skipfish web application scanner - version 2.10b

格式: skipfish [ 选项 ... ] -W wordlist -o output\_dir start\_url [ start\_url2 ... ]

认证和访问选项:

-A user:pass - 使用指定的HTTP身份验证凭据

-F host=IP - 假装“主机”解决了“IP”

-C name=val - append a custom cookie to all requests

-H name=val - 添加一个自定义HTTP头的所有要求

-b (i|f|p) - 使用标题因为IE / Firefox / iPhone一致

-N - 不要接受任何新的饼干

--auth-form url - 形式验证URL

--auth-user user - 形式验证的用户

--auth-pass pass -形式验证的密码

--auth-verify-url - 会话检测中的网址

爬行范围选项:

-d max\_depth - 最大爬行树深度 (16)

-c max\_child - 每个节点最大的每个节点(512)

-x max\_desc - 最大后裔每分指数 (8192)

-r r\_limit - 发送的请求的最大总数量 (100000000)

-p crawl% - 节点和链路爬行概率 (100%)

-q hex - 给定种子的重复概率扫描

-I string - 只有按照网址匹配的“字符串”

-X string - 排除网址匹配的“字符串”

-K string - 不要模糊参数命名为“字符串”

-D domain - 爬行跨站点链接到另一个域

-B domain -信任，但不要爬行，另一个域

-Z - 不要陷入5xx位置

-O - 不提交任何形式

-P - 不解析html，等找到新的链接

报告选项:

-o dir - 将输出写入指定的目录（所需的）

-M - 日志关于混合内容/非SSL密码警告

-E - 记录所有HTTP / 1 / 1.1 / HTTP缓存的意图不匹配

-U - 记录所有的外部网址和电子邮件

-Q - 完全抑制报表中的重复节点 -u

- 安静，禁用进度实时数据

-v - 使运行日志（stderr）

词典管理选项:

-W wordlist - 使用指定的读写词表（需要）

-S wordlist - 负荷补充只读表

-L - 不要自动学习网站的新关键字

-Y - 不在目录的蛮力模糊扩展

-R age - 清除的话击中超过“年龄”扫描前

-T name=val - 添加新的表格自动填充规则

-G max\_guess - 关键字猜测的最大数量 (256)

-z sigfile - 从这个文件中加载签名

性能设置:

-g max\_conn - 最大并发TCP连接，全球 (40)

-m host\_conn - 最大同时连接，每目标IP(10)

-f max\_fail - 最大连续HTTP错误数 (100)

-t req\_tmout - 总请求响应超时(20 s)

-w rw\_tmout - 个人网络I / O超时 (10 s)

-i idle\_tmout - 对闲置的HTTP连接超时 (10 s)

-s s\_limit - 响应大小限制(400000 B)

-e - 不要保持二进制响应报告

其他设置:

-l max\_req - 每秒最大请求数(0.000000)

-k duration -在给定的持续时间h后停止扫描：M

--config file - 加载指定的配置文件

Send comments and complaints to <heinenn@google.com>.