

# 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

## 开发商排行榜

名称

搜索

#	开发商	修复率
1	上海复翼软件开发有限公司	100%
2	上海万雍科技股份有限公司	100%
3	北京微瑞集智科技有限公司	100%
4	江苏宝和数据股份有限公司	100%
5	广东动易软件股份有限公司	100%
6	新华三技术有限公司	100%
7	奇安信网神信息技术（北京）股份有限公司	100%
8	成都思必得信息技术有限公司	100%
9	广东轩辕网络科技股份有限公司	100%
10	杭州智图软件开发有限公司	100%
11	广州数园网络有限公司	100%
12	福建新开普信息科技有限公司	100%
13	天津市基理科技股份有限公司	100%
14	上海耀源数据科技有限公司	100%
15	北京开元数据科技有限公司	100%
16	北京康巴北信息科技有限公司	100%
17	南京苏迪科技有限公司	100%

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：

教育漏洞报告平台

[首页](#)
[漏洞列表](#)
[排行榜](#)
[礼品中心](#)
[关于](#)

[注册](#)
[登录](#)

开发商名称：北京网瑞达科技有限公司

总数：18

修复率：83.33%

时间	标题	等级	作者
2022-07-24	安徽医科大学存在其他漏洞	严重	99iz
2022-05-10	东北大学秦皇岛分校存在弱口令	低危	7coinSec
2022-04-27	清华大学存在弱口令	中危	YGnight
2022-04-27	福建中医药大学存在弱口令	低危	YGnight
2022-04-26	阜阳师范学院存在弱口令	低危	YGnight
2022-04-26	上海工商职业技术学院存在弱口令	低危	YGnight
2022-03-04	无锡南洋职业技术学院存在敏感信息泄露	中危	Lsec
2022-01-29	西安外事学院存在弱口令	低危	Jane
2021-11-05	浙江东方职业技术学院存在弱口令	低危	Jane
2021-10-18	厦门大学存在弱口令	低危	Jane
2021-10-04	山西省财政税务专科学校存在弱口令	中危	TheThink3r
2021-10-04	上海济光职业技术学院存在弱口令	中危	TheThink3r
2021-10-04	复旦大学存在弱口令	低危	TheThink3r
2021-10-04	天津商务职业学院存在弱口令	低危	Jane
2021-10-04	浙江广厦建设职业技术学院存在弱口令	低危	Jane

«

1

2

»

开发商名称：北京博校文达科技股份有限公司

总数：27 修复率： 7.41%

时间	标题
2022-03-05	河北省教育厅存在弱口令
2022-03-05	陕西省教育厅存在弱口令
2022-03-05	北京市教育委员会存在弱口令
2022-03-05	河南省教育厅存在弱口令
2022-03-05	河北省教育厅存在弱口令
2022-03-05	海南省教育厅存在弱口令
2022-03-05	广西壮族自治区教育厅存在弱口令
2022-03-05	吉林省教育厅存在弱口令
2022-03-05	吉林省教育厅存在弱口令
2022-03-05	河北省教育厅存在弱口令
2022-03-05	海南省教育厅存在弱口令
2022-03-05	陕西省教育厅存在弱口令
2022-03-05	安徽省教育厅存在弱口令
2022-03-05	河北省教育厅存在弱口令
2022-03-05	河北省教育厅存在弱口令

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：

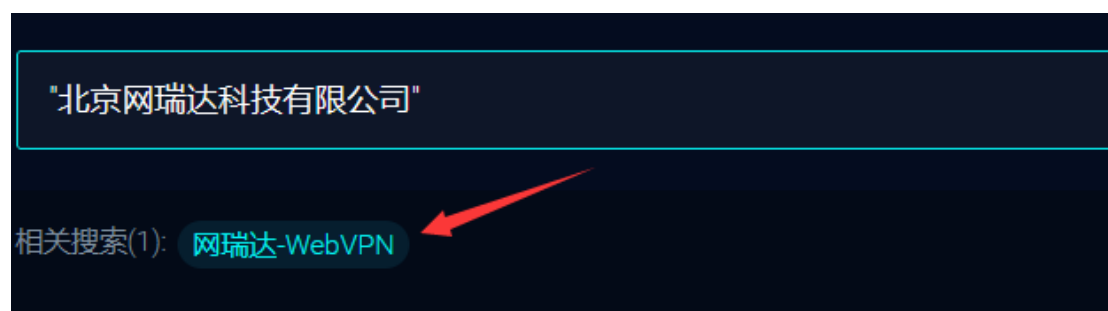
1. 先对应排行榜确定厂商：

教育漏洞报告平台 首页 漏洞列表 排行榜 ▾ 礼品中心 关于

开发商名称：北京网瑞达科技有限公司

总数：18 修复率： 83.33%

2. 然后使用某安全引擎进行系统查找



网站标题排名	
WebVPN系统	371
资源访问控制系统	154
吉林大学 VPN登录	66
WRD视频直播点播系统	18
网络应用认证	18

对于这些都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！

### 3. 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）

度

北京网瑞达网络应用认证系统操作手册

百度一下

Q 网页

文库

资讯

贴吧

知道

图片

地图

采购

视频

更多

百度为您找到相关结果约858,000个

搜索工具

网瑞达WebVPN系统使用说明



2020年2月23日

各位师生:为方便广大师生在校外更便捷、安全地访问学校相关业务系统 & 数据库资源,更好地助力学校教学、科研、管理和服务工作,信息化处以测试性运行方式推出了基于网页方式访问校内...

center.jsnu.edu.cn/f9/2b/c1701...

北京瑞达时代科技有限公司网络应用控制管理系统说明 图文 ...

6页

文档从互联网中收集,已重新修正排版,word 格式支持编辑,如有帮助欢迎下载支持。主要功能与用途 1 强大的协议识别引擎 R-BM强大的协议识别引擎不但可以识别各种明文的协议,如B...

百度文库

保障

网瑞达网关系统安装手册-2014080101 - 百度文库

27页 发布时间: 2022年04月12日

网瑞达网关系统安装手册-2014080101 系统安装手册 硬件要求 服务器要求 服务器 CPU 必须是支持 64 位构架,核心数量不少于 4、内存不小于 4G(建议 8G 或者更多)、磁盘空间...

百度文库

保障

网瑞达网关系统安装手册-2014080101 - 豆丁网

2018年3月5日 若将网络运维系统安装在虚拟化平台或 3bbe5b2fe5 分享于2018-03-05 21:12:10.

0 网瑞达网关系统安装手册-2014080101 文档格式: .pdf 文档页数: 27页 文档大小:...

豆丁网

北京瑞达时代科技有限公司网络应用控制管理系统说明...

2024年12月4日 北京瑞达时代科技有限公司网络应用控制管理系统说明 2024年12月4日 北京瑞达时代科技有

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。

系统安装完毕后默认第一块网卡的地址为 192.168.100.100。将一台具有浏览器的终端配置为和服务器相同地址段的 IP 如 192.168.100.90/255.255.255.，并将网络与服务器的第一块网卡连接起来通过浏览器访问 <http://192.168.100.100>。初始的管理员用户名为 admin 密码为 10@ding



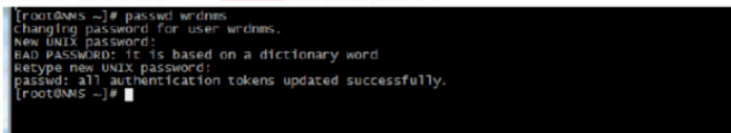
可以看见很多关键信息：

若将网络运维系统安装在了虚拟化平台或不可通过网线直连服务器的情况下，或熟悉 Linux，愿意使用命令行模式配置服务器 IP 时，可使用命令行配置。  
打开控制台到运维服务器，使用用户名:root，密码:@dm1n\$ 登陆命令行。

root 账号禁止远程登录访问，远程访问需要建立新用户。  
输入命令 `useradd wrdnms`（`wrdnms` 即为新用户名，请根据实际情况自行更改）



为新用户设置密码 `passwd wrdnms` 点击回车输入密码。



远程 SSH 登录的端口为 13911。

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：

网端达	www.wrdtech.cn	10011135277 1810032512 010-62222303 027-87540659 81910644 4006502886 caiwu@wrdtech.com caoxinan@wrdtech.com kqq@wrdtech.com congqun@gmail.com congqun@wrdtech.com	ICP备703597号	wrdtech.cn	北京网端达科技有限公司	企业状态: 开业 成立日期: 2010-08-25 注册资本: 2,375万(元) 法定代表人: 丛群	2022-02-24	5月前
网端达科技	www.webvpn.cn	010-62285865 18811135277 1810032512 010-62222303 027-87540659 81910644 4006502886 caiwu@wrdtech.com caoxinan@wrdtech.com kqq@wrdtech.com congqun@gmail.com congqun@wrdtech.com	ICP备703597号	webvpn.cn	北京网端达科技有限公司	企业状态: 开业 成立日期: 2010-08-25 注册资本: 2,375万(元) 法定代表人: 丛群	2022-02-24	5月前
北京网端达科技有限公司官网	www.wrdtech.com	010-62285865 18811135277 1810032512 010-62222303 027-87540659 81910644 4006502886 caiwu@wrdtech.com caoxinan@wrdtech.com kqq@wrdtech.com congqun@gmail.com congqun@wrdtech.com	ICP备703597号	wrdtech.com	北京网端达科技有限公司	企业状态: 开业 成立日期: 2010-08-25 注册资本: 2,375万(元) 法定代表人: 丛群	2022-02-24	5月前

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個通杀！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