**2022年全国大学生信息安全竞赛**

**作品报告**

**作品名称：基于国家双边关系的域名风险评估系统**

**电子邮箱：[1730916701@qq.com](mailto:1730916701@qq.com)**

**提交日期：**

目录

[摘要 3](#_Toc105506857)

[第一章 作品概述 3](#_Toc105506858)

[1.1背景分析 3](#_Toc105506859)

[1.2相关工作 4](#_Toc105506860)

[1.3特色描述 5](#_Toc105506861)

[1.4应用前景分析 5](#_Toc105506862)

[第二章 作品设计与实现 6](#_Toc105506863)

[2.1系统功能流程 7](#_Toc105506864)

[2.2系统核心功能实现 8](#_Toc105506865)

[2.3 系统界面设计 18](#_Toc105506866)

[第三章 作品分析与测试 25](#_Toc105506867)

[3.1作品测试方案 25](#_Toc105506868)

[3.2测试环境搭建与测试设备 26](#_Toc105506869)

[3.3测试数据 26](#_Toc105506870)

[3.4测试结果分析 26](#_Toc105506871)

[创新性说明 34](#_Toc105506872)

[第四章 总结 35](#_Toc105506873)

[参考文献 35](#_Toc105506874)

# 摘要

域名关乎着万千互联网用户能否正常访问网站。在如今的国家冲突中，针对域名的攻击与制裁已经成为了没有硝烟的战场，2021年6月23日，美国查封了伊朗广播电视联盟的33个域名，在前不久的俄乌冲突当中，西方网络注册商又屡屡对俄罗斯的域名进行制裁，并强制勒令俄罗斯的域名更换注册商。这些事例说明了，一个国家的域名能否在遭受解析过程中别国服务商制裁之下，仍然能够正常提供服务至关重要。本作品涉及一种基于国家双边关系，评估域名解析风险的方法，最终以网站的形式提供服务。其原理是通过程序实现域名对应IP的物理地址所处国家、注册商、NS服务商、CDN服务商等所属国家的信息查询。而后以国与国双边关系为基础，利用公式计算出不同国家得分。同时，先进行一定分析，之后采用主客观结合赋权的方法，即CRITIC法赋权与层次分析法，给出可以反映域名的顶级域、注册商、NS服务商、别名记录、IP所处物理地址、CDN服务商这几项属性在域名解析过程当中重要程度的权重。最后，将权重与各项属性背后实体的国家得分相结合，给出一个域名的安全性得分。以域名的得分结合域名的用途，流量对域名安全性进行综合评估，旨在提前发现一些风险高的域名及其背后的网络实体，使人们重点关注。

# 第一章 作品概述

## 1.1背景分析

当今社会，国与国之间的冲突，不仅仅是在现实当中，在网络领域也会有所体现，2021年6月23日，美国查封了伊朗广播电视联盟的33个域名，在前不久的俄乌冲突当中，西方网络注册商又屡屡对俄罗斯的域名进行制裁，并强制勒令俄罗斯的域名更换注册商。

随着科技的进步，上网已成为人们不可或缺的生活方式。域名作为伴随者互联网发展而早期出现的产物，其已成为互联网的核心。域名的安全性直接涉及到域名拥有者（个人和企业）的财产安全。而域名正常运行的背后，又关系着大量的互联网实体，这些实体为互联网生态的正常工作提供服务或者资源，例如域名注册商提供注册服务，解析服务提供商提供域名解析服务。同时，这些互联网实体之间又存在复杂的关系。只有这些网络实体全部能够正常服务，才能保证生态的正常工作，就可都导致无法域名正常解析。轻则影响网民的上网体验，给企业造成经济损失，重则影响国家的网络安全和社会稳定。

另一方面，各个国家或企业需要主动掌握所管辖范围内的重点域名的管理和运行情况，主动发现潜在的安全风险，及时发现问题和提供解决方案。当今世界处于动荡阶段，国家对抗日益明显，特别在网络对抗更是重中之重。目前很多重点域名在某些域名的数据主权上不可控，例如使用国外CDN和权威服务器，易导致数据泄漏和无法解析等。再比如，一些托管网站的IP属于境外服务器，易导致数据泄漏等。特别是，很多中国国内可访问的网站，未备案以及主机未在境内。 2022年政府工作报告中指出，我们要增强忧患意识，直面问题挑战。因此，极端情况下，当在域名安全方面，真正发生国家之间对抗时，中国能够提前部署与防护自身。我们以国家的双边关系为基础，建立评估模型，旨在对域名安全性完成一个合理的、全面的、综合性的评估系统。

## 1.2相关工作

### 1.2.1相关基础理论及技术介绍

#### 1.2.1.1域名相关基础理论

**域名起源**

IP地址是Internet主机的作为路由寻址用的数字型标识，但是它不容易被人所记忆，因此产生了域名这一种字符型标识。在计算机网络中，使用数字地址作为主机唯一标识的做法，可以追溯到今天的商业互联网出现之前的ARPANET[[[1]](#endnote-1)]时代。在早期的网络中，网络上的每个电脑检索存储在SRI（Stanford Research Institute）的一台电脑上HOST.TXT文件，它映射主机名到数字地址。而随着网络的迅速增长，这种使用HOST.TXT方法出现了流量负载、名字冲突和一致性等问题。因此，在1983年，DNS系统应运而生，域名也随之开始被广泛使用。在1985年3月15日，世界上第一个互联网域名为Symbolics.com被注册，现在它已经成为了一个历史网站。目前，互联网名称与数字地址分配机构（the Internet Corporation for Assigned Names and Numbers，ICANN）全面管理互联网域名空间的顶层开发和体系结构，它授权域名注册机构来进行域名登记和重新分配。

**域名解析**

域名是为了方便记忆而专门建立的一套地址转换系统，然而要访问一台互联网上的服务器，最终还必须通过IP地址才能实现，域名解析就是将域名重新转换为IP地址的过程。当应用过程需要将一个主机域名映射为IP地址时，就调用域名解析函数，解析函数将待转换的域名放在DNS请求中，以UDP报文方式发给本地域名服务器。本地的域名服务器查到域名后，将对应的IP地址放在应答报文中返回。但如果所请求的域名服务器不能回答该请求，则此域名服务器就暂成为DNS中的另一个客户，向根域名服务器发出请求解析，根域名服务器一定能找到下面的所有二级域名的域名服务器，这样以此类推，一直向下解析，直到查询到所请求的域名。



图 2-1域名www.×××.edu.cn解析流程

**权威服务器（NS服务器）**

对于一个特定的域名，必须将域名交由某个DNS服务器进行解析，才能将域名指向对应的IP地址，才能让客户通过域名访问对应的站点。这个负责最终解析域名的服务器就是权威服务器，即在图2-1中的miit.gov.cn。权威服务器与递归服务器不同，它不负责帮助客户端进行递归查询返回解析记录，它本身的用途就是对于域名进行解析设置操作。

每个特定的域名，权威DNS服务器可能并不相同。这种权威DNS服务器只对自己所拥有的域名进行域名解析，对于自己不负责域名则无法进行解析。比如递归DNS去taobao.com的权威DNS服务器查询baidu.com的域名肯定会查询失败。

一些大型的公司，对于权威DNS服务器可能会采用自建的方式。而对于一般的公司，大部分会将域名托管给比较知名的权威DNS服务商。中科三方云解析就是这类的服务产品。

**域名的别名（CNAME）**

别名记录（CNAME）也被称为规范名字。这种记录允许域名持有者将多个名字映射到同一台计算机。通常用于同时提供WWW和MAIL服务的计算机。例如，有一台计算机名为“cn.bluehost.com”（A记录）。它同时提供WWW和MAIL服务，为了便于用户访问服务。可以为该计算机设置两个别名（CNAME）：WWW和MAIL。这两个别名的全称就是“www.bluehost.com”和“mail.bluehost.com”。实际上他们都指向 “cn.bluehost.com”。同样的方法可以用于当使用者拥有多个域名需要指向同一服务器IP，此时使用者就可以将一个域名做A记录指向服务器IP然后将其他的域名做别名到之前做A记录的域名上，那么当您的服务器IP地址变更时您就无需每个域名更改指向了只需要更改做A记录的那个域名其他做别名的那些域名的指向也将自动更改到新的IP地址上了。举一个例子如下：

|  |  |  |
| --- | --- | --- |
| 别名 | 指向主机名 | 指向主机IP |
| www.bluehost.com | cn.bluehost.com | 127.0.0.1 |
| mail.bluehost.com | cn.bluehost.com | 127.0.0.1 |

表2-2

上面的主机IP为假设，以便于理解。当在浏览器输入别名www.bluehost.com 和mail.bluehost.com，等同于输入主机名cn.bluehost.com ，也等同于输入主机IP127.0.0.1。CNAME就是把别名指向（映射到）主机名。

**CDN服务**

CDN(Content Delivery Network)是指内容分发网络，也称为内容传送网络，这个概念始于1996年，是美国麻省理工学院的一个研究小组为改善互联网的服务质量而提出的。为了能在传统IP网上发布丰富的宽带媒体内容，他们提出在现有互联网基础上建立一个内容分发平台专门为网站提供服务，并于1999年成立了专门的CDN服务公司，为Yahoo提供专业服务。由于CDN是为加快网络访问速度而被优化的网络覆盖层，因此被形象地称为“网络加速器”。

简而言之，如果一个域名采用了CDN服务商，那么此域名背后服务器为用户提供所有信息内容都是通过CDN服务商的服务器转发到用户的主机上的。因此，这也是一个域名从解析到最终完成服务提供所必不可少的环节。

#### 1.2.1.2WHOIS服务相关理论

* **域名WHOIS服务理论**

WHOIS是一个基于TCP协议的面向事务的查询响应协议，被广泛的用于对互联网用户提供信息查询服务。WHOIS协议的具体标准在RFC3912，RFC1714中给出定义。域名WHOIS信息是其中重要的组成部分。域名WHOIS信息是基于RFC协议中WHOIS协议中非常重要的组成部分。域名WHOIS信息通常记录了域名注册者,拥有者,域名技术支持人员的相关信息，此域名的创建，到期与更新时间和域名DNS服务器，注册商及其它相关信息。简单说，WHOIS就是一个用来查询域名是否已经被注册，以及注册域名的详细信息的数据库（如域名所有人、域名注册商）。通过WHOIS来实现对域名信息的查询。早期的WHOIS查询多以命令列接口存在，但是现在出现了一些网页接口简化的线上查询工具，可以一次向不同的数据库查询。网页接口的查询工具仍然依赖WHOIS协议向服务器发送查询请求。WHOIS通常使用TCP协议43端口。每个域名/IP的WHOIS信息由对应的管理机构保存。域名WHOIS信息是描述域名特征非常重要的信息之一。

* **域名注册商**

域名注册商(domain name registrar)是一个商业实体或组织，它们由互联网名称与数字地址分配机构（ICANN）或者一个国家性的国家代码顶级域名（ccTLD）域名注册局委派，以在指定的域名注册数据库中管理互联网域名，向公众提供此类服务。包括域名的注册，续费，注销，转让及隐私保护服务。

* **域名**WHOIS**服务器**

域名WHOIS服务器是基于WHOIS协议中提供某些域名WHOIS信息查询的服务器。主要分为国家或地区WHOIS服务器与注册商WHOIS服务器两类。根据IETF标准 要求，WHOIS服务一般由WHOIS系统来提供。WHOIS系统是一个Client/Server系统。其中Client端主要负责：

1提供访问WHOIS系统的用户接口；

2生成查询并将其以适当的格式传送给Server；

3接收Server传回的响应，并以用户可读的形式输出。

Server端则主要负责接收Client端的请求并发回响应数据。作为Internet上核心服务之一的WHOIS服务，其Server端默认监听43号TCP端口，接收查询请求并产生响应。一般来说，Server端可以接收三种类型的信息查询：联系人、主机和域名。对于同一查询，Server端的输出应该具有一致性和稳定性。

#### 1.2.1.3量化评价国家双边关系理论

国际关系学的研究对象十分广泛 , 但其中一个最基本的研究对象是国家的双边关系 。随着这门学科的不断发展 , 国际关系研究从研究国家关系的性质变化逐渐走向研究国家关系的程度变化 , 从定性分析走向定量分析 。定量分析国家关系的基础是定量衡量国家的双边关系 。

要有效衡量国家双边关系友好或敌对的程度 , 核心问题是解决从事件赋值向关系赋值的转化 。我们的基本设想是 , 双边关系是由众多事件组成的 , 这些事件随着时间形成了一个 “事件流”, 对双边关系的衡量需要在事件累积和流动两个维度上同时进行衡量 。也就是说 , 对事件影响力进行累积是我们衡量的起点 , 测量事件影响力随时间流动的变化是衡量的过程 , 双边关系现状是衡量的终点 。从起点到终点之间的转化过程将是复杂的 , 因此将事件数值转化为双边关系数值的合理性 , 将取决于转化后的双边关系数值能否与实际经验相一致 , 至少要有很强的相似性 。为此 ,有如下定量衡量双边关系的流程 。

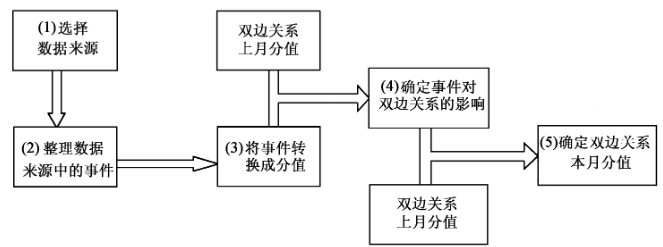


图 2-2 双边关系评估流程

在上图中 , 环节 (1) 是对数据来源进行选择 。从统计分析的角度来说 , 无须穷尽所有的公开数据来源 , 只要数据来源可靠就行 。例如 , 衡量中国与大国的双边关系 , 选择《人民日报》和中国外交部网站的事件数据就可基本满足需要 。环节 (2) 是将数据来源中与我们研究对象和研究范围有关的事件进行筛选和归类 。环节 (3) 是在 “冲突 —合作”这一维度上 , 根据对双边关系影响力的大小将已发生事件转换成一维的事件分值 , 即将当月发生的正负事件的分值相加 , 求得该月的事件总分值 。这一转换需按预先确定的事件分值表来实现 。设定事件分值表是为了保证转换过程具有较大的一致性和可比性 。  
环节 (4) 是把事件分值进一步转换成对双边关系的影响值 。环节 (4) 与环节 (3) 的区别在于 , 环节 (4) 的赋值需要考虑双边关系所处位置的影响 。这是因为 , 当双边关系的好坏程度处于不同水平时 , 同一事件对该双边关系的影响力不同 。例如 2001 年中美军机相撞事件 , 对两国关系产生了很大的负面影响 , 但是在朝鲜战争期间 , 中美间的一场空战就是平常事件 , 对两国关系的影响极小 。环节 (5) 是把由事件导致的双边关系的变化值叠加在上个月双边关系的分值上 , 得到当前的双边关系分值 。

#### 1.2.1.4 CRITIC赋权法的介绍

**概念**

CRITIC法是一种比熵权法和标准离差法更好的客观赋权法。

它是基于评价指标的对比强度和指标之间的冲突性来综合衡量指标的客观权重。考虑指标变异性大小的同时兼顾指标之间的相关性，并非数字越大就说明越重要，完全利用数据自身的客观属性进行科学评价。

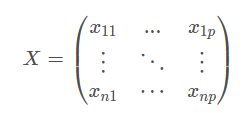
对比强度是指同一个指标各个评价方案之间取值差距的大小，以标准差的形式来表现。标准差越大，说明波动越大，即各方案之间的取值差距越大，权重会越高；

指标之间的冲突性，用相关系数进行表示，若两个指标之间具有较强的正相关，说明其冲突性越小，权重会越低。

对于CRITIC法而言，在标准差一定时，指标间冲突性越小，权重也越小；冲突性越大，权重也越大；另外，当两个指标间的正相关程度越大时，（相关系数越接近1），冲突性越小，这表明这两个指标在评价方案的优劣上反映的信息有较大的相似性。

**步骤**

假设有n个待评价样本，p项评价指标，形成原始指标数据矩阵：



其中表示第 i 个样本第 j 项评价指标的数值，例如：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **GDP** | **就业人数** | **财政支出** | **人均可支配收入** |
| 北京 | xx | xx | xx | xx |
| 上海 | xx | xx | xx | xx |
| 广州 | xx | xx | xx | xx |
| 深圳 | xx | xx | xx | xx |

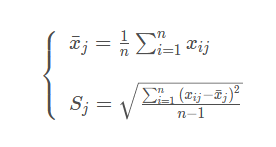
**（1）无量纲化处理**

为消除因量纲不同对评价结果的影响，需要对各指标进行无量纲化处理处理。

CRITIC权重法一般使用正向化或逆向化处理，不建议使用标准化处理，原因是如果使用标准化处理，标准差全部都变成数字1，即所有指标的标准差完全一致，这就导致波动性指标没有意义。

**（2）指标变异性**

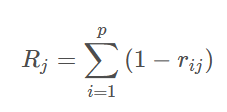
以标准差的形式来表现：



​ 表示第 j 个指标的标准差，在CRITIC法中使用标准差来表示各指标的内取值的差异波动情况，标准差越大表示该指标的数值差异越大，越能放映出更多的信息，该指标本身的评价强度也就越强，应该给该指标分配更多的权重。

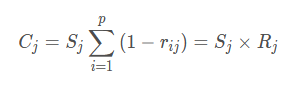
**（3）指标冲突性**

用相关系数进行表示



表示评价指标 i 和 j 之间的相关系数，使用相关系数来表示指标间的相关性，与其他指标的相关性越强，则该指标就与其他指标的冲突性越小，反映出相同的信息越多，所能体现的评价内容就越有重复之处，一定程度上也就削弱了该指标的评价强度，应该减少对该指标分配的权重。

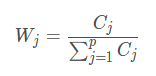
**（4）信息量**



越大，代表着第 j 个评价指标在整个评价指标体系中的作用越大，就应该给其分配更多的权重。

**（5）客观权重**

最终可以得到第 j 个指标的客观权重为：



举例说明最终效果如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **指标变异性** | **指标冲突性** | **信息量** | **客观权重** |
| GDP | xx | xx | xx | 0.42 |
| 就业人数 | xx | xx | xx | 0.23 |
| 财政支出 | xx | xx | xx | 0.15 |
| 人均可支配收入 | xx | xx | xx | 0.20 |

#### 1.2.1.5 层次分析法的介绍

层次分析法，简称AHP，是指将与决策总是有关的元素分解成目标、准则、方案等层次，在此基础之上进行定性和定量分析的决策方法。该方法是美国运筹学家匹茨堡大学教授萨蒂于20世纪70年代初，在为美国国防部研究"根据各个工业部门对国家福利的贡献大小而进行电力分配"课题时，应用网络系统理论和多目标综合评价方法，提出的一种层次权重决策分析方法。

该方法在本系统当中的应用方式如下：

**（1）比较权的确定**

将同一层次的各要素相对于目标要素进行两两比较判断，得出相对重要程度的比较权。

**（2）建立判断矩阵**

在确定各层次各因素之间的权重时，如果只是定性的结果，则常常不容易被别人接受，因而Saaty等人提出一致矩阵法，即不把所有因素放在一起比较，而是两两相互比较，对此时采用相对尺度，以尽可能减少性质不同的诸因素相互比较的困难，以提高准确度。如对某一准则，对其下的各方案进行两两对比，并按其重要性程度评定等级。为要素i与要素j重要性比较结果，**表2-3**列出Saaty给出的9个重要性等级及其赋值。按两两比较结果构成的矩阵称作判断矩阵。判断矩阵具有如下性质：

|  |  |
| --- | --- |
| 因素i比因素j | 量化值 |
| 同等重要 | 1 |
| 稍微重要 | 3 |
| 较强重要 | 5 |
| 强烈重要 | 7 |
| 极端重要 | 9 |
| 两相邻判断的中间值 | 2，4，6，8 |

表2-3比例标度表

**（3）计算出单层次权重**

计算判断矩阵的最大特征根以及相对应的特征向量，进行层次单排序，获得单一层次权重。

### 1.2.2总体工作内容介绍

本系统的完成工作涉及到以下五个方面：

1. **基础数据的获取**：获取大量域名资源，为模型确定进行基础数据支撑。
2. **双边关系分值确定的方法：**为了更好的满足本系统的需求，双边关系分值确定的方法应该能够正确地表示两个国家之间的关系，且必须要具有时效性。
3. **域名属性值的计算**：获取域名A记录、NS、注册商、CNAME等属性的国别信息，利用双边关系数据库为上述属性赋值，通过CRITIC和层次分析法AHP确定了计算公式中各项权重，并将权重代入公式计算出域名的属性值。
4. **域名风险评估**：根据域名属性值对域名的解析风险进行评估，基于域名属性值、域名流量以及所属机关性质确定公式计算影响值，根据影响值给出合理化建议。
5. **展示系统的完成：**使用基于JS的Vue3框架编写前端，基于python的Django框架编写后端，在执行用户查询的域名后以合理清晰的方式将结果直观地展示出来。

## 1.3特色描述

本系统的实现是基于对域名所属的所有实体对应的国家使用一种双边关系打分方法，所以本系统的特色有如下几点：

一、创新性

首次提出了，综合了域名服务相关多维度属性，进行打分的评估体系。具体而言就是创新性地对域名解析时的相关实体进行了合理评估，有助于让域名拥有者全面了解域名解析路径以及服务提供过程上的风险性。

二、实用性

本系统的评估结果具有从点到面的全面参考价值，从点来看，各种类型的企业，政府职能部门都可以根据本系统单一域名查询功能，了解到自己所管理或拥有域名在关于能否被正常解析这一问题之上的风险情况，并且跟据系统所给建议，可以采取进行服务商迁移等措施来提高域名的安全性，以降低当国与国冲突发生，国家级域名制裁到来时的损失。

从面来看，国家管理域名的相关机构，可以根据本系统的批量域名查询功能所现实的结果，对国家域名整体的安全性有一定的了解。并且颁布一些可以提高国家总体域名安全性的倡议或者方案。

三、可扩展性

具有较强的可扩展性，本系统设计的是一种针对域名背后实体实现综合评估的方法，如果今后需要修改评价的内容与评价的目的，只需要对模型进行稍加修改，选择不同的评价赋分标准即可。

四、数据时效性

一方面而言，实体背后对应的国家分值的确定是依据两国之间可以影响双边关系改变的重大事件，有合理的计算公式，注重事件的时效性。

另一方面而言，域名服务相关多维度属性，可以在系统中进行实时的获取，在域名经过整改之后也可以了解到最新的情况。

1. 评估合理性

本系统采用了主观赋权与客观赋权相结合的方法，综合其优势，使得各项属性的权重确定更加合理。

根据域名的性质类型（如政府，民用等）以及网站的日流量再结合以上所确定的域名得分确定了合理的公式计算其影响值，以更加贴合实际地为域名拥有者给出建议。

## 1.4应用前景分析

### 1.4.1国家网络安全对抗

数据主权已成为美国、欧盟、以及多国的共识和行动（包括立法和治理），尤其是在“棱镜门”之后成为“重中之重”的聚焦点。不实施数据主权原则，不仅数据安全和隐私处于危险之中，而且国家数据资产也无可避免地受到威胁。

美国与中国的对立的情况越来越严重，目前已经延伸到互联网领域，例如以国家安全威胁理由，限制“抖音”在美国的运作。预计在网络空间中的数据主权的问题，会越来越凸显，特别是，美国现在使用政治手段强制进行互联网的管理。

域名作为互联网的核心资源之一,国家需要对自有的域名，特别是重点域名的数据主权了解清楚，同时发现**潜在的数据泄漏和安全等问题**。当在域名方面，真正发生中美对抗时，中国能够提前部署与防护自身。另外，目前很多重点域名在某些域名的数据主权上不可控，例如使用国外CDN和权威服务器，易导致数据泄漏和无法解析等。再比如，一些托管网站的IP属于境外服务器，易导致数据泄漏等。特别是，很多中国国内可访问的网站，未备案以及主机未在境内。

* **潜在攻击**是指境外势力通过其可控的某个或某些域名主权属性进行攻击， 攻击形式可能包括拒绝服务、篡改或删除等，达到域名无法正常服务的目的。
* **数据泄漏**是指境外势力，利用其可控的域名主权信息，直接强制将域名的数据获取，域名的拥有方（中国）无法控制，或不知。例如，某域名的Web服务器是境外，或使用境外的CDN，境外组织可以直接获取Web服务器的数据或CDN的数据。

从另一方面而言，采用本系统的框架，可以完成对外国域名信息的获取。改变双边关系对应分值，即可完成对外国域名进行得分评估。因此，运用本系统分析某一敌对国家域名的情况，即可以寻找出那些薄弱的域名，进而对其进行数据泄露获取有用的信息，或者瘫痪其解析路径上重要环节，使之无法提供服务。

### 1.4.高风险域名的备案与治理

国家相关机构，可以使用本系统评估出那些在解析路径上风险较高的域名，进行备案，监控等，以便在国家级域名制裁到来时进行快速的应对。与此同时，在政府机关与银行企业这些至关重要的机构使用的域名中，对于那些风险较高的，国家相关机构可以勒令其进行整改，以规避潜在数据泄露的风险。

### 1.4.3域名异常解析时，及时发现某级问题

由于本系统能够获取一个域名解析环节所有的信息，因此，在某一域名出现解析故障导致用户不能访问的时候，可以综合本系统获取到的与此域名解析相关的各项属性，进行即时的排查，找出问题所处在的环节。

### 1.4.4分析新注册域名的情况

鉴于本系统可以进行快速，实时信息获取的特性。经过一定程度的扩展之后，可以完成对新注册域名情况的实时分析，进而了解新注册域名是否安全，以及总体分析某一时间段上注册域名的安全情况，乃至可以通过数月至一年的情况检测，来判断域名的注册者是否有逐渐意识到，在与域名服务相关的属性上，选择属于安全国家的服务商的重要性。

# 作品设计与实现

## 2.1系统功能流程

图1是本系统实施的整体功能流程示意图，系统以大量域名基础数据为基础，识别出域名的所有网络实体后确定域名得分计算公式，而后使用双边关系数据库中的数据赋值进行后续的评估。

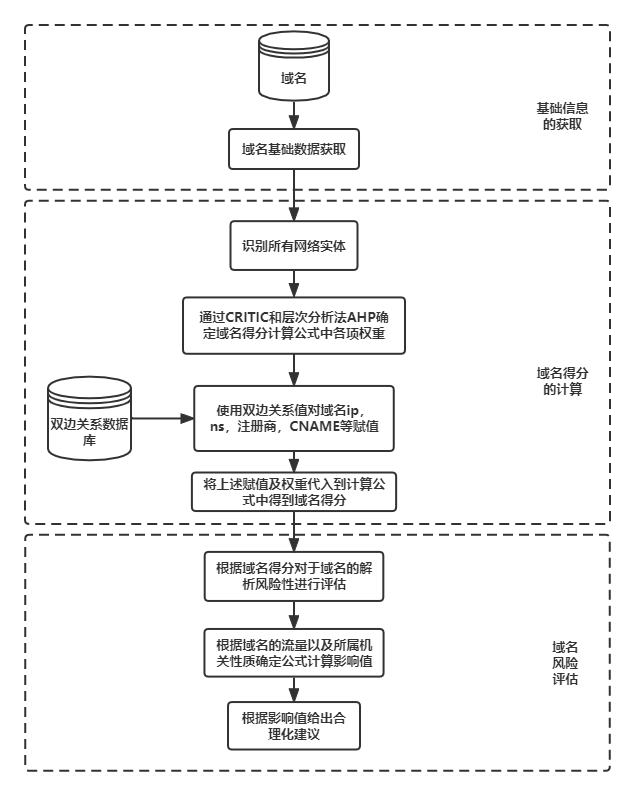
****

图1 整体功能流程示意图

下面是图中的符号说明

**1.基础域名数据集：**该数据集涵盖了Alexa排名前十万的中国域名，并且这些域名可以正常访问。

**2.域名基础数据获取：**获取域名的基础数据，包括域名NS服务器、域名IP及其所属国别、域名CNAME记录、域名顶级域基础信息（如域名根服务器所属国别）、域名CDN服务商及其国别、域名权威服务商及其国别。

**3.识别网络实体：**从基础数据中识别出与域名相关的网络实体，即域名注册商的国别、域名IP地址的国别、域名CNAME记录、域名根服务器所属国别以及域名所有NS信息，以上的所有实体在本方法中都会有一个分值。

**4.双边关系数据库：**该数据库来自于网络上各种权威机构对中国与其他国家及地区的双边关系值。

**5.双边关系值：**该数值取自于双边关系数据库，衡量的是两个国家之间的关系好坏程度，域名的所有实体的赋值都依赖于它。

**6.域名得分：**该值是域名解析风险性的度量值。

**7.域名得分计算公式**：通过CRITIC方法和层次分析法合理地确定了域名所有实体在计算公式中所要乘以的权重，将实体值代入计算便可以得出该域名的风险值。

**8.域名风险评估：**根据得到的域名得分对于域名的解析风险性进行评估，域名得分越低则说明域名解析风险性越高。

**9.影响值：**用于衡量域名遭受到攻击时所受的影响程度，主要根据域名流量以及域名性质（例如党政军，再例如，银行，娱乐等）计算。

**10.给出合理化建议：**根据域名的实体中分值与对应权重之积较低的给出相关建议（如权威服务商一项分值最低，则建议更换权威服务商等）

## 2.2系统核心功能实现

下面结合实施实例对本系统展开进一步的描述。针对不同的域名以及不同类型的域名，提取其各项属性背后的实体国家信息，然后依评分公式建立评分模型进行，最终分析得分结果以及提出改进建议，主要包括以下几个步骤：

### 2.2.1获取域名及其背后实体所相关的数据

在系统接收到输入的域名后，通过处理域名模块，判断输入的域名从字符组成上是否正确，如域名是否格式合法，顶级域是否存在。若检测到域名为合法的域名，则将合法的域名通过域名筛选模块，提取域名对获取各个部分信息的有效部分，分别送入不同的信息获取模块中，如将域名的顶级域提取，传入顶级域信息匹配模块，将一级域名提取，传入域名相关NS信息获取模块。

　　而后域名相关信息获取模块开始工作，系统会使用以下几种方式进行收集信息：

1.域名WHOIS查询，域名WHOIS信息是基于RFC协议中WHOIS协议中非常重要的组成部分。域名WHOIS信息通常记录了域名注册者、拥有者、域名技术支持人员的相关信息、此域名的创建、到期与更新时间和域名DNS服务器、注册商及其它相关信息。域名WHOIS信息中注册者相关信息与部分域名相关信息对描述域名特征有重要的作用，并能够为其他模块提供数据来源与基础。通过解析原始WHOIS记录，提取出WHOIS信息的关键字段，作为域名的特征项。

2.域名DNS记录递归查询，域名DNS记录递归查询可将域名的所有NS服务器以及其IP和其别名的NS服务器和IP查询出来，特别地，针对域名的NS服务器属性，因为这存在层级的关系，即解析目标域名的NS服务器NS1也需要NS服务器NS2来解析，因此，域名的NS服务商信息不仅与NS1有关，也与NS2有关，所以我们采用了递归的方式获取信息，足够反映这种层级关系。

3.IP地址的物理地址查询，IP定位的基本原理是利用IP设备的名字、注册信息或时延信息等来估计其地理位置。定位算法设计的基本原则是:在保证定位精度的前提下,尽量减少测量开销,同时兼具良好的扩展性,并能保护用户隐私.最初的定位算法通过向DNS服务器查询或者挖掘隐含在主机名中的信息来推测IP设备的地理位置。之后,一些定位算法根据时延与地理距离之间的线性关系来估测主机位置,并通过拓扑信息来减小定位误差。

4.域名CDN服务商查询，CDN服务商的查询是利用域名IP所有者查询工具以及利用HTTP头、CNAME记录、WHOIS信息综合分析出来的。

接下来，系统通过各个域名相关信息获取模块，获取到各项实体信息的国家属性，比如域名IP的物理地址在某国，域名的CDN服务商是某国的公司，能解析该域名的NS服务器属于某国的公司，该NS服务器的物理地址在某国等等。为了加快获取速度，我们在系统中搭建了分布式架构，编写了用于分配任务与调度的MANAGER模块和负责执行获取的WORKER模块。

最后一步是将上面所获取的域名及其对应信息存入事先建立好的数据库中，至此便完成了域名相关基础数据的获取。

### 2.2.2确定域名评分公式

首先，对于域名的每个属性（包括注册商，顶级域，NS服务，别名，物理IP地址，CDN服务商）都有独立的得分,我们将其分别规定为A1-A6。

下面，是具体的确定A1-A6的计算方式以及含义。对于提到的国家分值表，将在后面做详细的介绍。

A1 = 域名注册商公司或机构的所属国家对应分值表上的得分

A2 = 域名顶级域对于的顶级域服务器所在国家对于分值表上的得分，如com的顶级域服务器在美国，那么[www.baidu.com的A2](http://www.baidu.com的A2) = 美国对应分值。

A3 = ，n为可以直接解析域名的NS服务器数目。在求和式中的每一项（）表示与一个NS服务器相关的得分，其中为域名xxx.xxx.xxx对应的一个可以解析它的NS服务器ns1.xxx.xxx的直接得分，由该服务器本身的属性决定，具体计算方式为：

= 0.7\*此服务器IP地址对应物理地址的国家在分值表上得分+0.3\*此服务器所属公司对应的国家在分值表上得分。

所表示的是，如果将NS服务器ns1.xxx.xxx作为一个原域名，依照此方法对该域名NS属性打分的分数，反映了NS服务器地址有时需要被另一层NS服务器解析的情况。这是一个递归的过程，终止条件是此NS服务器可以直接被TLD（顶级域）服务器所解析，此时，该NS服务器的相关得分不再按照（）计算，而是直接为。

A4 =（ \*别名注册商所属国分值 + \*别名的NS服务分值（计算方式如A3））

其中，n表示一个域名别名的个数。A4部分表示了一个域名的别名，如[www.baidu.com](http://www.baidu.com)的别名[www.a.shifen.com](http://www.a.shifen.com)背后与域名解析相关属性的得分。

A5 =）

A6 = 该域名背后CDN服务商所属国家对应得分

下面，图2将以www.tmall.com为例，说明A1 - A6的获取与计算流程

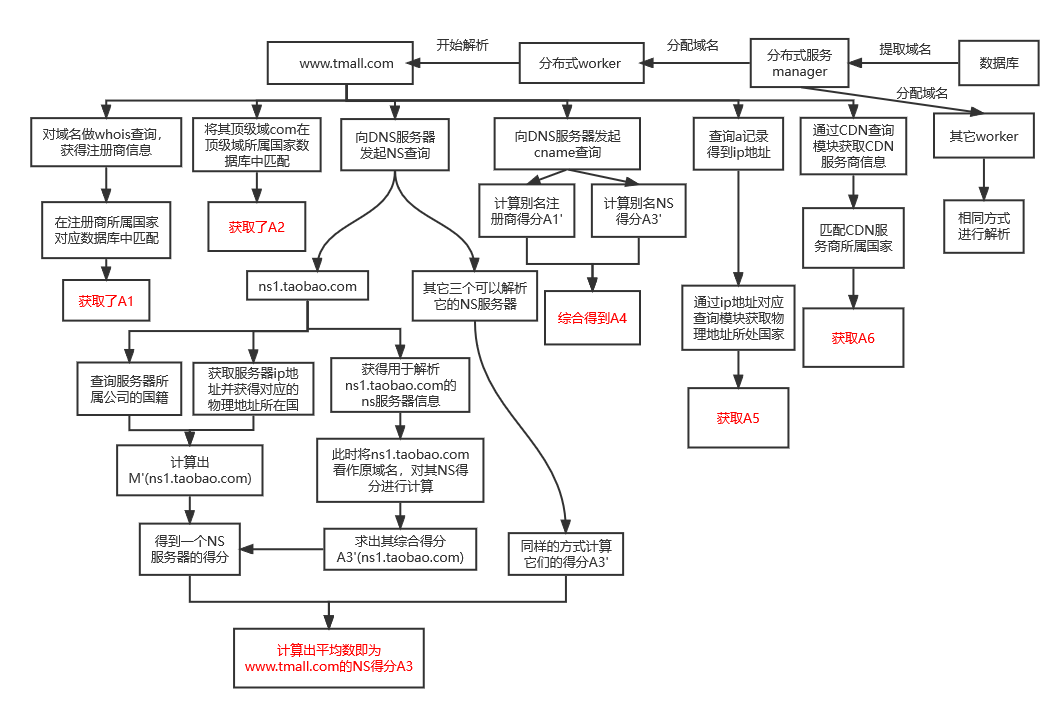


图2 实例www.tmall.com分析

至此为止，一个域名的单项得分A1-A6的确定是根据域名背后实体的国家属性，但需要注意的是，一个域名单项属性的安全性，不仅仅是与所选服务公司或企业本身的国籍有关，同时也与企业的自发行为有着很大关系。比如说，在俄乌战争期间，一些美国的域名注册商，比如Namecheaper宣布对俄域名展开制裁，但另一些注册商，出于利益原因，并未开展制裁活动。因此，尽管两者都是来自美国的注册商，他们的风险等级是不相同的，这一点需要在域名的单项得分上得到体现。

我们注意到不可忽视的一点是，即使是选择了国内的公司做为服务机构，这也并不代表这项属性就是完全安全的，因为还有可能发生网络攻击或者服务瘫痪等恶劣事件。比如百度公司在2010年由于baidu.com域名的DNS记录在美国注册商register.com处被非法篡改，导致域名无法被解析。

因此，我们需要按照具体服务公司的历史表现对域名属性的单项得分进行修正。在这里我们采用了黑名单机制。记录那些出现过重大威胁服务安全事件，以及进行过制裁行动的企业。如果一个域名选择了这些企业做为服务商，则对应属性将会有一定的减分，最终得到修正后的

减分的标准如下表:

|  |  |
| --- | --- |
| 公司或企业行为 | 对应分值 |
| 宣布对他国域名停止服务(不论种类） | -2 |
| 出现过严重规模的安全问题事件 | -2 |
| 官方宣布对他国表示谴责 | -1 |
| 出现中小规模的安全问题事件 | -1 |

在上述工作给出了A1-A6的六项得分之后，我们需要建立基于单项得分的综合评价模型并给出最终的评价。最终评价将会分为以下两个方面：一是绝对安全得分，二是相对安全得分。

由于从域名解析到域名背后的服务为客户所用是一个紧密相关的流程，所以，域名任意一项属性所对应的服务被拒绝，或者应服务的服务器数据被盗取，都将造成不可估量的损失。因此，我们设置了绝对安全得分来描述这一性质。该得分用P1来表示。

A1-A6中有任意一项小于0时则P1等于0。在其他一般情况下的计算公式为:

P1得分可以帮助我们判断出有风险域名和绝对安全的域名。当P1<0时，我们认为该域名是存在风险的，当P1>0时，我们认为该域名的各项属性，从国家层面来看是安全的。解释为只要域名的一项属性背后的实体国家是与中国不友好的国家，如即使[www.xxx.com](http://www.xxx.com)的注册商，顶级域背后机构全部在国内，IP地址对应的服务器也在国内，但是域名的DNS解析路径必须通过国外的NS服务器进行解析导致了A3<0，那这个域名的P1将会等于0，说明该域名存在风险。

此外不可忽视的是，在现实情况中，一个评估系统不仅需要识别出风险，还需要给出风险的等级，如上步提到一个只有A3<0的域名，但实际上这个域名的风险是很小的。

因此，我们又给出了相对安全得分P2的定义。

=

其中是各项属性的权重

特别地，当域名属性不存在，如一个域名不存在CDN服务,也没有别名时,此时该域名的, 直接按原式计算结果并不准确因此，我们需要对原来的P2进行修正，方法如下：

P2（修正后） =

而对于的值的确定，我们使用了层次分析法与CRITIC法。在查阅资料并且咨询专家后，我们用层次分析法给出了代表域名各项属性在解析时重要性的主观权重向量

然后在Alexa上选取国内访问量高的一部分域名，搜集其各项属性信息，并用公式计算各个域名 A1-A6得分，而后用CRITIC法对数据分析，得出了客观权重向量：

CRITIC法的基本思路是确定指标的客观权数以两个基本概念为基础。一是对比强度，它表示各个域名的同一指标取值差距的大小，以标准差的形式来表现，即标准化差的大小表明了各个域名的同一指标取值差距的大小。二是评价指标之间的冲突性，指标之间的冲突性是以指标之间的相关性为基础，如两个指标之间具有较强的正相关，说明两个指标冲突性较低。选用此方法可以有效的平衡数据本身分布对评分结果带来的影响，

比如一个域名IP对应的物理地址大多情况下与CDN服务商的国家直接挂钩，在CRITIC法的处理下，物理地址对应权重和CDN服务商对应的权重总和将会变小。又比如绝大多数域名的NS服务商都选择了中国，导致NS得分这项值在不同域名间差异很小，用CRITIC法处理后将会减少NS得分的权重,因此，可以突出其它差异较大属性对域名得分的影响，使评价结果对比鲜明，更加客观。

最后，采取主客观结合法的方式，按照 计算出权重，至此我们完成了域名评分公式的确定。

下面是域名背后各项属性重要性以及最终权重的确定的一个具体示例：

通过层次分析法与CRITIC法确定出w1- w6的值。

先通过查阅资料并且咨询专家，用层次分析法给出了代表域名各项属性在解析时重要性的主观权重向量[a1 a2 a3 a4 a5 a6]

主观部分的权重是根据域名的各项服务被服务商停止或者人为禁止之后，能否有反制措施，以及反制措施实施起来的成本来确定的。

首先，域名的注册商占有最重要的位置，注册商几乎承担了从域名的注册，到域名管理，最终为用户提供服务的各项任务，如在各级DNS服务器上登记域名的NS记录，登记域名背后提供服务的IP地址以及对域名提供的服务实施监督和管理等等。如果一个域名的注册商将域名设置为不可被解析的状态，同时禁止该域名迁移注册商，那么这个域名将完全不可用，并且域名持有者基本上没有任何措施对此进行反制。不仅如此，如果域名的各项信息比如各种DNS记录在注册商处遭到恶意的篡改，也会对域名持有者造成不可估量的损失。

其次，是域名的IP地址，NS服务商，CDN服务商以及别名。这些属性是域名用户可以较为方便得进行更改的，因此在遭受制裁或者攻击后影响较小。如域名持有者可以在NS服务商停止服务之后去寻找新的NS服务商，并且向域名的注册商进行登记，修改NS记录，即可完成反制，即使在找到替代服务商之前仍然会造成一些损失，比起在注册商直接将此域名标为不可解析状态，影响无疑小了很多。

最后，才是域名的顶级域部分。相较于以上的各项属性，采用属于外国顶级域的风险将会小很多。原因有以下两点：首先，域名的顶级域服务商在历史上从未有过封禁顶级域解析，即不允许根名称服务器解析特定域名的行为，即使在几年前制裁伊朗域名时，美国也是通过修改域名注册商信息来完成的。其次，我国有着完备的镜像根名称服务器体系，即使域名遭到国外根名称服务器的禁用，域名解析也可以在国内的镜像服务器上完成。

基于以上分析，给出的层次分析法打分矩阵如下：



得到主观权重如下：

[0.545,0.022,0.113,0.045,0.145,0.130]

之后，以国内Alexa排名前十万的域名为样本，对各项属性进行CRITIC法权重确定。得到客观权重如下：

[0.048,0.3518,0.2118,0.0488,0.2568,0.0858]

最后，得到了最终权重如下：

[0.296,0.188, 0.162, 0.046, 0.201, 0.107]

在所有的权重确定以后，我们接下来要制订出域名P2得分所处区间的相关描述表，该表可以对域名的相对安全得分做出初步的解读，如域名风险很低，风险较低，或者是风险严重等，是比较概括性的描述。

我们会试运行大量的域名，得出他们的P2得分，根据得分的总体分布情况，以及具体的得分值含义来制订此表。如分数x1为后10%的得分，那么得分小于x1即可被视作有严重的风险，但同时，一个域名的中如果有五项都小于0,不管该域名P2分数，也将被归为具有严重风险。

### 2.2.3确定国家分值关系表

在我国对双边关系的定量研究中，阎学通教授团队所研究的动态衡量双边关系的方法**[[[2]](#endnote-2)]** 能够较好地本系统的需求，以下是该方法的具体实现：

**步骤1，选择来源数据**

在各大官方平台（如中国外交部官网、人民日报等），以双边关系为关键词，爬取中国与目标国家间发生的事件以及事件发生的时间。

**步骤2，双边关系分值标准的设定**

该方法设定双边关系变化的分值范围为-9到9, 其中, -9代表两国关系最恶劣的情形, 9代表两国关系最友好的情形, 这是两种极限情况。两者的中值为0, 它表示两国关系处于绝对的非敌非友状态, 两个毫无关系的国家之间的关系可视为这种状态 (如柬埔寨与布基纳法索的关系) , 或是双边关系中的合作与冲突是绝对地各占50%的情况。双边关系在极端敌对或友好的状态下受事件影响的敏感性弱, 在绝对非敌非友状态下受事件影响的敏感性强 (参见图3) 。双边关系的这一客观特征, 在进行数值衡量时表现为, 双边关系的分值越接近0, 事件使双边关系分值变化的范围越大, 而双边关系分值越接近9或-9时, 事件使双边关系分值变化的范围越小。根据这一特征, 该方法采取逐级递减0.1的原则, 设定了从中值0到9和-9非等距间隔的国家双边关系数值标准。

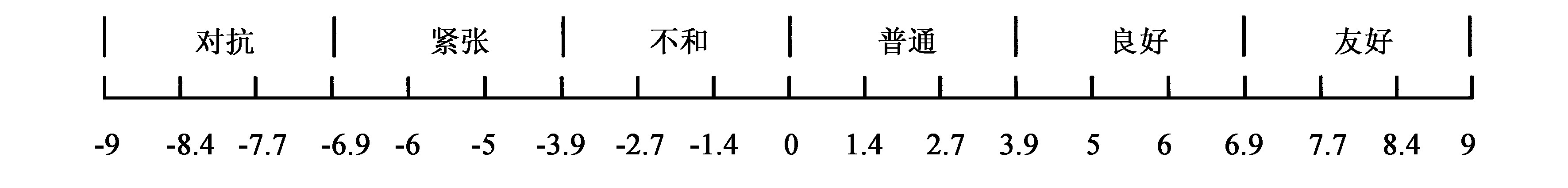


图3 国家双边关系数值标准

**步骤3，事件分值表的设定，**

为了避免赋值的随意性, 该方法依照事件数据分析中的通行做法, 设定一个确定的事件分值表来保证赋值的一致性。在事件数值分析中, 比较具有代表性的分值表有阿萨尔—斯隆分值标准、戈尔德施泰因分值标准和“世界事件互动测量”分值标准。但这些分值标准主要是用于分析冲突行为, 无法用于衡量双边关系, 为此该方法制定了一套与双边关系分值标准 (图3) 相一致的事件分值标准 (参见附录) 。设定这个事件分值表时, 我们坚持了完整性和排他性两个原则。完整性是指可能选取的事件都能按分值表赋予分值;排他性是指同一事件只适用于一个分值, 避免同一事件归入两个以上类别的可能。事件分值表是根据经验确定的, 但是在它确定以后不再改变, 从而避免了赋值的主观性和随意性。对初步得分进行归一化处理，加上中国得分，得到最终的国家关系分值表。

**步骤4， 事件影响力分值的计算，**

事件对双边关系分值的影响力取决 于本月两国关系中的事件和两国关系上月的分值这两个变量。事件的作用是使两国关系发生变化 (变好或变坏) , 但这种变化是在现有两国关系基础上发生的。在不同关系水平的基础上, 相同事件对两国关系的影响力不同。例如在两国关系已经很友好的情况下, 首脑会晤对双边关系的改善作用是很有限的。而在两国关系不好的情况下, 举行一次首脑会晤, 或者签订一项合作条约能起到明显改善双边关系的作用。为了解决事件在不同关系水平上的影响力不同的问题, 该方法根据双边关系分值标准 (图3) , 设计了如下的事件影响力计算公式:

表示事件在两国关系为时的分值

表示两国关系变化范围的绝对值

表示事件发生时两国关系的初始值

表示事件在事件分值表中的分值

因为两国关系的变化范围是[-N, N], 因此的取值范围为[-N, N], 在该方法中的取值范围为[-9, 9]。

上面的公式具有如下特点: (1) 当事件对两国关系起正向推动作用时, 即当时, 随着初始位置从对抗向友好的方向移动, 事件的正向推动作用逐渐减小。当两国关系达到最友好状态时, 正面事件的正向推动作用为0。例如, 1971年尼克松总统访华之前, 中美在越南战场上是敌对方, 美国总统尼克松访华使中美关系发生了质的变化, 而中美建立了正式外交关系后, 美国总统里根访华对双边关系的推动作用就远远小于尼克松访华的作用。 (2) 当事件对两国关系起负向推动作用时, 即当时, 随着两国关系初始位置从对抗向友好方向移动, 事件的负向推动作用逐渐增强。在两国关系最紧张的情况下, 负面事件的负向推动作用为0, 即任何负面事件都不能使两国关系的数值小于-。例如, 2000年美国总统小布什上台, 此时中美关系是非敌非友, 因此撞机事件使得双边关系严重倒退, 但在1965—1971年间援越战争时, 双方互为敌手, 中国军队在越南战场上打下美国轰炸机或是美军轰炸中国防空阵地, 对双边关系都没有重大影响。 (3) 当两国关系处于零位置, 即初始值为0时, 事件影响力分值等于事件分值表中的分值。 (4) 该公式具有对称性。当与的数值相同且符号相反时, 意味着推动力相同, 但方向相反。

**步骤5，两国关系当前分值的确定**

两国关系的本月分值等于两国关系的上月分值加上由事件引起的本月两国关系的变化值。上月分值的确定又依赖于上上个月的分值, 这意味着有了上上个月的分值才能获得上个月的分值。这一逆推过程可以是无休止的, 于是产生了第一次主观确定的初始值误差影响以后分值计算准确性的问题。该方法设计的影响力公式具有一种纠偏能力, 随着统计时间的延长可以纠正初始值误差, 从而解决了确定上个月分值的准确度难题。

### 2.2.4评估域名遭到攻击的影响以及给出建议

首先是评估域名影响力，我们利用Alexa等平台获取了一个域名的访问量a。手动输入或者根据域名对应网站出现的关键词判断出域名对应服务的类型，如社交媒体娱乐网站，银行或商业机构官网，党政军网站。

评估出域名影响力。的计算公式因服务类型而异，且与访问量直接挂钩。

如计算娱乐网站时，，而计算银行，购物网站时。

而后是在系统中给出改进建议。在这一步中系统会先选出A1-A6得分中乘以权重w后最低的项，将此项的分值赋值为在国家分值表中我们国家所对应的得分。然后重新计算域名的P1以及P2，与原得分进行对照。最终给出如：“将此域名迁至国内注册商管理下，相对风险得分将会被优化27%”的建议。

## 2.3 系统界面设计

### 2.3.1 系统技术栈介绍

**前端**：采用最新的Vue3.js框架，相较于Vue2.js运行速度更快，编译所占体积更小； ElementPlus组件库，是传统组件库Element-UI的升级版，更好的支持Vue3.0；Typescript，与传统的Javascript而言，ts支持类型检查，更好的代码风格有利于后期升级与维护；Echarts绘图，一个基于 JavaScript 的开源可视化图表库； Vuex4状态管理工具；Axios，基于传统Ajax封装的前端网络请求库。

**后端**：Django框架，采用传统MVC模式，有完整的路由系统，安全性更高；一些python的依赖库，例如beautifulsoup4、dnspython、numpy、whois、pandas等。

**数据库**： MongoDB分关系型数据库。

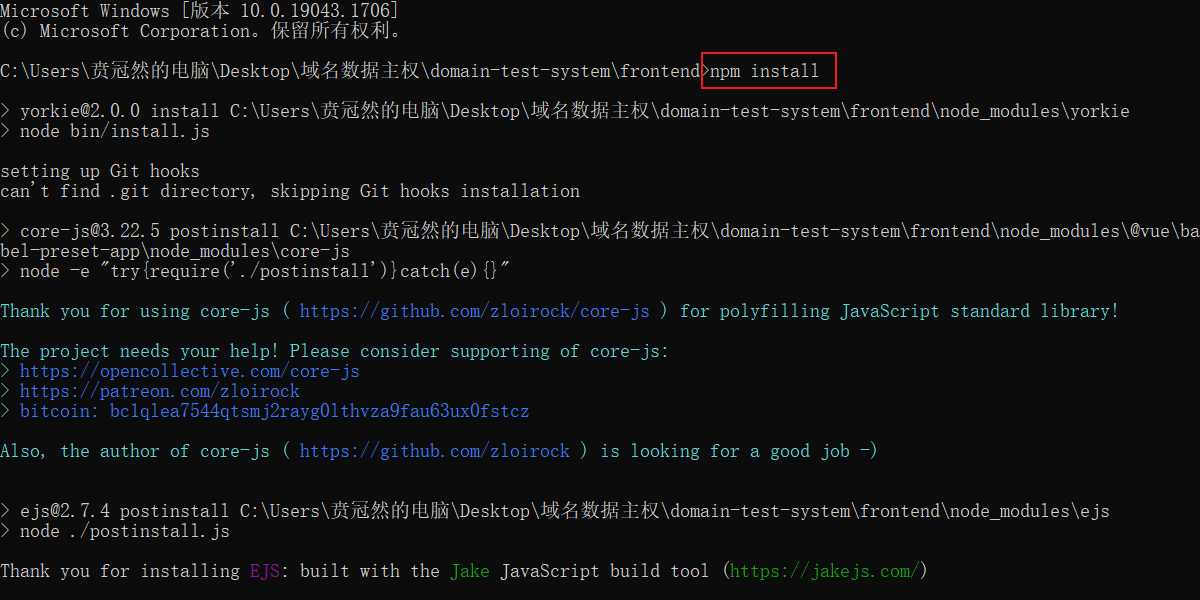
**其他**：git分布式版本控制系统、gitee代码托管仓库。

### 2.3.2 系统运行说明

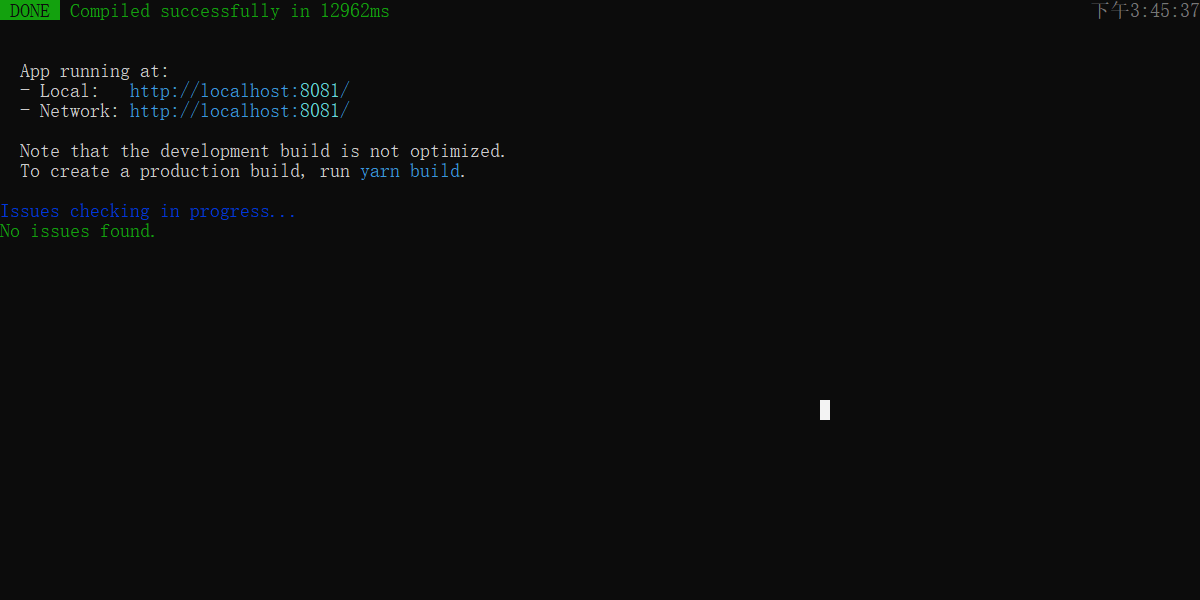
**以Windows系统为例:**

前端：

1. 在Nodejs 环境下，进入前端项目根目录/frontend，打开终端，输入命令**npm install**安装项目所需依赖。



1. 依赖安装完毕后，再次输入命令 **npm run serve**，启动前端项目。



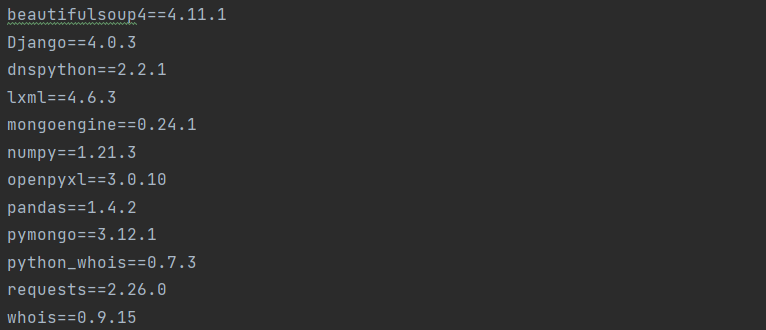
1. 在浏览器(推荐chrome)输入**<http://localhost:8081/>** 预览项目。



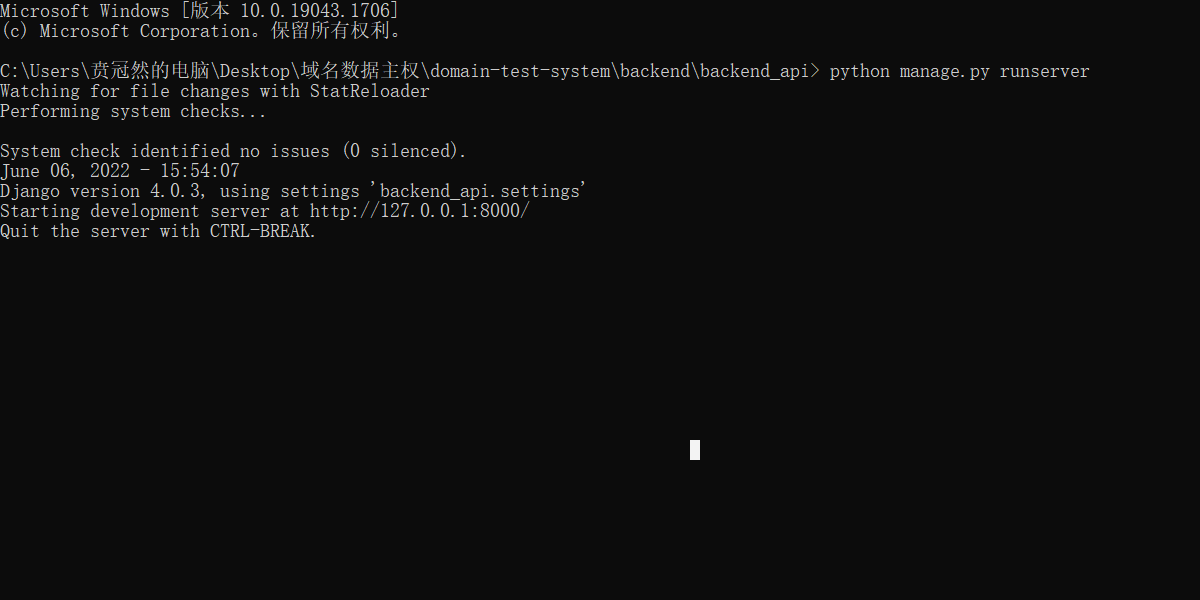
后端：

* 1. 在后端项目运行根目录 /backend/backend\_api 打开终端，输入命令**pip install -r requirements.txt**安装项目所需依赖。

项目所需依赖如下图：



* 1. 再次输入命令 **python manage.py runserve** 启动后端项目

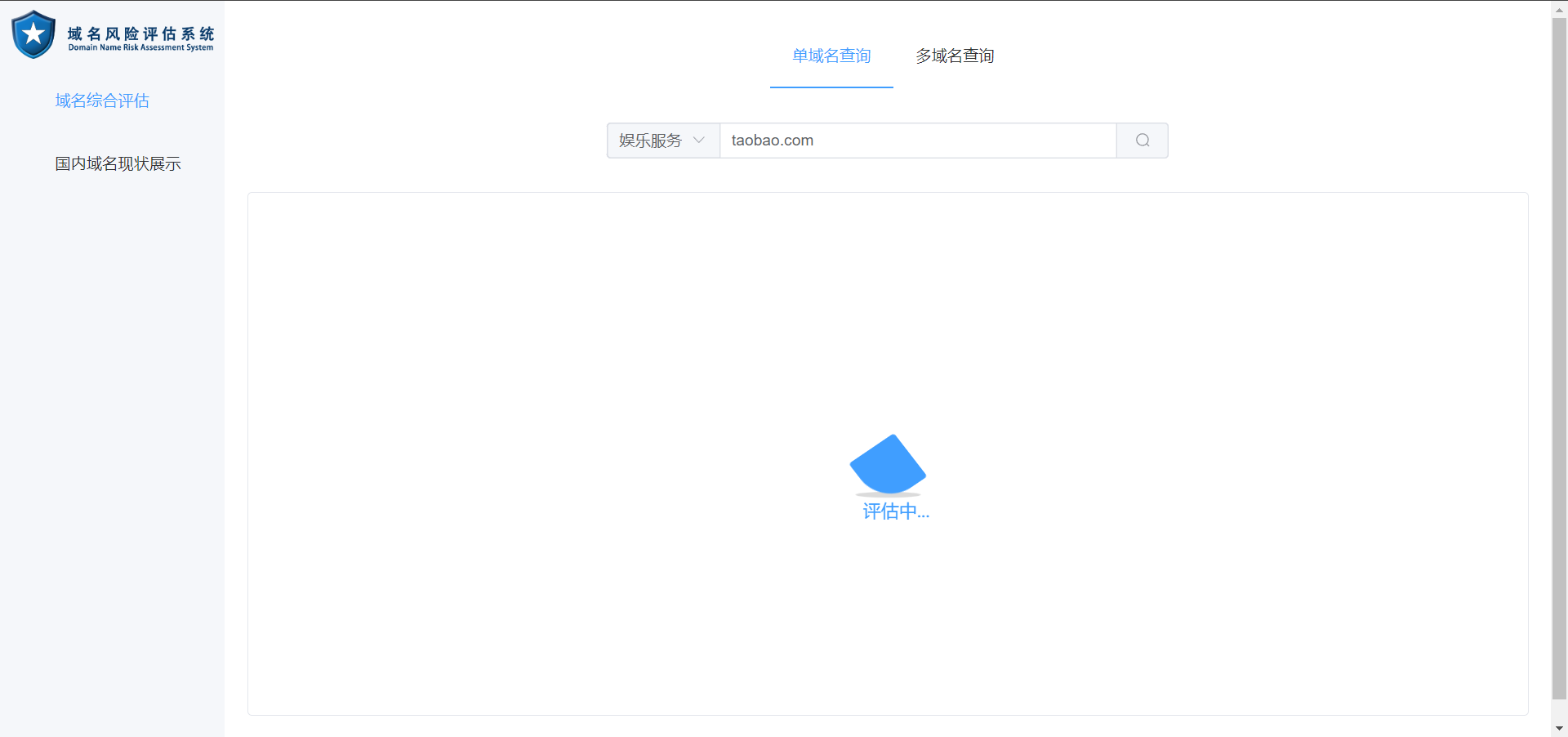


### 2.3.1 系统运行展示

单域名查询主界面(未查询状态)，输入域名和域名类型即可进行域名评估，如图2-1



评估过程中使用动画缓冲，缓解用户等待焦虑，如图2-2



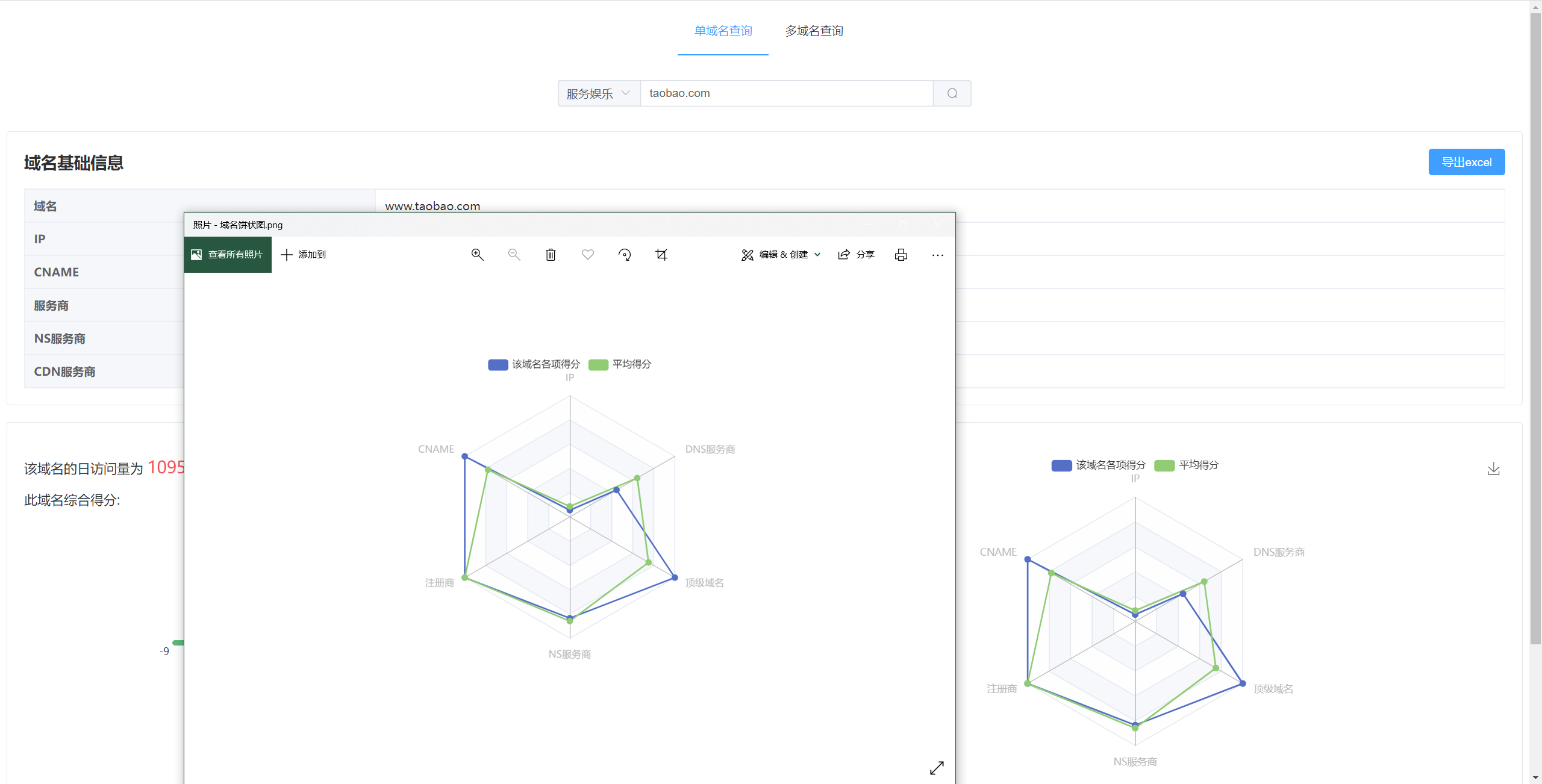
单页面查询结果展示，包含了所评估域名基础信息，综合评估，以及具体分析。如图2-3.

其中基础信息包括域名IP、CNAME、服务商、NS服务商、CDN服务商；综合评估包括该域名的日访问量、综合得分、以及该域名的各项得分与该类域名平均各项得分的雷达图，旨在突出该域名六大核心指标相较于平均水平的高低，进而找到域名的安全性问题。

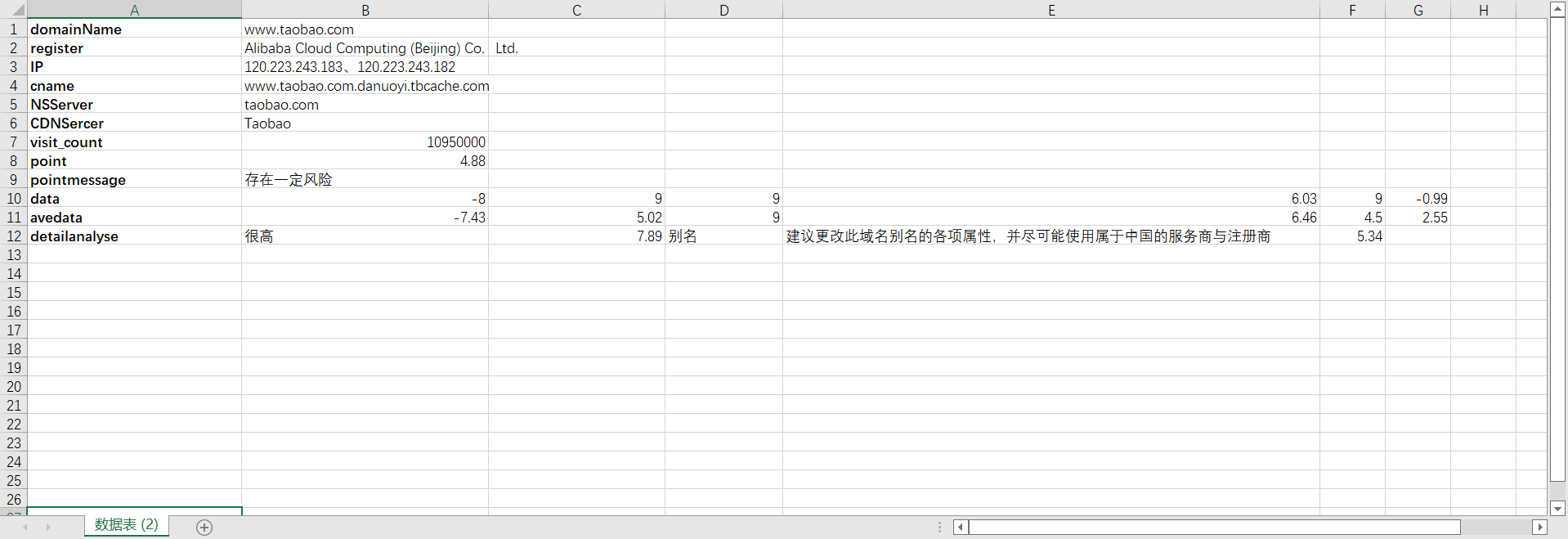




下载结果图：

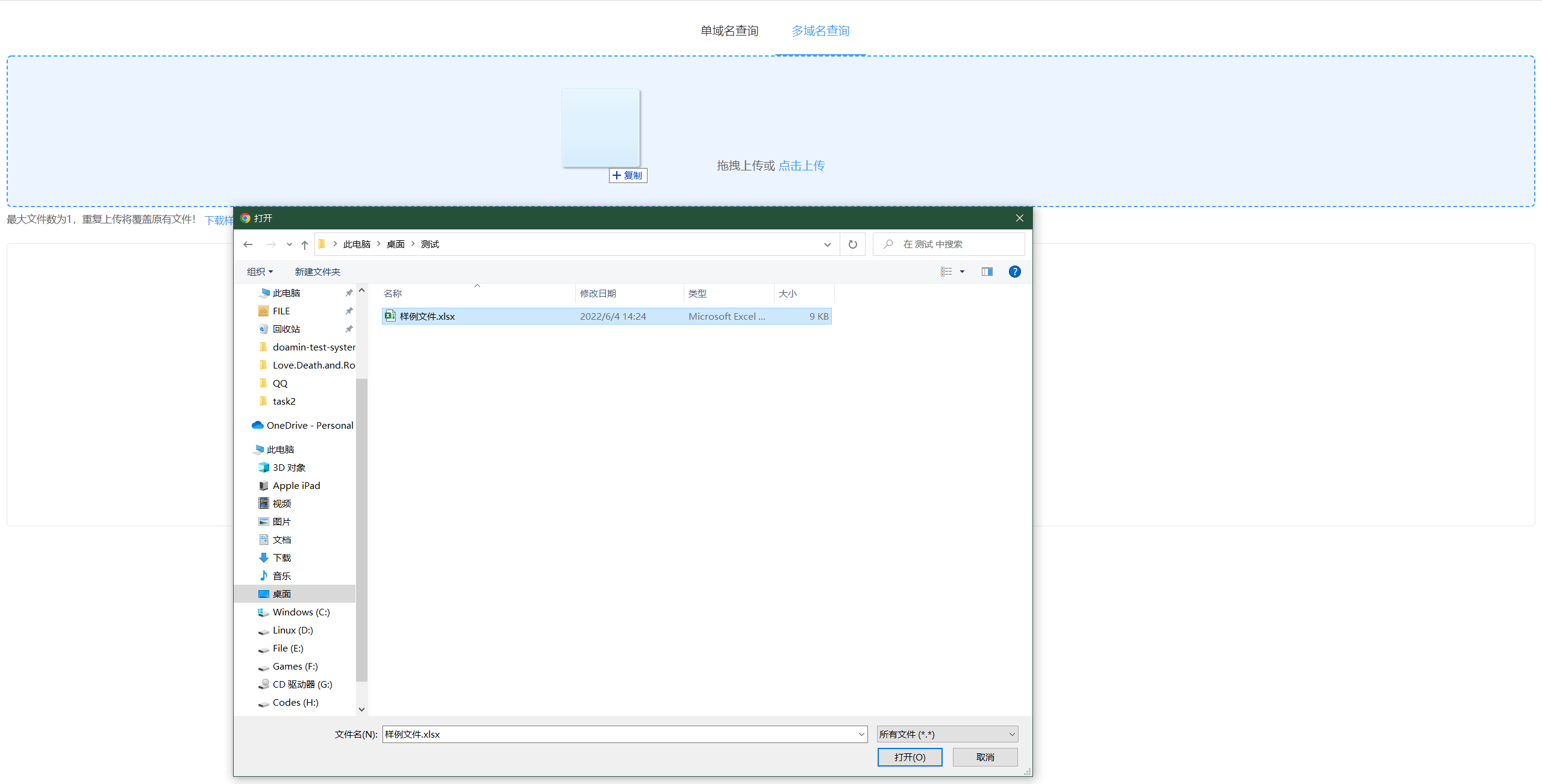


导出excel：

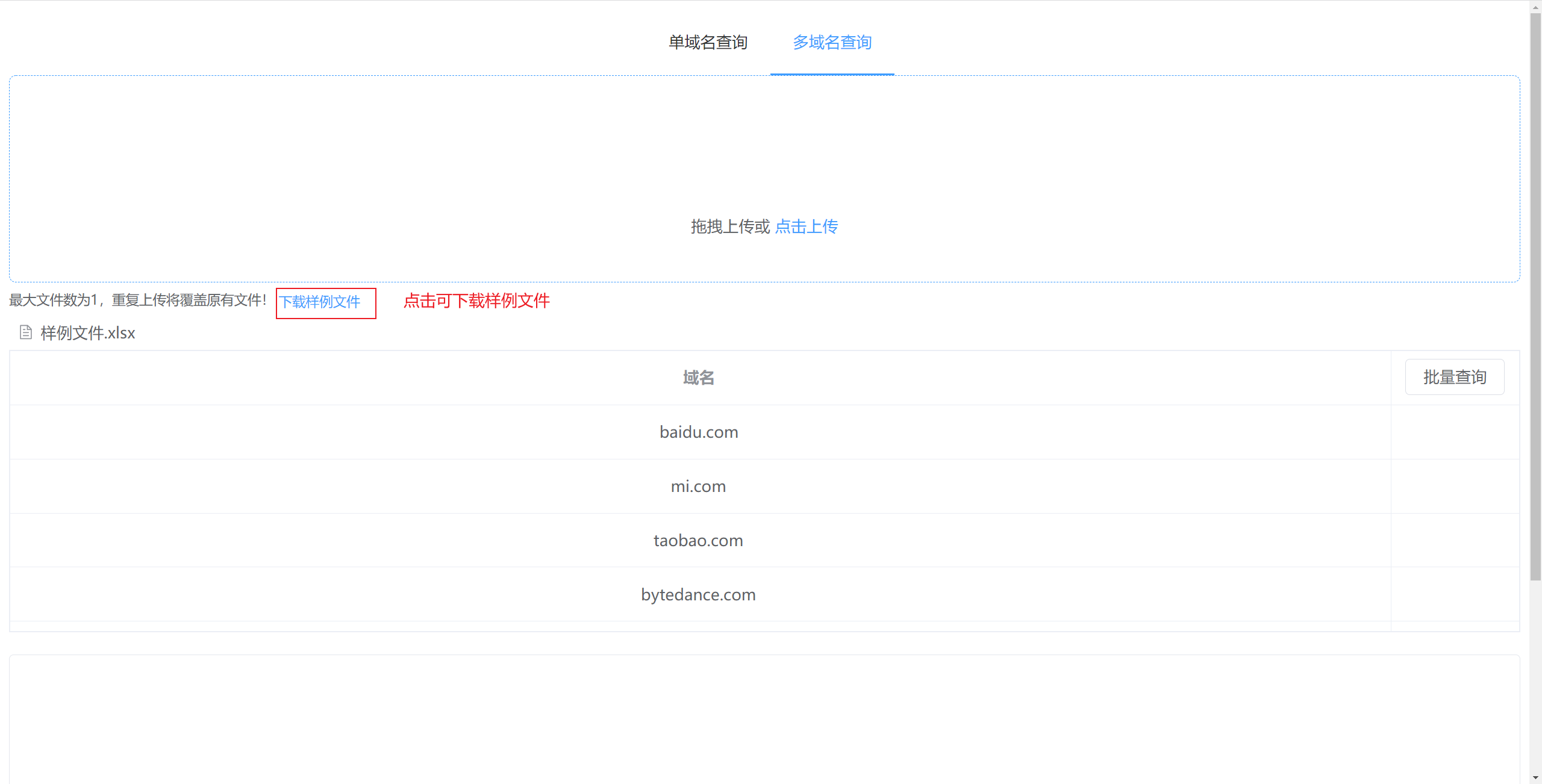


多域名查询：

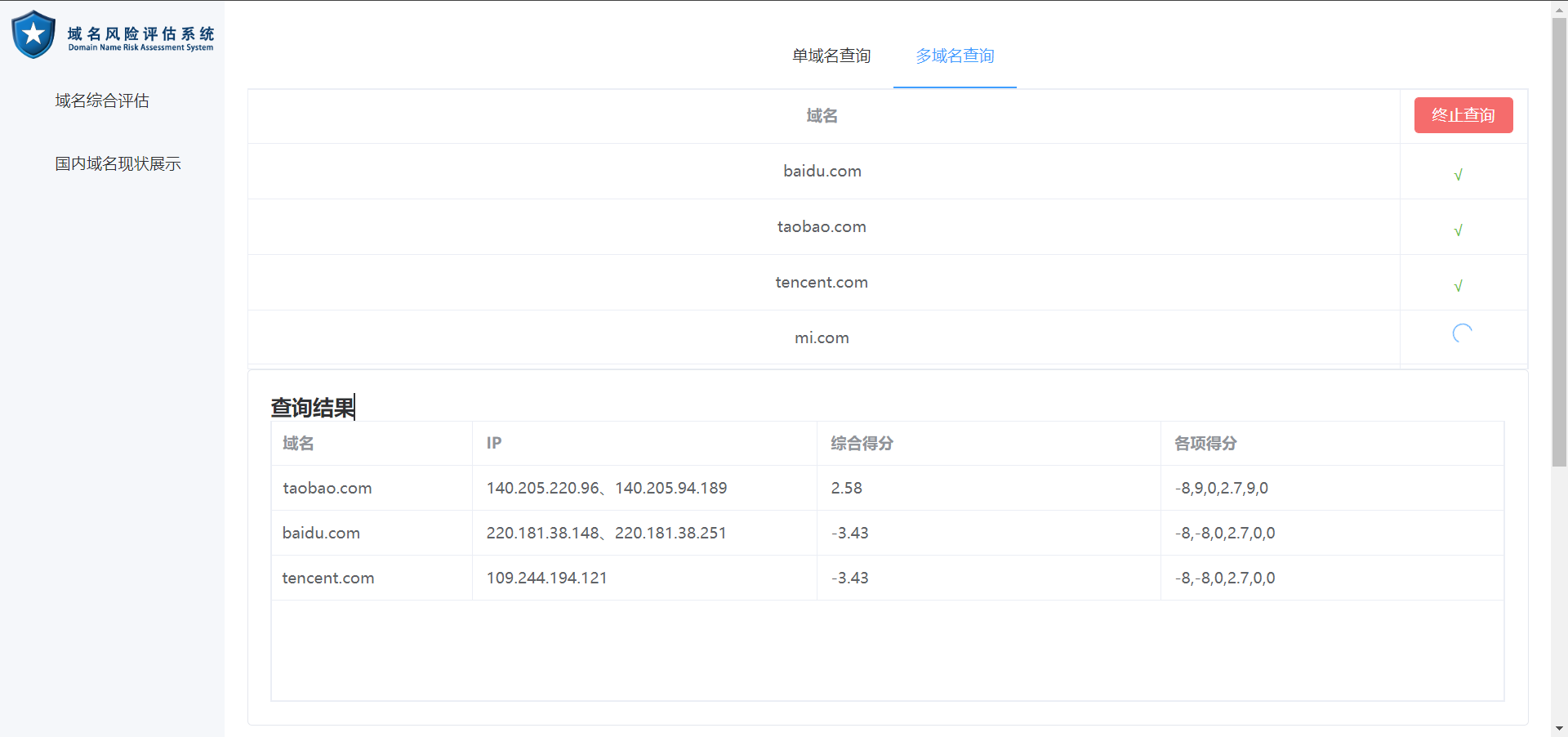
上传文件：



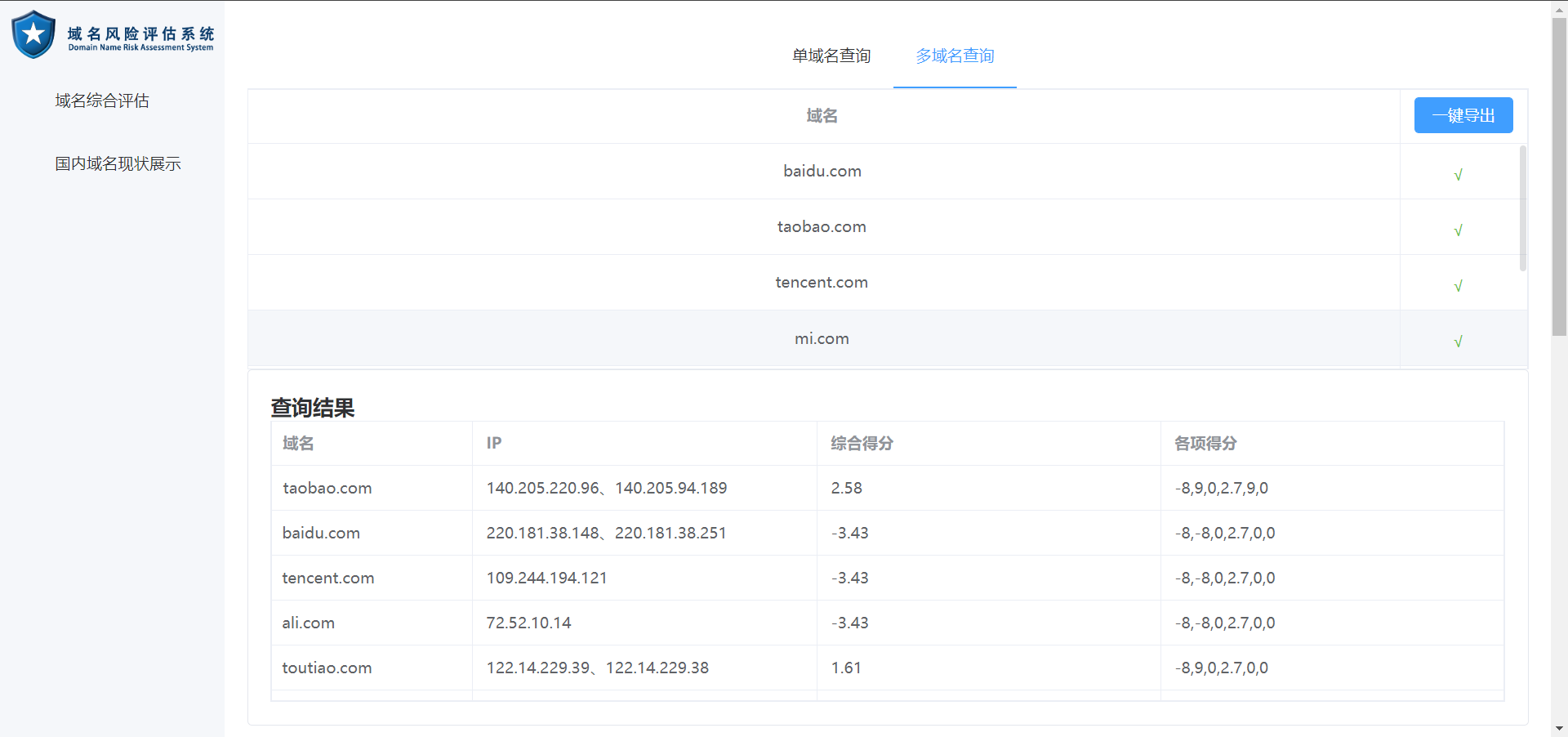
上传后：

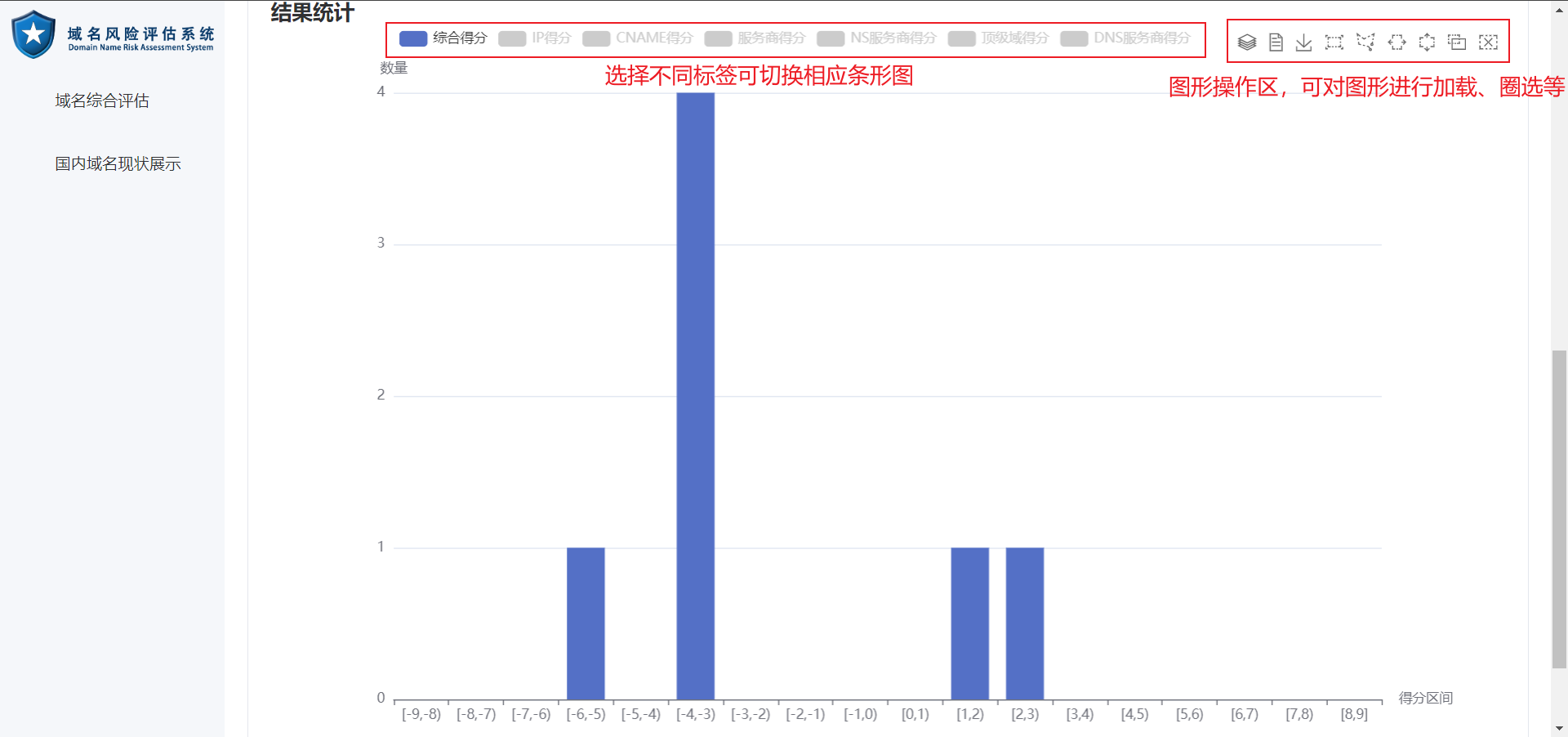


批量查询中：

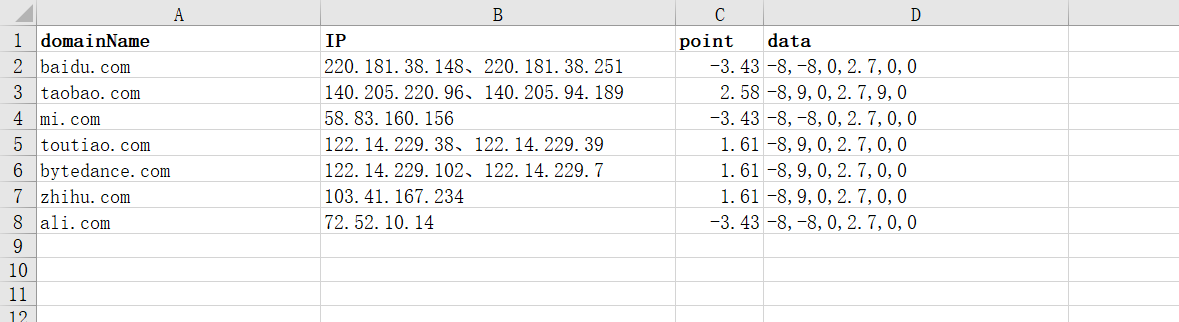


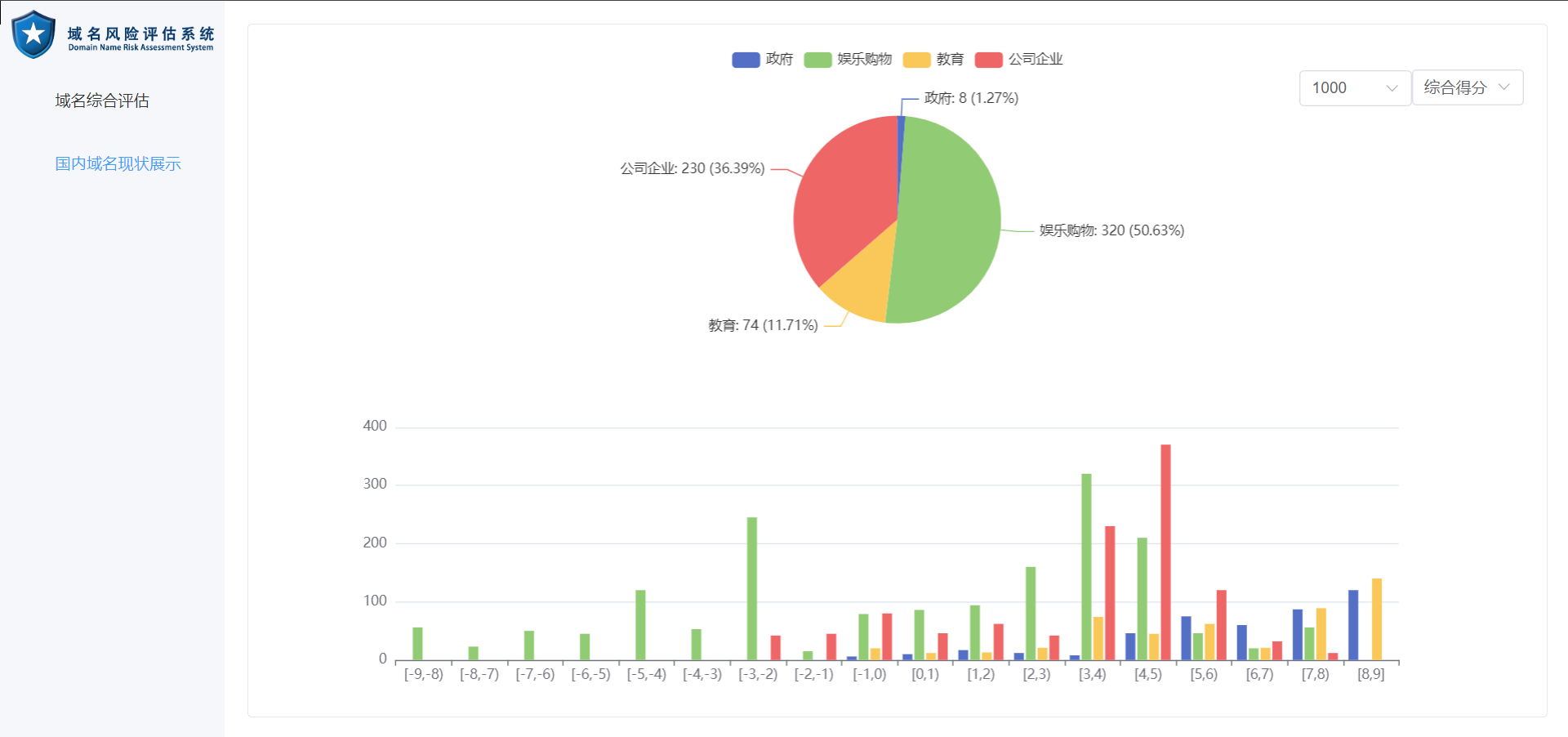
查询完毕：

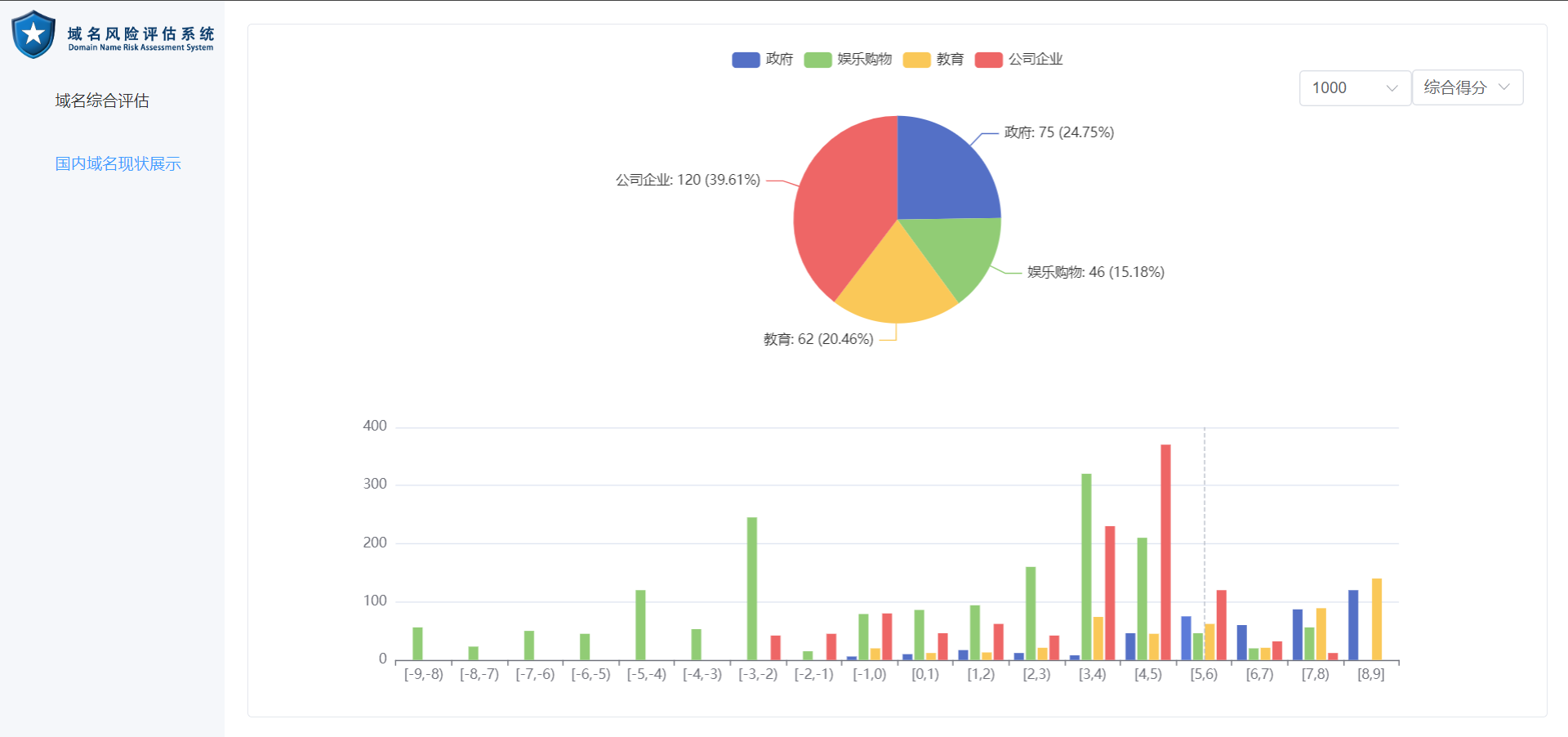




导出excel：







### 2.3.1 系统功能说明：

1. 单域名详细评估

2. 多域名批量评估

3. 一键导出评估结果为Excel

4. 绘制评估结果图，并支持图像选择与下载。

5. 提出提高域名安全性的建议

6. 支持上传Excel文件进行批量查询

# 作品分析与测试

## 3.1作品测试方案

关于本作品的测试，主要分为两个方面来进行，一是本作品的评估是否具有现实的参考意义，二是本作品运行的速度以及查询的正确性分析。

关于第一方面的测试，也需要分数个部分进行，首先是国内Alexa排名前100、1000域名各项得分情况的整体观察。其次是对于国内域名进行分类测试，观察每一种域名背后实体的特征，最后是进行国内外域名情况的对比，由于俄罗斯在俄乌战争期间遭受了包括勒令迁移注册商等较多的制裁，所以观察这些经历制裁与调整之后的域名背后实体属性的情况将会有较大的参考价值。如果俄罗斯域名的整体得分普遍偏高，那么就可以说明本作品还是具有一定的预测价值。

关于第二方面的测试，我们准备进行两部分，第一部分，是对于单域名查询的测试，第二部分是对于多域名查询功能的测试，在这部分的测试中，我们主要需要验证的是网站运行的稳定性以及查询的效率，速度，等方面，主要是验证作品应用时的性能。

## 3.2测试环境搭建与测试设备

第一方面的测试，采用自己的PC机进行，因为此机性能较好，可以进行多线程与多线程的利用，加快获取速率。

第二方面的测试，网站的后台采用了华为云服务器，然后我们将在PC端对查询功能进行测试。

## 3.3测试数据

本次测试，国内域名部分采用的是从Alexa爬取的国内排名靠前的域名样本，来自网站<http://www.alexa.cn/siterank/>。

俄国域名部分采用的是来自网站http://www.sbup.com/country/ru/12000/的数据。

## 3.4测试结果分析

### 3.4.1 第一部分测试

#### 3.4.1.1分类域名得分情况分析

我们首先对国内的四个类型域名（分别为政府机关类型、高校教育类型、购物娱乐类型、企业银行类型）中较为知名的前30个域名使用该评分体系进行打分。具体得分分布情况如下：

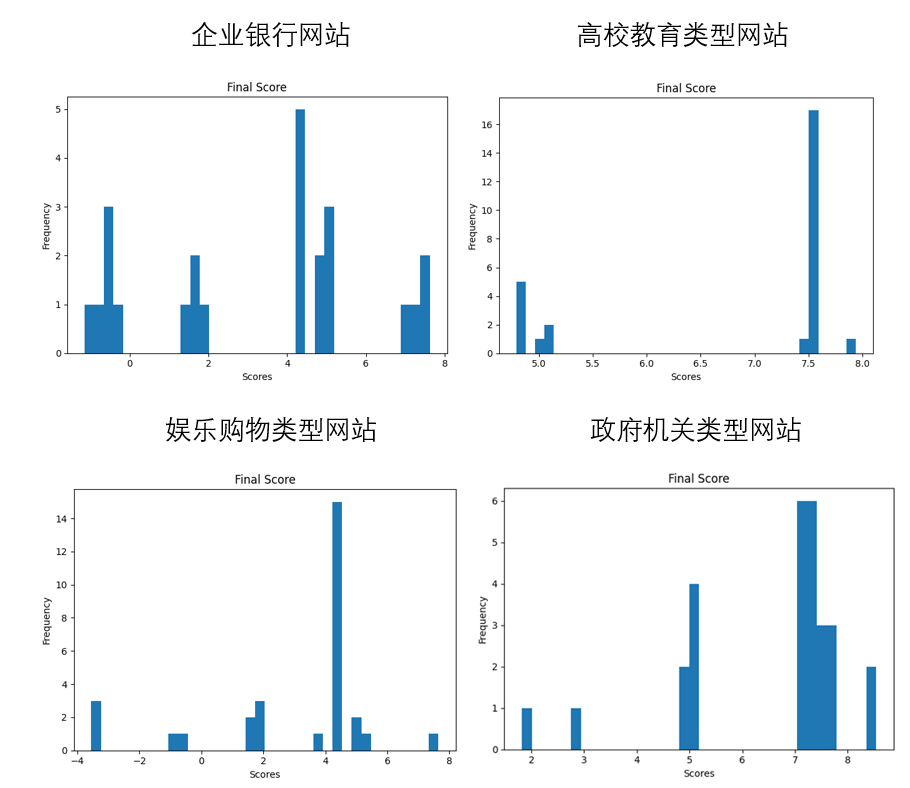


图 4-1国内分类网站对应域名得分情况

可以看见，高校教育类型网站与政府机关类网站的整体得分偏高，这与现实情况相吻合，此二类网站会有更多可能涉及到国家层面的重要信息，因此也更需要提防解析路径上存在着的风险，所以域名在注册的时候，往往会更加重视其背后实体的选择。值得注意的是，只有政府机关类型域名出现了得分为9分的，即在本评价体系中可以视作不存在风险的网站，经过分析，这是由于此类型网站的顶级域往往为.cn，较其它域名而言更加安全。

但是，不可忽略的是，在政府机关类型网站中，还存在着一些低分的域名，如tv.cctv.com，这些域名背后那些不安全的实体，无疑是国家域名安全性的一种隐患，需要采取措施，如选用其它的NS服务商，改变域名别名的注册信息等等。

在实验得到数据后，发现了风险的存在，正是能体验本系统实际应用价值。总而言之，政府机关与高校教育类网站对应域名总体得分即使较高，但也存在着个别得分较低的风险域名，这些域名是我国数据安全方面的隐患，因此，相关部门需要对于个别重要职能机构的域名进行整改，进而消除其风险。另一方面，国家需要对那些影响力较大的娱乐购物类网站对应域名进行密切监控，因为即使此类网站无法对我国数据安全造成直接威胁，但是敌对势力仍然可以从日常网站访问，解析的过程中获取大量的相关数据。

#### 3.4.1.2国内Alexa排名前1000域名得分情况分析

我们对国内Alexa排名前1000的域名进行了打分评估，得到的情况如下：

首先是总体得分情况

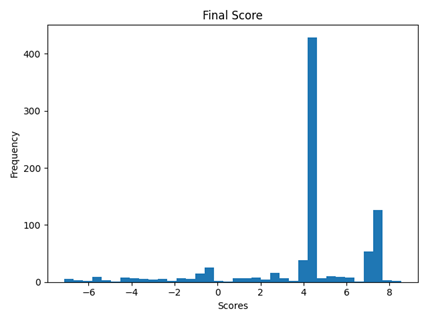


图 3-2 国内TOP1000域名得分情况

在所有域名中，大多数域名都处于中间分段（3-6），有小部分域名得分较高(>7)有极小部分域名得分偏低（<0）,但是即便如此，得分为八分以上，即可以认定为不存在风险的域名还是很少的，所以大部分域名在解析安全性上仍有提升的空间。因此，可以得出结论：绝大部分的域名持有者，可以通过本系统对自己的域名进行查询和分析，得到相应的建议并且进行改进，以提升自己域名的安全性和可用性。

接下来，观察各项具有代表性指标的得分情况，如下图：

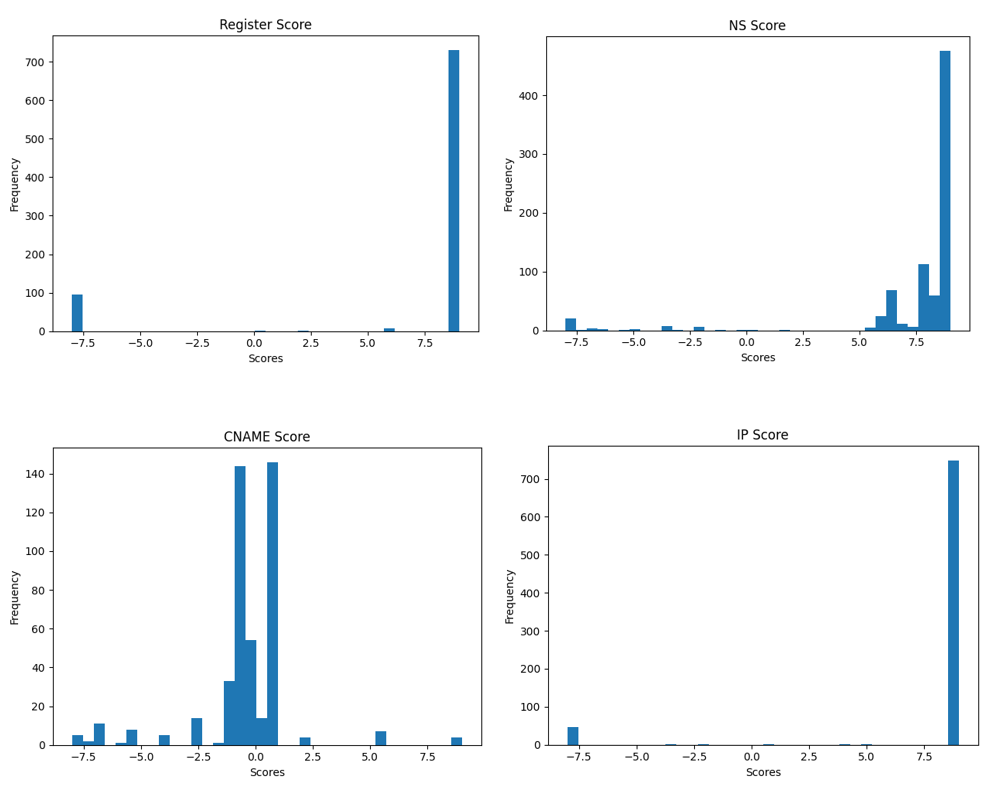


图 3-3国内TOP1000域名单项得分情况

在IP与注册商这两项属性上，绝大部分的域名得分为9分，即说明这些域名采用了中国的注册商以及服务器位于中国。在这两项属性得低分的域名往往是一些拥有者就在国外的域名，如[www.google.com](http://www.google.com) 与 github.com。可以得出结论:大部分国内域名在注册商选择与服务器IP选择上都避免了解析路径被中断的风险。

但是，与此同时，可以观察到别名得分和NS得分这两项得分情况并不是非常乐观。经过对于一些域名别名构成属性的具体分析，别名得分较低的原因是域名的别名采用了国外的注册商，这可能由于国外注册商相较于国内注册商价格普遍偏低，以及不受管制导致的。

在NS服务商这一项存在着少部分得分在5-7.5之间的域名，这是由于NS服务器解析涉及到层层递归，造成解析路径上不可避免的存在着拥有国家不属于中国的NS服务器，或者物理地址位于境外的NS服务器，这也造成了一定解析上的风险。

就总体而言，国家相关机构掌握了这些数据之后可以颁布一系列的规定，或者进行号召。如对于总体得分情况不佳的CNAME属性，可以呼吁域名拥有者尽量选择国内的注册商进行域名别名的注册。

以上分析表明，运用本系统可以对一组域名打分后进行综合分析，可以得到一些具有价值的结论，并且对这组域名整体情况具有了解与掌控，这也体现了本系统的应用价值。

#### 3.4.1.3 俄罗斯Alexa排名前1000域名的得分情况分析

为此，我们首先根据双边关系评分体系给出了俄罗斯与其它国家的双边关系得分如下表：



表 3-1 俄罗斯双边关系得分表

之后运用系统查询得到的总体得分情况如下：

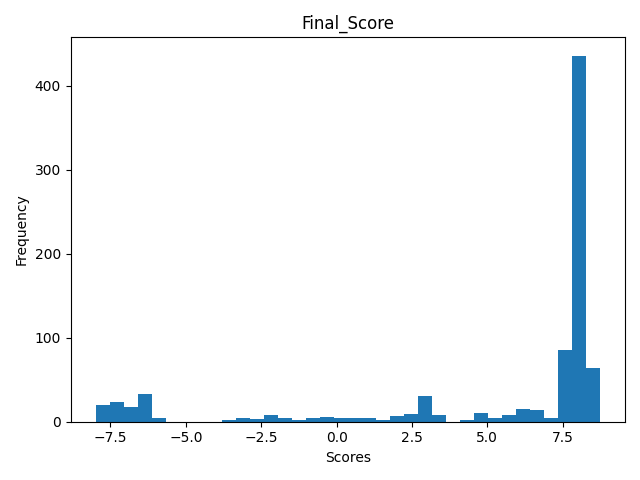


图 3-4俄罗斯TOP1000域名得分情况

可以看见，俄罗斯排名前1000的域名，在整体得分上，呈现着两极分化的形式，首先，较大一部分的域名获得了8分以上的高分，甚至有不少9分的域名，这与中国域名中寥寥的9分域名有着巨大的差距，我们认为这是由于俄罗斯的域名大多采用.ru为顶级域，而中国情况则相反，大多采用.com做为顶级域。其次，在得分占比最多的注册商这项，有不少的俄罗斯域名拥有者在以美国为首的北约国家注册机构在宣布对.ru属性域名发动制裁之后,纷纷将注册商迁移至本国注册商之下，这使得了域名的安全性得到进一步的提升。

但是与此同时，极低分的域名占比略大于我国，根据分析，这可能是由于这些域名本来就是属于那些与俄罗斯关系极差的国家，但是这些域名对应着的以娱乐社交性质为主的网站还是深受俄罗斯民众欢迎，并且俄罗斯政府当时并未对访问外网进行严格的控制，如来自美国的Google.com,youtube.com,facebook.com等等。

总体而言，经历过一轮制裁的俄罗斯，在其域名总体得分上比我国域名情况要好，这也正好体现出了本系统的评分，对于真正的制裁，具有预警的价值。如果国内域名可以根据本系统的评分结果对背后实体属性进行一定修改，可以有效避免风险来临时的损失。

### 第二部分测试

**系统网络测试**

使用网络请求分析软件对单域名查询时的网络带宽以及延时情况进行观测如下：

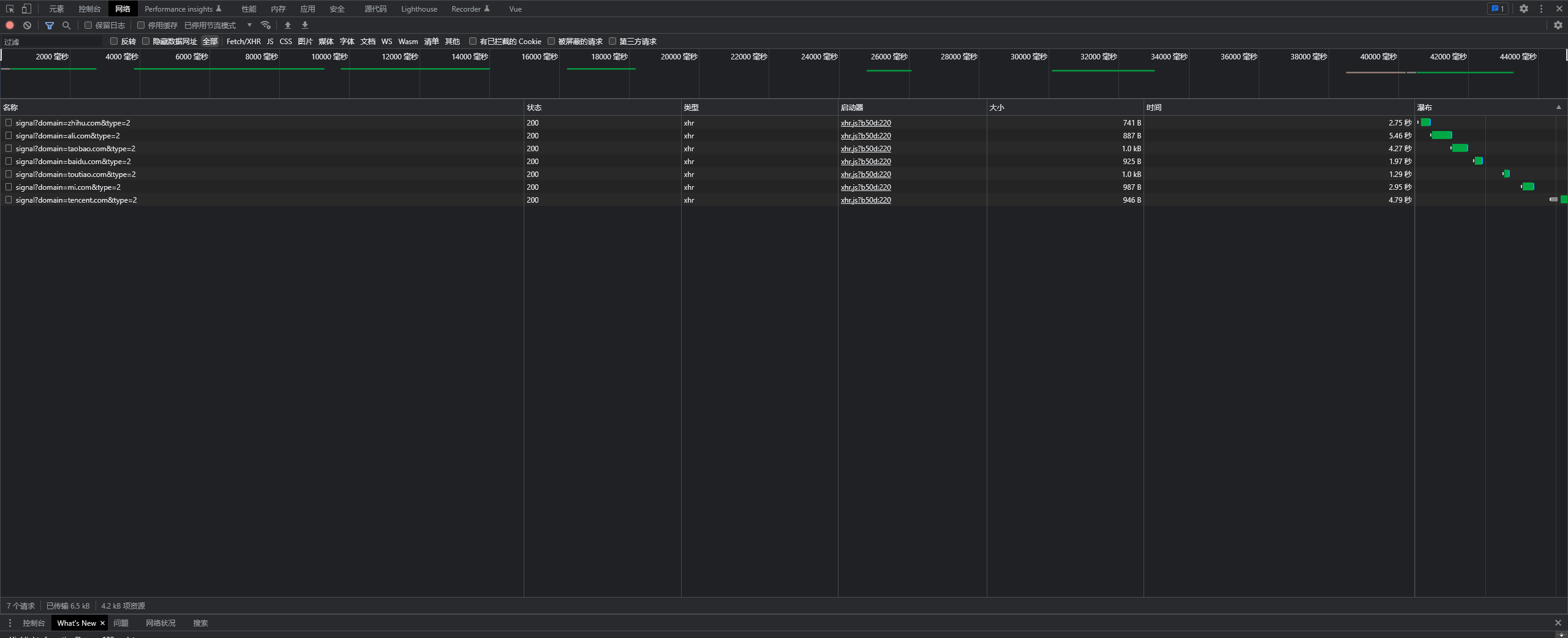


图 3-5单项查询时网络请求发送以及响应状态

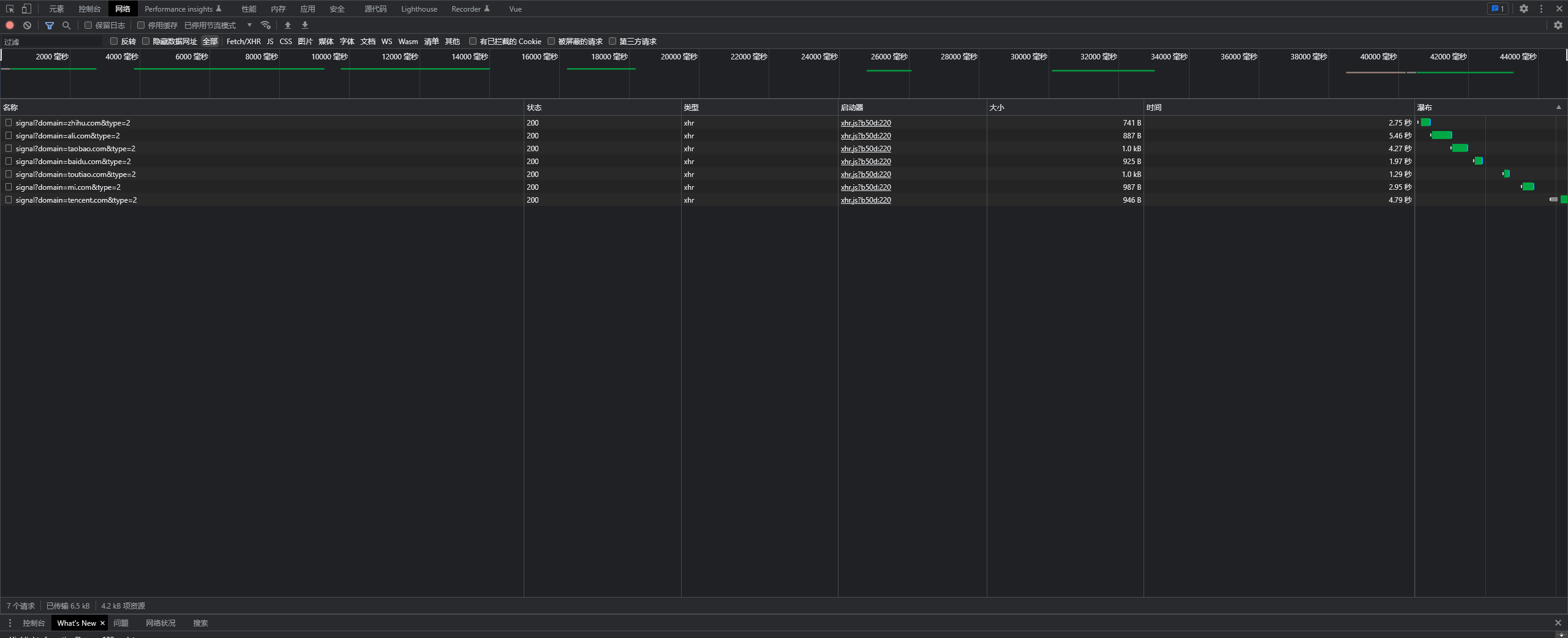


图 3-6单项查询时网络请求响应时间以及占用带宽情况

进行多次单域名查询，可以看到响应时间可以控制在1s-6s以内，占用带宽在0.5KB-1KB之间，测试结果较为理想。

多域名查询时的网络带宽以及延时情况进行观测如下：

对七个域名进行一次批量查询，观察网络资源占用情况及响应时间。情况如图3-7，图3-8所示。

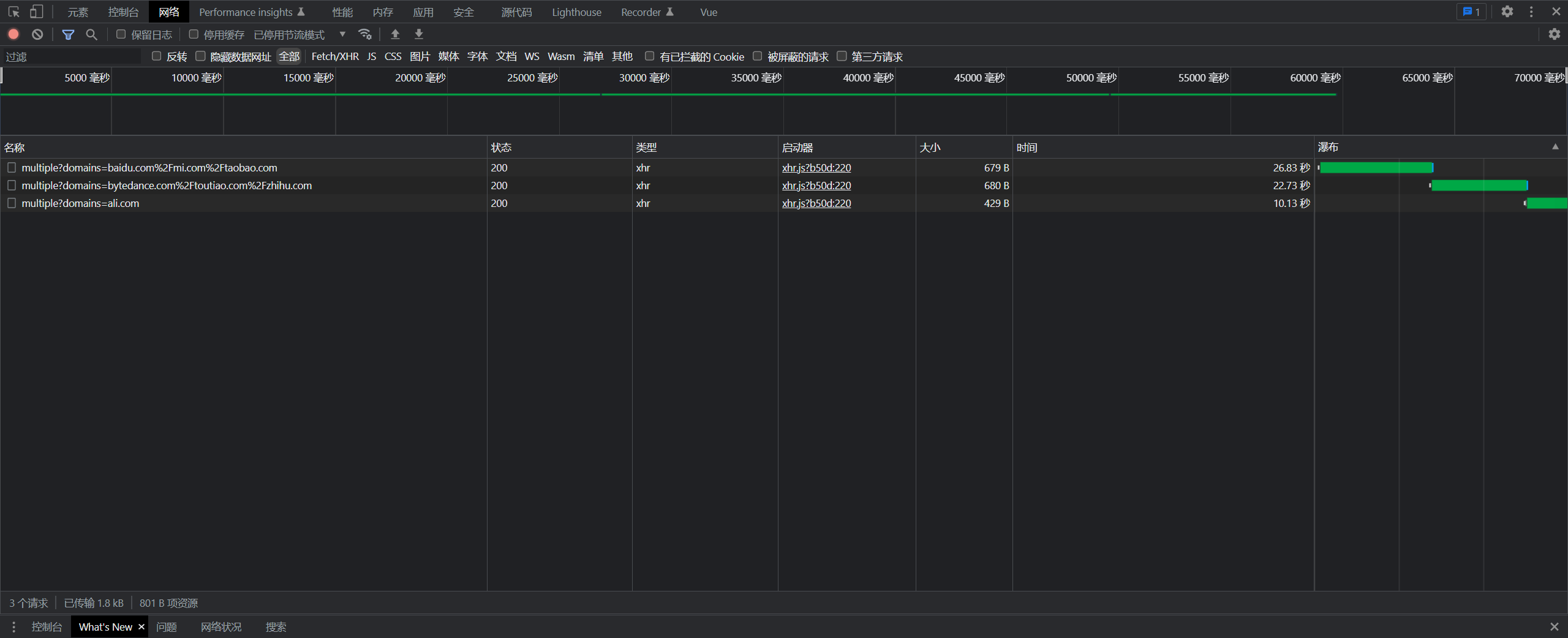


图 3-7多域名查询时网络请求发送以及响应状态

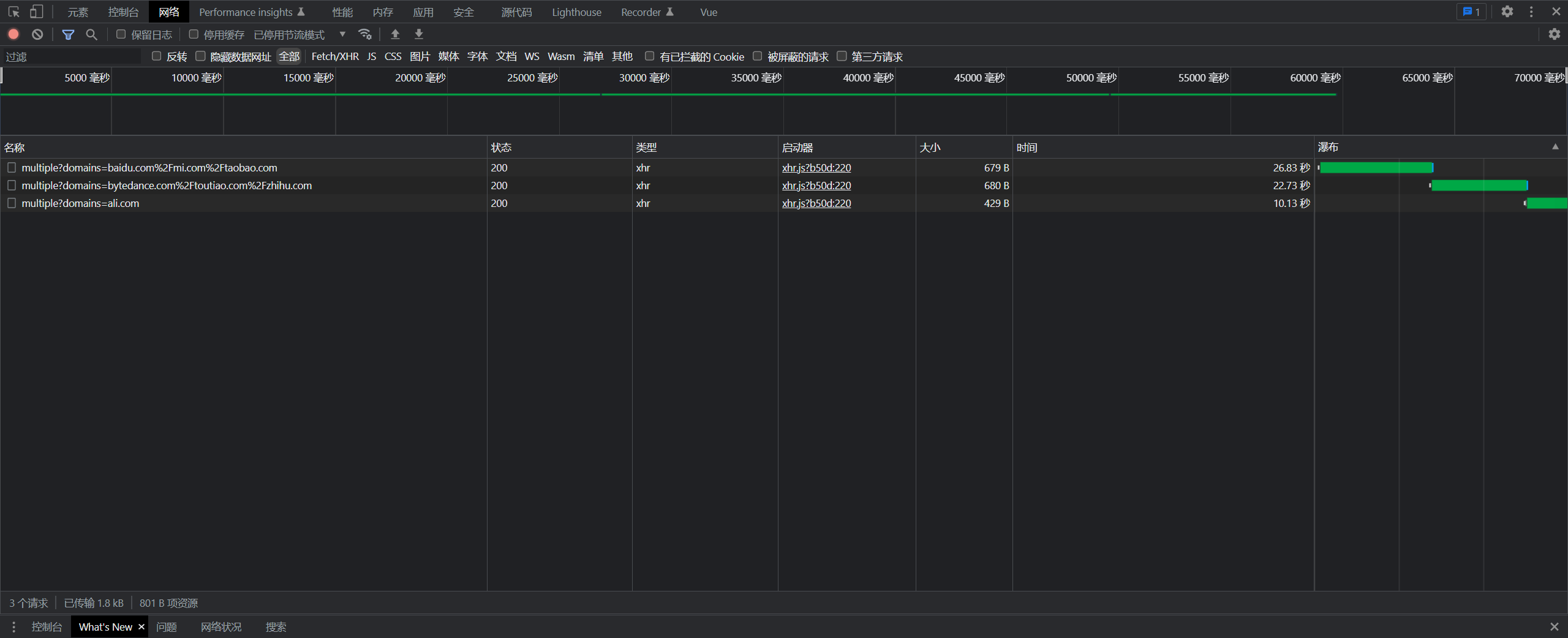


图 3-8多域名查询时网络请求响应时间以及占用带宽情况

系统将七个域名进行分组，每三个域名一组，进行分片查询，以保证查询的稳定性。对于每组查询，带宽可以保证在0.7KB以内，响应时间可以控制在30s以内，测试结果较为理想。

**系统健全性测试**

单域名查询时，对于非法字段的输入，系统会进行正则判断，会对非法输入进行拦截，如图3-9。



图 3-9 系统拦截非法输入示意图

对于多域名批量查询重复上传文件的情况，系统只会保留最近一次上传的文件，如图3-10。

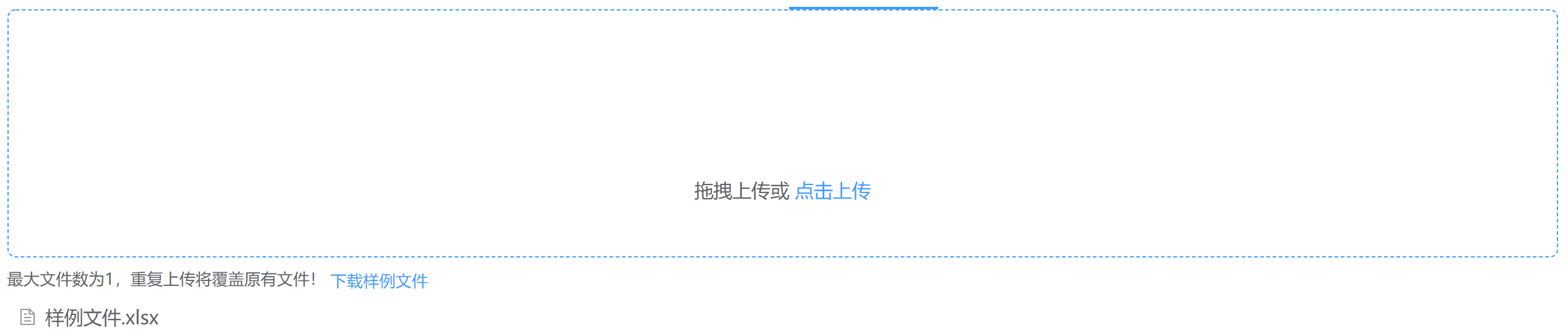


图 3-10 系统保留文件示意图

批量查询时，若等待时间过长，用户可随时终止查询，如图3-11，3-12。终止查询之后，系统将会保留当前查询到的结果并进行输出，如图3-13。



图 3-11查询中示意图

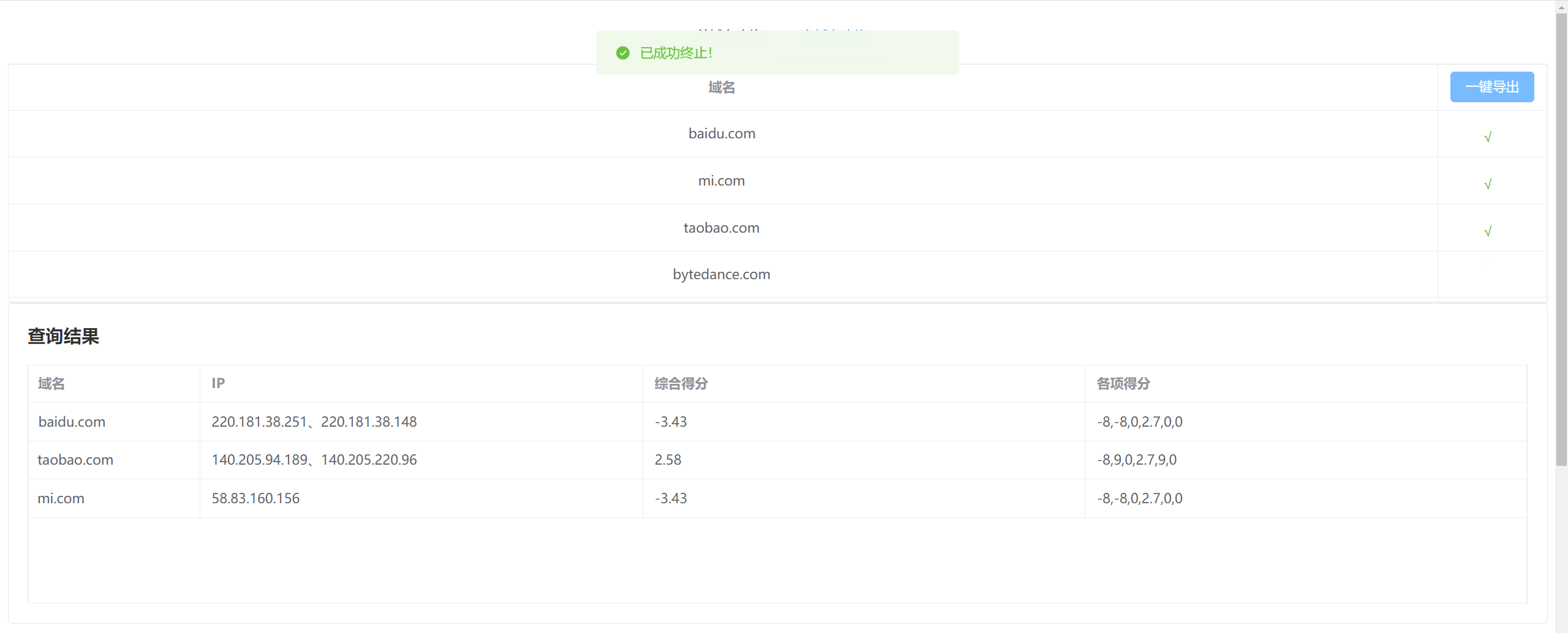


图 3-12 终止查询功能示意图

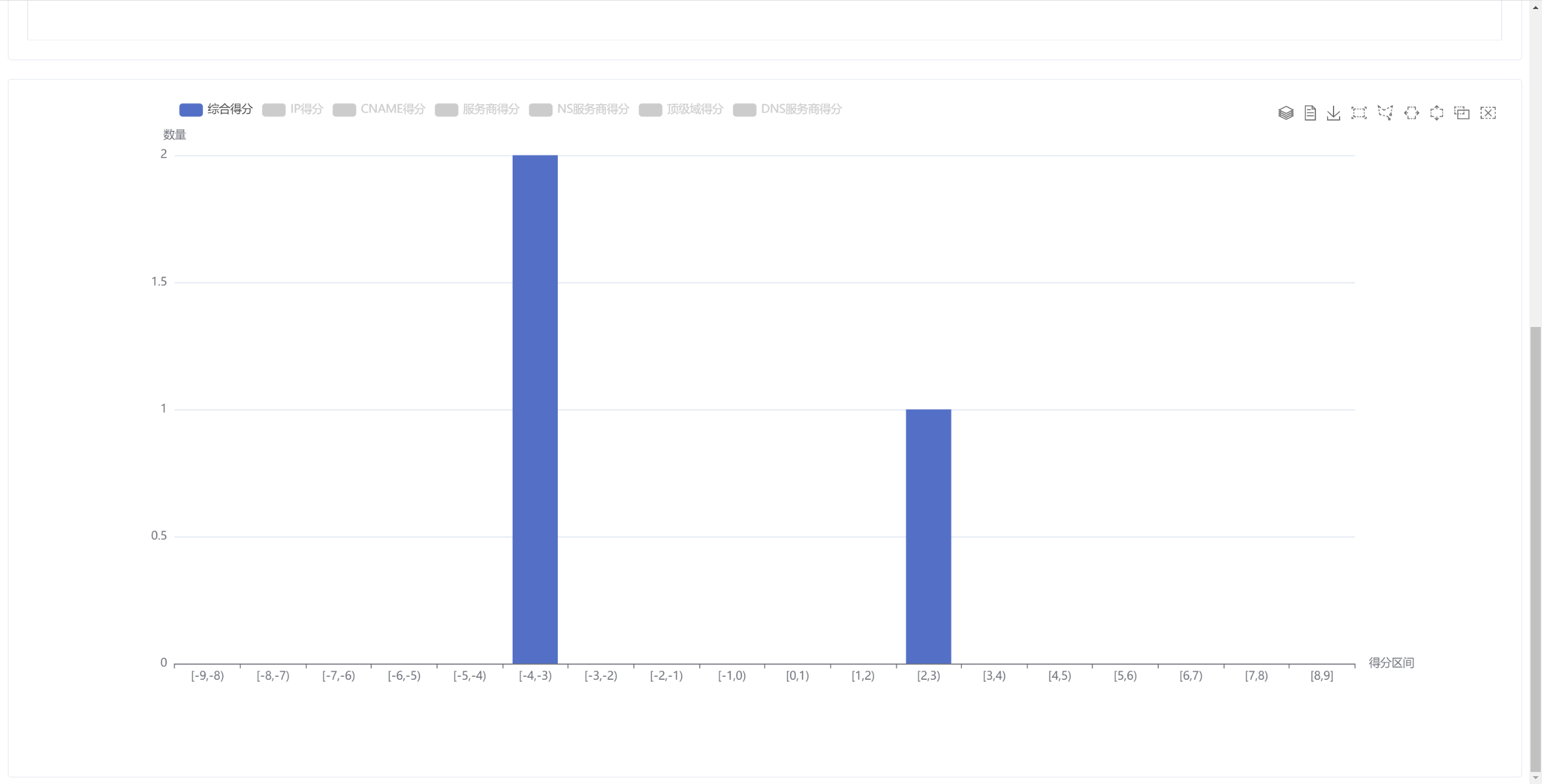


图 3-13 终止查询后显示当前已查询得到的结果

# 第四章 创新性说明

1.本系统针对我国对于现有的域名安全评估方法较少，缺少一个全面的、具体的域名安全评估模型且域名安全问题对于国家在互联网环境中的主动地位的重要性，首次提出了一种以国家双边关系为基础，根据实体历史情况与实体所属国家加入与网络安全相关组织进行的域名背后实体打分的域名安全性评估模型，以用于捍卫我国的域名数据主权。

本系统使用了层次分析法将域名所有与解析相关的重要属性作为一个系统，按照分解、比较判断、综合的思维方式进行决策分析以及使用CRITIC权重法确定了域名评分计算公式中各实体分值所占的比重，形成了一个合理、清晰、有效、直观的体系进行评分。

本系统的评分具有可扩展性，不仅仅可以对域名与提供解析的相关实体根据国家双边关系进行打分，而且在更改获取的域名属性以及其评分方法之后可以进行代表着其它意义的评分，比如以与域名流量有关的属性作为评分的各项指标，将域名的流量按照区间进行划分然后评分便可得到该域名的综合活跃度。

# 第五章 总结

本系统首次考虑域名从开始解析到最终为用户提供服务路径上的风险，提出了一种基于国家双边关系的域名安全性评估模型，评估域名解析风险的方法。通过分析域名的服务IP地址、CNAME名称、CDN服务商、域名解析商（包括实体和使用的域名）等国别信息，通过对各类基础信息赋予权重，对域名安全性进行综合评估，旨在提前发现存在风险的重点域名及其背后的网络实体，以便及时防范潜在的服务风险。同时，在评估方式的确定上，本系统的创新性地使用了国家双边关系这一概念，同时运用了层次分析法、CRITRIC权重法科学地确定了评分系统的核心公式。此外本系统还确定了一个计算域名遭受攻击后带来的影响的公式，系统将域名按照用途划分以确定公式的形式，而后将域名的打分带入其中后便可获得该域名所受攻击后带来的影响。

在用户的使用上，本系统的前端页面为用户提供了两种方法——多域名查询和单域名查询，单域名查询可以详细了解某一个域名的风险性，多域名查询能够对一批量的域名做一个综合性的评估，了解到各方面的信息，如域名风险性高的实体，域名实体怎样处理以提高安全性等。不论是多域名查询还是单域名查询，系统都会给出详细合理的策略以提高域名的安全性。

经过一定的分析，目前我国域名的风险情况相较于刚刚经历过制裁，进行了大量相关服务商更替的俄罗斯域名而言，并不算乐观，而问题主要集中于域名的别名（CNAME）以及顶级域上，因此国家相关部门可以呼吁广大域名拥有者在国内的域名注册商处进行域名别名的注册，并且注册域名时尽可能采用.cn为根域名。

同时，不同分类域名的得分存在着明显的差异，高校教育类域名和政府机关类域名的得分要明显好于购物娱乐与银行企业类域名。然而不容忽视的是，高校教育类域名和政府机关类域名当中仍然存在着少许高风险域名，这将会是我国数据安全的隐患，国家相关部门可以以此为参照对其进行整改以消除风险。

# 参考文献

1. [↑](#endnote-ref-1)
2. [1]鄢仁祥, 宾梵翔, 朱克耀,等. 域名解析方法,域名服务器及域名系统: CN, CN1756263 A[P]. 2006.

   [2]阎学通,周方银.国家双边关系的定量衡量[J].中国社会科学,2004(06):90-103+206.

   [3]娜琳. 论蒙古国与美国的双边关系[J]. 当代亚太, 2007(2):5.

   [4]吴心伯. 中美经贸关系的新格局及其对双边关系的影响[J]. 复旦学报：社会科学版, 2007(1):10.

   [5]王垚, 胡铭曾, 李斌,等. 域名系统安全研究综述[J]. 通信学报, 2007, 28(009):91-103.

   [6]赵琬清, 张沛, 马严. 面向网站服务的CDN服务发现方法研究[J]. 中国教育网络, 2018(1):2.

   [7]唐广良. 域名注册环节存在的问题及国内外的相关规定[J]. 电子知识产权, 2000(12):3.

   [8]段再昱. 论域名的知识产权保护[D]. 广西师范大学.

   [9]袁合才, 辛艳辉. 基于AHP和CRITIC方法的水资源综合效益模型[J]. 安徽农业科学, 2011, 39(4):3.

   [10]王伟. 我国P2P网络借贷平台风险评价——基于熵权法和CRITIC法[J]. 金融理论与实践, 2016(12):5.

   [11]郭金玉, 张忠彬, 孙庆云. 层次分析法的研究与应用[J]. 中国安全科学学报, 2008, 18(5):6.

   [12]郭金玉, 张忠彬, 孙庆云. 层次分析法的研究与应用[J]. 中国安全科学学报, 2008, 18(5):6. [↑](#endnote-ref-2)