WEB渗透系列之侦查：SKIPFISH

> Skipfish是一款Web应用安全侦查工具。Skipfish会利用递归爬虫和基于字典的探针生成一幅交互式网站地图。最终生成的地图会在通过安全检查后输出。

一、使用参数

```
skipfish [options] -o outpu-directory target-url
```

1. 字典

`skipfish`自带的字典文件位于目录`/usr/share/skipfish/dictionaries/`下，共有四个字典。分别为大中小及扩展名。

```
ls -l /usr/share/skipfish/dictionaries/
```

字典参数：

```
-W wordlist    - 指定一个可读写的字典
-S wordlist    - 指定一个附加的只读字典
```

2. 文件输出

将结果输出到指定文件夹。

```
-o dir     - 指定一个目录以输出结果
```

3. 目标链接

可以直接指定一个域名或主机。

二、扫描演示

此次设定目标为位于局域网的网站`https://terratest.earth.local`。字典使用`complete.wl`。保存结果到文件夹`earth`。

1. 开始扫描

```
skipfish -o earth -S /usr/share/skipfish/dictionaries/complete.wl
https://terratest.earth.local
```

> 扫描过程中，可以按下空格键查看扫描细节。

2. 查看结果

扫描结束后会在文件夹`earth`下生成许多文件，进入文件夹`earth`并打开文件`index.html`来查看结果。

```
firefox index.html
```

> 结果总共包括三个部分：
>
> - 爬取结果
> - 文件类型概览
> - 问题类型概览