str0nkus / NeverlanCTF-2019-Writeups



■ README.md

[Console]

Question:

You control the browser https://challenges.neverlanctf.com:1120

Answer

- 1. I spent a long time trying to find the md5 hash "7b1ece53a46f4a5a2995b9cf901bf457" on several sites to see what it was, but no luck.
- 2. The question text lead to "You are incontrol of the browser" so i tried to tweak some stuff in the source of the code.
- 3. First i tried to change the MD5 hash to see if it had any effect, it did not.
- 4. I ended up with changing the getThat to "Y":

```
var foo = document.getElementById("p");
                         function what(){
                             var input = document.getElementById("pass").value;
if( md5(input) == "7blece53a46f4a5a2995b9cf901bf457" ){
    getThat('Y');
}else{getThat('N')}
                             ction getThat(strg){
                                  // Note: There is no data sent to the key.php file...
// jquery ajax reference: https://api.jquery.com/jQuery.ajax/
                                   $.ajax({
                                       type: 'GET',
                                        url: '1/key.php',
                                        success: function (file_html) {
                                             // success
                                            foo.innerHTML=(file_html)
                                   foo.innerHTML = "Nope, try again";
                         .
/* This function makes a md5 hash of whatever is passed to it. You DON'T have to
        var md5=function(r){function n(r,n){return r<<n|r>>>>32-n}function t(r,n){var t, e=2147483648&r,u=2147483648&n,t=1073741824&r,o=1073741824&n,f=(1073741823&r)+(1073741823&n)
html body script (text)
 Console What's New
                         ▼ | ⊙ | Filter
▶ ( top
                                                                                                       Default levels ▼
> getThat('Y')
 undefined
```

5. This gave me the flag:

> test	submit submit		
Password: flag{cons	sole_controls_js}		
-lag:			
iag.			
flag{console_co			