FOFA搜索语法

本课程仅用于教学用途

中华人民共和国网络安全法

中华人民共和国刑法

社会主义核心价值观

详情百度搜索以上“关键词”+site:gov.cn

参考资料

1~FOFA规则列表
https://fofa.so/library

2~FOFA规则专题
https://fofa.so/subject

3~FOFA搜索语法
https://fofa.so/help

4~NOSEC安全讯息平台
https://nosec.org/home/index

5~goby扫描器
https://gobies.org/

6~赵武的自留地

第一部分

1~title="南京"　网站标题包含南京

2~ip="117.122.213.197"　查找特定IP

3~ip="117.122.213.0/24"　查询C段IP

4~port="3306"　所有开放3306端口

5~host="pjzhang.cn"　所有包含pjzhang.cn的域名

6~domain="pjzhang.cn"　显示所有子域名

7~icon_hash="-1374555452"　网站icon图标

第二部分

1~after="2018-01-01"　2018-01-01之后的资产

2~before="2019-01-01"　2019-01-01之前的资产

3~city="Nanjing"　城市是南京的

4~region="Guangdong"　省份是广东

5~country="de"　国家是德国

6~asn="56044"　自治系统号码，Autonomous System number，自治系统(制定自己的路由策略，并以此为准在一个或多个网络群体中采用的小型单位，例如ISP)

7~org="China Mobile communications corporation"　中国移动

第三部分

1~status_code=”401" 返回码是401

2~404 Not Found 直接搜索

3~header="thinkphp" 响应头包含thinkphp，例如X-Powered-By: ThinkPHP

4~body="thinkphp" 响应包中包含thinkphp

5~protocol="ftp"
使用FTP协议的服务，针对应用层协议，例如ssh，telnet，http

6~base_protocol="udp"，针对传输层协议，tcp和udp

7~cert="pjzhang.cn" 组织验证型证书中包含pjzhang.cn

第四部分

1~banner="Basic realm"　响应头内容含有Basic realm

2~type="service"　目前支持的所有服务类型，type="subdomain"

3~os="windows"　所有windows系统

4~server="Apache/2.4"　所有Apache/2.4的系统

5~server="huawei"　server包含关键词huawei

6~app="JIRA"　JIRA应用系统

第五部分

1~is_ipv6=true　所有IPV6服务，is_ipv6=false，is_ipv4=false

2~ip_ports="21,22"　IP开放有21和22端口的

3~ip_ports=="80,443"　IP只开放80和443端口

4~ip_country="De"　查询IP来自德国的

5~ip_region="Guangdong"　查询IP来自广东的

6~ip_city="Guangzhou"　查询IP来自广州的

第六部分

1~ip_after="2019-01-01"　2019年1月1日之后发现的IP

2~ip_before="2019-01-01"　2019年1月1日之后发现的IP

3~port_size="2"　端口开放数量等于6个的资产

4~port_size_gt="3"　端口开放数量大于3个的资产

5~port_size_lt="3"　端口开放数量小于3个的资产

第七部分

1~&& 和，|| 或，!= 不等于，() 边界

2~title="powered by" && title="wordpress"

3~title="powered by" && title!="wordpress"

4~port="3306" && country="de" && os="windows"

5~title="360天眼" && header="nginx"

6~title="360天眼" || title="瑞星"

制作视频相关软件

1-WPS演示

2~迅捷屏幕录像工具

3~爱奇艺视频助手

共勉

早睡早起，学好英语。
少看手机，多多实践。

感谢筒子们观看咯！