**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

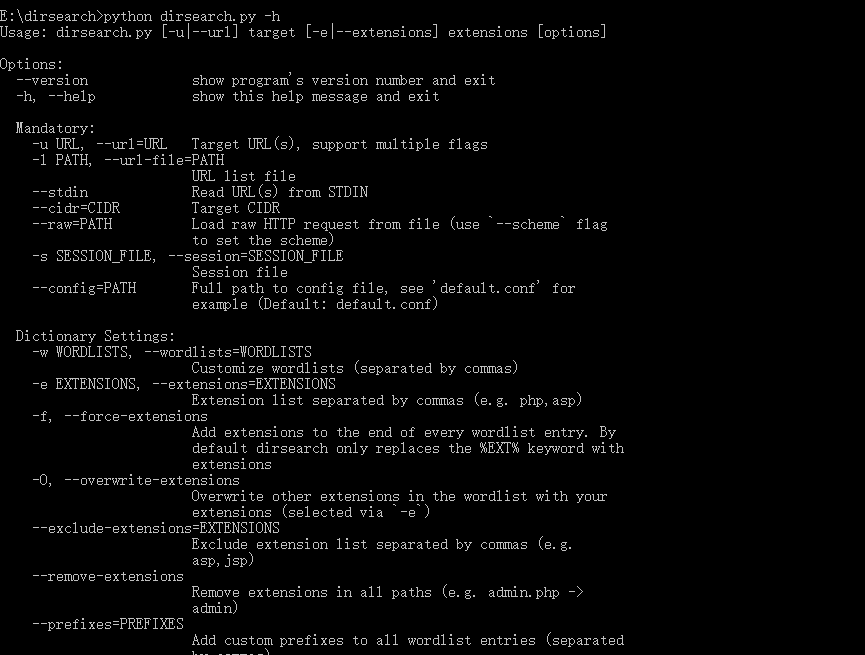
安装页面—>可以二次安装进而绕过

Phpinfo—>会暴漏配置信息

...

**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：

-u：指定有效的目标URL

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

-e： 指定要搜索的文件扩展名

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

-l： 批量爆破URL

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

-x：排除指定的状态码

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

-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

-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

--cookie：设置cookie

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