**目录爆破都能发现哪些信息？**

后台目录—>弱口令、万能密码、爆破

备份文件—>获取数据库信息，甚至是网站的源码

上传接口—>通过上传拿到webshell

管理接口—>弱口令、爆破

安装页面—>可以二次安装进而绕过

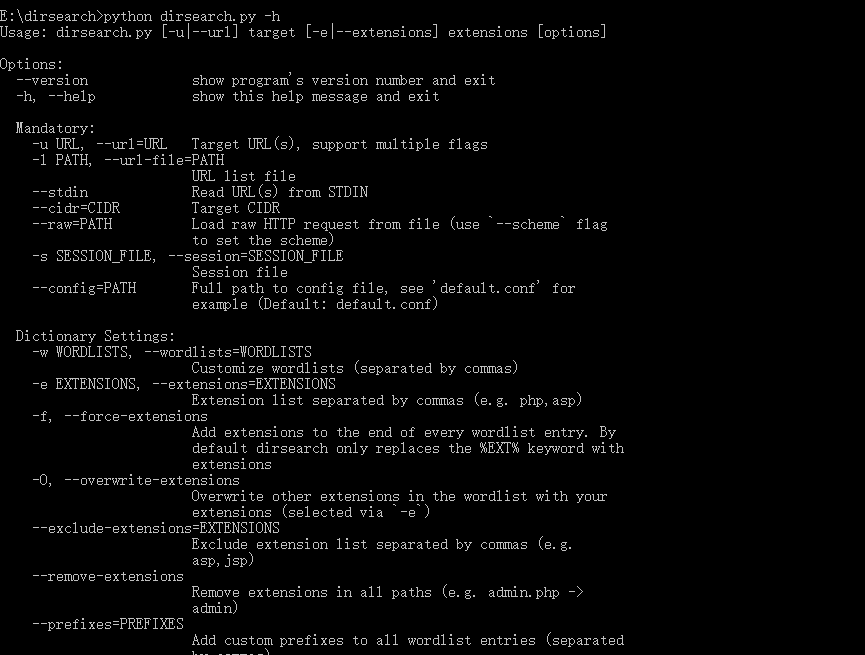
Phpinfo—>会暴漏配置信息

未认证的接口—>泄露敏感信息

...

**参数介绍**

-h：在目录搜索中使用‘-h’可获取完整的参数列表和潜在的配置设置



常用的参数：

1、**-u：指定有效的目标URL**

python dirsearch.py -u "http://example.com"

2、**-e：指定要搜索的文件扩展名，会替换掉字典中%EXT%为指定的extensions**

python dirsearch.py -u "http://example.com" -e php,jsp

3、**-l：批量爆破URL**

python dirsearch.py -u "http://example.com" -l url.txt

4、**-x：排除指定的状态码**

python dirsearch.py -u "http://example.com" -x 403

5、**-r：递归爆破，通常和-R结合（跑出目录后，继续跑目录下面的目录**）

python dirsearch.py -u "http://example.com" -r -R 3 //设置递归层数为3

6、**-w：指定字典的路径，dirsearch默认字典在db目录下**

python dirsearch.py -u "http://example.com" -w db\dir.txt

7、**--cookie：设置cookie**

python dirsearch.py -u "http://example.com" --cookie session=xxx

8、-t：设置线程，默认情况下线程数为30，如果想加快速度，可以增加线程，（不建议增加线程，因为线程过大的话，会导致DOS，导致后面的爆破就会不准确）

9、**--exclude-regex：通过正则匹配排除响应**

python dirsearch.py -u "http://example.com" --exclude-regex '^not found$'

10、**--format：format报表格式（可用:simple、plain、json、xml、md、csv、html，可在default.conf中修改默认报表格式）**

python dirsearch.py -u "http://example.com" --format json -o target.json