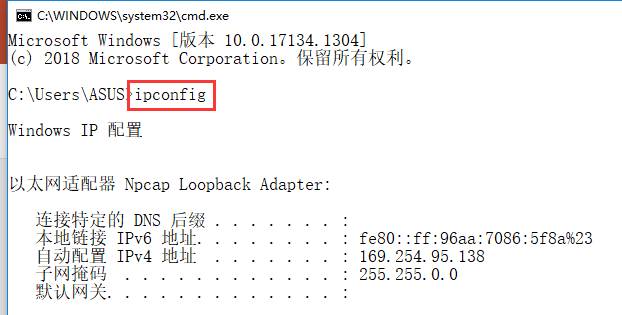
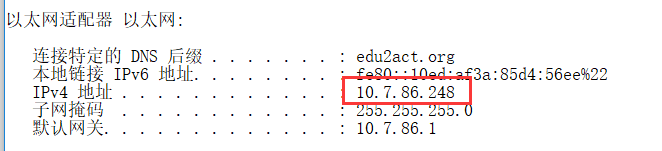
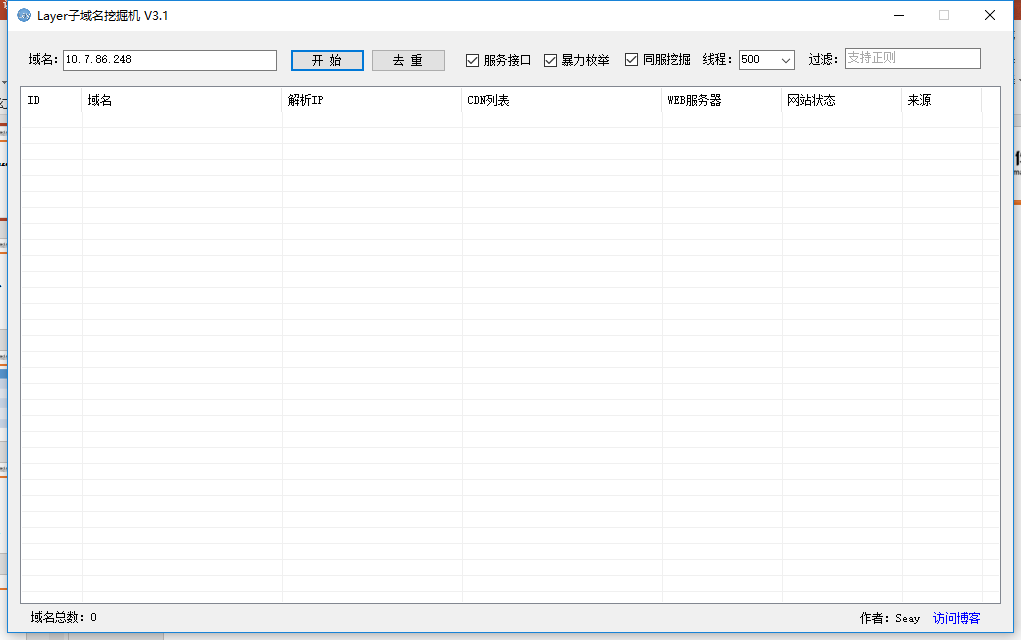
# 收集域名信息

## 收集对应IP地址---10.7.86.248





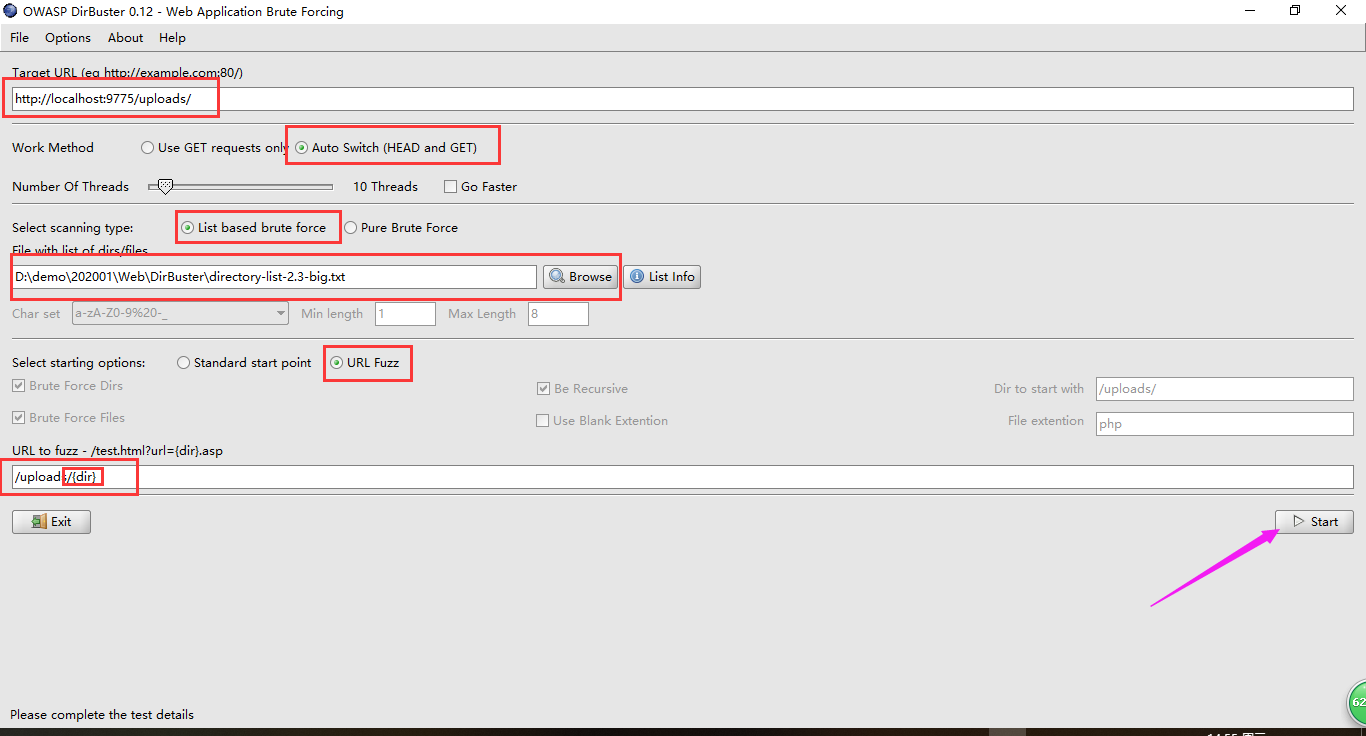
## 收集子域名信息---本地IP没有收集到子域名

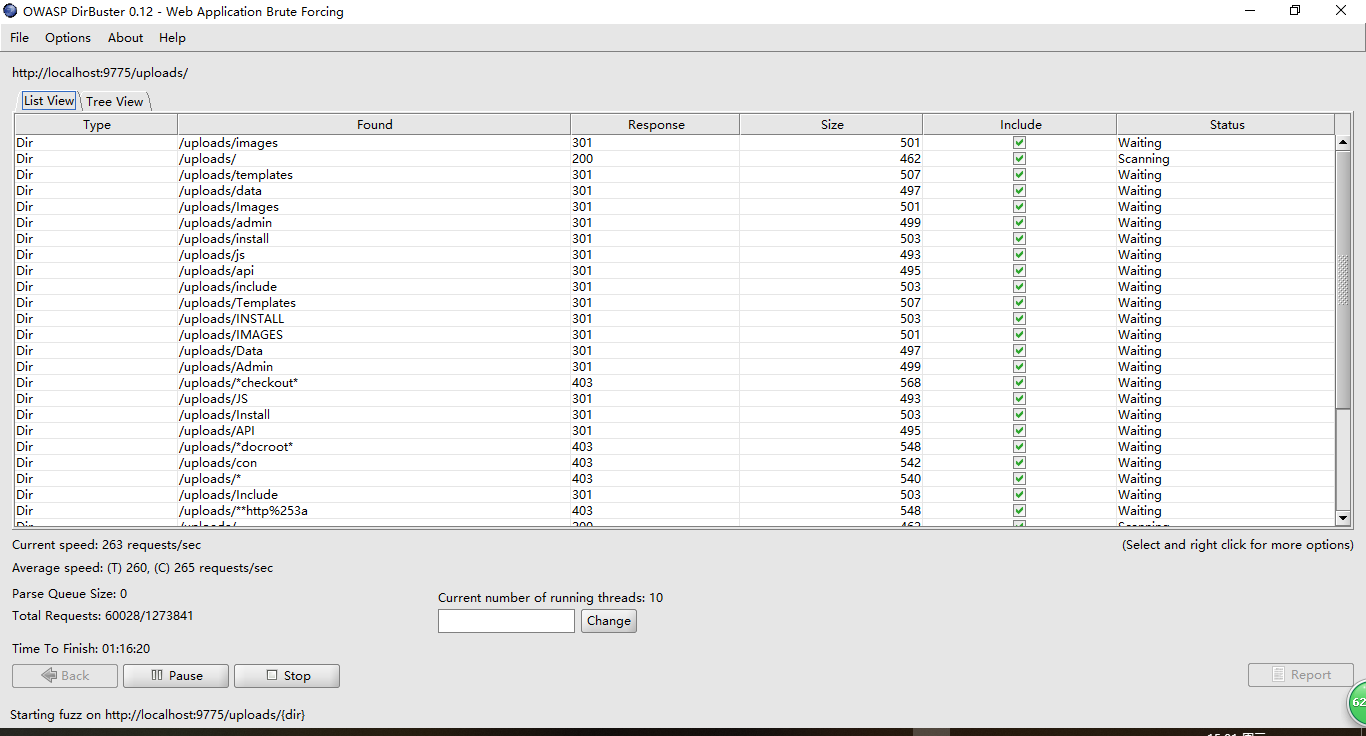


# 敏感目录

## Dirbuster

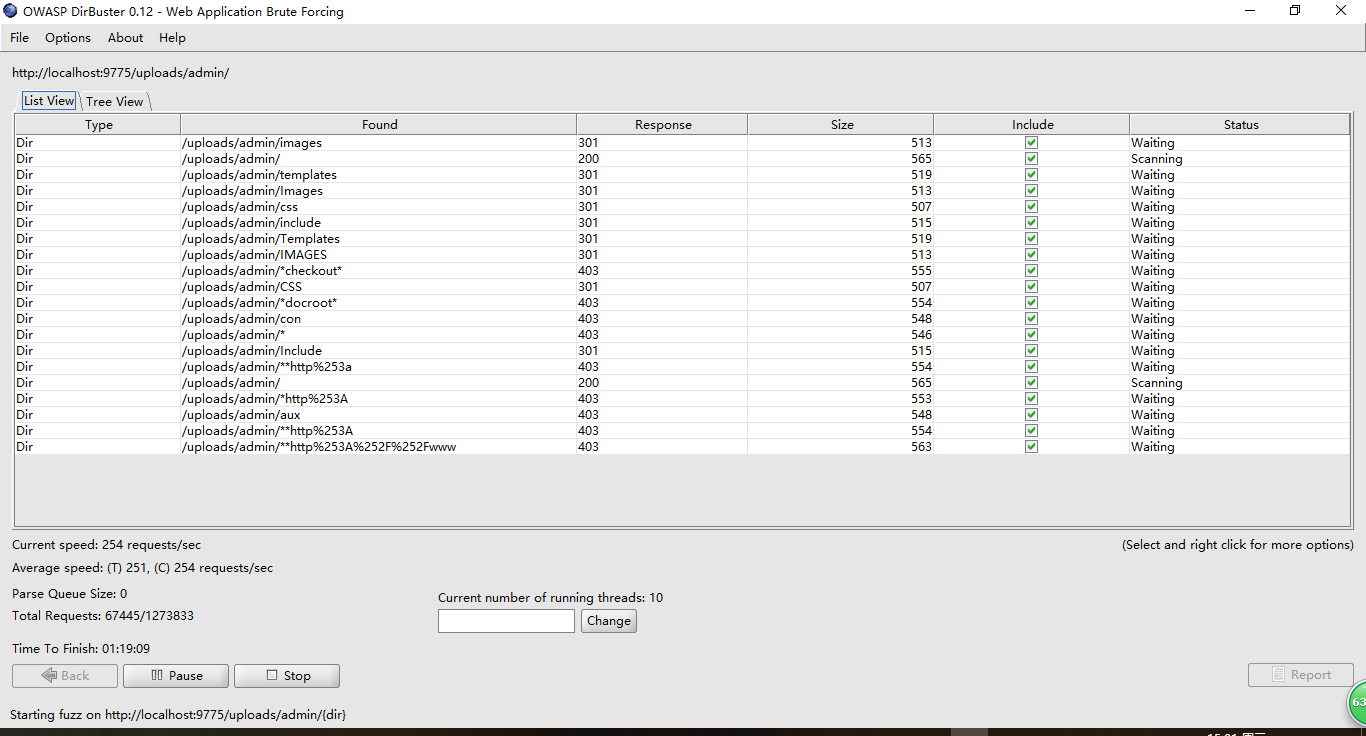
### <http://localhost:9775/uploads/>



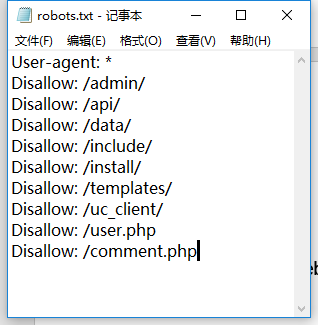


### <http://localhost:9775/uploads/admin/>

### 



## Robots.txt---D:\demo\202001\Web\phpdemo\bluecms\_1.6\uploads



## 后台目录

D:\demo\202001\Web\phpdemo\bluecms\_1.6\uploads\admin

## 安装包

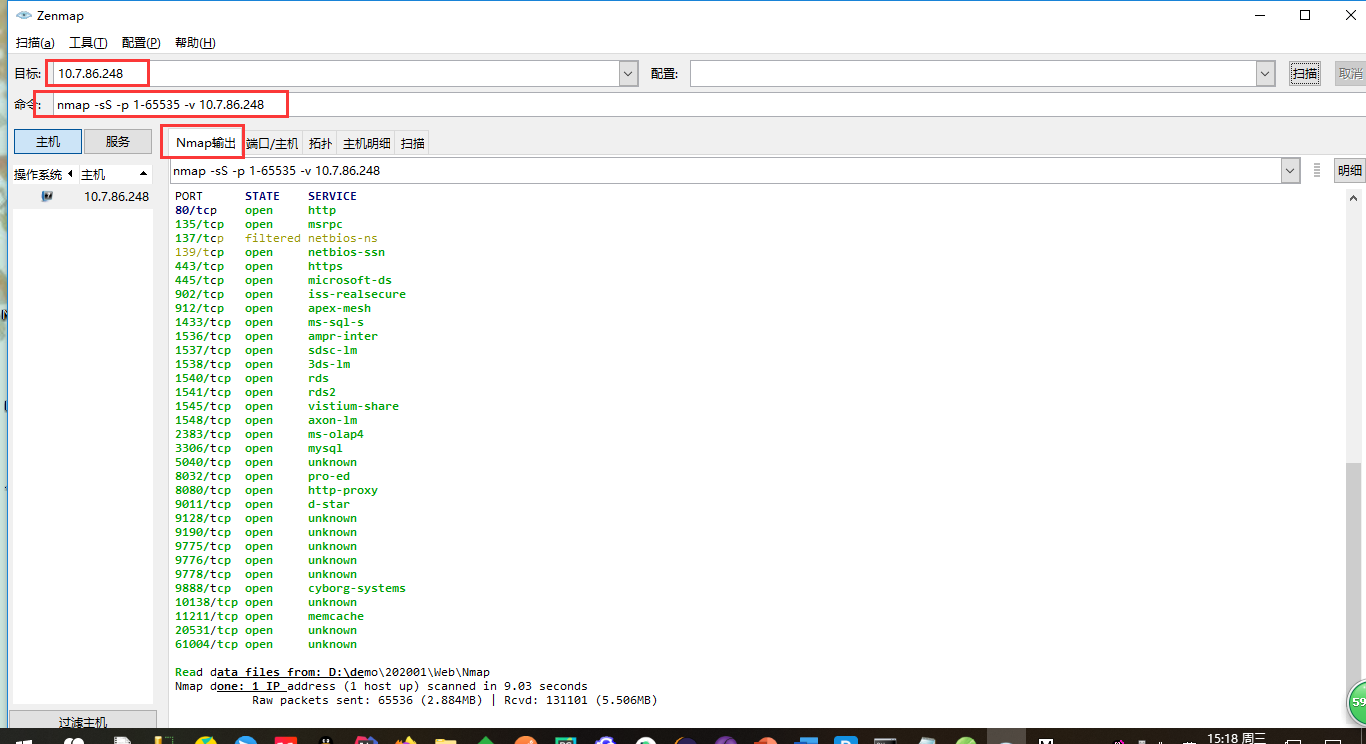
D:\demo\202001\Web\phpdemo\bluecms\_1.6\uploads\install

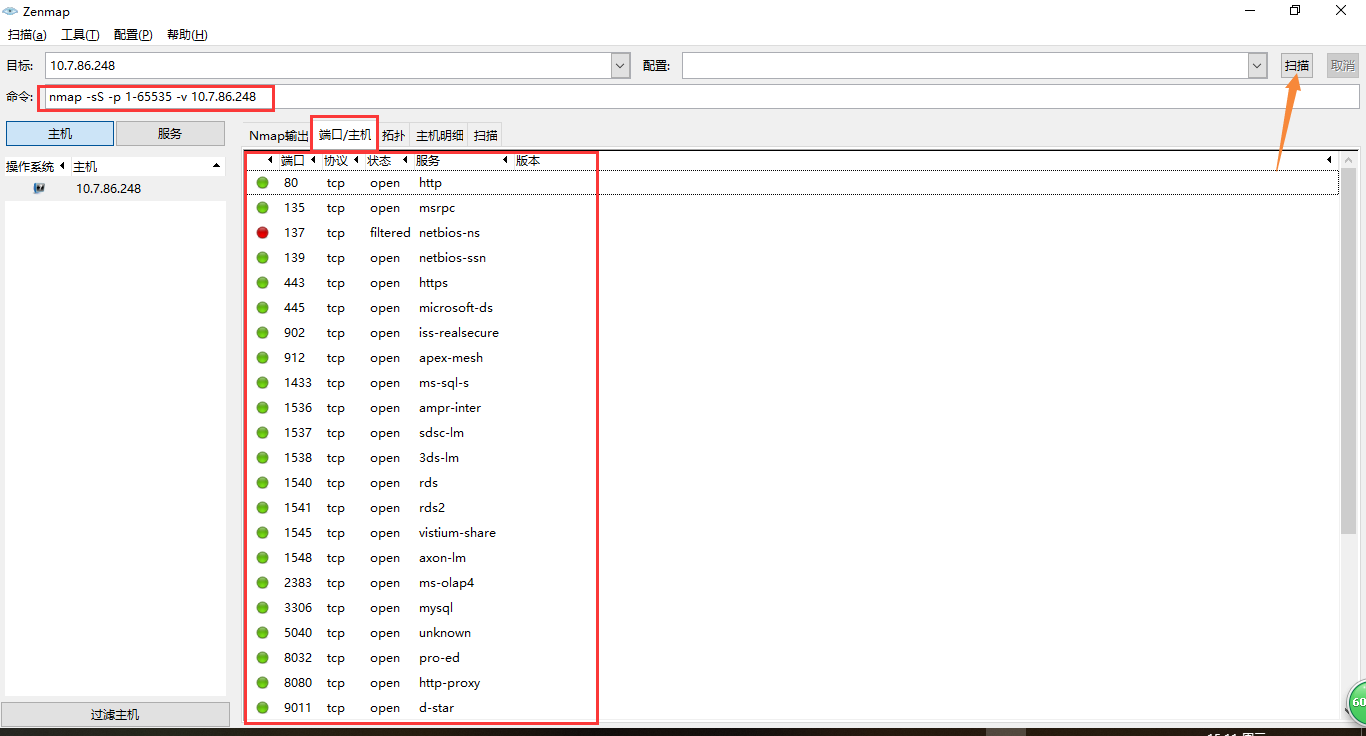
## 上传目录

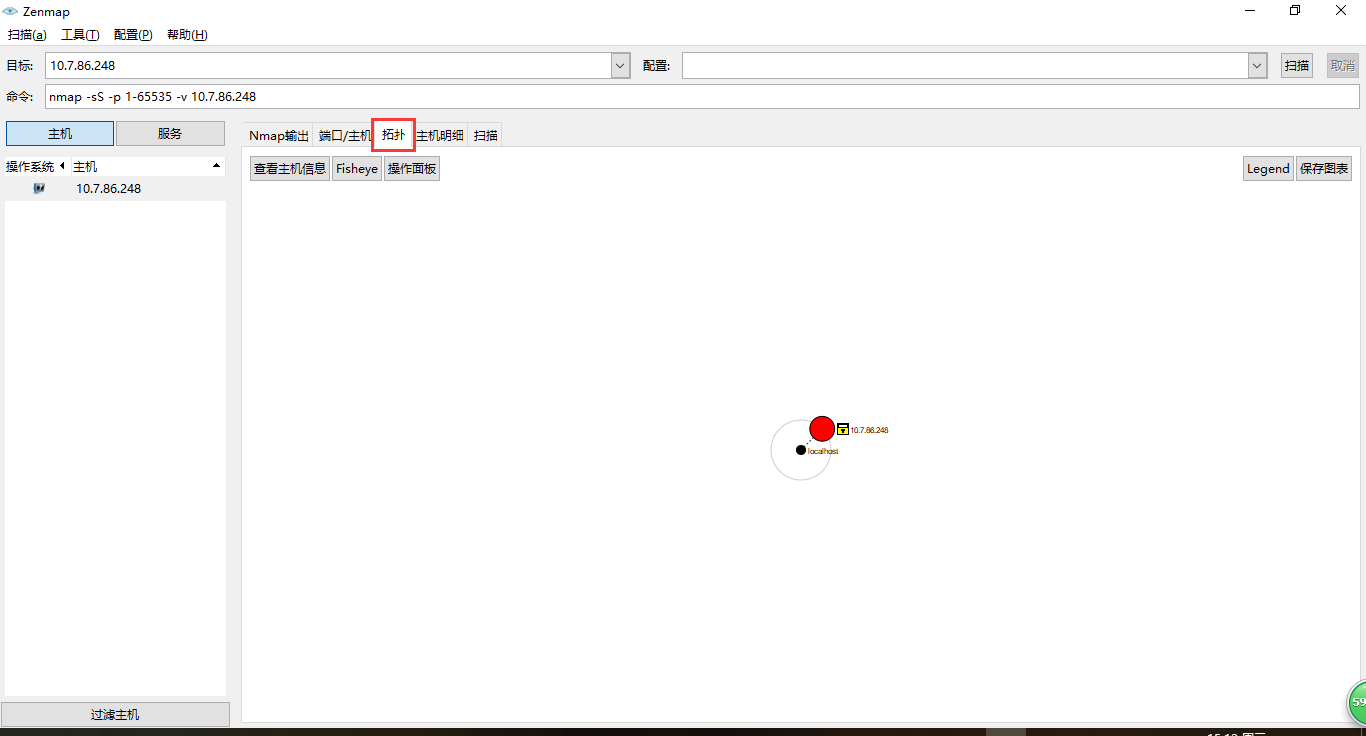
D:\demo\202001\Web\phpdemo\bluecms\_1.6\uploads\data\upload

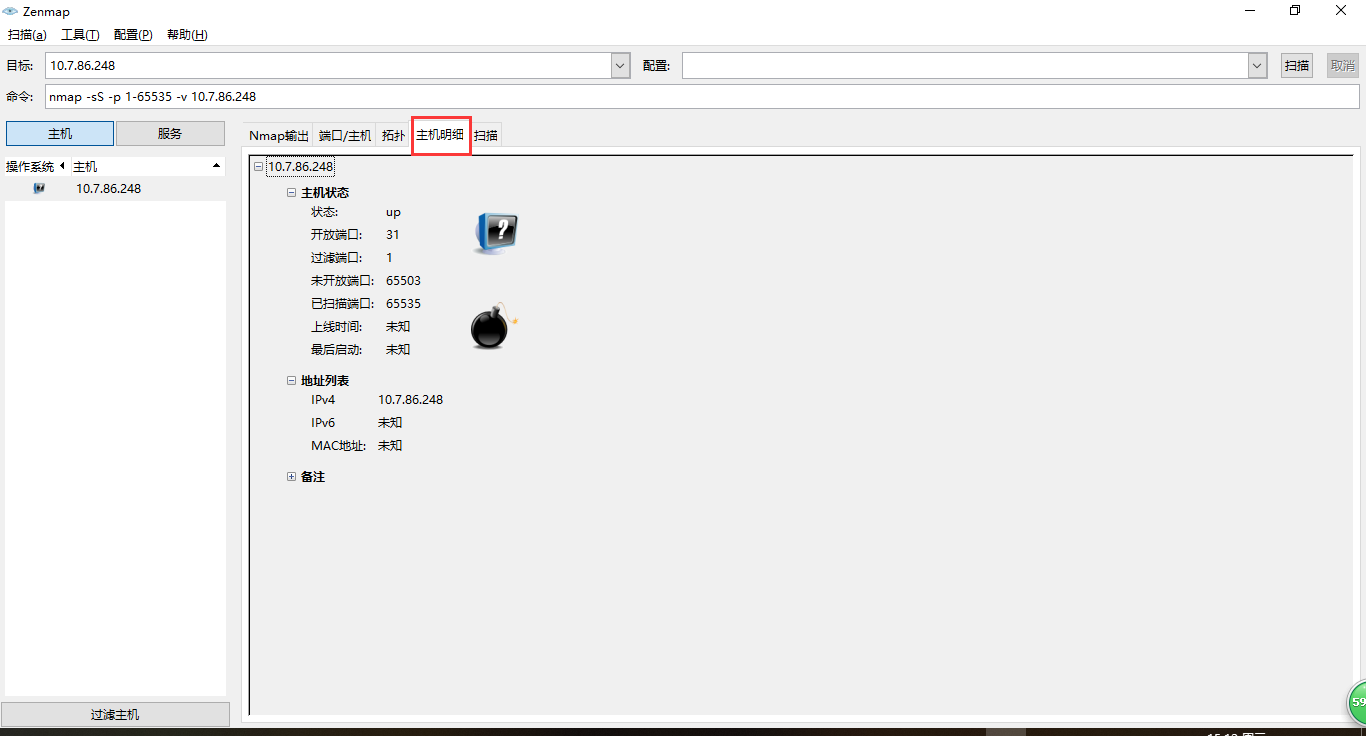
# 端口扫描

## Nmap



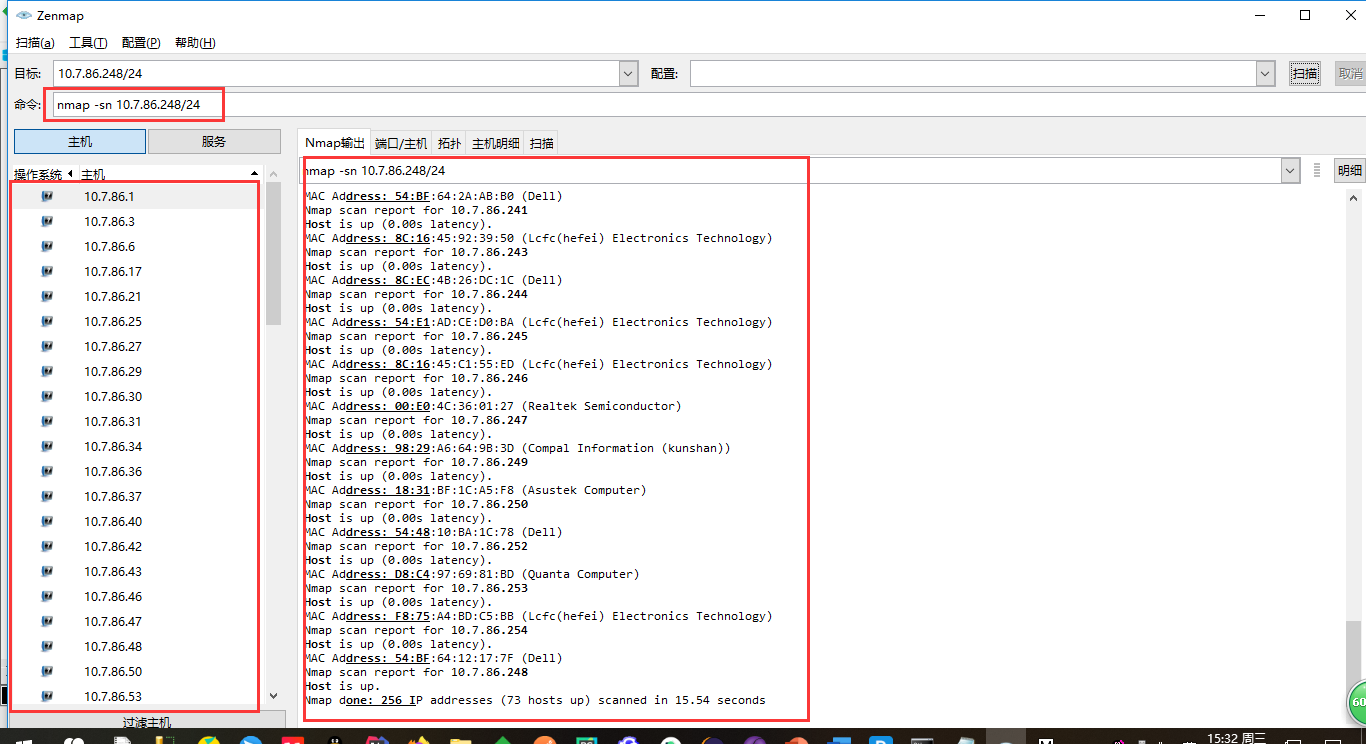






# 旁站C段

## Nmap



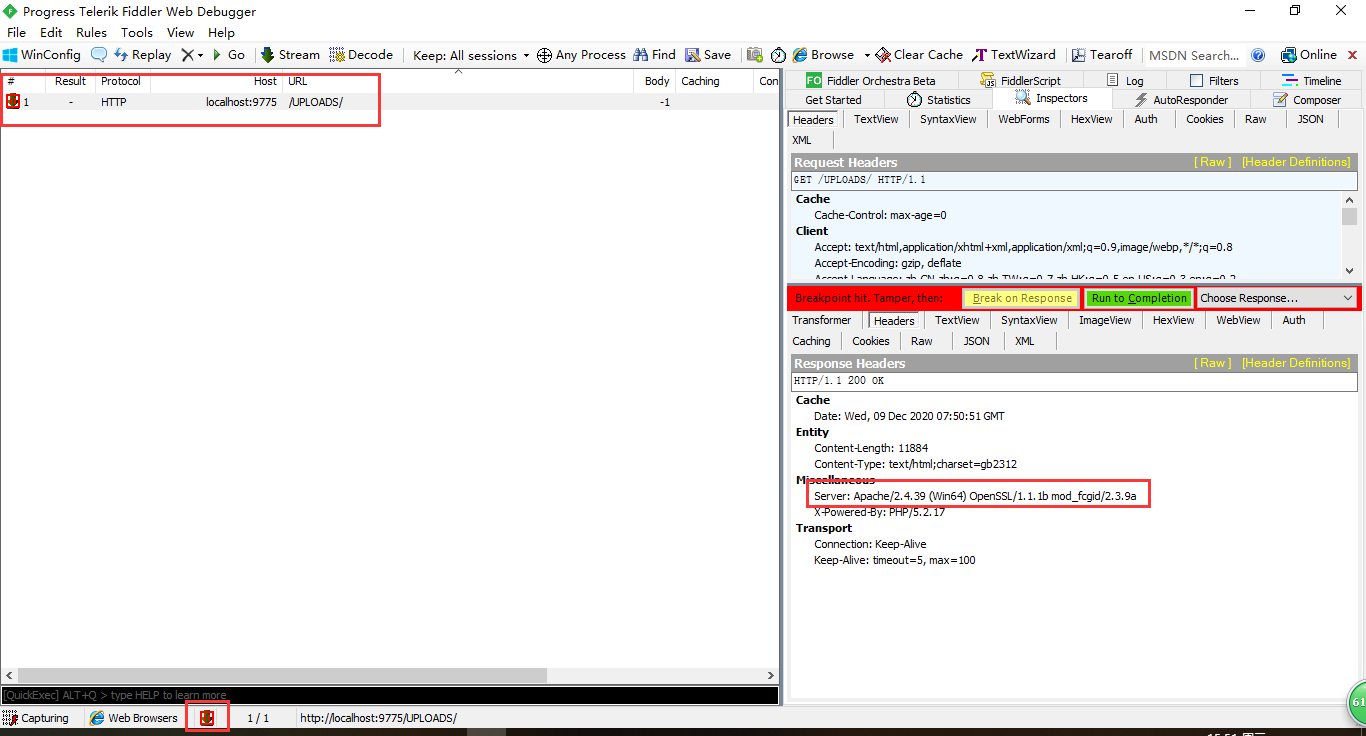
# 整站分析

## 服务器的操作系统---Windows

将http:// localhost:9775/uploads/这个url中某些字母改为大写:

http://localhost:9775/UPLOADS/,仍然能访问，则判断其是Windows系统

## 网站容器---Apache



## 脚本类型---php

## 数据库类型---mysql