寻找网站后台路径的N种姿势

作者: LANDGREY ● 创建时间 2017年7月27日 23:16 ● 更新时间 2017年8月24日 20:29

下列方法无刻意排列顺序，仅为备忘记录。

一：间接接触

0x01: search

```
1. 直接搜索目标可能存在的相关后台路径
site:target.com intitle:"后台|登录|登陆|验证码|管理员|服务系统|系统登录|认证码|验证身份|管理系统|管理后台|管理平台

2. 尝试搜索一些文档型资料路径，判断是否包含后台路径
site:target.com filetype:"doc | docx | pdf | xls | xlsx | ppt | pptx"

3. 在目标链接较少的情况下，可以浏览网站所有路径，顺便观察组成特点，构造出后台路径
site:target.com
```

二：直接接触

0x02: view the site

```
1. 查看robots.txt文件，查看是否存在网站后台路径
2. 使用传统路径爆破方式，猜测可能存在的后台路径
3. 识别网站是否是常见CMS或框架，使用对应的默认路径尝试
4. 直接浏览目标网站，注意网站界面的左手方和底部，查看是否有后台直达链接
5. 注意观察Cookies等HTTP头信息，寻找特殊Banner，搜索相关应用框架信息，确定后台路径
6. 寻找网站页面源码中的特殊Banner，去google搜索或Github等平台查找源码信息，确定后台路径
7. 尝试手工或自动fuzzing网站，致使其报错，查看是否有相关路径信息，进而猜测后台路径信息
8. 查看网站页面源码，注意链接路径(特别是上传的图片、文件等资源链接)，验证是否包含后台路径
9. 利用网站的特殊文件(通常需要扫描)，如整站源码压缩备份文件、phpinfo页面、默认探针文件、README、Lisense文件、部署
10. 网站爬虫(通常使用爬虫工具，如AWVS、Netsparker、Burpsuite)，爬取网站链接，分析提取后台路径信息
```

0x03: open mind

1. 端口扫描，判断后台是否部署在同一主机的其它端口
2. 子域名收集，判断后台是否部署在子域名的某台主机上
3. 利用漏洞(如旁站漏洞、XSS、任意文件读取)，间接获得后台路径地址
4. 结合网站鲜明的特征信息(个人博客名、域名、机构名)，构造可能存在的后台路径
5. 网站有开发者、外包公司等信息，尝试社工方式联系客服等相关人员(如想买相同系统,希望看个样例后台页面)，套出默认后台

三：此路不通，绕道而行

<