

Web - ScriptingLanguage - 50 points

Kévin DUVERGER

Table des matières

1 Résolution ScriptingLanguage :

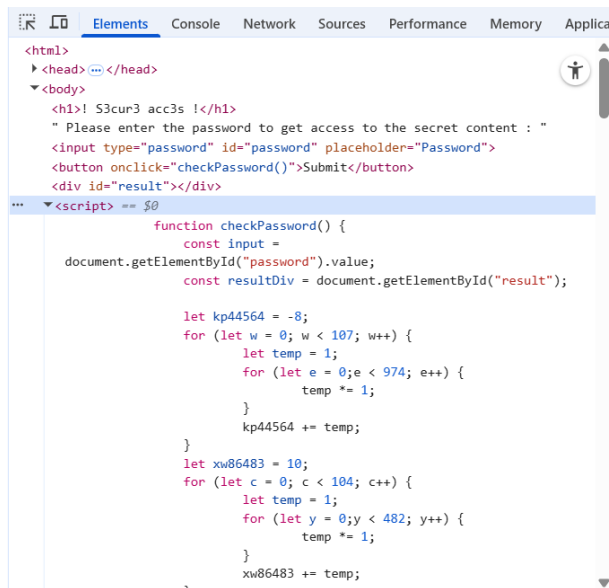
2

1 Résolution ScriptingLanguage :

Voici une nouvelle fois la page qui nous est proposé pour ce challenge (sur <http://146.59.227.136:23416>) :

! S3cur3 acc3s !

Please enter the password to get access to the secret content :



Cette fois-ci on le flag ne semble pas être directement dans la page, mais la fonction `checkPassword` du javascript semble être d'un grand intérêt (il n'y a pas de requête vers une plateforme d'authentification dedans, donc il très probable que le code n'ait subi qu'une obfuscation mineure, ce que l'on va tester).

Voici donc le code de cette fonction :

```

1 function checkPassword() {
2   const input = document.getElementById("password").value;
3   const resultDiv = document.getElementById("result");
4
5   let kp44564 = -8;
6   for (let w = 0; w < 107; w++) {
7     let temp = 1;
8     for (let e = 0; e < 974; e++) {
9       temp *= 1;
10    }
11    kp44564 += temp;
12  }
13  let xw86483 = 10;
14  for (let c = 0; c < 104; c++) {
15    let temp = 1;
16    for (let y = 0; y < 482; y++) {
17      temp *= 1;
18    }
19    xw86483 += temp;
20  }
21  let ngzov41442 = 5;
22  for (let d = 0; d < 116; d++) {
23    let temp = 1;
24    for (let x = 0; x < 687; x++) {
25      temp *= 1;
26    }
27    ngzov41442 += temp;
28  }
29  let ig78961 = 6;
30  for (let i = 0; i < 106; i++) {
31    let temp = 1;
32    for (let s = 0; s < 693; s++) {
33      temp *= 1;
34    }
35    ig78961 += temp;
36  }
37  let rn54489 = 5;
38  for (let p = 0; p < 111; p++) {
39    let temp = 1;
40    for (let l = 0; l < 295; l++) {
41      temp *= 1;
42    }
43    rn54489 += temp;
44  }

```

```
45 let bniy31863 = -4;
46 for (let c = 0; c < 109; c++) {
47   let temp = 1;
48   for (let y = 0; y < 46; y++) {
49     temp *= 1;
50   }
51   bniy31863 += temp;
52 }
53 let cw79849 = 8;
54 for (let e = 0; e < 107; e++) {
55   let temp = 1;
56   for (let w = 0; w < 30; w++) {
57     temp *= 1;
58   }
59   cw79849 += temp;
60 }
61 let ppifg53691 = -5;
62 for (let u = 0; u < 72; u++) {
63   let temp = 1;
64   for (let g = 0; g < 432; g++) {
65     temp *= 1;
66   }
67   ppifg53691 += temp;
68 }
69 let bsgv52010 = 8;
70 for (let e = 0; e < 76; e++) {
71   let temp = 1;
72   for (let w = 0; w < 106; w++) {
73     temp *= 1;
74   }
75   bsgv52010 += temp;
76 }
77 let kqhd15996 = -2;
78 for (let r = 0; r < 72; r++) {
79   let temp = 1;
80   for (let j = 0; j < 467; j++) {
81     temp *= 1;
82   }
83   kqhd15996 += temp;
84 }
85 let gtyt91013 = -10;
86 for (let r = 0; r < 133; r++) {
87   let temp = 1;
88   for (let j = 0; j < 780; j++) {
89     temp *= 1;
90   }
91   gtyt91013 += temp;
92 }
93 let itykw12500 = -2;
94 for (let n = 0; n < 121; n++) {
95   let temp = 1;
96   for (let n = 0; n < 605; n++) {
97     temp *= 1;
98   }
99   itykw12500 += temp;
100 }
101 let ks47777 = 5;
102 for (let t = 0; t < 46; t++) {
103   let temp = 1;
104   for (let h = 0; h < 483; h++) {
105     temp *= 1;
106   }
107   ks47777 += temp;
108 }
109 let skd50420 = -7;
110 for (let t = 0; t < 105; t++) {
111   let temp = 1;
112   for (let h = 0; h < 872; h++) {
113     temp *= 1;
114   }
115   skd50420 += temp;
116 }
117 let tsyal55384 = -8;
118 for (let z = 0; z < 103; z++) {
119   let temp = 1;
120   for (let b = 0; b < 196; b++) {
121     temp *= 1;
122   }
123   tsyal55384 += temp;
```

```
124 }
125 let eh43430 = 7;
126 for (let s = 0; s < 42; s++) {
127   let temp = 1;
128   for (let i = 0; i < 438; i++) {
129     temp *= 1;
130   }
131   eh43430 += temp;
132 }
133 let lt65904 = -1;
134 for (let q = 0; q < 116; q++) {
135   let temp = 1;
136   for (let k = 0; k < 197; k++) {
137     temp *= 1;
138   }
139   lt65904 += temp;
140 }
141 let kx99301 = 4;
142 for (let e = 0; e < 91; e++) {
143   let temp = 1;
144   for (let w = 0; w < 859; w++) {
145     temp *= 1;
146   }
147   kx99301 += temp;
148 }
149 let ifqqr94477 = 10;
150 for (let m = 0; m < 106; m++) {
151   let temp = 1;
152   for (let o = 0; o < 878; o++) {
153     temp *= 1;
154   }
155   ifqqr94477 += temp;
156 }
157 let ge39345 = 3;
158 for (let e = 0; e < 45; e++) {
159   let temp = 1;
160   for (let w = 0; w < 509; w++) {
161     temp *= 1;
162   }
163   ge39345 += temp;
164 }
165 let vox87732 = 8;
166 for (let x = 0; x < 40; x++) {
167   let temp = 1;
168   for (let d = 0; d < 548; d++) {
169     temp *= 1;
170   }
171   vox87732 += temp;
172 }
173 let rs60516 = 7;
174 for (let e = 0; e < 88; e++) {
175   let temp = 1;
176   for (let w = 0; w < 395; w++) {
177     temp *= 1;
178   }
179   rs60516 += temp;
180 }
181 let ty85695 = 6;
182 for (let p = 0; p < 45; p++) {
183   let temp = 1;
184   for (let l = 0; l < 210; l++) {
185     temp *= 1;
186   }
187   ty85695 += temp;
188 }
189 let nmk21077 = -10;
190 for (let r = 0; r < 107; r++) {
191   let temp = 1;
192   for (let j = 0; j < 223; j++) {
193     temp *= 1;
194   }
195   nmk21077 += temp;
196 }
197 let dpk83916 = -1;
198 for (let c = 0; c < 116; c++) {
199   let temp = 1;
200   for (let y = 0; y < 116; y++) {
201     temp *= 1;
202   }

```

```

203     dpk83916 += temp;
204 }
205 let ld49684 = -6;
206 for (let n = 0; n < 127; n++) {
207     let temp = 1;
208     for (let n = 0; n < 790; n++) {
209         temp *= 1;
210     }
211     ld49684 += temp;
212 }
213 let poo64369 = -1;
214 for (let d = 0; d < 126; d++) {
215     let temp = 1;
216     for (let x = 0; x < 171; x++) {
217         temp *= 1;
218     }
219     poo64369 += temp;
220 }
221
222 if (input.charCodeAt(0) == kp44564 && input.charCodeAt(1) == xw86483 && input.charCodeAt(2) ==
ngzov41442 && input.charCodeAt(3) == ig78961 && input.charCodeAt(4) == rn54489 && input.
charCodeAt(5) == bniy31863 && input.charCodeAt(6) == cw79849 && input.charCodeAt(7) ==
ppifg53691 && input.charCodeAt(8) == bsgv52010 && input.charCodeAt(9) == kqhd15996 && input.
charCodeAt(10) == gtyt91013 && input.charCodeAt(11) == itykw12500 && input.charCodeAt(12) ==
ks47777 && input.charCodeAt(13) == skd50420 && input.charCodeAt(14) == tsyal55384 && input.
charCodeAt(15) == eh43430 && input.charCodeAt(16) == lt65904 && input.charCodeAt(17) == kx99301
&& input.charCodeAt(18) == ifqqr94477 && input.charCodeAt(19) == ge39345 && input.charCodeAt(20)
== vox87732 && input.charCodeAt(21) == rs60516 && input.charCodeAt(22) == ty85695 && input.
charCodeAt(23) == nmk21077 && input.charCodeAt(24) == dpk83916 && input.charCodeAt(25) ==
ld49684 && input.charCodeAt(26) == poo64369) {
223     resultDiv.textContent = "Correct !";
224     resultDiv.style.color = "green";
225 } else {
226     resultDiv.textContent = "Incorrect !";
227     resultDiv.style.color = "red";
228 }
229 }

```

Comme vous pouvez le voir, la dernière partie du code teste si les différentes variables représentent bien les lettres du mot de passe (qui semble être de 27 caractères), ça nous permet de voir ce qui se passe mais ça ne nous donne pas le flag.

Pour avoir le flag, il faut probablement s'intéresser aux boucles pour récupérer les différents caractères. La première chose intéressante est la variable `temp` et comme vous pouvez le voir dans tous les cas elle vaut toujours 1 (car continuer à multiplier par 1 après ne sert à rien). On peut donc supprimer tout cela ce qui nous donne le code suivant :

```

1 function checkPassword() {
2     ...
3
4     let kp44564 = -8;
5     for (let w = 0; w < 107; w++) {
6         kp44564 += 1;
7     }
8     let xw86483 = 10;
9     for (let c = 0; c < 104; c++) {
10        xw86483 += 1;
11    }
12    let ngzov41442 = 5;
13    for (let d = 0; d < 116; d++) {
14        ngzov41442 += 1;
15    }
16    let ig78961 = 6;
17    for (let i = 0; i < 106; i++) {
18        ig78961 += 1;
19    }
20    let rn54489 = 5;
21    for (let p = 0; p < 111; p++) {
22        rn54489 += 1;
23    }
24    let bniy31863 = -4;
25    for (let c = 0; c < 109; c++) {
26        bniy31863 += 1;
27    }
28    let cw79849 = 8;
29    for (let e = 0; e < 107; e++) {
30        cw79849 += 1;
31    }
32    let ppifg53691 = -5;
33    for (let u = 0; u < 72; u++) {
34        ppifg53691 += 1;

```

```
35 }
36 let bsgv52010 = 8;
37 for (let e = 0; e < 76; e++) {
38   bsgv52010 += 1;
39 }
40 let kqhd15996 = -2;
41 for (let r = 0; r < 72; r++) {
42   kqhd15996 += 1;
43 }
44 let gtyt91013 = -10;
45 for (let r = 0; r < 133; r++) {
46   gtyt91013 += 1;
47 }
48 let itykw12500 = -2;
49 for (let n = 0; n < 121; n++) {
50   itykw12500 += 1;
51 }
52 let ks47777 = 5;
53 for (let t = 0; t < 46; t++) {
54   ks47777 += 1;
55 }
56 let skd50420 = -7;
57 for (let t = 0; t < 105; t++) {
58   skd50420 += 1;
59 }
60 let tsyal55384 = -8;
61 for (let z = 0; z < 103; z++) {
62   tsyal55384 += 1;
63 }
64 let eh43430 = 7;
65 for (let s = 0; s < 42; s++) {
66   eh43430 += 1;
67 }
68 let lt65904 = -1;
69 for (let q = 0; q < 116; q++) {
70   lt65904 += 1;
71 }
72 let kx99301 = 4;
73 for (let e = 0; e < 91; e++) {
74   kx99301 += 1;
75 }
76 let ifqqr94477 = 10;
77 for (let m = 0; m < 106; m++) {
78   ifqqr94477 += 1;
79 }
80 let ge39345 = 3;
81 for (let e = 0; e < 45; e++) {
82   ge39345 += 1;
83 }
84 let vox87732 = 8;
85 for (let x = 0; x < 40; x++) {
86   vox87732 += 1;
87 }
88 let rs60516 = 7;
89 for (let e = 0; e < 88; e++) {
90   rs60516 += 1;
91 }
92 let ty85695 = 6;
93 for (let p = 0; p < 45; p++) {
94   ty85695 += 1;
95 }
96 let nmk21077 = -10;
97 for (let r = 0; r < 107; r++) {
98   nmk21077 += 1;
99 }
100 let dpk83916 = -1;
101 for (let c = 0; c < 116; c++) {
102   dpk83916 += 1;
103 }
104 let ld49684 = -6;
105 for (let n = 0; n < 127; n++) {
106   ld49684 += 1;
107 }
108 let poo64369 = -1;
109 for (let d = 0; d < 126; d++) {
110   poo64369 += 1;
111 }
112 ...
113
```

114 }

Et nous pouvons maintenant simplifier les boucles par leur valeurs :

```
1 function checkPassword() {
2   ...
3
4   let kp44564 = 99;
5   let xw86483 = 114;
6   let ngzov41442 = 121;
7   let ig78961 = 112;
8   let rn54489 = 116;
9   let bniy31863 = 105;
10  let cw79849 = 99;
11  let ppifg53691 = 67;
12  let bsgv52010 = 84;
13  let kqhd15996 = 70;
14  let gtyt91013 = 123;
15  let itykw12500 = 119;
16  let ks47777 = 51;
17  let skd50420 = 98;
18  let tsyal55384 = 95;
19  let eh43430 = 49;
20  let lt65904 = 115;
21  let kx99301 = 95;
22  let ifqqr94477 = 116;
23  let ge39345 = 48;
24  let vox87732 = 48;
25  let rs60516 = 95;
26  let ty85695 = 51;
27  let nmk21077 = 97;
28  let dpk83916 = 115;
29  let ld49684 = 121;
30  let poo64369 = 125;
31  ...
32 }
```

Et en convertissant tout cela en chaîne on obtient : `crypticCTF{w3b_1s_t00_3asy}`.