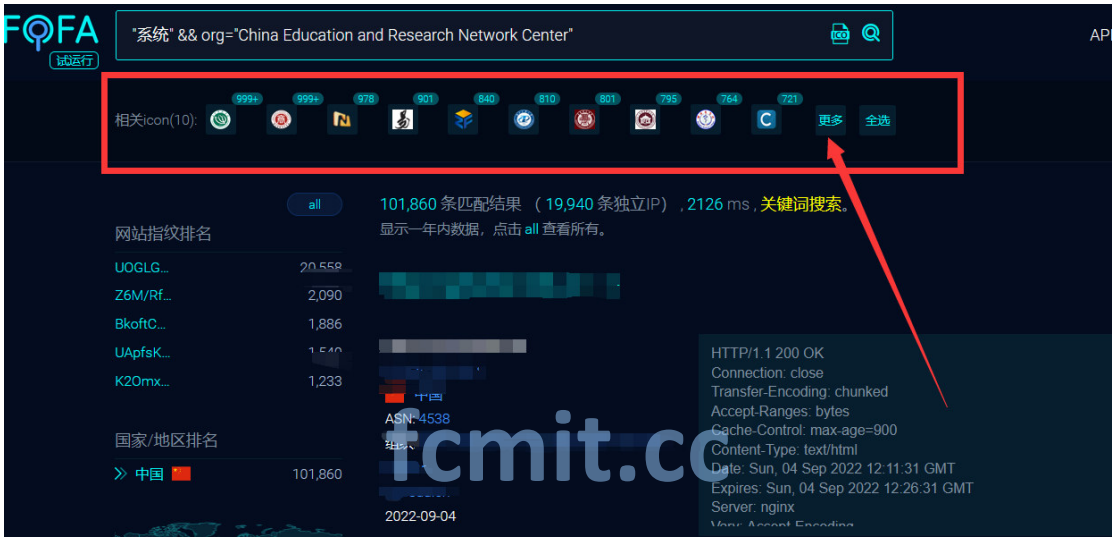
edusrc 挖掘技巧

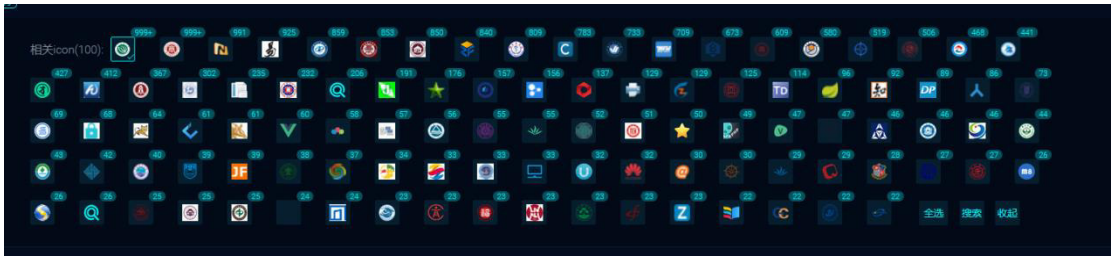
对于新人刚开设挖 edusrc 的时候需要花大量的时间来找系统和信息收集，当你遇见的系统又 waf 的时候可以适当的放弃别再这上面花时间了，列入 sql 注入，一个单引号尝试报错和闭合（最多就是把简单的绕过尝试一下）如果不行，那就果断放弃，xss 的话在 edu 的模块是不需要花大量时间，但是为了后面的企业 src 可以更好的理解 xss 可以尝试挖掘一些（在控制台弹窗测试，因为未授权，出了问题别找我）这就是对于 top10 漏洞的技巧。

主要还是说一些系统的收集方法：

1. 利用 fofa 语句：“系统” && org=“China Education and Research Network Center”



我们可以看见红色框内是有很多图标，这些有可能就是系统的指纹，fofa 直接给你归纳好的，接着点进去查看即可：



现在我们只需要一个一个图标打开然后用傻瓜式渗透顺序打一通：

例如上图所示，我们可以看见独立的 xx 条 ip 那么就是说这个系统有 xx 个用户在使用，点击

查看：

标准的某某系统后台，而且暴露出用户手册。

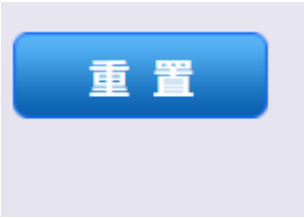
第一个就是弱口令操作：admin /admin　admin/123456　admin/admin888 这样的，最好的方法就是自己积累一个常用字典，当然还可以去全网寻找这一套模板的管理员手册，在后面就是 github 去寻找一下，最后都没有办法的话,那就放弃

第二个自然就是 top10：万能密码（sql）、xss 漏洞的挖掘

第三个：逻辑漏洞分析

首先还是先使用 f12 查看页面源码，说不定管理员密码写在页面中的！

然后可以注意到功能点是密码重置点



那么我们可以简单的两个操作，首先就是获取登录数据包进行修改返回包看看是否可以成功登录，如果登录成功就是逻辑一个，不能登录成功那就绕开进行下一步测试，第二个操作就是我们分析 js，查找重置密码的接口，看看接口是否存在未授权

这个功能点没有的的话，那就换下一个功能点：

显而易见的是查询功能，那么第一反应是 sql 注入，如果有 waf,可以轻微尝试绕过，因为 edu 中的系统相对于企业中就脆弱多了，当然 sql 注入理解的越深入，那么你挖 sql 注入的概率越大，任然常规操作，可以看看逻辑漏洞是否可以直接爆出密码这些。

当所有功能点和方法都尝试完后，你都没有收获，那么你可以进行下一个操作，信息收集来获取管理密码进入后台（这个后面讲，前面也有讲过）

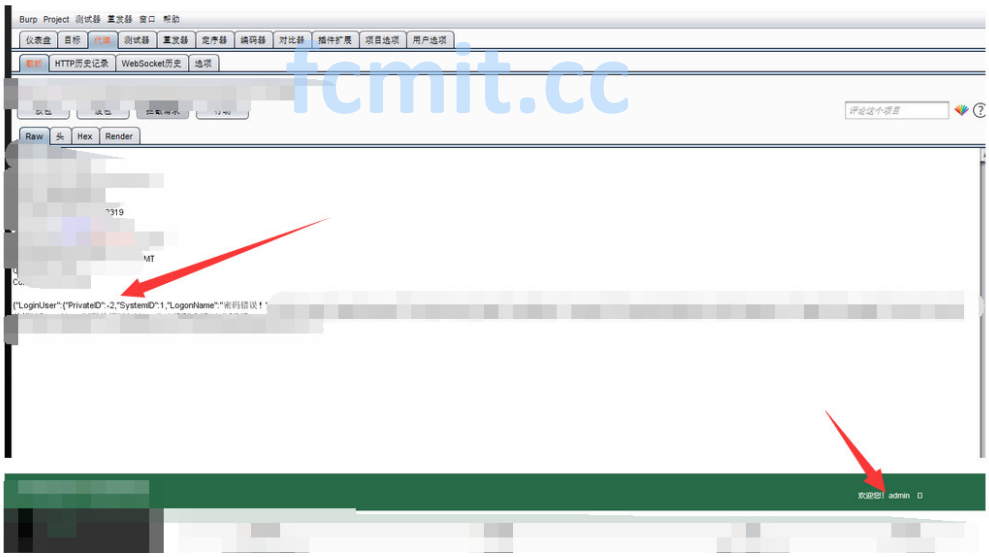
案例：

使用语法，这里需要自己灵活收关键字，只要组织对应是 edu，那么站点都是可以收纳的，我们可以看出来是 41 个独立 ip，那就是有 41 个学校在使用

下一步任意点进去可以看见是一个系统后台：

常规的都操作了，这里就是这么简单，修改返回包：

4.将抓取的包拦截，获取返回包，将第一个-2改为1，然后放包即可进入后台：



这也是我第一个在 edu 的通杀，当然今天在写这个文章的时候二开了他，有想法的师傅的自己测试

免责声明：

请勿使用该星球分享的技术进行违法乱纪的事情，由于传播、利用本星球所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，本星球及作者不为此承担任何责任，一旦造成后果请自行承担！