# edusrc技巧

对于一些速度上分的方法，之前在星球写过一两种，但是随着edu平台的跟新，我发现他多了一个开发商排行，这样等于是给我们列出来了edu用户的系统公司，就可以节省我们的时间再去查找开发商来找对应的系统



那么我们知道这些开发商后，我们只需要把这些开发商是产品进行收集，然后某安全搜索引擎进行产品查找不就可以达到系统通杀的效果呢？

我们任意看几个：

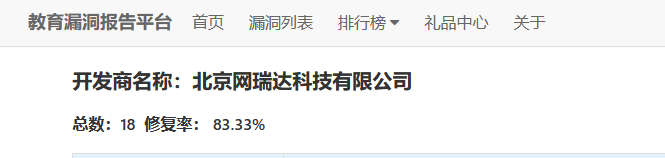




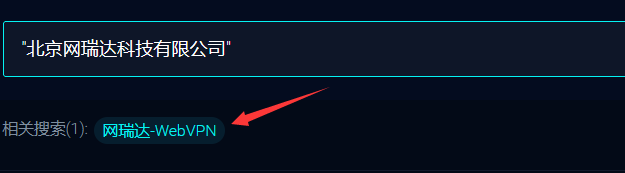
可以看见对于系统的弱口令通杀还是通杀挺多的，当你通过弱口令进入后台后，继续挖掘可以扩大rank值

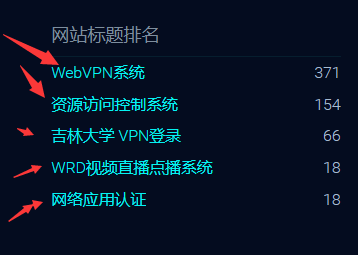
具体操作：

1. 先对应排行榜确定厂商：



1. 然后使用某安全引擎进行系统查找





对于这些都是属于网瑞达公司的这个产品，点进去你可以发现全是教育网段的！

1. 确定系统寻找手册弱口令：

你也可以先尝试常见弱口令，比如admin/admin admin/123456一类的，不成功就是寻找手册

关键字查找方法：xxxxx（公司名部分关键字任意组合）xxxxx（某某系统）操作手册、默认密码、管理员手册（这里自己补充能涉及密码的关键词）



可以看见有很多文档，需要自己花自己整理，找到有效的数据。



可以看见很多关键信息：



在我们的眼里这些是弱口令，但是在运维眼里这些密码均为强口令了，给自己减少工作量，有多少运维会去改密码呢？

当然如果你没办法找到手册，那就自己构造密码：方法也很简单，通过企查查一类的网站对公司信息收集：



可以得知网站命令习惯：wrd wrdtech webvpn 这一类信息（这里的信息你收集的越多，构造的字典爆破的机会越大，其余同理，自己扩展）

我们就可以利用wrd这些来组合密码，比如wrd@123 wrd@admn123456 wrd!@#qwe123 这样构造弱口令去爆破，这里你可以花1--2天 如果一旦突破那么就是一个通杀！相对于还是划算，没成功就等于锻炼了信息收集能力。

第三个地方：github直接找关于这个公司的仓库，收集关于密码的样式，如果能直接找到，那最好，找不到密码就看看能不能遇见一些命名格式然后通过第二个方法自己构造字典

进入后台后，剩下的操作就靠你自己了