# **[HTTP Authorization](https://www.cnblogs.com/findumars/p/5107574.html)**

POST /goform/ser2netconfigAT HTTP/1.1  
Host: 192.168.16.254  
Connection: keep-alive  
Authorization: Basic YWRtaW46YWRtaW4= //笔者注释，Authorization: "Basic 用户名和密码的base64加密字符串"

Content-Length: 23

uart=9600,8,n,1&save=1

用中文简述一下http auth的过程：  
  
客户端发送http请求  
服务器发现配置了http auth，于是检查request里面有没有"Authorization"的http header  
如果有，则判断Authorization里面的内容是否在用户列表里面，Authorization header的典型数据为"Authorization: Basic jdhaHY0="，其中Basic表示基础认证， jdhaHY0=是base64编码的"user:passwd"字符串。如果没有，或者用户密码不对，则返回http code 401页面给客户端。  
标准的http浏览器在收到401页面之后，应该弹出一个对话框让用户输入帐号密码；并在用户点确认的时候再次发出请求，这次请求里面将带上Authorization header  
  
一次典型的访问场景是：  
浏览器发送http请求（没有Authorization header）  
服务器端返回401页面  
浏览器弹出认证对话框  
用户输入帐号密码，并点确认  
浏览器再次发出http请求（带着Authorization header）  
服务器端认证通过，并返回页面  
浏览器显示页面  
使用http auth的场景不会用cookie，也就是说每次都会送帐号密码信息过去。然后我们都知道base64编码基本上等于明文。这削弱了安全。  
由于种种缺点，http auth现在用的并不多。不过在路由器等场合还是有应用的，原因是http auth最简单，使用起来几乎是零成本。  
在你需要做访问控制，又不想拖上SSO、数据库之类的东西的时候，http auth不失为一个简洁的选项。