实战笔记之二维码劫持漏洞

白帽技术与网络安全 昨天

以下文章来源于冷渗透 ， 作者N10th

冷渗透

黑产研究，渗透测试，漏洞挖掘，记录非常规思路的hackdom。

思考了一段时间
情报类的实战笔记
不适合未经脱敏地外放
以后，我会去掉具体细节
跟大家分享思路。

这次面向白帽子师傅们，

分享一个实战中
碰到的二维码劫持漏洞案例

0x01 场景再现

vue类型的网站，登录口，有三种登陆方式。

（ps:你要是只看到了两种登陆方式，抬头反思三秒钟）

选择扫码登录，弹出“微信扫码登录”
直觉告诉我，这里可能存在漏洞。

0x02 漏洞分析

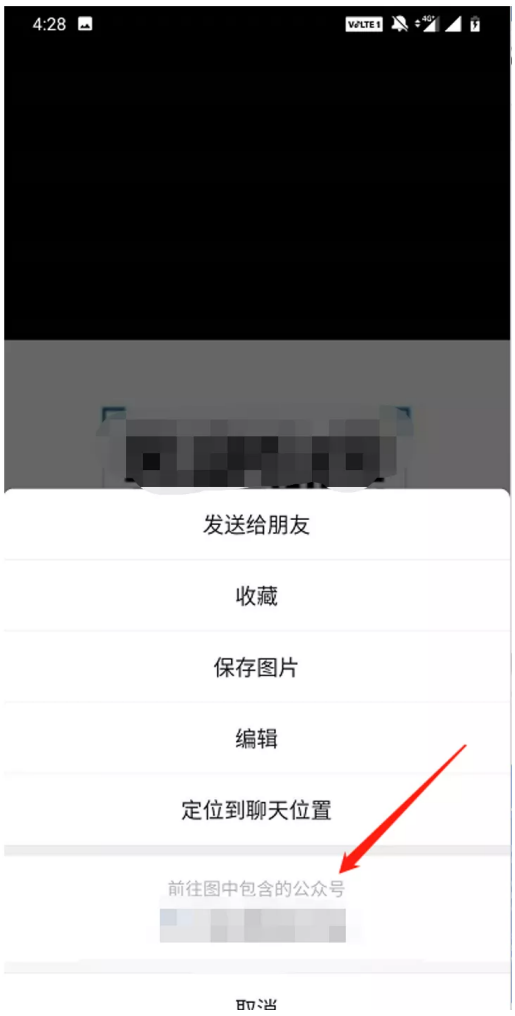
微信扫码后，显示需要关注该网站的公众号

待微信绑定公众号后，即可注册/登录。

注册了一个账号后。

再进行扫码登录

扫码>> 弹出“前往包含的公众号”

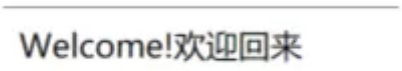


“点击授权”

微信网页跳转，>>>点击确认登录

会发现浏览器Web端页面跳转，

登录成功！



分析

①浏览器Web端分析

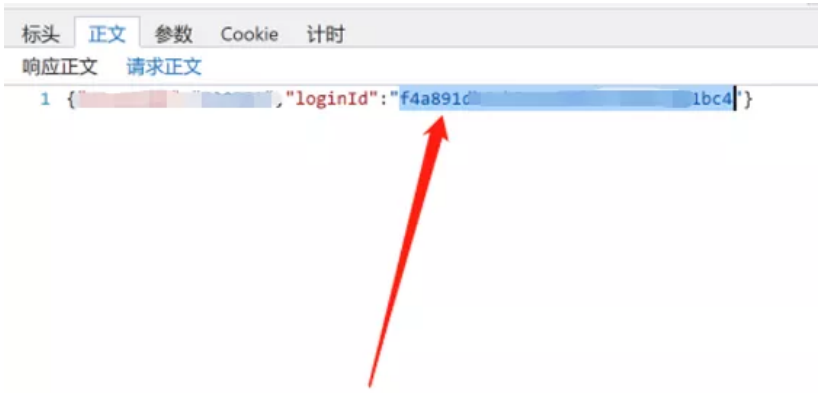
回到最开始的地方，Web端网站的扫码登录入口点

此时，浏览器进入二维码轮循状态，

不断向服务器发送请求，

判断是否扫描了二维码。

点开任意一个轮循环发送的请求数据包



你会发现post body的其中一个参数，“loginId”。

记住这个值：f4a891xxxxxxxx

②微信客户端分析

在扫码前往公众号后，需要“点击授权”确认后，即可成功登录。

我们在微信PC端，提取这个“点击授权”的URI超链，进行分析

https://xxxx.com/#/login/auth?loginId=f4a891xxxxxxxxxxxxxxx

发现携带了参数loginId值，并且与上一步中的loginId值相同！

有什么用呢?

一旦受害者扫码

攻击者能否“代替”对方点击授权，如何代替?

因为我们有了loginId，通过自行构造出“点击授权”的URI

构造漏洞利用思路：

两个身份：受害者，攻击者。

前提条件：受害者注册了该网站，可用微信扫码直接登录

攻击场景：攻击者打开该网站，选择微信扫码登录。

截图，截取二维码发给受害者。

受害者扫码>>点击“前往该公众号”

攻击者获取loginId 构造“点击授权”的URI链接

从而完成账户入侵

0x03 漏洞复现

① 打开登录网站

②点击扫码登录

③记录轮循数据包的loginId值f4a89xxxxxxxxxx

④直接截取web端登录的二维码图片，发给受害者

有个前提：

二维码在有效期内，因为时间过长，二维码会失效

受害者视角

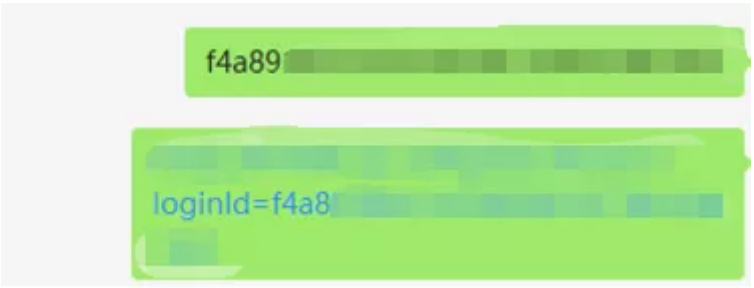
受害者扫码

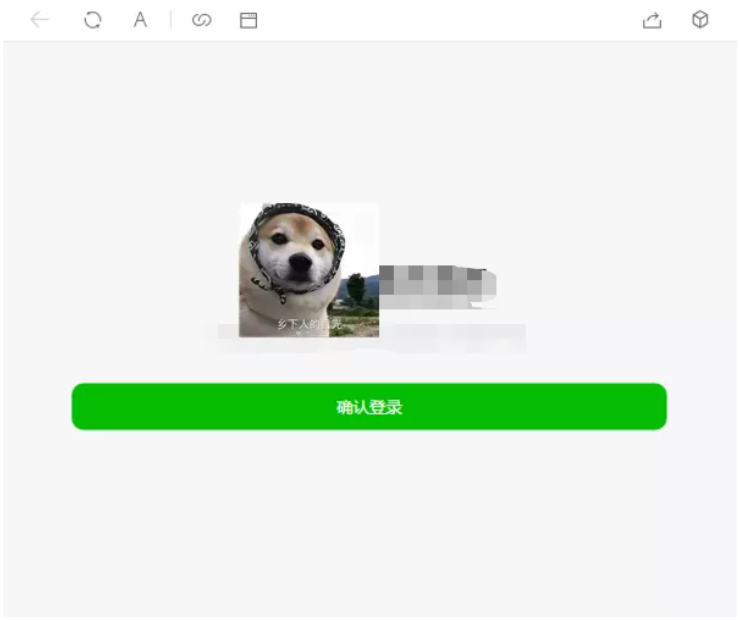
一旦点击“前往图中包含的公众号”。

此时，我们视角转换，
不需要关心受害者会接下来进行什么操作，
他都已经沦陷了

攻击者视角
通过loginId值的拼接
自行构造出URI
https://xxxx.com/#/login/auth?loginId=f4a89xxxxxxxxxx

攻击者微信客户端直接打开该链接



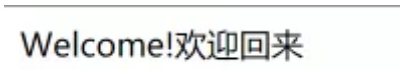


点击“确认登录”

OK

Web端浏览器页面跳转

使用受害者账户登录成功！



至此，完成复现。

总结

如果要真正用到社工钓鱼，可以自行搭建一个服务器

用于对接该网站的扫码登录入口

从而保证二维码更新，不失效。

这个，已经看过很多大师傅写过了

就不再重复。

希望有用，如果没有

我想下篇或许会有。