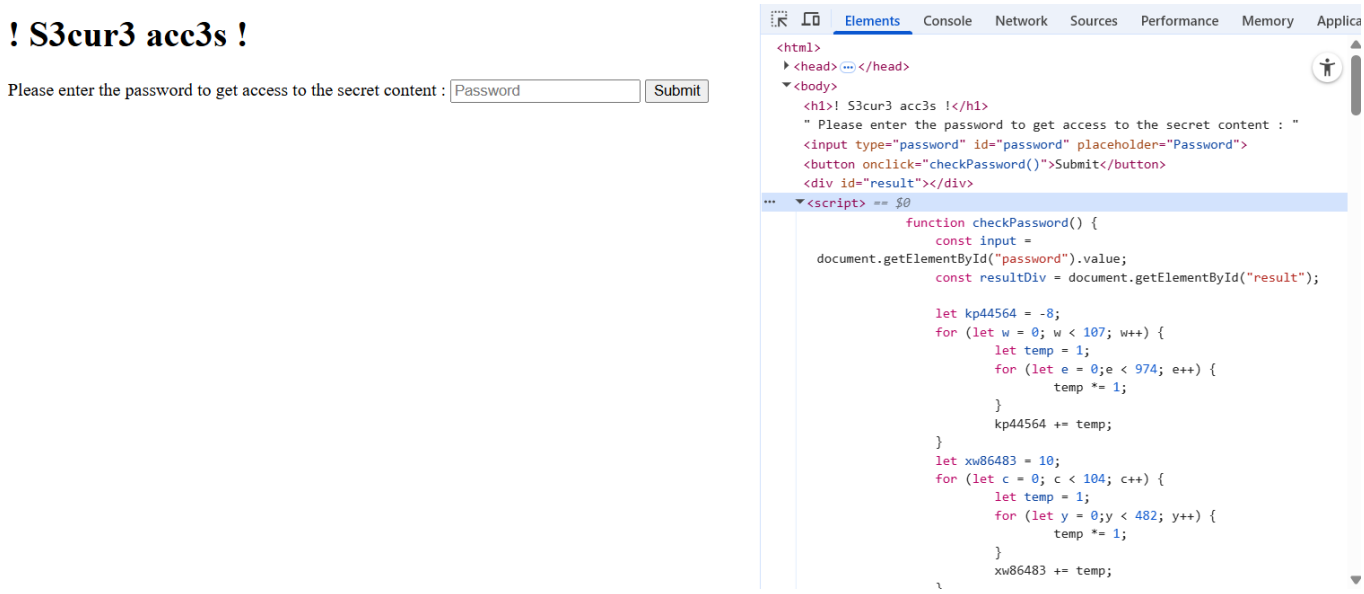
Web - ScriptingLanguage - 50 points

Kévin DUVERGER

Table des matières

1 Résolution ScriptingLanguage :

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



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 :

```
function checkPassword() {
    const input = document.getElementById("password").value;
    const resultDiv = document.getElementById("result");

    let kp44564 = -8;
    for (let w = 0; w < 107; w++) {
        let temp = 1;
        for (let e = 0;e < 974; e++) {
            temp *= 1;
        }
        kp44564 += temp;
    }
    let xw86483 = 10;
    for (let c = 0; c < 104; c++) {
        let temp = 1;
        for (let y = 0;y < 482; y++) {
            temp *= 1;
        }
        xw86483 += temp;
    }
    let ngzov41442 = 5;
    for (let d = 0; d < 116; d++) {
        let temp = 1;
        for (let x = 0;x < 687; x++) {
            temp *= 1;
        }
        ngzov41442 += temp;
    }
    let ig78961 = 6;
    for (let i = 0; i < 106; i++) {
        let temp = 1;
        for (let s = 0;s < 693; s++) {
            temp *= 1;
        }
        ig78961 += temp;
    }
    let rn54489 = 5;
    for (let p = 0; p < 111; p++) {
        let temp = 1;
        for (let l = 0;l < 295; l++) {
            temp *= 1;
        }
        rn54489 += temp;
    }
```

```
    let bniy31863 = -4;
    for (let c = 0; c < 109; c++) {
        let temp = 1;
        for (let y = 0;y < 46; y++) {
            temp *= 1;
        }
        bniy31863 += temp;
    }
    let cw79849 = 8;
    for (let e = 0; e < 107; e++) {
        let temp = 1;
        for (let w = 0;w < 30; w++) {
            temp *= 1;
        }
        cw79849 += temp;
    }
    let ppifg53691 = -5;
    for (let u = 0; u < 72; u++) {
        let temp = 1;
        for (let g = 0;g < 432; g++) {
            temp *= 1;
        }
        ppifg53691 += temp;
    }
    let bsgv52010 = 8;
    for (let e = 0; e < 76; e++) {
        let temp = 1;
        for (let w = 0;w < 106; w++) {
            temp *= 1;
        }
        bsgv52010 += temp;
    }
    let kqhd15996 = -2;
    for (let r = 0; r < 72; r++) {
        let temp = 1;
        for (let j = 0;j < 467; j++) {
            temp *= 1;
        }
        kqhd15996 += temp;
    }
    let gtyt91013 = -10;
    for (let r = 0; r < 133; r++) {
        let temp = 1;
        for (let j = 0;j < 780; j++) {
            temp *= 1;
        }
        gtyt91013 += temp;
    }
    let itykw12500 = -2;
    for (let n = 0; n < 121; n++) {
        let temp = 1;
        for (let n = 0;n < 605; n++) {
            temp *= 1;
        }
        itykw12500 += temp;
    }
    let ks47777 = 5;
    for (let t = 0; t < 46; t++) {
        let temp = 1;
        for (let h = 0;h < 483; h++) {
            temp *= 1;
        }
        ks47777 += temp;
    }
    let skd50420 = -7;
    for (let t = 0; t < 105; t++) {
        let temp = 1;
        for (let h = 0;h < 872; h++) {
            temp *= 1;
        }
        skd50420 += temp;
    }
    let tsyal55384 = -8;
    for (let z = 0; z < 103; z++) {
        let temp = 1;
        for (let b = 0;b < 196; b++) {
            temp *= 1;
        }
        tsyal55384 += temp;
```

```
    }
    let eh43430 = 7;
    for (let s = 0; s < 42; s++) {
        let temp = 1;
        for (let i = 0;i < 438; i++) {
            temp *= 1;
        }
        eh43430 += temp;
    }
    let lt65904 = -1;
    for (let q = 0; q < 116; q++) {
        let temp = 1;
        for (let k = 0;k < 197; k++) {
            temp *= 1;
        }
        lt65904 += temp;
    }
    let kx99301 = 4;
    for (let e = 0; e < 91; e++) {
        let temp = 1;
        for (let w = 0;w < 859; w++) {
            temp *= 1;
        }
        kx99301 += temp;
    }
    let ifqqr94477 = 10;
    for (let m = 0; m < 106; m++) {
        let temp = 1;
        for (let o = 0;o < 878; o++) {
            temp *= 1;
        }
        ifqqr94477 += temp;
    }
    let ge39345 = 3;
    for (let e = 0; e < 45; e++) {
        let temp = 1;
        for (let w = 0;w < 509; w++) {
            temp *= 1;
        }
        ge39345 += temp;
    }
    let vox87732 = 8;
    for (let x = 0; x < 40; x++) {
        let temp = 1;
        for (let d = 0;d < 548; d++) {
            temp *= 1;
        }
        vox87732 += temp;
    }
    let rs60516 = 7;
    for (let e = 0; e < 88; e++) {
        let temp = 1;
        for (let w = 0;w < 395; w++) {
            temp *= 1;
        }
        rs60516 += temp;
    }
    let ty85695 = 6;
    for (let p = 0; p < 45; p++) {
        let temp = 1;
        for (let l = 0;l < 210; l++) {
            temp *= 1;
        }
        ty85695 += temp;
    }
    let nmk21077 = -10;
    for (let r = 0; r < 107; r++) {
        let temp = 1;
        for (let j = 0;j < 223; j++) {
            temp *= 1;
        }
        nmk21077 += temp;
    }
    let dpk83916 = -1;
    for (let c = 0; c < 116; c++) {
        let temp = 1;
        for (let y = 0;y < 116; y++) {
            temp *= 1;
        }
```

```
        dpk83916 += temp;
    }
    let ld49684 = -6;
    for (let n = 0; n < 127; n++) {
        let temp = 1;
        for (let n = 0;n < 790; n++) {
            temp *= 1;
        }
        ld49684 += temp;
    }
    let poo64369 = -1;
    for (let d = 0; d < 126; d++) {
        let temp = 1;
        for (let x = 0;x < 171; x++) {
            temp *= 1;
        }
        poo64369 += temp;
    }

    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) {
        resultDiv.textContent = "Correct !";
        resultDiv.style.color = "green";
    } else {
        resultDiv.textContent = "Incorrect !";
        resultDiv.style.color = "red";
    }
}
```

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 :

```
function checkPassword() {
    ...

    let kp44564 = -8;
    for (let w = 0; w < 107; w++) {
        kp44564 += 1;
    }
    let xw86483 = 10;
    for (let c = 0; c < 104; c++) {
        xw86483 += 1;
    }
    let ngzov41442 = 5;
    for (let d = 0; d < 116; d++) {
        ngzov41442 += 1;
    }
    let ig78961 = 6;
    for (let i = 0; i < 106; i++) {
        ig78961 += 1;
    }
    let rn54489 = 5;
    for (let p = 0; p < 111; p++) {
        rn54489 += 1;
    }
    let bniy31863 = -4;
    for (let c = 0; c < 109; c++) {
        bniy31863 += 1;
    }
    let cw79849 = 8;
    for (let e = 0; e < 107; e++) {
        cw79849 += 1;
    }
    let ppifg53691 = -5;
    for (let u = 0; u < 72; u++) {
        ppifg53691 += 1;
```

```
    }
    let bsgv52010 = 8;
    for (let e = 0; e < 76; e++) {
        bsgv52010 += 1;
    }
    let kqhd15996 = -2;
    for (let r = 0; r < 72; r++) {
        kqhd15996 += 1;
    }
    let gtyt91013 = -10;
    for (let r = 0; r < 133; r++) {
        gtyt91013 += 1;
    }
    let itykw12500 = -2;
    for (let n = 0; n < 121; n++) {
        itykw12500 += 1;
    }
    let ks47777 = 5;
    for (let t = 0; t < 46; t++) {
        ks47777 += 1;
    }
    let skd50420 = -7;
    for (let t = 0; t < 105; t++) {
        skd50420 += 1;
    }
    let tsyal55384 = -8;
    for (let z = 0; z < 103; z++) {
        tsyal55384 += 1;
    }
    let eh43430 = 7;
    for (let s = 0; s < 42; s++) {
        eh43430 += 1;
    }
    let lt65904 = -1;
    for (let q = 0; q < 116; q++) {
        lt65904 += 1;
    }
    let kx99301 = 4;
    for (let e = 0; e < 91; e++) {
        kx99301 += 1;
    }
    let ifqqr94477 = 10;
    for (let m = 0; m < 106; m++) {
        ifqqr94477 += 1;
    }
    let ge39345 = 3;
    for (let e = 0; e < 45; e++) {
        ge39345 += 1;
    }
    let vox87732 = 8;
    for (let x = 0; x < 40; x++) {
        vox87732 += 1;
    }
    let rs60516 = 7;
    for (let e = 0; e < 88; e++) {
        rs60516 += 1;
    }
    let ty85695 = 6;
    for (let p = 0; p < 45; p++) {
        ty85695 += 1;
    }
    let nmk21077 = -10;
    for (let r = 0; r < 107; r++) {
        nmk21077 += 1;
    }
    let dpk83916 = -1;
    for (let c = 0; c < 116; c++) {
        dpk83916 += 1;
    }
    let ld49684 = -6;
    for (let n = 0; n < 127; n++) {
        ld49684 += 1;
    }
    let poo64369 = -1;
    for (let d = 0; d < 126; d++) {
        poo64369 += 1;
    }

    ...
```

```
}
```

Et nous pouvons maintenant simplifier les boucles par leur valeurs :

```
function checkPassword() {
    ...

    let kp44564 = 99;
    let xw86483 = 114;
    let ngzov41442 = 121;
    let ig78961 = 112;
    let rn54489 = 116;
    let bniy31863 = 105;
    let cw79849 = 99;
    let ppifg53691 = 67;
    let bsgv52010 = 84;
    let kqhd15996 = 70;
    let gtyt91013 = 123;
    let itykw12500 = 119;
    let ks47777 = 51;
    let skd50420 = 98;
    let tsyal55384 = 95;
    let eh43430 = 49;
    let lt65904 = 115;
    let kx99301 = 95;
    let ifqqr94477 = 116;
    let ge39345 = 48;
    let vox87732 = 48;
    let rs60516 = 95;
    let ty85695 = 51;
    let nmk21077 = 97;
    let dpk83916 = 115;
    let ld49684 = 121;
    let poo64369 = 125;
    ...
}
```

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