

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_53146913/article/details/123586659

版权



[CTF-web](#) 同时被 2 个专栏收录

19 篇文章 0 订阅

订阅专栏



[渗透之路](#)

9 篇文章 0 订阅

订阅专栏

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/xiaozhi/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

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。

域名检查

域名注册商:	DNSPod, Inc. (域名未在阿里云注册)	域名有效期:	🟢 域名在有效期内
域名状态:	🟢 域名状态正常		

DNS检查

DNS服务商:	f1g1ns1.dnspod.net, f1g1ns2.dnspod.net (未使用阿里云解析DNS)	本地DNS检测:	点击下载本地检测工具
DNS服务商解析结果:	A 111.231.70.44 TXT flag(just_seesee)	223.5.5.5解析结果:	A 111.231.70.44 TXT flag(just_seesee)
递归解析追踪:	🟢 域名递归解析正常	TTL生效时间:	域名TTL生效时间为 600 秒 提示: 如果域名记录修改不久, 请等待TTL生效时间后再次检测

网站检查

备案检查:	🟡 网站未备案, 请咨询网站服务器提供商	工信部黑名单网站:	🟢 网站不在工信部黑名单中
Ping 检查:	🔴 无法Ping通网站IP地址, 请联系IP地址提供商	网站状态检查:	🔴 网站访问超时, 请联系网站服务器提供商

本地系统信息

操作系统信息:	Windows	浏览器版本:	Firefox 98.0
Flash 版本:	未开启	Cookie 状态:	🟢 可用
JavaScript 状态:	🟢 开启	LocalStorage 状态:	🟢 开启
代理信息:	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0		

CSDN @菜菜zhao

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

```

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');

```

CSDN @菜菜zhao

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](#)