Web安全攻防之敏感信息泄露

　　软件敏感信息

　　\* 操作系统版本

　　可用namp扫描得知

　　\* 中间件的类型、版本

　　http返回头

　　404报错页面

　　使用工具(如whatweb)

　　\* Web程序(cms类型及版本、敏感文件)

　　可用whatweb、cms\_identify

　　Web敏感信息

　　\* phpinfo()信息泄漏

　　http://[ip]/test.php和http://[ip]/phpinfo.php

　　\* 测试页面泄漏在外网

　　test.cgi、phpinfo.php、info.php等

　　\* 编辑器备份文件泄漏在外网

　　http://[ip]/.test.php.swp

　　http://[ip]/test.php.bak

　　http://[ip]/test.jsp.old

　　http://[ip]/cgi~

　　常见编辑器备份后缀

　　\* 版本管理工具(如git)文件信息泄漏

　　http://[ip]/.git/config

　　http://[ip]/CVS/Entriesp

　　http://[ip]/.svn/entriesp

　　\* HTTP认证泄漏漏洞

　　http://[ip]/basic/index.php

　　Web目录开启了HTTP Basic认证，但未限制IP，导致可暴力破解账号、密码

　　\* 管理后台地址泄漏

　　http://[ip]/login.php

　　http://[ip]/admin.php

　　http://[ip]/manager.php

　　http://[ip]/admin\_login.php

　　\* 泄漏员工邮箱、分机号码

　　泄漏邮箱及分机号码可被社工，也可生成字典

　　\* 错误页面暴漏信息

　　面熟sql错误、php错误、暴漏cms版本等

　　\* 探针文件

　　\* robots.txt

　　\* phpMyAdmin

　　\* 网站源码备份文件(www.rar/sitename.tar.gz/web/zip等)

　　\* 其他

　　网络信息泄漏

　　\* DNS域传送漏洞

　　\* 运维监控系统弱口令、网络拓扑泄漏

　　zabbix弱口令、zabbix sql注入等

　　第三方软件应用

　　\* github上源码、数据库、邮箱密码泄漏

　　搜类似：smtp 163 password关键字

　　\* 百度网盘被员工不小心上传敏感文件

　　\* QQ群被员工不小心上传敏感文件

　　敏感信息搜集工具

　　https://github.com/ring04h/weakﬁlescan

　　https://github.com/lijiejie/BBScan

　　whatweb

　　dnsenum

　　github

　　示例

