附件：IP为“10.113.242.105”内网系统存在SQL注入万能密码漏洞

|  |  |
| --- | --- |
| **所属单位** | 国电电力（新疆新能源） |
| **IP地址** | 10.113.242.105 |
| 主要问题 | SQL注入 |
| **减分情况** |  |
| **弱口令** | 无 |
| **验证结果** | 通过万能密码（admin’or 1=1-- -)可进入机房动力和环境监控系统的后台。 |
| **整改要求** | 1.对进入数据库的特殊字符（'"\尖括号&\*;等）进行转义处理，或编码转换。  2.严格限制变量类型，数据库中的存储字段必须对应为int型。  3.数据长度应该严格规定，能在一定程度上防止比较长的SQL注入语句无法正确执行。  4.网站每个数据层的编码统一，建议全部使用UTF-8编码，上下层编码不一致有可能导致一些过滤模型被绕过。  5.严格限制网站用户的数据库的操作权限，给此用户提供仅仅能够满足其工作的权限，从而最大限度的减少注入攻击对数据库的危害。  6.避免网站显示SQL错误信息，比如类型错误、字段不匹配等，防止攻击者利用这些错误信息进行一些判断。 |