**注意：**

**如果反馈为非本单位资产，必须提供单位盖章的证明函。**

|  |  |
| --- | --- |
| **漏洞名称** | SQL注入 |
| **漏洞单位** | 江苏省扬州中学 |
| **漏洞类型** | SQL注入 |
| **危害等级** | 高 |
| **漏洞定位** | http://61.155.62.50:40001/omdev/smdat0.asp |
| **漏洞信息和验证过程** | POST /omdev/smdat0.asp HTTP/1.1  Host: 61.155.62.50:40001  Content-Length: 15  Accept: application/json, text/javascript, \*/\*; q=0.01  X-Requested-With: XMLHttpRequest  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.127 Safari/537.36  Content-Type: application/x-www-form-urlencoded  Origin: http://61.155.62.50:40001  Referer: http://61.155.62.50:40001/A3-512.asp?sid=7  Accept-Encoding: gzip, deflate  Accept-Language: zh-CN,zh;q=0.9  Cookie: user=  Connection: close  itype=512&sid=7  电脑萤幕画面  描述已自动生成 |
| **漏洞修复建议** | 1、过滤危险字符，如（单引号'；双引号";"and";"or";"select";分号;括号等）  2、sql执行参数，进行正确的参数绑定；  3、使用函数对接收参数进行转义 |