|  |  |
| --- | --- |
| **漏洞分类** | **漏洞名称（按实际修改）** |
| 代码执行 |  |
| 注入 | SQL、LDAP、XPath、NoSQL查询语句、OS命令、XML解析器、表达式语言(EL)/OGNL、SMTP/IMAP 、ORM、XXE、HPP、SSI |
| 失效的身份认证 | 密码自动填充、用户枚举、暴力破解、默认密码、弱密码、弱密保、缺少/失效的多因素认证、会话固定、会话保持、登录失败次数限制、会话ID暴露在URL中 |
| 敏感信息泄露 | 密码、财务数据、医疗数据、PII数据 |
| 未授权访问 |  |
| 不安全的配置 | 不安全的默认配置、不必要的服务/功能、测试页面、错误处理机制向用户披露堆栈跟踪或其他大量错误信息、应用程序服务器/框架（如：Struts、Spring、ASP.NET）/库文件/数据库等没有进行安全配置、错误的HTTP头配置、目录列举、明文存储密码、弱hash存储密码 |
| 跨站脚本攻击（XSS） | 反射型XSS、存储型XSS、DOM Based XSS |
| 跨站请求伪造（CSRF） |  |
| 服务端请求伪造（SSRF） |  |
| 越权 | 水平越权、垂直越权 |
| 不安全的反序列化 |  |
| 拒绝服务 |  |
| 使用含有已知漏洞的组件 |  |
| 任意文件上传 |  |
| 文件包含 | 任意文件读取 |
| 不严格的数据合法性校验 |  |
| 业务逻辑 | 密码找回、短信轰炸、金额/商品数量篡改 |
| 其他 |  |