CTF比赛

本工具仅供参考使用

网络安全竞赛，破解题目获取"Flag"。

- **模式**：解题（逆向/Web/密码学）、攻防（实时攻防）。
- CTF主要分为五个方向，Web、pwn、crypto、misc和reverse（逆向）

CTF-Web解题思路

通过给出对应的web应用服务地址，参赛者需要利用web安全知识，寻找对应应用的漏洞点，利用漏洞点越权，获取管理后台、webshell、服务器权限、内网权限等，再利用这些权限读取flag字符串提交。

主要知识点
Web常规漏洞

业务逻辑漏洞

WAF绕过

Burpsuite安装

Burpsuite 是用于攻击 web 应用程序的集成平台。它包含了许多 Burp 工具，这些不同的 Burp 工具通过协同工作，有效的分享信息，支持以某种工具中的信息为基础供另一种工具使用的方式发起攻击。这些工具设计了许多接口，以促进加快攻击应用程序的过程。所有的工具都共享一个能处理并显示 HTTP 消息，持久性，认证，代理，日志，警报的一个强大的可扩展的框架。它主要用来做安全性渗透测试。其多种功能可以帮我们执行各种任务.请求的拦截和修改,扫描 web 应用程序漏洞,以暴力破解登陆表单,执行会话令牌等多种的随机性检查。

原文链接：https://blog.csdn.net/qq_41314882/article/details/147096711a

安装教程: https://www.52pojie.cn/thread-1544866-1-1.html

https://www.52pojie.cn/thread-1953331-1-1.html

数据包

-方法

1、常规请求-Get

2、用户登录-Post

•get：向特定资源发出请求（请求指定页面信息，并返回实体主体）；

•post：向指定资源提交数据进行处理请求（提交表单、上传文件），又可能导致新的资源的建立或原有资源的修改；

Request请求数据包数据格式

host:主机或域名

accept:指浏览器或者是其他用户可以接收板的MIME文件的格式

user-aget:客户浏览器的名称

host:对应网址的URL中的web名称和端口号

accept-encoding:表示浏览器可以接受的编码方式

connetcting：表示是否需要持久连接

referer:表示当前请求是从哪一个URL过来

cookie:表示客户端传递给服务器的cookie信息

Response返回数据包数据格式

状态行：协议版本，数字形式的状态代码和状态描述，各元素之间空格分开

响应头标：包含服务器的类型，日期，长度，内容类型

空行：响应头与响应体之间用空行分开

响应数据：服务器返回给客户端的实际数据

原文链接：https://blog.csdn.net/m0_74120514/article/details/139033876

源码开发语言类型

ASP，ASPX，PHP，Java，Python，Go，Javascript等

语言开发框架组件

PHP：Thinkphp Laravel YII CodeIgniter CakePHP Zend等

JAVA：Spring MyBatis Hibernate Struts2 Springboot等

Python：Django Flask Bottle Turbobars Tornado Web2py等

Javascript：Vue.js Node.js Bootstrap JQuery Angular等

Wappalyzer - Technology profile

Wappalyzer，这款强大的跨平台工具，犹如一位网站技术的侦探，能够深入剖析网站所采用的各种技术。无论是内容管理系统（CMS）、电商平台、Web框架，还是服务器软件、分析工具等，它都能一一检测并揭示。简而言之，只需轻点一键，便能轻松洞悉一个网站的全方位技术细节。

安装教程:https://blog.csdn.net/qq_40168905/article/details/128649639（火狐浏览器）

火狐代理安装

扩展页面搜索"FoxyProxy"

链接:https://blog.csdn.net/qq_41210660/article/details/129826226

火狐HackBar安装

链接:https://blog.csdn.net/weixin_44657888/article/details/123515537

目录扫描工具：dirsearch-master

https://github.com/maurosoria/dirsearch

文件上传漏洞

HG泄露（Mercurial）

Mercurial（通常简称为 HG）是一种分布式版本控制系统，用于管理软件源代码或其他文件集的变更历史。当提到“HG 泄露”，我们通常指的是 Mercurial 仓库或其中包含的敏感信息被未经授权的个人或系统访问的情况。

链接: https://blog.csdn.net/qq_69100706/article/details/140505075

链接:https://blog.csdn.net/Fly_hps/article/details/139531219

SVN泄露

SVN（subversion）是程序员常用的源代码版本管理软件。在使用 SVN 管理本地代码过程中，使用 svn checkout 功能来更新代码时，项目目录下会自动生成隐藏的.svn文件夹（Linux上用 ls 命令看不到，要用 ls -al 命令），其中包含重要的源代码信息。

造成SVN源代码漏洞的主要原因是管理员操作不规范，一些网站管理员在发布代码时，不愿意使用“导出”功能，而是直接复制代码文件夹到WEB服务器上，这就使得.svn隐藏文件夹被暴露于外网环境，黑客对此可进一步利用：

链接:https://developer.aliyun.com/article/1612352

`$_FILES` 是一个预定义的全局数组，用于在 PHP 中处理 HTTP 文件上传。要有效利用 `$_FILES`，您需要遵循以下步骤：

1. 检查文件上传是否成功： 使用 `isset()` 函数检查 `$_FILES` 数组中是否存在指定的文件。例如，检查名为 `file_upload` 的文件是否已上传：

```php
if (isset($_FILES['file_upload'])) {
    // 文件上传成功
} else {
    // 文件上传失败
}
```

检查文件大小： 使用 `$_FILES['file_upload']['size']` 获取上传文件的大小。您可以使用 `if` 语句检查文件大小是否符合您的要求。例如，检查文件大小是否小于 2MB：

```php
if ($_FILES['file_upload']['size'] < 2097152) {
    // 文件大小小于 2MB
} else {
    // 文件大小大于等于 2MB
}
```

链接: https://www.yisu.com/ask/97835858.html

UPLOAD_PATH

`UPLOAD_PATH` 需在代码其他位置定义（如 `define('UPLOAD_PATH', 'uploads')`）

1. `||` **的作用**：
    - 表示逻辑“或”（OR），即只要满足 **任意一个条件**，整个表达式就为 `true`。
    - 例如：
        - 如果文件类型是 `image/jpeg`，条件成立。
        - 如果文件类型是 `image/png`，条件也成立。

        - 只要满足其中一个，就允许文件上传。
2. **对比逻辑与（`&&`）**：
    - 如果此处用逻辑与（`&&`），则必须 **同时满足所有条件**，但文件类型不可能同时是 `image/jpeg`、`image/png` 和 `image/gif`，因此条件永远不成立。