EMP组件任意文件上传

漏洞特征

漏洞原理

利用方法

漏洞特征

请求头特征：Content-Type: multipart/form-data; boundary=
请求体（body）中包含恶意代码（如一句话木马）
指纹：inurl:EMP_SID

漏洞原理

程序处理请求的Servlet代码中，当请求报文的报文头中包含分隔符“boundary=”时，认为该请求为“multipath/form-data”类型，默认执行文件上传处理，并上传到固定目录，文件在后续业务流程中选择是否进行解析。

利用方法

通过任意接口调用，在request header里添加Content-Type: multipart/form-data; 触发系统文件上传功能，将form-data里写入恶意代码，并POST写入指定目录。