

AdventOfCTF-4

Challenge

126 Solves

×

4
400

web

There are people who think you can hide important things by making it hard to read.

Visit <https://04.adventofctf.com> to start the challenge.

Unlock Hint for 200 points

Flag

Submit

Advent of CTF 4

Your daily dose of CTF for December

Hello, User unknown

If you have access to it the special present will be shown below:

NOPE This user has no access to the flag.

As in previous challenges a login.js script gets loaded:

```

function startup() {
    key = localStorage.getItem('key');

    if (key === null) {
        localStorage.setItem('key', 'eyJ1c2VyYWQiOjB9.1074');
    }
}

var _0x1fde=['charCodeAt'];
(function(_0x93ff3a,_0x1fded8){
    var _0x39b47b=function(_0x54f1d3){
        while(--_0x54f1d3){
            _0x93ff3a['push'](_0x93ff3a['shift']());
        }
    };
    _0x39b47b(++_0x1fded8);
})(_0x1fde,0x192));
var _0x39b4=function(_0x93ff3a,_0x1fded8){
    _0x93ff3a=_0x93ff3a-0x0;
    var _0x39b47b=_0x1fde[_0x93ff3a];
    return _0x39b47b;
};
function calculate(_0x54f1d3){
    var _0x58628b=_0x39b4,_0xc289d4=0x0;
    for(let _0x19ddf3 in text){
        _0xc289d4+=text[_0x58628b('0x0')](0x19ddf3);
    }return _0xc289d4;
}

function check() {
    key = localStorage.getItem('key');
    hash = window.location.search.split('?')[1];

    if (key !== null && hash !== 'token='+key) {
        parts = key.split('.');
        text = atob(parts[0]);
        checksum = parseInt(parts[1]);

        count = calculate(text);

        if (count == checksum) {
            setTimeout(function(){
                window.location="index.php?token=" + key;
            }, 5000);
        }
    }
}

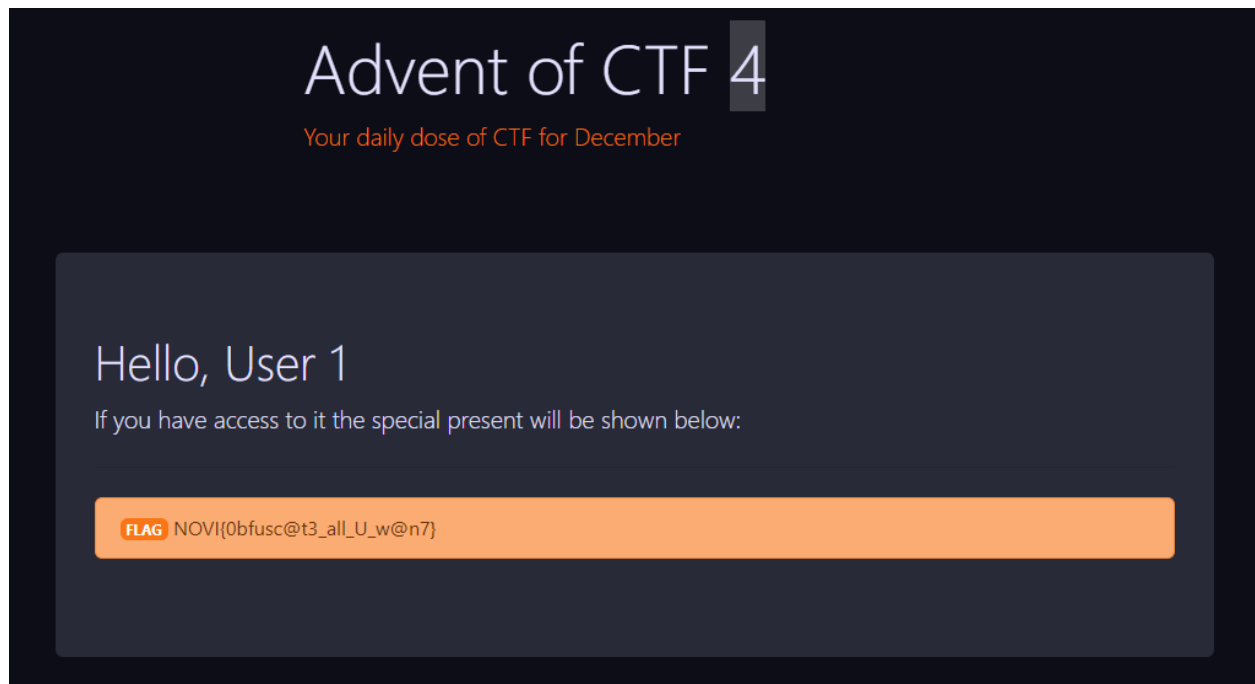
startup();
check();

```

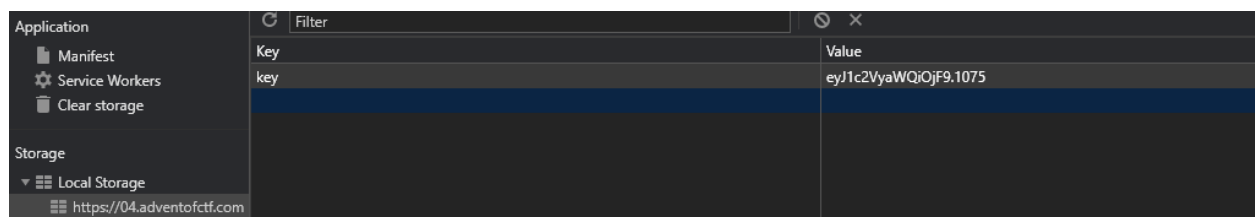
This time the javascript code is obfuscated.

To get the flag edit the url to have a GET parameter token set to the value: eyJ1c2VyaWQiOjF9.1075 which is the base64encoding of {"userid":1}.1075.

04.adventofctf.com/index.php?token=eyJ1c2VyaWQiOjF9.1075



The flag apperas only for 5 seconds, after that we get sent to <https://04.adventofctf.com/index.php?token=eyJ1c2VyaWQiOjB9.1074> you can see why in the source code. To stay on the flag page we need to edit our local storage to have the value: eyJ1c2VyaWQiOjF9.1075



And then refresh the page.

Advent of CTF 4

Your daily dose of CTF for December

Hello, User 1

If you have access to it the special present will be shown below:

FLAG NOVI{0bfusc@t3_all_U_w@n7}

Flag: NOVI{0bfusc@t3_all_U_w@n7}

