

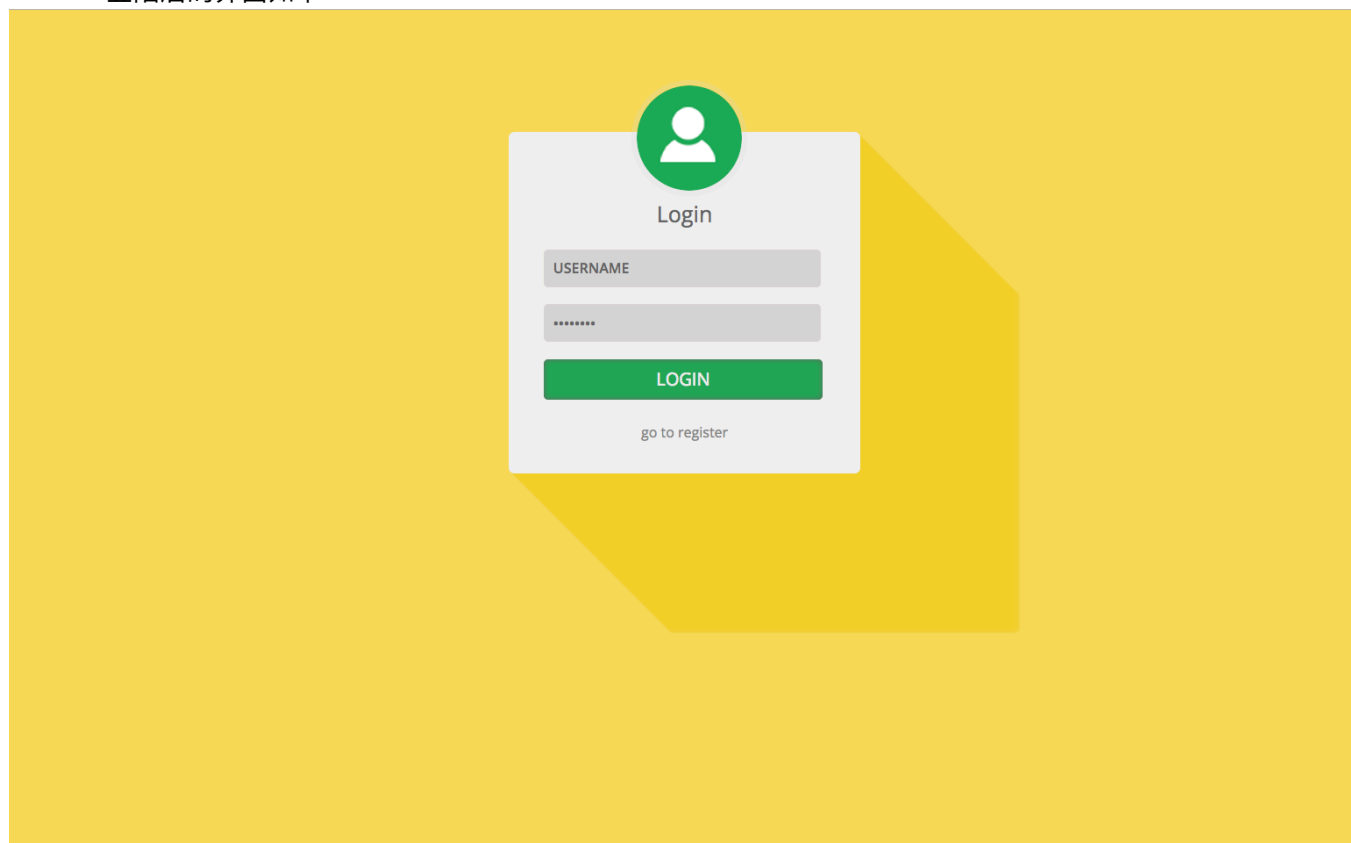
全国大学生信息安全竞赛WP-2018

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。

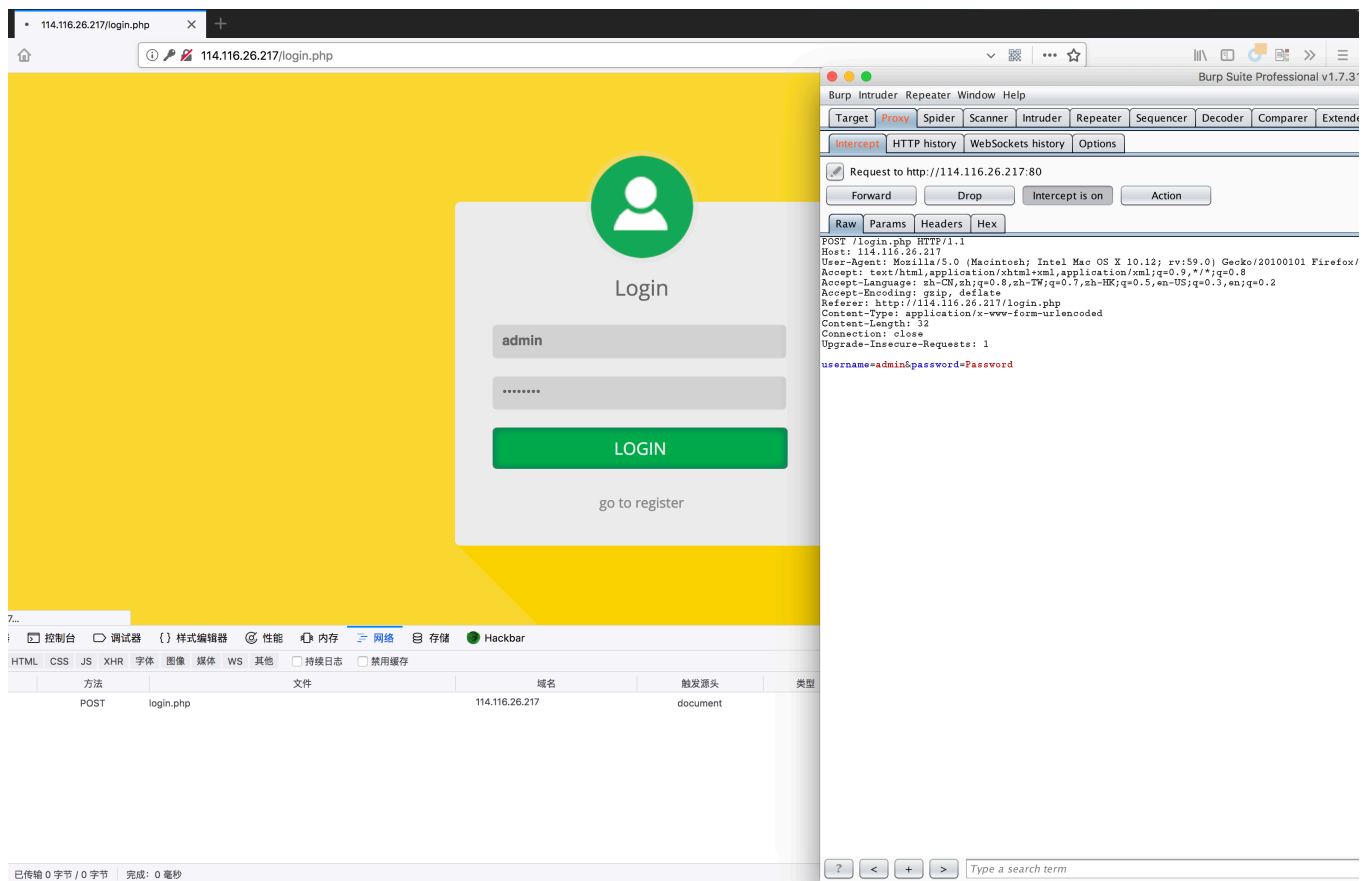
查看源代码发现，登陆界面输入空值时，空值会被填充，说明可能将密码置空值传送到服务端时，服务端会自动帮我们填充正确密码，话不多说开始实战。以下是观测环节：

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

```

13 <div class="main">
14 <div class="login-form">
15 <h1>Login</h1>
16 <div class="head">
17 
18 </div>
19 <form method="post" action="login.php">
20 <input type="text" class="text" name="username" value="USERNAME" onfocus="this.value = '';"
  onblur="if (this.value == '') {this.value = 'USERNAME'};" >
21 <input type="password" name="password" value="PASSWORD" onfocus="this.value = '';"
  onblur="if (this.value == '') {this.value = 'Password'};">
22 <div class="submit">
23 <input type="submit" value="LOGIN" >
24 </div>
25 <p><a href="register.php">go to register</a></p>
26 </form>
27 </div>
28 </div>
29 </body>
30 </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。

116.26.217/login.php

114.116.26.217/login.php

Login

admin

LOGIN

go to register

116.26.217/login.php

114.116.26.217/login.php

POST /login.php HTTP/1.1
Host: 114.116.26.217
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://114.116.26.217/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Connection: close
Upgrade-Insecure-Requests: 1
username=admin&password=

网络

POST login.php 114.116.26.217

#	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=eyJ0eXAiOiJKV1QiLCJhbGciOiJIJzA5NTYiLCJraWQiOiIzMSJ9.eyJ1Y291bnRtaW4ifQ.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

RequestResponse

RawHeadersHexHTMLRender

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
ciscn{2a36b5f78a1d6a107212d82ee133c421}

114.116.26.217/index.php

114.116.26.217/index.php

Hello admin
ciscn{2a36b5f78a1d6a107212d82ee133c421}

看器控制台调试器样式编辑器性能内存网络存储Hackbar

HTMLCSSJSXHR字体图像媒体WS其他

文件

域名

触发源

类型

传输

大小

0毫秒

10.24秒

20.48秒

30.72秒

40.96

12

POST

login.php

114.116.26.217

document

html

822 字节

493 字节

19302 ms

10

GET

index.php

114.116.26.217

document

html

684 字节

493 字节

18792 ms

10

GET

style.css

114.116.26.217

stylesheet

css

已缓存

31.31 KB

10

GET

css?family=Open+Sans:600italic,400,300,600,700

fonts.googleapis.com

stylesheet

css

已缓存

11.95 KB

已传输 44.22 KB / 1.47 KB 完成: 38.22 秒

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:

Flag in your Hand

Type in some token to get the flag.

Tips: Flag is in your hand.

Token:

Get flag!

Flag in your Hand

Type in some token to get the flag.

Tips: Flag is in your hand.

Token:

Get flag!

Wrong!

RGbVgZugIoKV/y865FghFw

```
1 html文件如下:
2 <html>
3   <head>
4     <title>Flag in your Hand</title>
5     <style type="text/css">
6       body {
7         padding-left: 30%;
8       }
9
10    #flag {
11      font-family: Garamond, serif;
```

```
12         font-size: 36px;
13     }
14
15     #flagtitle {
16         font-family: Garamond, serif;
17         font-size: 24px;
18     }
19
20     .rightflag {
21         color: green;
22     }
23
24     .wrongflag {
25         color: red;
26     }
27 </style>
28 <script src="script-min.js"></script>
29 <script type="text/javascript">
30     var ic = false;
31     var fg = "";
32
33     function getFlag() {
34         var token = document.getElementById("secToken").value;
35         ic = checkToken(token);
36         fg = bm(token);
37         showFlag()
38     }
39
40     function showFlag() {
41         var t = document.getElementById("flagTitle");
42         var f = document.getElementById("flag");
43         t.innerText = !!ic ? "You got the flag below!!" : "Wrong!";
44         t.className = !!ic ? "rightflag" : "wrongflag";
45         f.innerText = fg;
46     }
47 </script>
48 </head>
49 <body>
50     <h1>Flag in your Hand</h1>
51     <p>Type in some token to get the flag.</p>
52     <p>Tips: Flag is in your hand.</p>
53     <div>
54         <p>
55             <span>Token:</span>
56             <span><input type="text" id="secToken"/></span>
57         </p>
58         <p>
59             <input type="button" value="Get flag!" onclick="getFlag()" />
60         </p>
61     </div>
62     <div>
63         <p id="flagTitle"></p>
64         <p id="flag"></p>
65     </div>
66 </body>
67 </html>
```

68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88

```
1 js文件如下:
2 function hm(s) {
3     return rh(rstr(str2rstr_utf8(s)));
4 }
5 function bm(s) {
6     return rb(rstr(str2rstr_utf8(s)));
7 }
8 function rstr(s) {
9     return binl2rstr(binl(rstr2binl(s), s.length * 8));
10 }
11 function checkToken(s) {
12     return s === "FAKE-TOKEN";
13 }
14 function rh(ip) {
15     try {
16         hc
17     } catch (e) {
18         hc = 0;
19     }
20     var ht = hc ? "0123456789ABCDEF" : "0123456789abcdef";
21     var op = "";
22     var x;
23     for (var i = 0; i < ip.length; i++) {
24         x = ip.charCodeAt(i);
25         op += ht.charAt((x >>> 4) & 0x0F) + ht.charAt(x & 0x0F);
26     }
27     return op;
28 }
29 function rb(ip) {
30     try {
31         bp
32     } catch (e) {
33         bp = '';
34     }
35     var b = "ABCDEFGHijklmnopqrstuvwxyz0123456789+/-";
```

```

36     var op = "";
37     var len = ip.length;
38     for (var i = 0; i < len; i += 3) {
39         var t = (ip.charCodeAt(i) << 16) | (i + 1 < len ? ip.charCodeAt(i + 1) << 8 : 0) |
40         (i + 2 < len ? ip.charCodeAt(i + 2) : 0);
41         for (var j = 0; j < 4; j++) {
42             if (i * 8 + j * 6 > ip.length * 8)
43                 op += bp;
44             else
45                 op += b.charAt((t >>> 6 * (3 - j)) & 0x3F);
46         }
47     }
48     return op;
49 }
50 function ck(s) {
51     try {
52         ic
53     } catch (e) {
54         return;
55     }
56     var a = [118, 104, 102, 120, 117, 108, 119, 124, 48, 100, 101, 102];
57     if (s.length == a.length) {
58         for (i = 0; i < s.length; i++) {
59             if (a[i] - s.charCodeAt(i) != 3)
60                 return ic = false;
61         }
62         return ic = true;
63     }
64     return ic = false;
65 }
66 function str2rstr_utf8(input) {
67     var output = "";
68     var i = -1;
69     var x, y;
70     while (++i < input.length) {
71         x = input.charCodeAt(i);
72         y = i + 1 < input.length ? input.charCodeAt(i + 1) : 0;
73         if (0xD800 <= x && x <= 0xDBFF && 0xDC00 <= y && y <= 0xDFFF) {
74             x = 0x10000 + ((x & 0x03FF) << 10) + (y & 0x03FF);
75             i++;
76         }
77         if (x <= 0x7F)
78             output += String.fromCharCode(x);
79         else if (x <= 0x7FF)
80             output += String.fromCharCode(0xC0 | ((x >>> 6) & 0x1F), 0x80 | (x & 0x3F));
81         else if (x <= 0xFFFF)
82             output += String.fromCharCode(0xE0 | ((x >>> 12) & 0x0F), 0x80 | ((x >>> 6) &
83             0x3F), 0x80 | (x & 0x3F));
84         else if (x <= 0x1FFFFF)
85             output += String.fromCharCode(0xF0 | ((x >>> 18) & 0x07), 0x80 | ((x >>> 12) &
86             0x3F), 0x80 | ((x >>> 6) & 0x3F), 0x80 | (x & 0x3F));
87     }
88     return output;
89 }
90 function rstr2binl(input) {
91     var output = Array(input.length >> 2);

```



```

89     for (var i = 0; i < output.length; i++)
90         output[i] = 0;
91     for (var i = 0; i < input.length * 8; i += 8)
92         output[i >> 5] |= (input.charCodeAt(i / 8) & 0xFF) << (i % 32);
93     return output;
94 }
95 function binl2rstr(i) {
96     var o = "";
97     for (var j = 0; j < i.length * 32; j += 8)
98         o += String.fromCharCode((i[j >> 5] >>> (j % 32)) & 0xFF);
99     return o;
100 }
101 function binl(x, len) {
102     s = binl2rstr(x);
103     x[len >> 5] |= 0x80 << ((len) % 32);
104     x[((len + 64) >>> 9) << 4] = len;
105     var a = 1732584193;
106     var b = -271733879;
107     var c = -1732584194;
108     var d = 271733878;
109     for (var i = 0; i < x.length; i += 16) {
110         var olda = a;
111         var oldb = b;
112         var oldc = c;
113         var oldd = d;
114         a = ff(a, b, c, d, x[i + 0], 7, -680876936);
115         d = ff(d, a, b, c, x[i + 1], 12, -389564586);
116         c = ff(c, d, a, b, x[i + 2], 17, 606105819);
117         b = ff(b, c, d, a, x[i + 3], 22, -1044525330);
118         a = ff(a, b, c, d, x[i + 4], 7, -176418897);
119         d = ff(d, a, b, c, x[i + 5], 12, 1200080426);
120         c = ff(c, d, a, b, x[i + 6], 17, -1473231341);
121         b = ff(b, c, d, a, x[i + 7], 22, -45705983);
122         a = ff(a, b, c, d, x[i + 8], 7, 1770035416);
123         d = ff(d, a, b, c, x[i + 9], 12, -1958414417);
124         c = ff(c, d, a, b, x[i + 10], 17, -42063);
125         b = ff(b, c, d, a, x[i + 11], 22, -1990404162);
126         a = ff(a, b, c, d, x[i + 12], 7, 1804603682);
127         d = ff(d, a, b, c, x[i + 13], 12, -40341101);
128         c = ff(c, d, a, b, x[i + 14], 17, -1502002290);
129         b = ff(b, c, d, a, x[i + 15], 22, 1236535329);
130         ck(s);
131         a = gg(a, b, c, d, x[i + 1], 5, -165796510);
132         d = gg(d, a, b, c, x[i + 6], 9, -1069501632);
133         c = gg(c, d, a, b, x[i + 11], 14, 643717713);
134         b = gg(b, c, d, a, x[i + 0], 20, -373897302);
135         a = gg(a, b, c, d, x[i + 5], 5, -701558691);
136         d = gg(d, a, b, c, x[i + 10], 9, 38016083);
137         c = gg(c, d, a, b, x[i + 15], 14, -660478335);
138         b = gg(b, c, d, a, x[i + 4], 20, -405537848);
139         a = gg(a, b, c, d, x[i + 9], 5, 568446438);
140         d = gg(d, a, b, c, x[i + 14], 9, -1019803690);
141         c = gg(c, d, a, b, x[i + 3], 14, -187363961);
142         b = gg(b, c, d, a, x[i + 8], 20, 1163531501);
143         a = gg(a, b, c, d, x[i + 13], 5, -1444681467);
144         d = gg(d, a, b, c, x[i + 2], 9, -51403784);

```

```

145     c = gg(c, d, a, b, x[i + 7], 14, 1735328473);
146     b = gg(b, c, d, a, x[i + 12], 20, -1926607734);
147     a = hh(a, b, c, d, x[i + 5], 4, -378558);
148     d = hh(d, a, b, c, x[i + 8], 11, -2022574463);
149     c = hh(c, d, a, b, x[i + 11], 16, 1839030562);
150     b = hh(b, c, d, a, x[i + 14], 23, -35309556);
151     a = hh(a, b, c, d, x[i + 1], 4, -1530992060);
152     d = hh(d, a, b, c, x[i + 4], 11, 1272893353);
153     c = hh(c, d, a, b, x[i + 7], 16, -155497632);
154     b = hh(b, c, d, a, x[i + 10], 23, -1094730640);
155     a = hh(a, b, c, d, x[i + 13], 4, 681279174);
156     d = hh(d, a, b, c, x[i + 0], 11, -358537222);
157     c = hh(c, d, a, b, x[i + 3], 16, -722521979);
158     b = hh(b, c, d, a, x[i + 6], 23, 76029189);
159     a = hh(a, b, c, d, x[i + 9], 4, -640364487);
160     d = hh(d, a, b, c, x[i + 12], 11, -421815835);
161     c = hh(c, d, a, b, x[i + 15], 16, 530742520);
162     b = hh(b, c, d, a, x[i + 2], 23, -995338651);
163     a = ii(a, b, c, d, x[i + 0], 6, -198630844);
164     d = ii(d, a, b, c, x[i + 7], 10, 1126891415);
165     c = ii(c, d, a, b, x[i + 14], 15, -1416354905);
166     b = ii(b, c, d, a, x[i + 5], 21, -57434055);
167     a = ii(a, b, c, d, x[i + 12], 6, 1700485571);
168     d = ii(d, a, b, c, x[i + 3], 10, -1894986606);
169     c = ii(c, d, a, b, x[i + 10], 15, -1051523);
170     b = ii(b, c, d, a, x[i + 1], 21, -2054922799);
171     a = ii(a, b, c, d, x[i + 8], 6, 1873313359);
172     d = ii(d, a, b, c, x[i + 15], 10, -30611744);
173     c = ii(c, d, a, b, x[i + 6], 15, -1560198380);
174     b = ii(b, c, d, a, x[i + 13], 21, 1309151649);
175     a = ii(a, b, c, d, x[i + 4], 6, -145523070);
176     d = ii(d, a, b, c, x[i + 11], 10, -1120210379);
177     c = ii(c, d, a, b, x[i + 2], 15, 718787259);
178     b = ii(b, c, d, a, x[i + 9], 21, -343485551);
179     a = sa(a, olda);
180     b = sa(b, oldb);
181     c = sa(c, oldc);
182     d = sa(d, oldd);
183 }
184 return Array(a, b, c, d);
185 }
186 function cmn(q, a, b, x, s, t) {
187     return sa(br(sa(sa(a, q), sa(x, t)), s), b);
188 }
189 function ff(a, b, c, d, x, s, t) {
190     return cmn((b & c) | ((~b) & d), a, b, x, s, t);
191 }
192 function gg(a, b, c, d, x, s, t) {
193     return cmn((b & d) | (c & (~d)), a, b, x, s, t);
194 }
195 function hh(a, b, c, d, x, s, t) {
196     return cmn(b ^ c ^ d, a, b, x, s, t);
197 }
198 function ii(a, b, c, d, x, s, t) {
199     return cmn(c ^ (b | (~d)), a, b, x, s, t);
200 }

```

```

201 function sa(x, y) {
202     var lsw = (x & 0xFFFF) + (y & 0xFFFF);
203     var msw = (x >> 16) + (y >> 16) + (lsw >> 16);
204     return (msw << 16) | (lsw & 0xFFFF);
205 }
206 function br(n, c) {
207     return (n << c) | (n >>> (32 - c));
208 }

```

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。

Flag in your Hand

Type in some token to get the flag.

Tips: Flag is in your hand.

Token:

You got the flag below!!

NJezTQtHEJwhYKMdogQyng

finish.