（1）【未授权访问】

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **被测对象** | 执法处 重点排污单位超标异常电子告知与督办平台 | | | **问题编号** |  |
| **URL/IP** | https://m.gdeei.cn/duban/#/login | | | | |
| **漏洞类型** | 未授权访问 | | | | |
| **漏洞描述** | 未授权访问漏洞，是在攻击者没有获取到登录权限或未授权的情况下，或者不需要输入密码，即可通过访问接口，获取应用系统敏感信息。 | | | | |
| **漏洞等级** | □超危 □高危 ☑中危 □低危 | | | | |
| **风险评估** | 未经过验证即可访问系统业务信息。 | | | | |
| **整改建议** | 常见的修复方法：在系统中，加入用户身份认证机制或者tonken验证，防止可被直接通过连接就可访问到用户的功能进行操作，简而言之，一定对系统重要功能点增加权限控制，对用户操作进行合法性验证，。 | | | | |
| **检测时间** | 2024年12月02日 | **检测人员** |  | | |
| **整改结果** |  | | | | |
| **漏洞证明** | | | | | |
| 第一步：通过收集前端源码信息获取接口，如下：    第二步，构造拼接请求，发现大量接口存在未授权访问 | | | | | |
| **整改情况记录** | | | | | |
|  | | | | | |