

周报7

Web基础:

TCP/IP协议:

TCP/IP是传输控制协议和网际协议的简称，是一种允许不同网络之间进行信息传输的协议集合。

IP协议(网际互联协议)，他是网络层

作用：将不同类型的物理网络互联在一起，将不同格式数据帧转换为IP数据包，将不同的格式数据包的物理地址转换为统一的IP地址

TCP协议(传输控制协议)位于传输层，是面向链接的协议。

域名DNS:

一个Ip地址可以对应多个域名，那么我们在渗透测试的时候就要吧域名转换为IP地址，转换方法有ping域名或者说我们直接使用在线解析域名工具，直接将域名转换为IP地址。其中.uk代表美国，.fr代表法国，.jp代表日本，.cn代表中国。.com说明是企业，.edu代表教育机构，.gov代表政府，.mil代表军事部门，

URI:

什么是URI，就是统一资源定位符，即网址。并且URL分为三部分组成，协议名称(包括http，ftp，file)，主机名，文件名。因为比较熟悉URL则一部分，所以就不举例子说明URL这个地址了。

PHP:

php基础:

isset()函数：判断括号内的变量是不是空的，如过是空的，那么就返回false，否则返回true

function 用于用户声明自定义函数

file_put_contents() 函数把一个字符串写入文件中

file_get_contents() 函数把整个文件读入一个字符串中

is_valid() 检查对象变量是否已经实例化，即实例变量的值是否是个有效的对象

strlen 计算字符串长度

php序列化与反序列化:

序列化就是将代码转化为二进制，而反序列化就是讲二进制转化为代码。

作用：传输数据。


序列化serialize()这个函数是序列化的函数，可以将代码转化为二进制。

```
1 <?php
2 class test                                //定义一个test类
3 {
4     public $test1="11";
5     protected $test2="hh";
6     private $test3="nn";
7 }
8 $a=new test();                            //类test实例化成一个对象，并赋值给a
9 echo serialize($a);                      //序列化对象a
10 ?>
1
2 //输出  O:4:"test":3:{s:5:"test1";s:2:"11";s:8:" * test2";s:2:"hh";s:11:" test test3";s:2:"nn";}
```

反序列化unserialize()这个函数是用来进行反序列化的

备份文件就是某个url的备份文件

常见的网站源码备份文件后缀:
tar.gz, zip, rar, tar

常见的网站源码备份文件名:
web, website , backup, back, www, wwwroot, temp

```
D:\dirsearch-master>python dirsearch.py -u http://659ca908-14e3-4ce9-8070-e151a5f8f991.node3.buuoj.cn/ -e *  
v0.4.1  
Extensions: php, jsp, jsf, asp, aspx, do, action, cgi, pl, html, htm, js, json, json, tar.gz, tgz | HTTP method: GET  
Threads: 30 | Wordlist size: 15897  
Error Log: D:\dirsearch-master\logs\errors-21-06-18_10-55-39.log  
Target: http://659ca908-14e3-4ce9-8070-e151a5f8f991.node3.buuoj.cn/  
Output File: D:\dirsearch-master\reports\659ca908-14e3-4ce9-8070-e151a5f8f991.node3.buuoj.cn\_21-06-18_10-55-39.txt  
[10:55:39] Starting:  
[10:55:40] 503 - 194B - /asp.bak  
[10:55:40] 503 - 194B - /asp  
[10:55:40] 503 - 194B - /cgi  
[10:55:40] 429 - 166B - /jsf.bak  
[10:55:40] 429 - 166B - /aspx.bak  
[10:55:40] 503 - 194B - /pl.bak  
[10:55:40] 429 - 166B - /js.bak  
[10:55:40] 503 - 194B - /action.bak  
[10:55:40] 429 - 166B - /js  
[10:55:40] 503 - 194B - /cgi.bak  
[10:55:40] 429 - 166B - /json.bak  
[10:55:40] 429 - 166B - /aspx  
[10:55:40] 429 - 166B - /htm.bak  
[10:55:40] 429 - 166B - /httpd.conf
```

就像上边一样，直接用dirreach扫描目标文件。

dirreach安装以及扫描：

dirreach的安装：

首先，我们先要确定自己的kali安装的是不是最新版本，如果说不是最新版本的话，我们需要来在root命令框里边执行代码，让kali更新道最新版本，就是使用git安装，我们需要输入git clone <https://github.com/maurosoria/dirsearch.git> —depth-1 ,这个代码就是将github上克隆dirsearch的代码库到本地。我们试一下可不可以这个 cd dirsearch 如果可以的话就成功这一步了。第二我们需要安装mysql模块，就是输入mysql- connerctor -python来安装，安装完成后的话我们运行python3 dirsearch.py -u <http://baidu.com> -e php ,txt -t 50。第三步的话我们需要安装defusedcsv模块，输入命令 pip3 install defusedcsv。第四步我们需要安装，httpx_ntlm模块，我们使用pip3来安装这个模块，输入pip3 install httpx_ntlm ,然后再安装requests_toolbelt模块，输入命令pip3 install requests_toolbelt那么最后我们就可以来扫描了。

dirsearch扫描：

假如说我们需要扫描

就像这个样子我们使用dirsearch来扫描python3 dirsearch.py -u <http://aq.fxamn.top> -e php,txt -t 10 这个网站的目录。以上状态为200的就都是开放的，我们就可以直接去访问了。