WEB- 信息搜集 小集合

原创

菜菜zhao 于 2022-03-20 10:39:03 发布 30 收藏
分类专栏： CTF-web 渗透之路 文章标签： 渗透测试

0x01 查看网页源代码

查看源代码 通过在url头部添加 view-source:

0x02 bp抓包

通过burpsuite抓包 flag在返回的响应数据包里面

或者f12 network里可以看到头部信息。

0x03代码泄露

CTFHUBWeb技能树——信息泄露writeup_青小俊的博客-CSDN博客_ctfhub技能树

直接访问url/www.zip,获得flag

git代码泄露，直接访问url/.git/index.php

信息svn泄露,直接访问url/.svn/

考察vim缓存信息泄露，直接访问url/index.php.swp

0x05 文件泄露

https://www.cnblogs.com/xiaozi/p/12397114.html

robots.txt文件，直接访问url/robots.txt获得flag

phps文件泄露，直接访问index.phps。获得flag

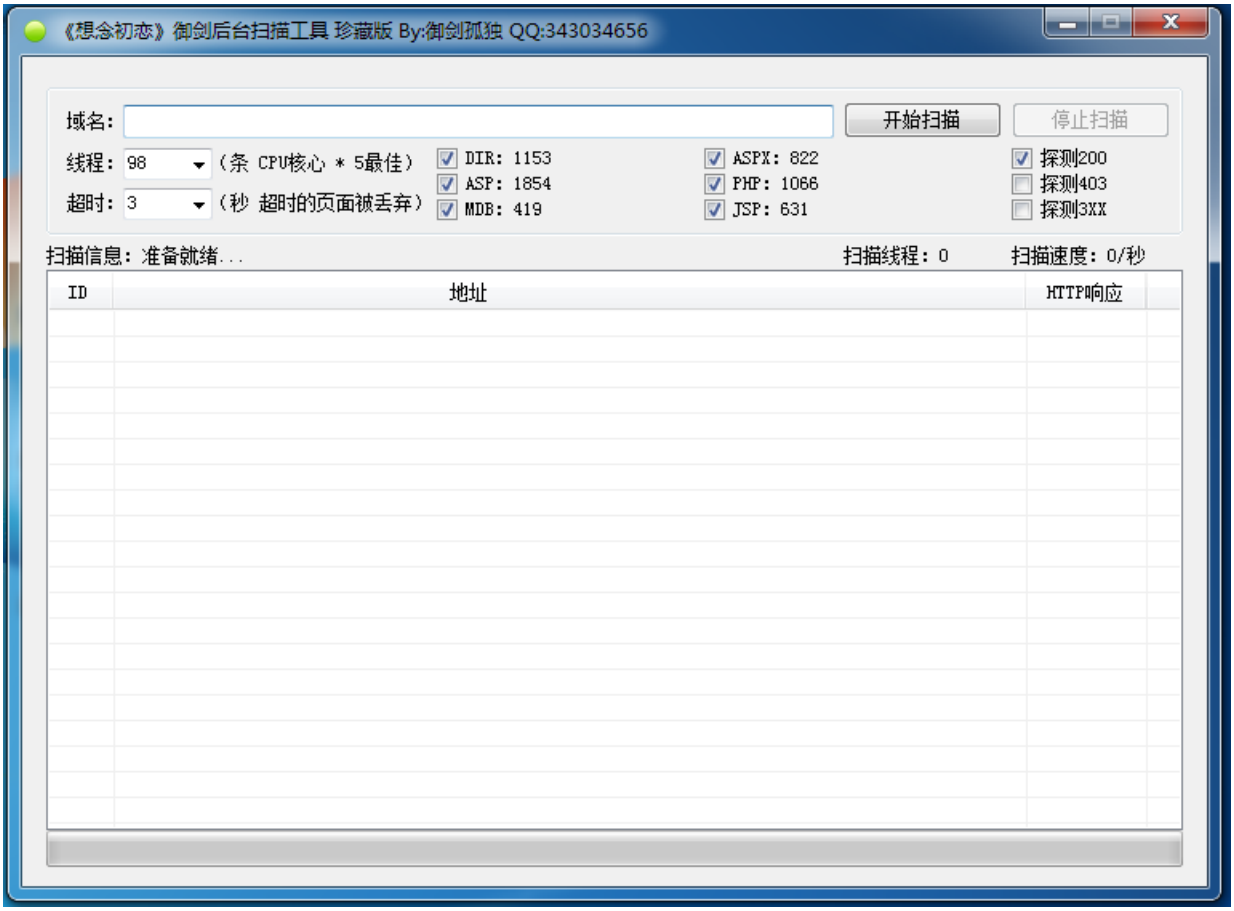
网站备份压缩文件

管理员将网站源代码备份在Web目录下，攻击者通过猜解文件路径，下载备份文件，导致源代码泄露。
常见的备份文件后缀：

- .rar
- .zip
- .7z

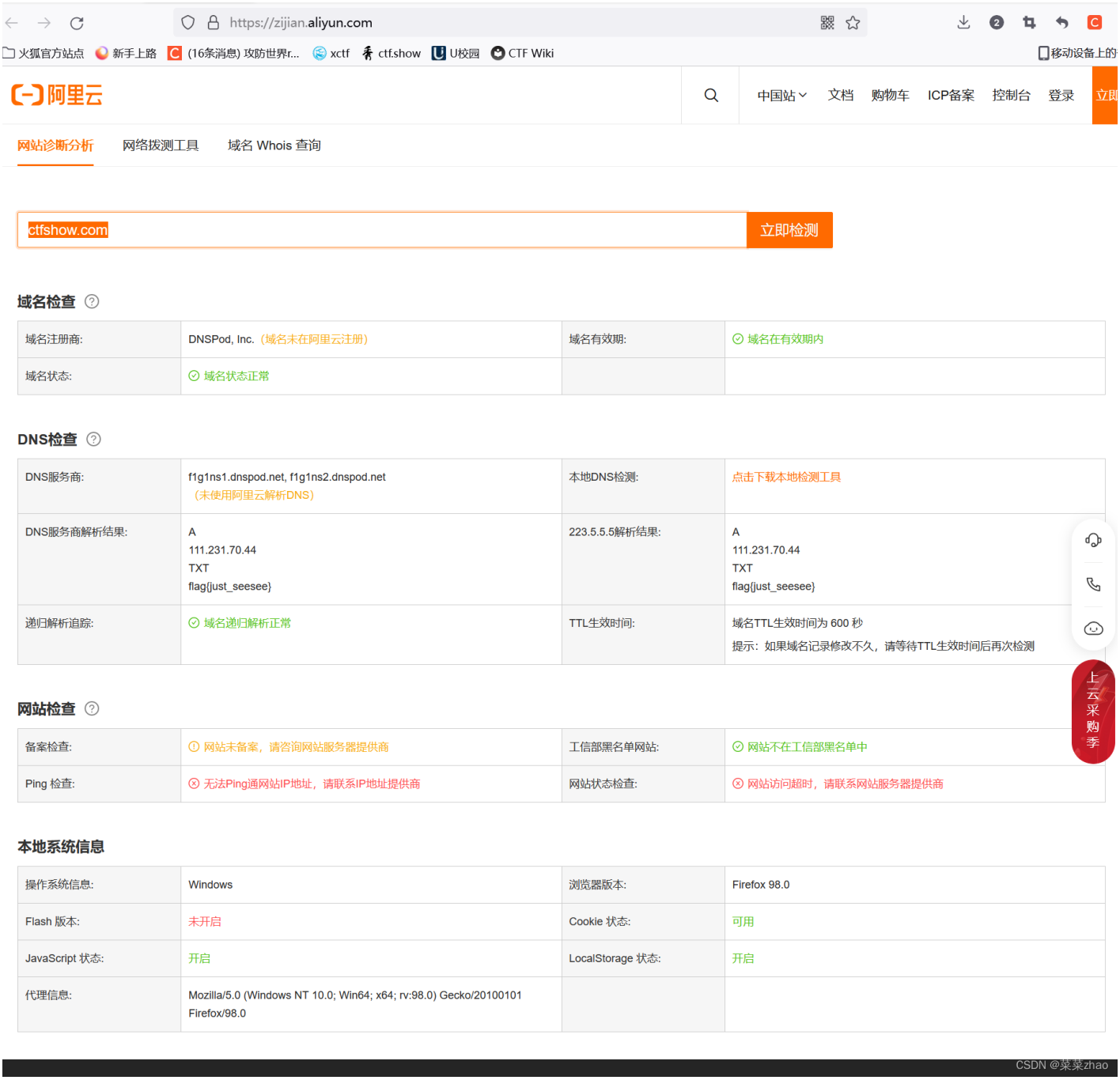
- .tar.gz
- .bak
- .txt
- .old
- .temp

漏洞利用工具：御剑



0x06 域名隐藏信息查询

通过dns检查查询flag 阿里云网站运维检测平台 TXT 记录，一般指为某个主机名或域名设置的说明。



0x07 源码默认泄露信息

小0day:某编辑器最新版默认配置下，如果目录不存在，则会遍历服务器根目录

雅黑php探针

位置：放于网站根目录下

功能：

雅黑PHP探针	PHP参数	组件支持	第三方组件	数据库支持	性能检测	网速检测	MySQL检测	函数检测	邮件检测	探针下载

0x08 备份的sql文件泄露敏感信息

访问url/back.sql 自动下载sql备份文件 获取flag

```sql
CREATE DATABASE IF NOT EXISTS ctfshow;
USE ctfshow;

--
-- Table structure for table `products`
--

CREATE TABLE IF NOT EXISTS `products` (
  `product_id` int(11) NOT NULL,
  `name` varchar(100) NOT NULL,
  `sku` varchar(14) NOT NULL,
  `price` decimal(15,2) NOT NULL,
  `image` varchar(50) NOT NULL,
  PRIMARY KEY (`product_id`),
  UNIQUE KEY `sku` (`sku`)
) ENGINE=InnoDB AUTO_INCREMENT=4 DEFAULT CHARSET=utf8;

CREATE TABLE `ctfshow_secret` (
  `secret` varchar(255) DEFAULT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8;


INSERT INTO `ctfshow_secret` VALUES ('ctfshow{3d40fe50-6648-4414-a2b3-43ff05a5fec8}');

--
-- Dumping data for table `products`
--

INSERT INTO `products` (`product_id`, `name`, `sku`, `price`, `image`) VALUES
(1, 'Iphone', 'IPHO001', '400.00', 'images/iphone.jpg'),
(2, 'Camera', 'CAME001', '700.00', 'images/camera.jpg'),
(3, 'Watch', 'WATC001', '100.00', 'images/watch.jpg');
```


解题参考链接：

Ctfshow web 入门1~20题（萌新向）_base呗的博客-CSDN博客_ctfshow 萌新web17