攻防世界-web simple_js

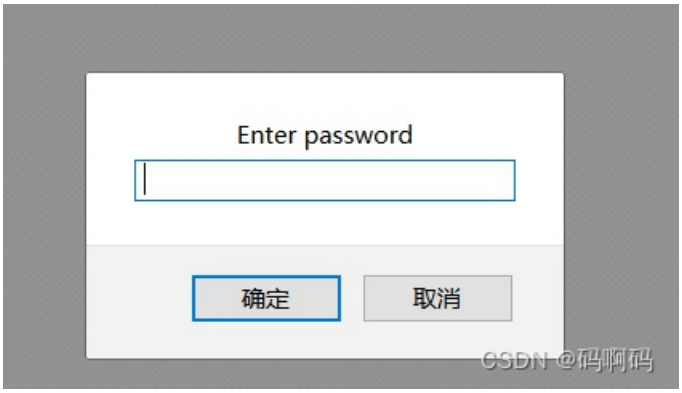
原创

码啊码 于 2022-02-09 10:48:21 发布 539 收藏

分类专栏： CTF 文章标签： 前端 javascript 安全 web安全

本文链接：https://blog.csdn.net/m0_48108919/article/details/122836168

题目描述：小宁发现了一个网页，但却一直输不对密码。(Flag格式为 Cyberpeace{xxxxxxxx})



随便输入一个密码，提示人造密码

再查看一下题目叫简单的js，尝试禁用网站的js无果

分析js代码

```
<script type="text/javascript">
    function dechiffre(pass_enc){
        var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
        var tab  = pass_enc.split(','); //split()用于把一个字符串分割成字符串数组
                var tab2 = pass.split(',');var i,j,k,l=0,m,n,o,p = "";i = 0;j = tab.length;
                        k = j + (l) + (n=0);
                        n = tab2.length;
                        for(i = (o=0); i < (k = j = n); i++ ){o = tab[i-l];p += String.fromCharCode((o = tab2[i]
));
                                if(i == 5)break;}
                        for(i = (o=0); i < (k = j = n); i++ ){
                        o = tab[i-l];
                                if(i > 5 && i < k-1)
                                        p += String.fromCharCode((o = tab2[i]));
                        }
        p += String.fromCharCode(tab2[17]);
        pass = p;return pass;
    }
    String["fromCharCode"](dechiffre("\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x
2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c\x35\x30"));

    h = window.prompt('Enter password');
    alert( dechiffre(h) );

</script>
```

看到有一段编码：

\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c\x35\x30

\x是C/C++里普通的转义字符，\x后面跟的字符即为十六进制的字符串

把\x转换为%，将字符串转换为URL编码

%35%35%2c%35%36%2c%35%34%2c%37%39%2c%31%31%35%2c%36%39%2c%31%31%34%2c%31%31%36%2c%31%30%37%2c%34%39%2c%35%30

通过在线工具解码http://www.jsons.cn/urlencode/得

55,56,54,79,115,69,114,116,107,49,50

进行ASCII码转换得：786OsErtk12

提示flag格式为Cyberpeace{xxxxxxxx}，提交Cyberpeace{786OsErtk12}成功