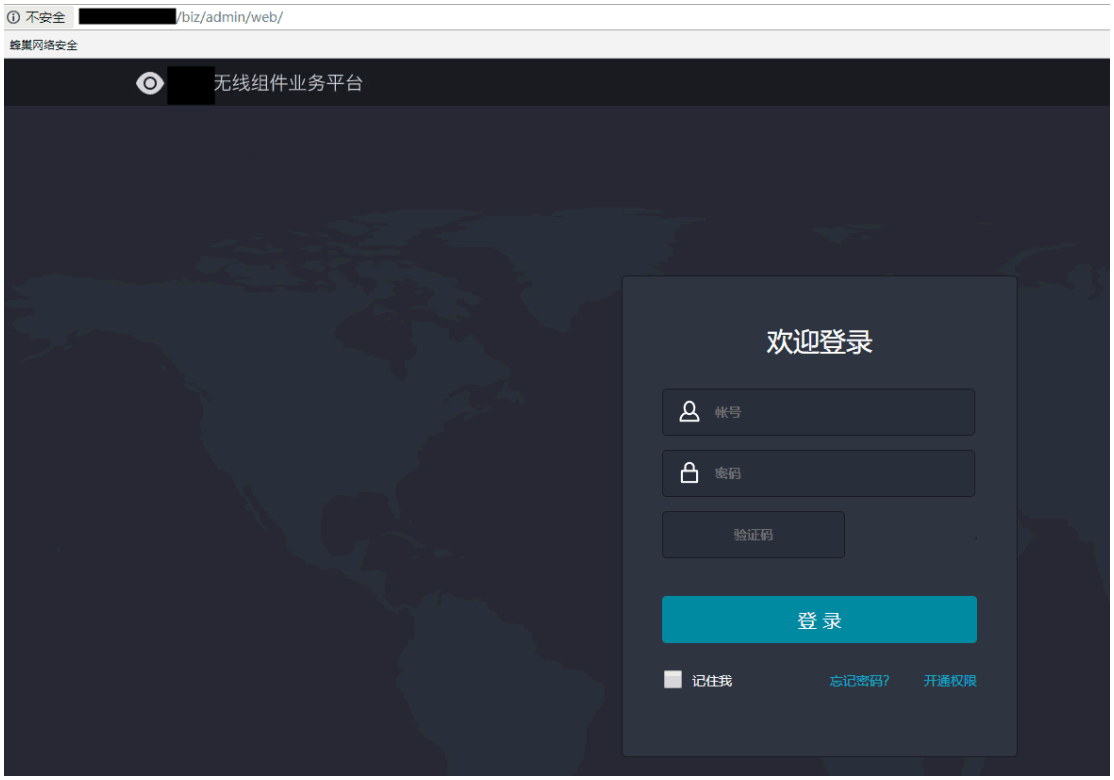
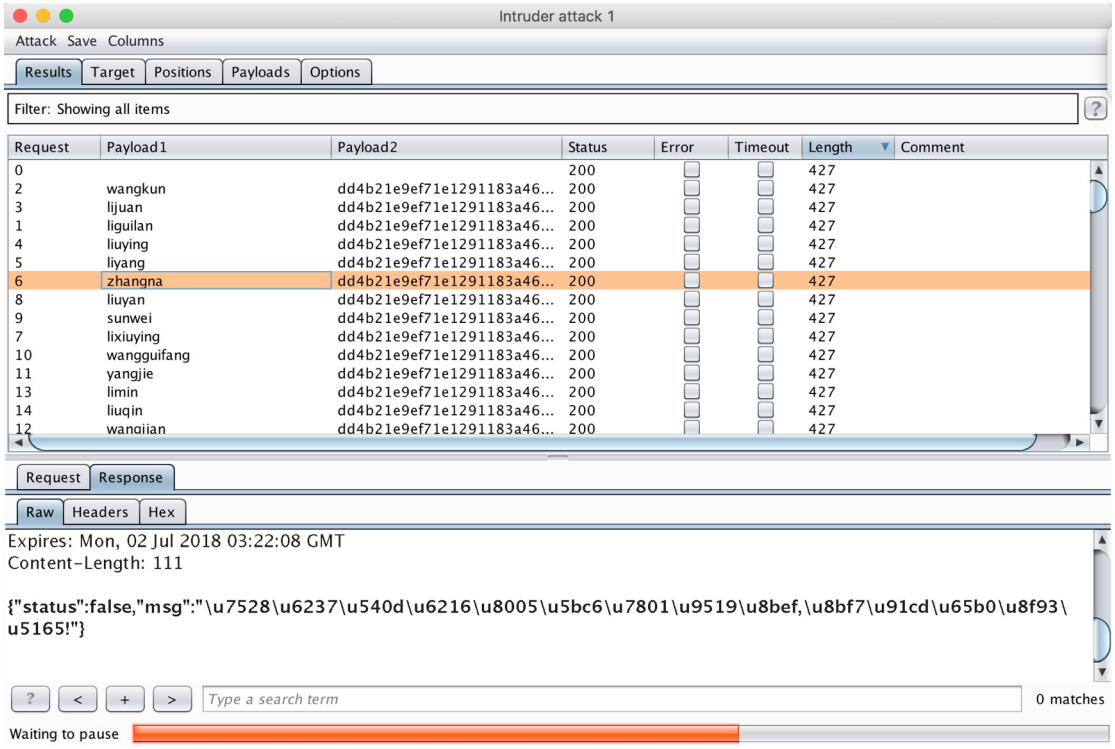
这次是为了响应 i 春秋的一个活动，挖了一下某家 src，有一个很好的点想分享一下。

目标站点如下



在检查目标站点的登陆流程时发现，该站点登陆接口缺少验证码，用户名为明文，密码为 md5 加密，可直接通过 burp 进行爆破，如下图所示。



等了一会无果，在翻源代码的时候发现申请账号要向某个邮箱发邮件，记下来邮箱地址：chenting1@**.com，试了下 chenting/123456 没进去，就换思路了

信息泄露

```
                userimg: vcode,
                remember: remember
            },
            success: function(rdata) {
                if (rdata.status) {
                    window.G.common.deleteCookie("check");
                    location.href = '/admin/main.htm';
                }else{
                    //login.loginErrorNum++;
                    //login.changeVcode();
                    //if (login.loginErrorNum >= 3) {
                    //    login.checkvcode = true;
                    //    $("#index_vcode").show();
                    //    if (!window.G.common.getCookie("check")) {
                    //        window.G.common.setCookie("check", true, 0, "/", "", 0);
                    //    }
                    //}
                    login.showError(rdata.msg);
                }
            },
            error: function() {
                login.showError("权限检查失败，请联系管理员，谢谢！");
            }
        });
    };

    //显示错误信息
    login.showError = function(str) {
        login.hasSubmit = false;
        $('#error_tips').text(str);
    };

    //切换验证码
    login.changeVcode = function() {
        $('#src_vcode').attr('src', '/biz/admin/web/vcode.php?'+Math.random());
    };

    $(document).keydown(function(event){
        if (event.keyCode == 13) {  //回车键
            login.submit();
        }
    });
</script>
</html>
```

首页源码泄漏了后台地址，经过尝试发现还有一个登陆接口为/biz/admin/web/

查看源码，发现源码中存在登陆后的跳转 url（admin/landing.htm），如下图所示。

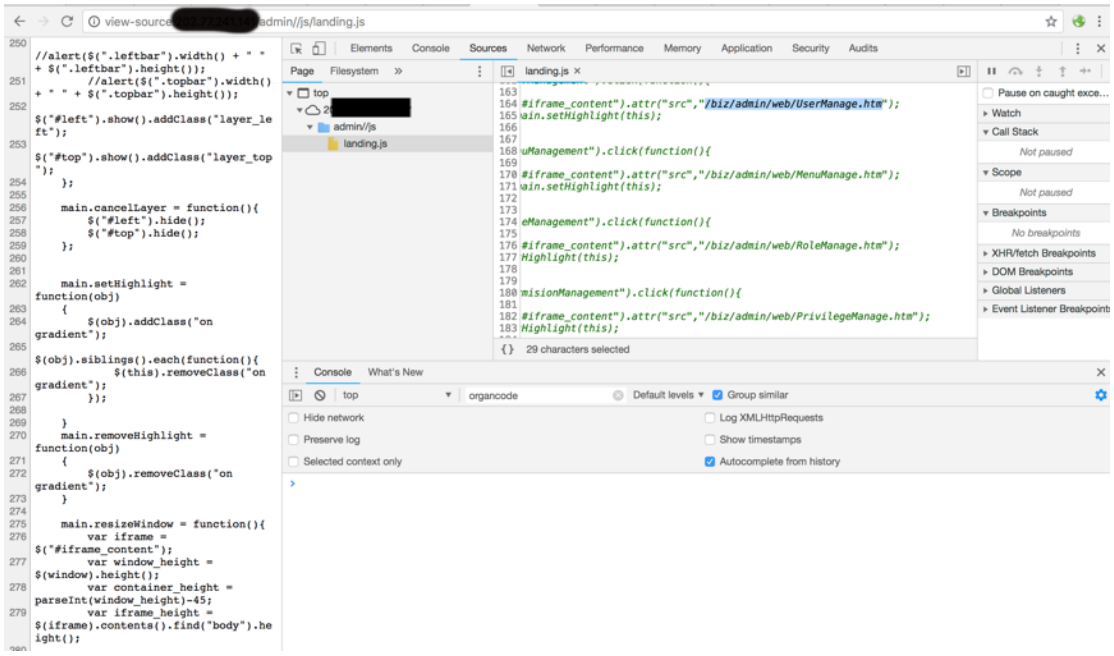
```
    //删除cookie
    login.deleteCookie = function(name, path, domain) {
        if (login.getCookie(name))
        {
            document.cookie = name + '=' +
                    ((path) ? ';path=' + path : '') +
                    ((domain) ? ';domain=' + domain : '') +
                    ';expires=Thu, 01-Jan-1970 00:00:01 GMT';
        }
    };

    login.checkSessionId = function(sid) {
        var sid = sid || login.getQuery('session') || login.getCookie('loginkey');      //第三方单点登录
        if (sid) {
            $.ajax({
                type: 'POST',
                url: '/json.php?mod=CheckUser&act=checkSession',
                data: '&sid=' + sid,
                dataType: 'json',
                success: function(rdata) {
                    if (rdata.status) {
                        //location.href = 'http://ams.yixun.com/admin/main.htm';
                        location.href = '/admin/landing.htm';
                    } else {
                        console.log(rdata.msg);
                    }
                },
                error: function() {
                    alert("session校验接口调用失败");
                }
            });
        } else if (login.getCookie("username") && login.getCookie('id_hash')) {    //直接在智网平台登录
            $.ajax({
                url: '/json.php?mod=SecureCookie&act=islogin',
                cache: false,
                success: function(para) {
                    if (para == 'true')
                    {
                        //location.href = 'http://ams.yixun.com/admin/main.htm';
                        location.href = '/admin/landing.htm';
                    }
                }
            });
        }
    };
</script>
</html>
```

接下来继续找了找 js，发现在正常的请求中，存在部分 js 加载请求 404。

#	Host	Method	URL	Params	Edited	Status
449	http://[redacted]	GET	/web/admin/js/web.dialog.js			404
450	http://[redacted]	GET	/web/admin/js/landing.js			404

猜测可能是路径写错了，因为其他的 js 都可以正常加载，然后通过拼接加猜测，发现去掉/web 即可访问到该 js。



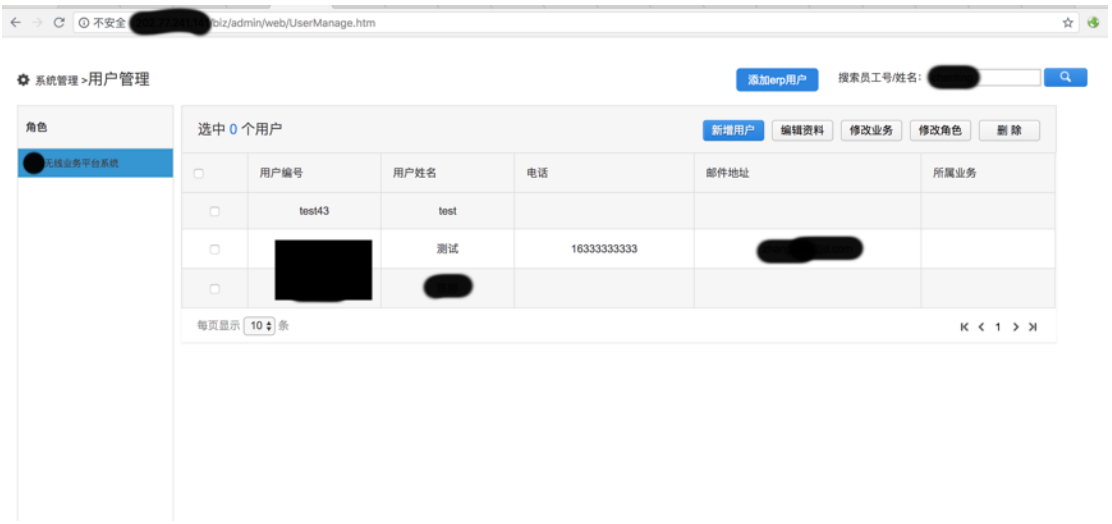
这个 js 中泄漏了一些后台的功能，且均存在未授权。

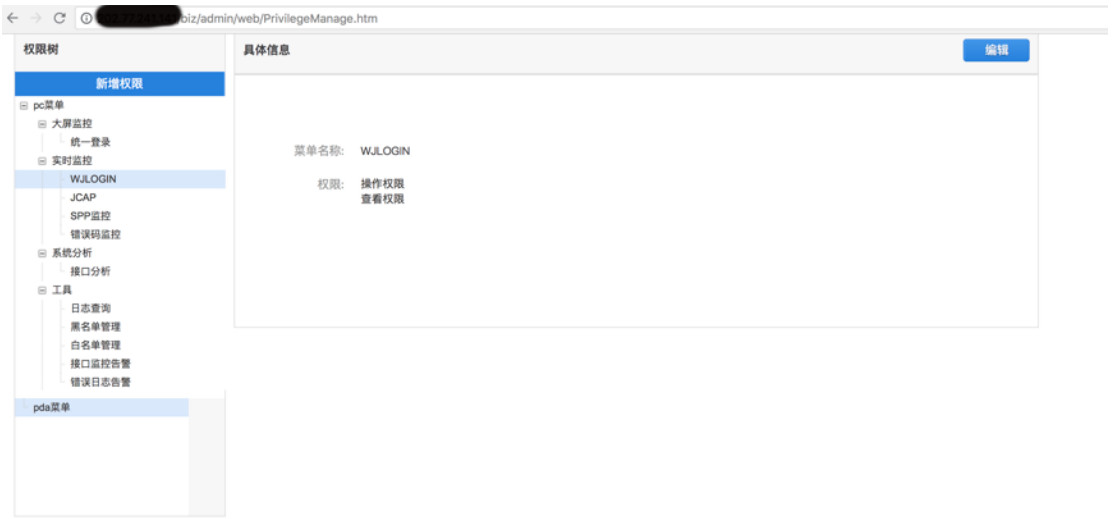
用户管理：http://***.**.***.***/biz/admin/web/UserManage.htm

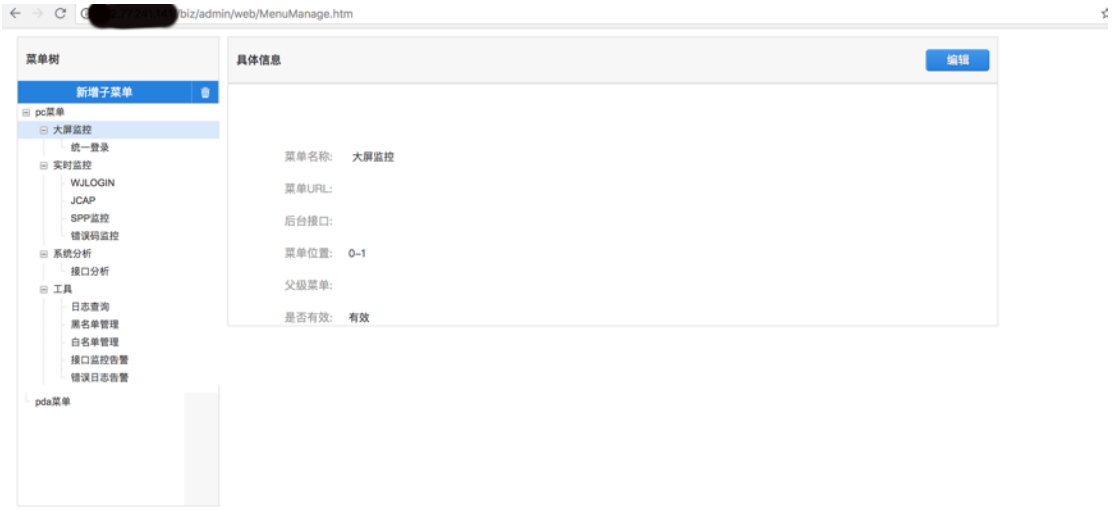
权限管理：http://***.**.***.***/biz/admin/web/PrivilegeManage.htm

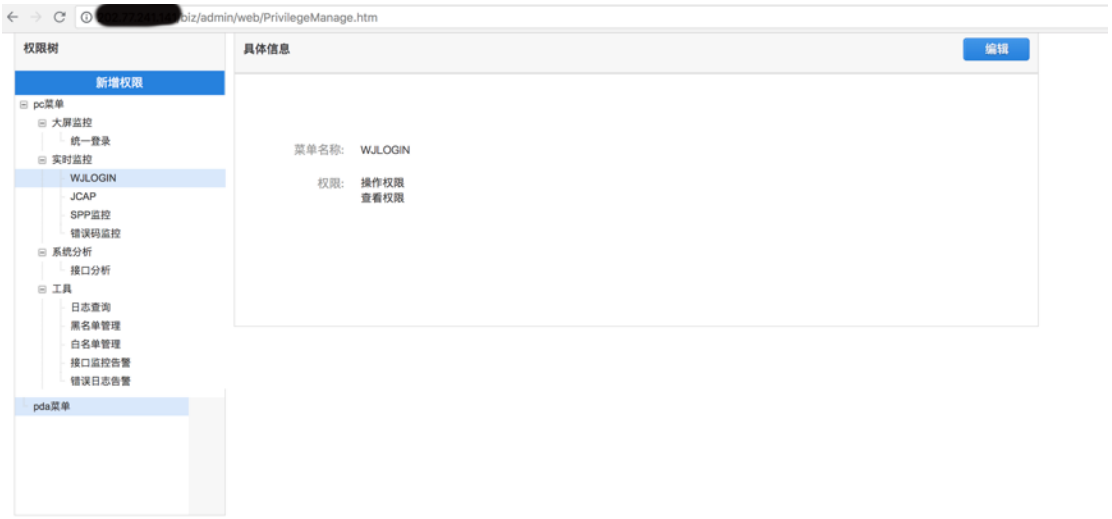
菜单管理：http://***.**.***.***/biz/admin/web/MenuManage.htm

角色管理：http://***.**.***.***/biz/admin/web/RoleManage.htm

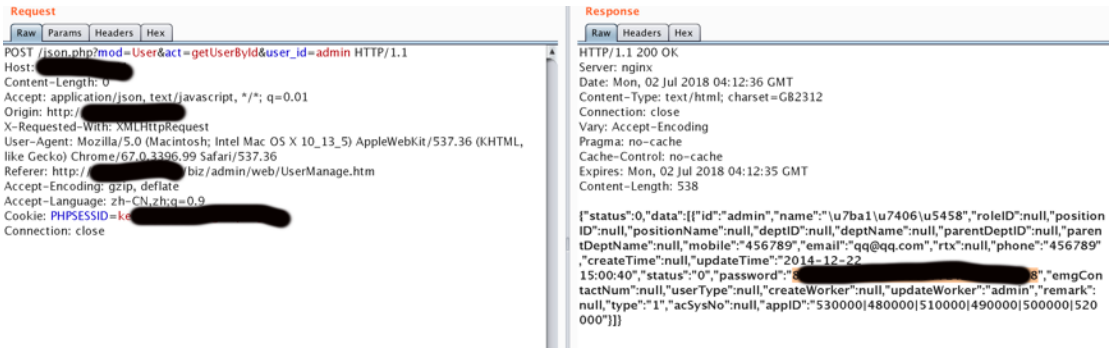






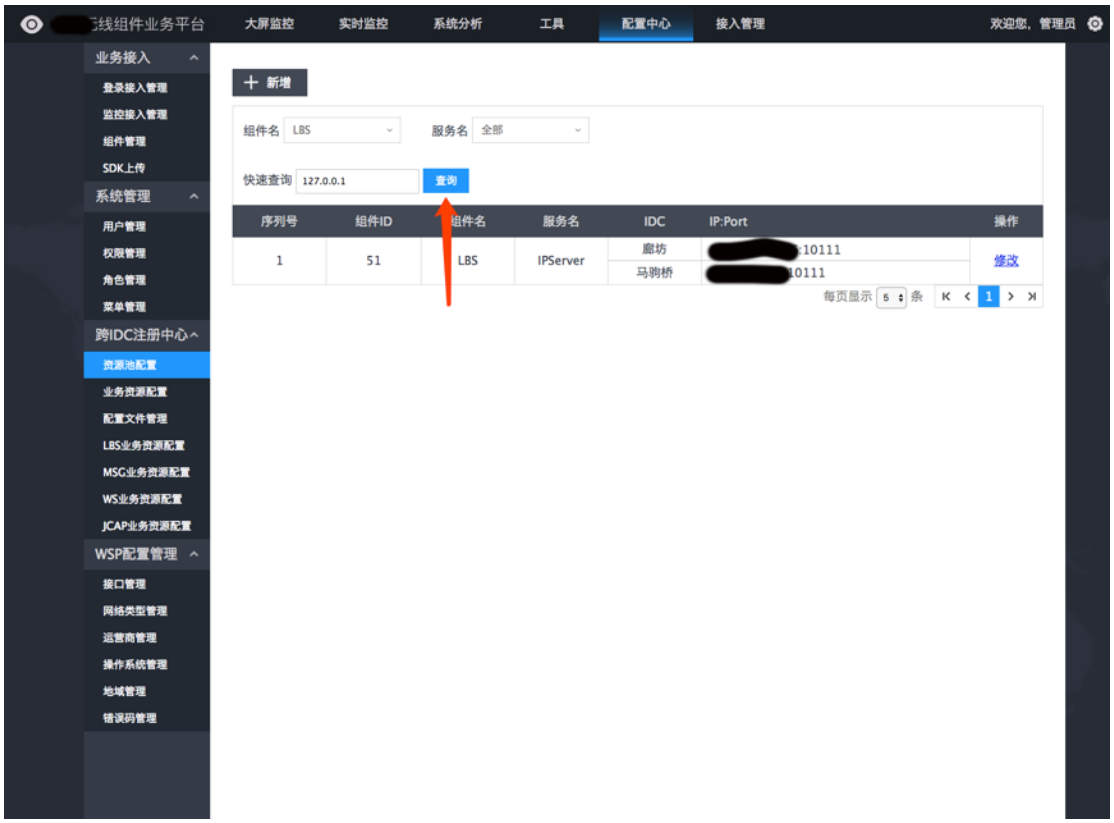


在用户管理处发现了部分账号，搜索员工号/姓名的功能处存在敏感信息泄露，将员工的全部信息都返回了，包括密码密文，可通过此处进行遍历。

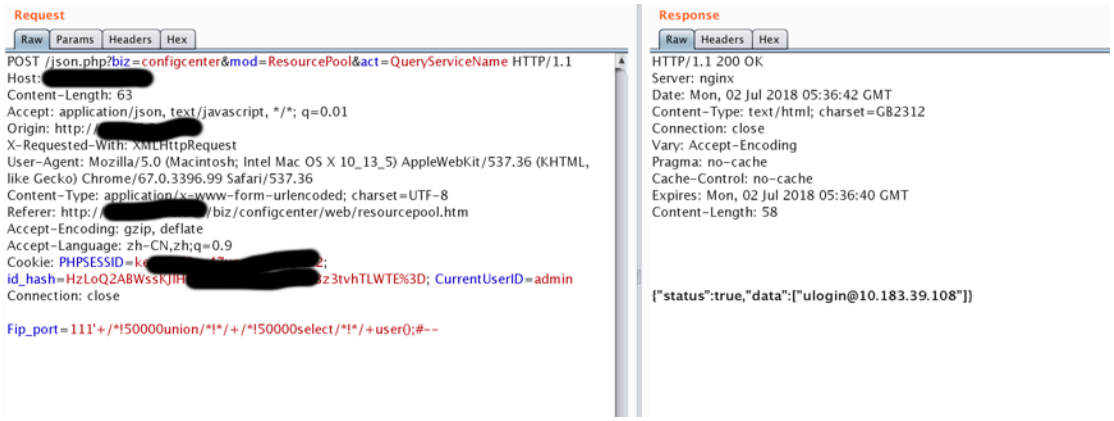


于此处获取到了两个账号作为测试，chenting/******，admin/******

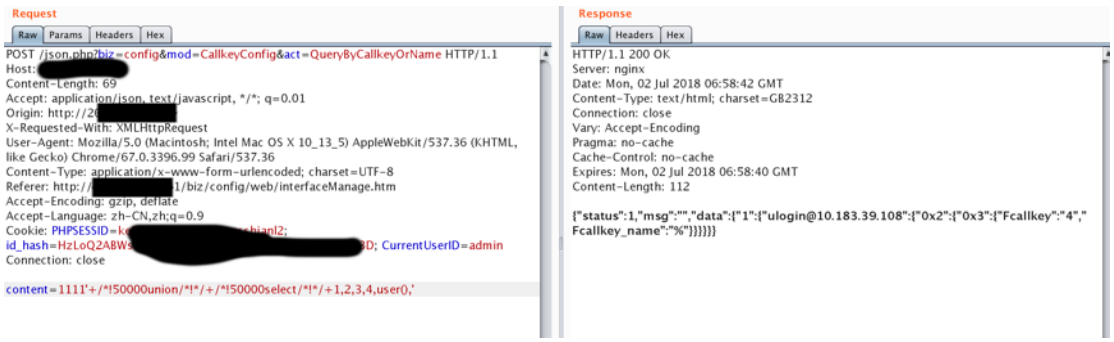
使用 admin 账号成功于首页登陆。



在后台里面的功能里发现一个 sql 注入，配置中心-资源池配置-查询功能，如下图所示。Sql 注入有拦截，使用注释绕过了。



感觉系统里所有的查询都是存在注入的，比如 WSP 配置管理-接口管理-查询功能。



然后发现其实整个系统也存在未授权访问的问题，只是正常情况下没有 url，不容易找到功能点而已。

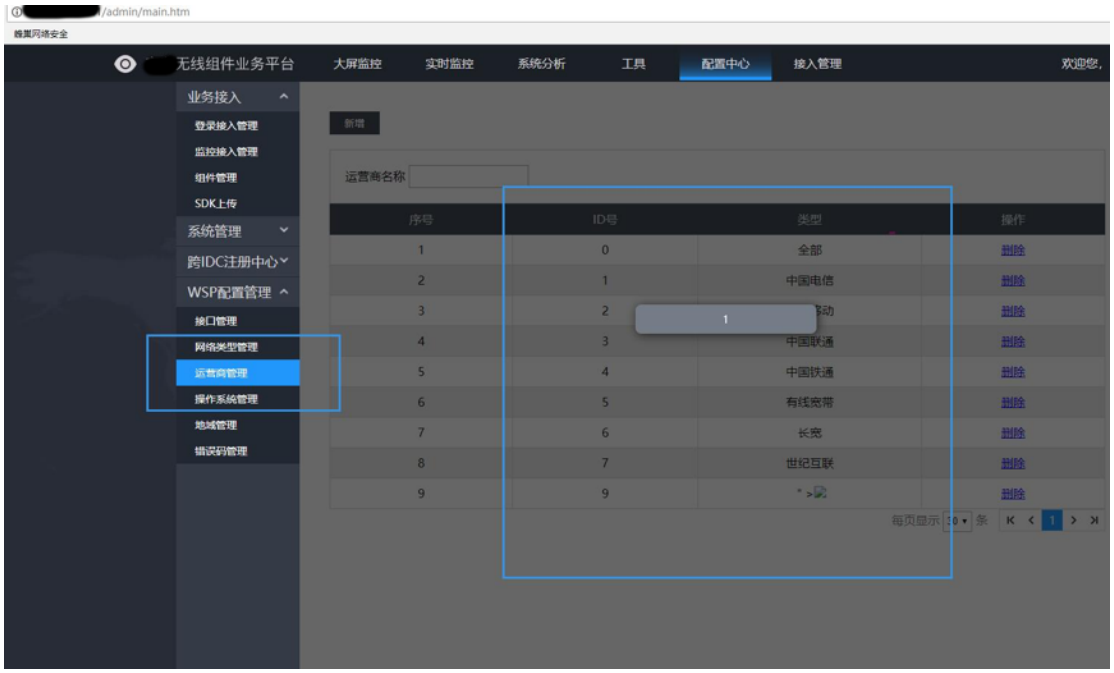
例如：http://***.**.***.***/biz/dashboard/web/interfaceNew.htm?com=wjlogin

http://***.**.***.***/biz/monitor/web/interface-split.htm?com=jcap

存储型 xss

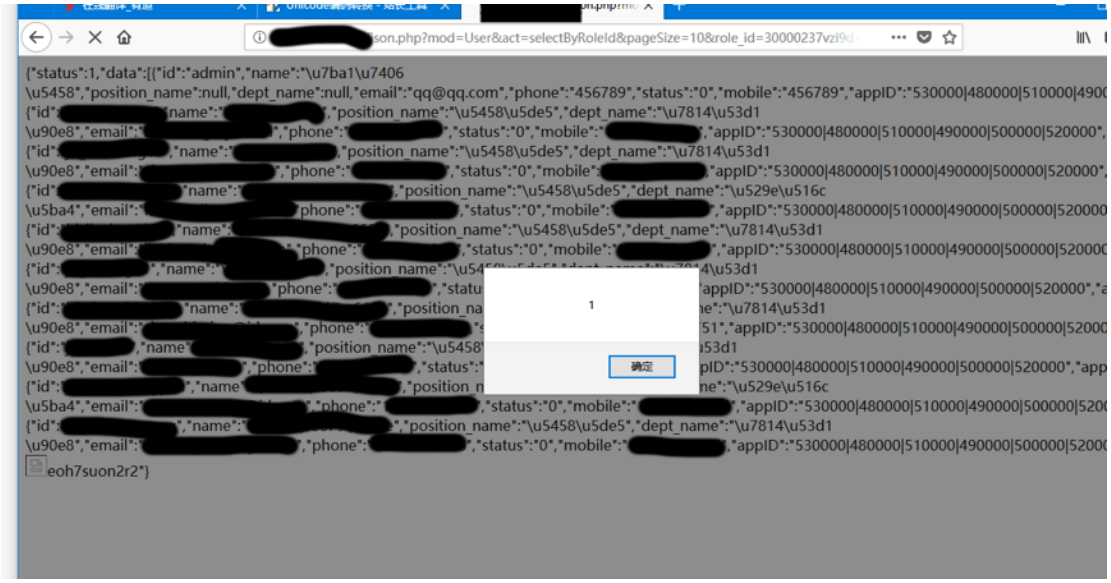
添加运营商　类型参数写 xsspayload

保存 触发

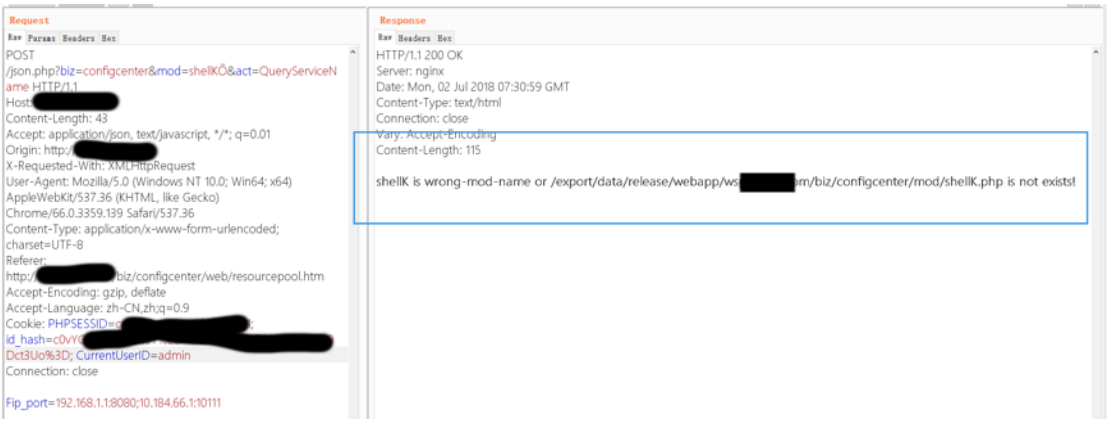


反射型 xss

http://***.**.***.**/json.php?mod=User&act=selectByRoleId&pageSize=10&role_id=30000237vzi9d%3Cimg%20src%3da%20onerror%3dalert(1)%3Eeoh7suon2r2



网站路径泄露　　修改 mod 参数 任意数值



总结：

面对一个登陆页面，信息收集或许是最好的攻击方式，本次测试从源码及 js 泄漏的信息出发，由信息泄漏找到了未授权，从而发现越权查询管理员信息，拿到管理员账号密码，然后进入系统，发现存在大量员工数据信息、sql 注入和 xss 等漏洞。

后面与审核交流，该系统是内网系统，由于员工配置错误才导致暴露在外网。建议大家注意提高安全意识。