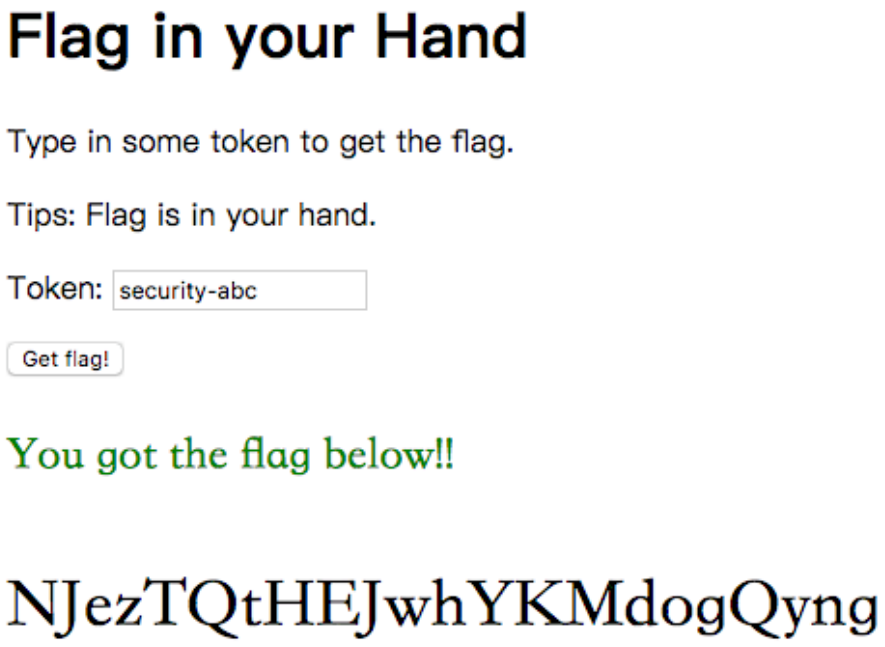
```
function sa(x, y) {
    var lsw = (x & 0xFFFF) + (y & 0xFFFF);
    var msw = (x >> 16) + (y >> 16) + (lsw >> 16);
    return (msw << 16) | (lsw & 0xFFFF);
}
function br(n, c) {
    return (n << c) | (n >>> (32 - c));
}
```

整个文件的运行过程从getFlag函数开始，整个文档的核心是找到ic控制的函数，这是出题者善意的标示，让我得知输入什么数才能获得flag。

浏览js文件我们发现了ic的控制模块。

```
}
function ck(s) {
    try {
        ic
    } catch (e) {
        return;
    }
    var a = [118, 104, 102, 120, 117, 108, 119, 124, 48, 100, 101, 102];
    if (s.length == a.length) {
        for (i = 0; i < s.length; i++) {
            if (a[i] - s.charCodeAt(i) != 3)
                return ic = false;
        }
        return ic = true;
    }
    return ic = false;
}
```

s是输入的token，可见之要s的每个字符的unicode是比a数组小3即正确，通过在线编码解码网址：https://www.sojson.com/unicode.html，得到flag。



finish.