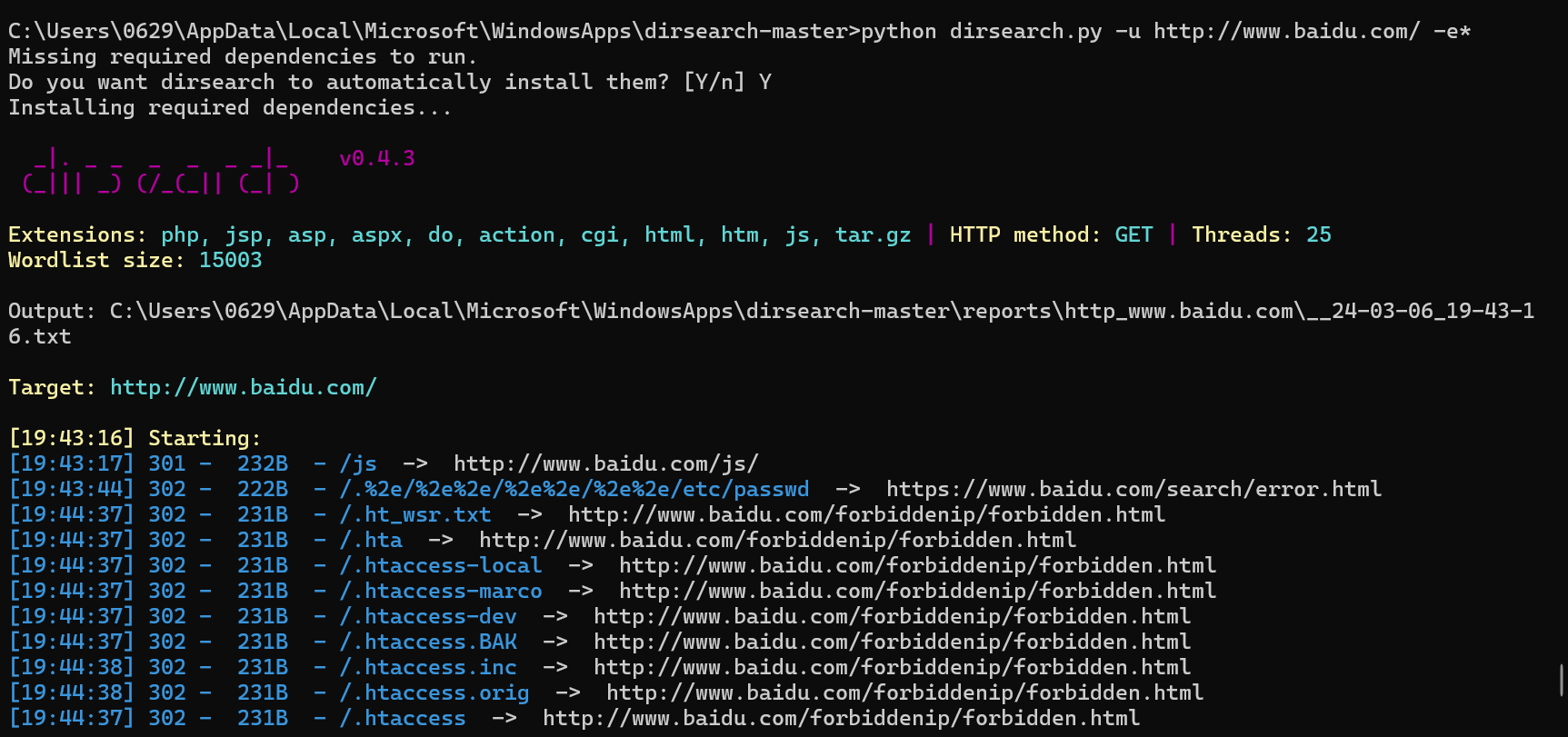
工具：dirsearch

使用方法：通过目录“C:\Users\0629\AppData\Local\Microsoft\WindowsApps\dirsearch-master”打开命令提示行

使用代码：python dirsearch.py -u http://www.baidu.com/ -e\*



任意文件读取：

漏洞成因：

<?php

$filename = $\_GET['file'];

if(isset($filename)){

readfile($filename);

}

?>

敏感文件：

Linux：

/etc/passwd // 账户信息

/etc/shadow // 账户密码文件

/etc/my.conf //mysql 配置文件

/etc/httpd/conf/httpd.conf // Apache配置文件

/usr/local/app/apache2/conf/httpd.conf //Apache2默认配置文件

/usr/local/app/apache2/conf/extra/httpd-vhost.conf //虚拟网站配置

/usr/local/app/php5/lib/php.ini //PHP相关配置

Windows：

C:\boot.ini //查看系统版本

C:\Windows\System32\inetsrv\MetaBase.xml //IIS配置文件

C:\Windows\repair\sam //存储系统初次安装的密码

C:\Program Files\mysql\my.ini //Mysql配置

C:\Program Files\mysql\data\mysql\user.MYD //Mysql root密码

C:\Windows\php.ini //php配置信息

文件读取漏洞的触发点们：

3.中间件/服务器相关触发点

3.1 Nginx错误配置----------------------------------------------------------------------nginx.conf

Location /static{

Alias /home/myapp/static/;

}

如果配置文件中包含上面这段内容，很可能是运维或者开发人员想让用户可以访问static目录（一般是静态资源目录）。

如果用户请求的Web路径是/static…/，拼接到alias上就变成了/home/myapp/static/…/，此时便会产生目录穿越漏洞，并且穿越到了myapp目录。

假设服务器上存在一个文件路径为/var/www/html/index.php的文件，攻击者通过任意文件读取漏洞想要读取该文件的内容，而服务器的Nginx配置文件/etc/nginx/nginx.conf中包含以下

错误配置：

location ~ \.(php)$ {//使用了一个正则表达式来匹配所有以.php结尾的URL

include fastcgi\_params;

fastcgi\_pass unix:/var/run/php-fpm/php-fpm.sock;//php-fpm是php解释器

fastcgi\_param SCRIPT\_FILENAME /var/www/html$fastcgi\_script\_name;

}

这个配置的意思是将以.php结尾的请求交给PHP解释器处理，并将文件路径设置为/var/www/html加上请求的文件名。这里存在一个问题，就是如果攻击者发送以下请求：

http://example.com/index.php/../../../etc/passwd

由于Nginx的正则表达式匹配，$fastcgi\_script\_name会被设置为/index.php/../../../etc/passwd