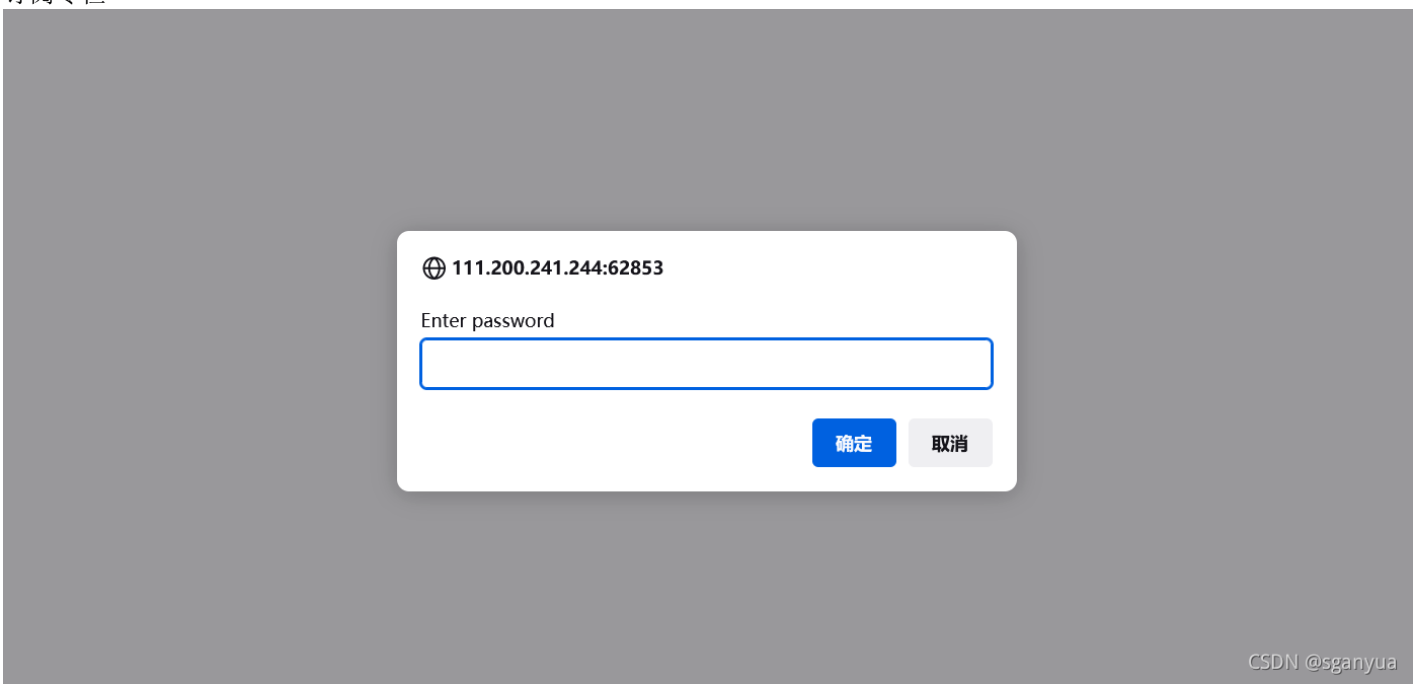
[simple_js]writeup

原创

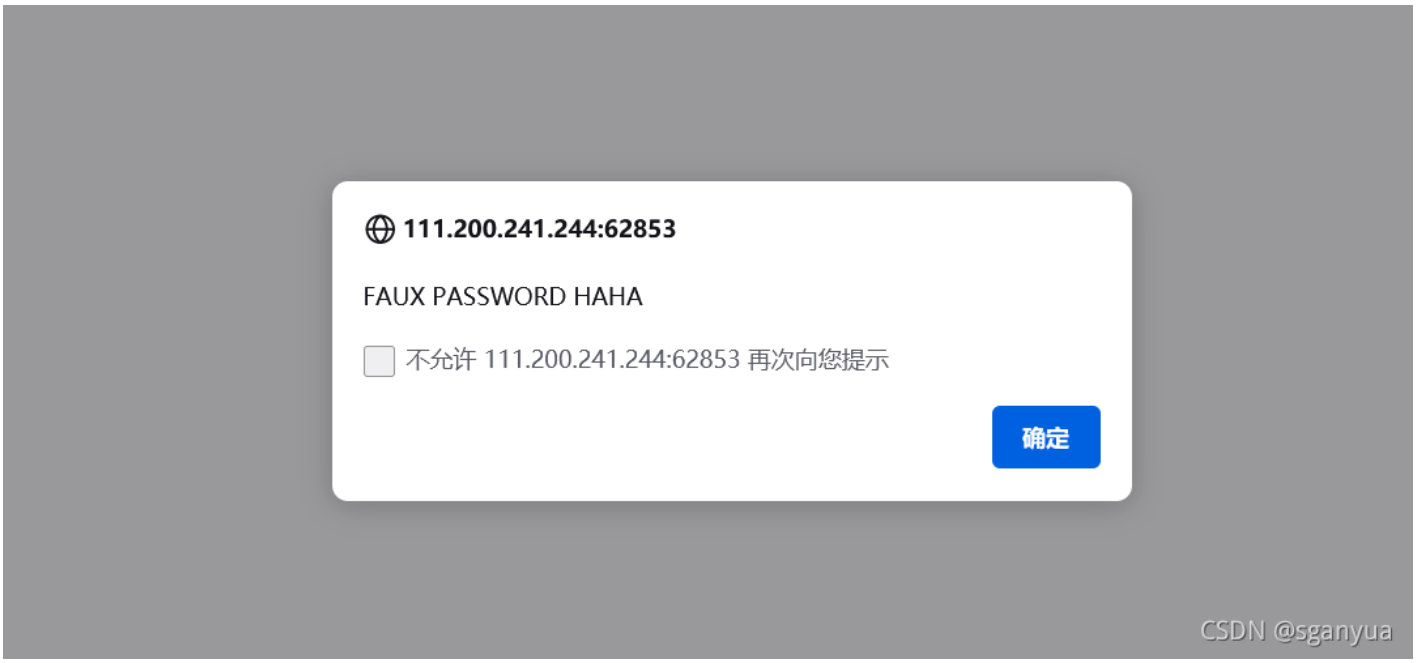
sGanYu 于 2021-08-30 11:38:06 发布 751 收藏
分类专栏： 渗透测试 攻防世界 文章标签： js 安全漏洞 渗透测试


渗透测试 同时被 2 个专栏收录
75 篇文章 4 订阅
订阅专栏


攻防世界
12 篇文章 0 订阅
订阅专栏



打开页面后，无论在输入框中输入任何内容都回显一个结果



右击或按f12查看源代码，得到一段脚本代码

```
<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(',');
                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 = ta
                                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;
    }
</script>
```

这里记录两种方法：

一种是非常简单的利用base16编码进行解码，得到数字后，对照ascii码表，以逗号作为分隔符查询即可获得flag

55,56,54,79,115,69,114,116,107,490,5

base16解码地址

另一种方法是看一个大神利用js简化得到flag，感觉很有意思，就记录下来

split()主要是用于对一个字符串进行分割成多个字符串数组，逻辑上可见它只是将内容为逗号分隔的数字的字符串转成相应编码的字符串，将这段js简化

```
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(',');
               var tab2 = pass.split(',');
               var i=0,j,k,m,n,o,p = "",l=0;
                       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;
   }
```

去除多余的变量

```
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(',');
        var tab2 = pass.split(',');
        var i=0,n,p = "",j,k,m,o,l=0;
            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=n-1)  p += String.fromCharCode((o = tab2[i]));
            }
    p += String.fromCharCode(tab2[17]);
    pass = p;
    return pass;
  }
```

将删除线去除进行整理

```
function dechiffre(){
            var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
            var tab2 = pass.split(',');
            var i=0,n,p = "";
                    k = j + (l) + (n=0);
                    n = tab2.length;
                    for(i = 0; i < k = j = n; i++ ){
                        p += String.fromCharCode(tab2[i]);
                        if(i == 5)break;
                    }
                    for(i = 0; i < k = j = n; i++ ){
                        if(i > 5 && i < k=n-1)  p += String.fromCharCode(tab2[i]);
                    }
      p += String.fromCharCode(tab2[17]);

      return pass;
  }
```

将两个if循环合并

```
function dechiffre(){
               var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
               var tab2 = pass.split(',');
               var i=0,p = "",n;
                       n = tab2.length;
                       for(i = 0; i < tab2.length -1; i++ ){
                           p += String.fromCharCode(tab2[i]);
                       }
       p += String.fromCharCode(tab2[17]);

       return p;
}
```

将末尾并入

```
function dechiffre(){
               var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
               var tab2 = pass.split(',');
               var i=0,p = "",n;
                       n = tab2.length;
                       for(i = 0; i < tab2.length; i++ ){
                           p += String.fromCharCode(tab2[i]);
                       }

       return p;
}
```

更改一下代码，将下方的字符串代替函数中的字符串

```
String["fromCharCode"]
(dechiffre("\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\x2

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

最后得到，保存为txt文档，将后缀改为html，然后打开得到flag

```
<html>
<head>
    <title>JS</title>
    <script type="text/javascript">
function dechiffre(){
                var pass = "\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x2c\x3
                var tab2 = pass.split(',');
                var i=0,p = "";
                        for(i = 0; i < tab2.length; i++ ){
                            p += String.fromCharCode(tab2[i]);
                        }
        return p;
 }
alert(dechiffre());//弹出常量
</script>
</head>
<body></body>
</html>
```