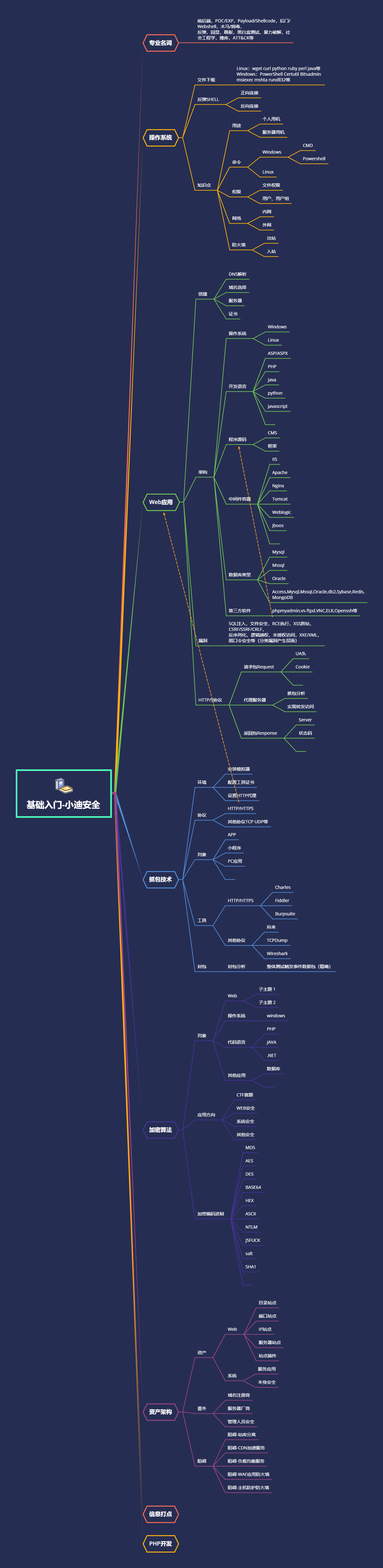
信息打点-资产泄漏&CMS识别&Git监控&SVN&DS\_Store&备份



#知识点：

CMS指纹识别源码获取方式

习惯&配置&特性等获取方式

3、托管资产平台资源搜索监控

#详细点：

参考：https://www.secpulse.com/archives/124398.html

源码泄漏原因：

1、从源码本身的特性入口

2、从管理员不好的习惯入口

3、从管理员不好的配置入口

4、从管理员不好的意识入口

5、从管理员资源信息搜集入口

源码泄漏集合：

composer.json

git源码泄露

svn源码泄露

hg源码泄漏

网站备份压缩文件

WEB-INF/web.xml 泄露

DS\_Store 文件泄露

SWP 文件泄露

CVS泄露

Bzr泄露

GitHub源码泄漏

演示案例：

* 直接获取-CMS识别-云悉指纹识别平台
* 习惯不好-备份文件-某黑阔博客源码泄漏
* 配置不当-GIT泄漏-某程序员博客源码泄漏
* 配置不当-SVN泄漏-某国外小伙子源码泄漏
* 配置不当-DS\_Store泄漏-某开发Mac源码泄漏
* PHP特性-composer.json泄漏-某直接搭建源码泄漏
* 下载配合-WEB-INF泄露-RoarCTF-2019-EasyJava
* 资源监控-GITHUB泄漏-语法搜索&关键字搜索&社工

相关利用项目：

CMS识别：https://www.yunsee.cn/

备份：敏感目录文件扫描-7kbscan-WebPathBrute

CVS：https://github.com/kost/dvcs-ripper

GIT：https://github.com/lijiejie/GitHack

SVN：https://github.com/callmefeifei/SvnHack

DS\_Store：https://github.com/lijiejie/ds\_store\_exp

GITHUB资源搜索：

in:name test #仓库标题搜索含有关键字

in:descripton test #仓库描述搜索含有关键字

in:readme test #Readme文件搜素含有关键字

stars:>3000 test #stars数量大于3000的搜索关键字

stars:1000..3000 test #stars数量大于1000小于3000的搜索关键字 forks:>1000 test #forks数量大于1000的搜索关键字

forks:1000..3000 test #forks数量大于1000小于3000的搜索关键字 size:>=5000 test #指定仓库大于5000k(5M)的搜索关键字 pushed:>2019-02-12 test #发布时间大于2019-02-12的搜索关键字 created:>2019-02-12 test #创建时间大于2019-02-12的搜索关键字 user:test #用户名搜素

license:apache-2.0 test #明确仓库的 LICENSE 搜索关键字 language:java test #在java语言的代码中搜索关键字

user:test in:name test #组合搜索,用户名test的标题含有test的

关键字配合谷歌搜索：

site:Github.com smtp

site:Github.com smtp @qq.com

site:Github.com smtp @126.com

site:Github.com smtp @163.com

site:Github.com smtp @sina.com.cn

site:Github.com smtp password

site:Github.com String password smtp

涉及资源：

[补充：涉及录像课件资源软件包资料等下载地址](https://docs.qq.com/doc/DQ3Z6RkNpaUtMcEFr)