顾名思义，网络投票就是在网络上进行的投票活动，但和其他类型的投票不同的是：网络投票是建立在网络投票系统上的，而结果完全由程序输出，无需人工参与。这既是网络投票系统的优点也是其缺点，没有了人工的参与，其结果很可能被黑客利用。而网络投票系统本身的技术含量并不高，对于连续投票的验证能力薄弱，只要黑客掌握了原理，就可以轻松地实现连续刷票，对投票结果进行作弊。那么，黑客是如何突破网络投票系统的，又是如何实现无限制刷票的呢？下面我们就来对此进行揭密。  
      
网络投票的验证方式  
      
     参与过网络投票活动的朋友都知道，当我们给其中某一项投票后，马上进行再次投票，投票将不会成功，提示你“您已经投过票了”，那么网络投票系统是如何知道你已经投过票了呢？这就是网络投票系统的内置防刷功能在起作用。  
     在我们投出第一票的时候，第一种情况是：投票系统自动记录下我们的IP地址，存入数据库，并且规定该IP地址多少时间内不准投票。如果我们马上再次投票，投票系统会将我们这次投票时使用的IP地址与其数据库中的IP地址进行比对，如果存在，则投票不成功。  
     第二种情况是：我们投的第一票成功后，投票系统会将投票成功的信息保存在本地的Cookies文件中，并且在Cookies中注明投票成功的时间，同时在程序中规定多少时间内不准再次投票。如果我们马上再次投票，程序会读取保存在Cookies信息中的投票成功时间，并与服务器中的时间比对，如果符合拒绝条件，则投票不成功。  
     总的来说，网络投票程序的防刷系统采用的原理就是IP验证和Cookies验证，当然还有采用诸如身份验证等其他验证方式的网络投票系统，不过目前网络上90％的网络投票系统都是采用前者的验证方式。而前者的验证安全性是很低的，通过一些工具就可以轻松突破这些验证，实现连续投票。

突破IP验证，网络代理来帮忙

     对于突破采用IP验证方式的网络投票系统，我们可以借用网络上丰富的代理资源。使用代理对投票系统进行投票后，投票系统记录下的IP地址是代理的，而不是我们自己的IP地址。如果想再次投票，只需更换一个代理即可。由于使用代理投票留下的IP地址都不一样，对于投票系统而言，这是属于正常的投票行为，因此是不会对我们的投票进行拒绝的。下面我们来看看使用代理突破验证的方法。  
     寻找网络代理资源  
     利用网络代理资源来突破投票系统的验证，当然需要大量的网络代理资源。这些资源我们可以在一些专门的网络代理发布网站寻找。例如“代理中国”等网站，每天都有上万个网络代理公布。找到代理资源后，我们需要验证这些代理的连通性，以保证代理能够正常使用。验证代理的连通性我们可以借助一款名叫“花刺代理验证”的软件。  
     将代理资源保存为“IP:端口号”的形式，每行一个，以此格式制作一个代理列表，并保存为文本文档。列表制作完成后运行“花刺代理验证”，点击界面右侧的“导入”按钮，将我们制作的代理列表导入进来，然后点击“验证全部”即可。软件会自动验证所有的代理，并将可用的代理显示出来。验证完成后，我们点击“清理”按钮，将无法连接的代理清除掉。最后点击“导出选定”，将可用的代理保存为列表。  
图1.验证可以使用的代理资源  
     最后在软件的代理信息栏中选中一个代理，点击“设为IE代理”，并用IE浏览投票网站即可。至此，我们已经可以突破投票系统的IP验证了，但是这样投票的效率很低，而且操作略显繁琐，是最基本的刷票方法。  
     巧用广告作弊软件  
     上文中用手动设置代理的方法虽然可以突破验证，但是却效率低下。其实我们可以借助一些广告作弊软件，来达到自动更换IP地址刷票的效果。下载“心奇广告作弊”，运行后切换到“设置”标签，在“刷新选项”中勾选“代理刷新”这样程序就会自动更换代理来刷新IE。接着勾选“是否关闭IE”并将其时间设置为5秒，其他保持默认即可。最后点击“导入代理”按钮将我们刚才导出的代理列表导入到软件中来。设置完成后在软件的“网站”文本框中填入投票系统的网址，并将其打开。一切就绪后，点击“开始”按钮，软件会自动弹出IE，一段时间后又会自动关闭，我们就趁这段时间进行投票。虽然也需要人工操作，但是效率已经有了大大的提高。  
图2.设置广告作弊软件

拦截Cookies，避开投票系统验证

     除了IP验证外，网络投票系统的另一种防刷票验证方式是Cookies验证。我们在投票系统上成功投票后，会在本机的C:\Documents and Settings\用户名\Cookies文件夹下生成一个Cookies文件，这个文件中包含了投票成功的时间等信息。当第二次投票时，投票系统会首先检测Cookies文件夹中有没有这个Cookies文件，如果没有，则认为这位用户是第一次投票，可以成功投票。因此我们可以在投票成功后进入系统的Cookies文件夹，将这个投票成功后生成的Cookies文件删除，这样就可以马上再次投票，Cookies验证也就这样轻易得被我们破解了。  
     同样的，我们手工删除投票系统生成Cookies文件虽然可以突破Cookies验证，但仅仅是突破了验证而已，其效率之的低下，完全谈不上刷票。因此我们必须借助一些工具，以达到快速刷票的目的。  
     手工删除Cookies是一件很麻烦的事，如果我们设置IE的属性，使之不允许保存Cookies，那么投票系统同样检测不到Cookies，其效果是一样的。这里我们可以借助一款名叫“Cookie Pal”的软件，这款软件可以对Cookies进行实时的检测，允许你自动接受或拒绝网站在本机保存Cookies。  
     安装“Cookie Pal”，完成后运行，切换到“过滤器”选项，我们需要将投票网站的Cookies添加到“拒绝cookie”菜单。点击“新的...”按钮，将投票网站的服务器名字添加进去。这样投票网站就无法在本机生成Cookies了，如果你无法确定投票网站的服务器名称，可以选中“未知服务器cookie”标签中的“全部拒绝”单选框。选中该项后，所有网站的Cookies文件都将被拒绝。  
图3：询问如何处理Cookies  
     打开IE浏览器，进入投票网站，成功投票后，“Cookie Pal”会自动拦截Cookies，并询问你允许还是禁止Cookies，这里我们当然选择“禁止Cookies”，并勾选“将我的决定应用到来自此网站的所有cookie”。这样我们就可以突破Cookies验证并在投票网站上连续投票了。

本地提交数据包，实现快速刷票

     至此，我们已经完全突破了投票系统的验证，接下来的问题是如何才能快速的实现刷票。我们都知道，在投票系统上进行投票，实际上是向投票系统发送了一个数据包，但是在IE中进行操作的话，从打开页面→选择投票对象→发送，这个过程会占用我们很多的时间，影响刷票的效率。如果我们能离开IE，直接发送数据包给投票系统，那么这个速度就要快的多了，也就能实现所谓的刷票。  
     既然我们可以利用本地提交数据包的原理来进行刷票，那么这个数据包该如何获取，又该如何提交呢？  
     获取数据包  
     获取数据包可以使用著名的网络数据包监视工具WSockExpert。首先用IE打开投票网站，注意不要投票。然后运行WSockExpert，点击工具栏上的“打开”按钮，在弹出的进程列表中双击IE，并选中投票网站的进程，点击“打开”。接着回到IE的投票网站页面，选择一项进行投票。返回WSockExpert，我们可以看到程序已经捕捉到了很多数据包，在这些数据包中，我们可以找到一个以“POST”开头的数据包，这就是我们本机发送给投票系统的数据包。  
图4：捕获我们需要的数据包  
     本地提交数据包  
     下载本地提交数据包工具websend.exe，在其“URL”一项中填入投票网站的地址，然后将我们刚才捕获的“POST”数据包中的内容复制到其“发送内容”文本框中即可。接着我们只要点击一下“SEND”按钮就可以把数据包发送出去，以后每点击一下“SEND”按钮，就等于投了一票。如果配合“按键精灵”等鼠标点击模拟软件，则可以实现快速数票。据统计，一分钟可以刷将近1200票，可见其对投票结果的影响力。  
图5：本地提交数据包  
小贴示：本地递交数据包的方法只适用于采用Cookies验证的投票系统，而对采用IP验证的投票系统来说则不起任何作用。

增加验证机制，还网络投票的公平性

     很多网络投票系统虽然都有防刷票验证能力，但是仅仅具有IP验证或Cookies验证是不够的。在这两种验证的基础上，投票系统的编写者在编写程序的时候可以对投票者增加来路检测、Session验证等验证方法，或者加入复杂的验证码系统。这样即使不能完全杜绝刷票，也可以影响黑客刷票的效率，减少黑客对投票结果的干扰。不过，即使黑客再高明，管理员也可以在服务器上看到刷票的踪迹，黑客刷票后无可避免的会在服务器上留下大量相同的IP地址，或者同一网段的IP地址，这是无法销毁的证据，因此提醒对于想通过刷票来达到某种目的的朋友，请保持投票的公证性，否则你的投票对象很可能因为你而被取消资格