

实训答辩

周俊宇

2024年6月28日

修改密码

```
var userPwd = data.field.userPwd;
var userPwd2 = data.field.userPwd2;

if (userPwd !== userPwd2) {
  layer.msg("两次密码输入不一致", {icon: 5});
  return false;
}

var userName = localStorage.getItem('username'); // 假设用户名存储在localStorage中

$.ajax({
  url: "/user/changePassword",
  type: "post",
  cache: false,
  contentType: "application/json;charset=utf-8",
  headers: {
    'Authorization': localStorage.getItem('token')
  },
  data: JSON.stringify({
    userName: userName,
    userPwd: userPwd
  }),

```

后端：

```
@Override
public ResponseResult changePassword(User user) {
    // 原密码是否正确
    User db_user = userMapper.selectByUserName(user.getUserName());
    if (!bCryptPasswordEncoder.matches(user.getOldPwd(), db_user.getUserPwd())){
        return new ResponseResult<>(1003, "原密码错误！");
    }

    // 设置修改时间
    user.setUpdateTime(new Timestamp(System.currentTimeMillis()));
    // 处理密码
    user.setUserPwd(bCryptPasswordEncoder.encode(user.getUserPwd()));
    userMapper.updateByUserNameSelective(user);
    return new ResponseResult<>(0, "修改成功！");
}
```

<<

🏠

修改密码 ×

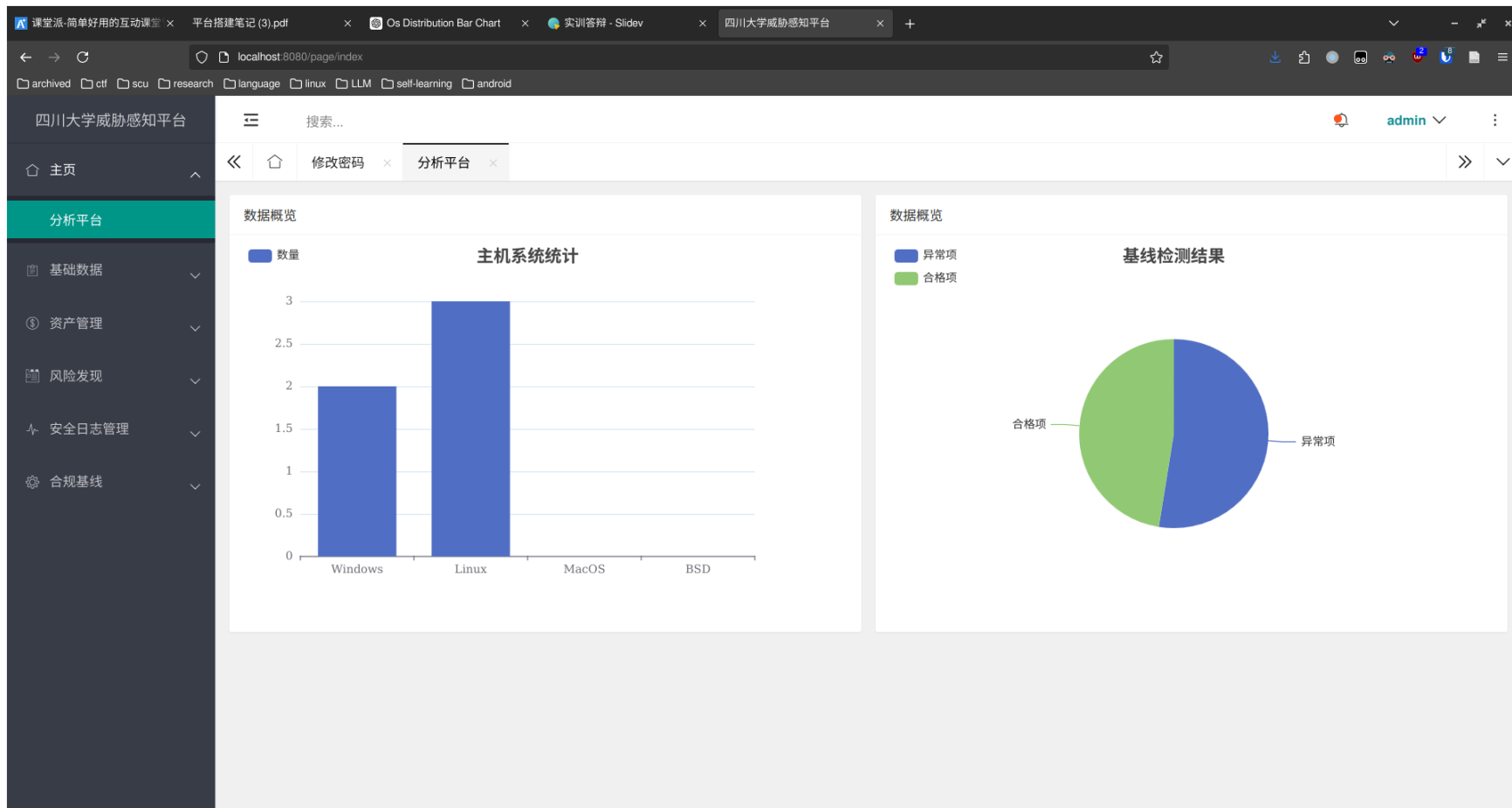
原始密码*

登录密码*

确认密码*

确认

主页数据统计



基础数据

课堂派-简单好用的互动课堂

平台搭建笔记 (3).pdf

Os Distribution Bar Chart

实训答辩 - Slidew

四川大学威胁感知平台

localhost:8080/page/index

archivedctfscuresearchlanguagelinuxLLMself-learningandroid

四川大学威胁感知平台

主页

基础数据

用户管理

角色管理

权限管理

资产管理

风险发现

安全日志管理

合规基线

搜索...

admin

修改密码

分析平台

用户管理

用户名

请输入用户名

删除

添加

<input type="checkbox"/>	ID	用户名	用户角色	状态	创建时间	更新时间	最后登录时间	操作
<input type="checkbox"/>	8	cindy	3	正常	2024-6-24 16:22:48	2024-6-24 16:19:43	2024-6-24 16:22:49	<div>编辑删除</div>
<input type="checkbox"/>	6	alice	2	正常	2024-6-24 16:58:49	2024-6-24 14:57:15	2024-6-24 16:58:49	<div>编辑删除</div>
<input type="checkbox"/>	2	tomcat	2	正常	2024-5-24 14:21:0			<div>编辑删除</div>
<input type="checkbox"/>	1	admin	1	正常	2024-6-24 21:44:47	2024-6-24 14:55:43	2024-6-24 21:44:47	<div>编辑删除</div>

<1>

到第

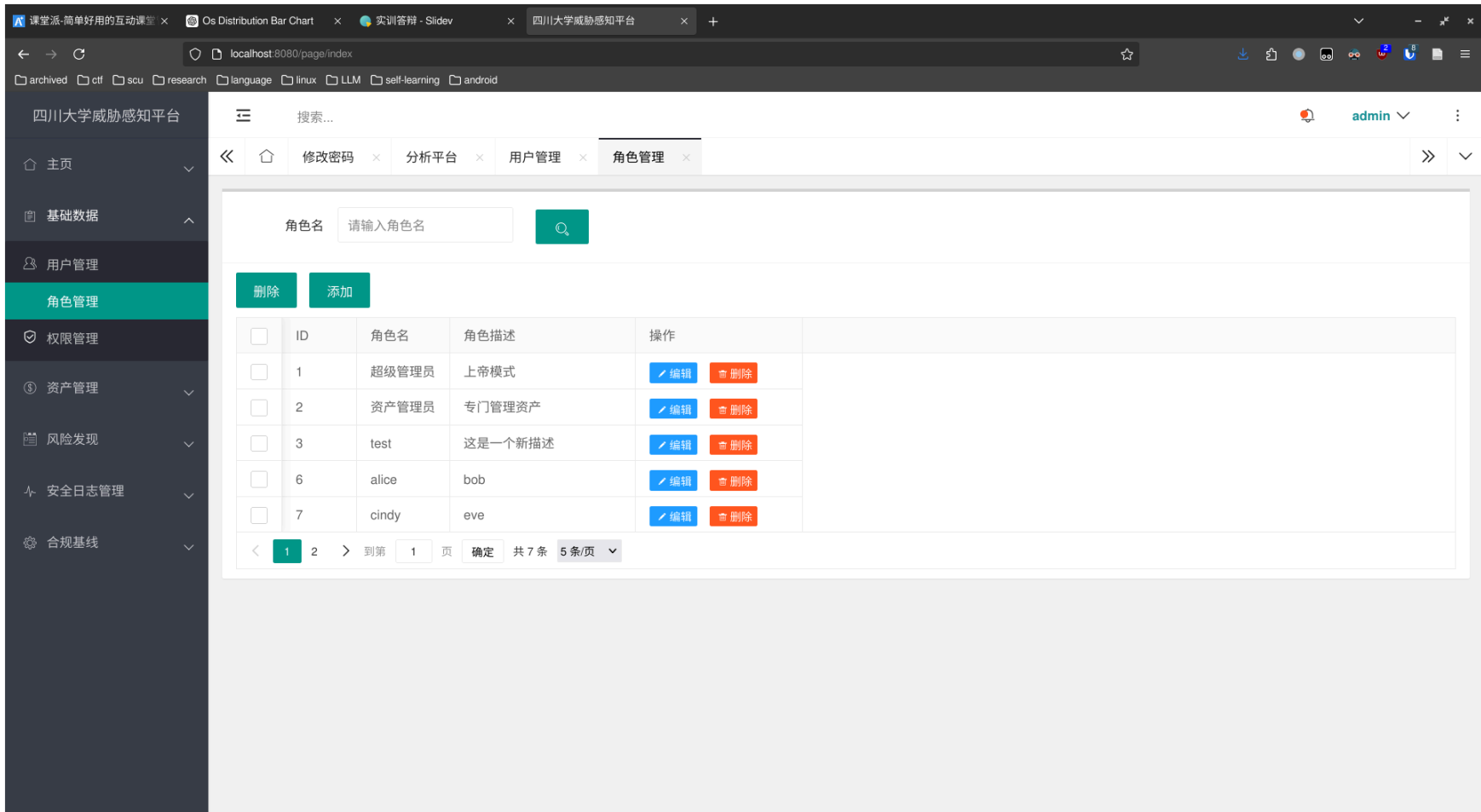
1

页

确定

共 4 条

5 条/页



资产管理

课堂派-简单好用的互动课堂

Os Distribution Bar Chart

实训答疑 - Slidev

四川大学威胁感知平台

localhost:8080/page/index

archivedctfscuresearchlanguagelinuxLLMself-learningandroid

四川大学威胁感知平台

主页

基础数据

资产管理

主机列表

账号资产

服务资产

进程资产

软件资产

风险发现

安全日志管理

合规基线

搜索...

admin

修改密码

分析平台

用户管理

角色管理

主机列表

主机名

请输入关键字

时间搜索

开始时间

结束时间

删除

< 1 >

到第 1 页

确定

共 5 条

5 条/页

课堂派-简单好用的互动课堂

Os Distribution Bar Chart

实训答疑 - Slidew

四川大学威胁感知平台

localhost:8080/page/index

archivedctfscuresearchlanguagelinuxLLMself-learningandroid

四川大学威胁感知平台

搜索...

admin

修改密码

分析平台

用户管理

角色管理

主机列表

账号资产

主机名

所有主机

删除

	ID	MAC地址	账号名字	账号是否有危险	全称	SID	SID...	操作
<input type="checkbox"/>	2	B8:81:98:C3:0E:79	root	正常	root	0	UID	<div><div>详情</div><div>删除</div></div>
<input type="checkbox"/>	3	B8:81:98:C3:0E:79	daemon	正常	daemon	1	UID	<div><div>详情</div><div>删除</div></div>
<input type="checkbox"/>	4	B8:81:98:C3:0E:79	bin	正常	bin	2	UID	<div><div>详情</div><div>删除</div></div>
<input type="checkbox"/>	5	B8:81:98:C3:0E:79	sys	正常	sys	3	UID	<div><div>详情</div><div>删除</div></div>
<input type="checkbox"/>	6	B8:81:98:C3:0E:79	sync	正常	sync	4	UID	<div><div>详情</div><div>删除</div></div>

<

1

2

3

...

23

>

到第

1

页

确定

共 113 条

5 条/页

主页

基础数据

资产管理

主机列表

账号资产

服务资产

进程资产

软件资产

风险发现

安全日志管理

合规基线

课堂派-简单好用的互动课堂

Os Distribution Bar Chart

实训答疑 - Slidev

四川大学威胁感知平台

localhost:8080/page/index

archivedctfscuresearchlanguagelinuxLLMself-learningandroid

四川大学威胁感知平台

admin

修改密码分析平台用户管理角色管理主机列表账号资产服务资产

主机名所有主机

删除

	ID	MAC地址	协议	端口	状态	服务名称	产品	版本	扩展信息	操作	
<input type="checkbox"/>	13	F4:8E:38:EA:84:21	tcp	631	open	ipp	CUPS	2.4		查看详情 删除	
<input type="checkbox"/>	14	F4:8E:38:EA:84:21	tcp	902	open	vmware-...	VMware ...	1.10	Uses VN...	查看详情 删除	
<input type="checkbox"/>	15	F4:8E:38:EA:84:21	tcp	3306	open	mysql	MySQL	8.0.37-0...		查看详情 删除	
<input type="checkbox"/>	16	F4:8E:38:EA:84:21	tcp	8080	open	http-proxy				查看详情 删除	
<input type="checkbox"/>	17	F4:8E:38:EA:84:21	tcp	631	open	ipp	CUPS	2.4		查看详情 删除	

123

到第1页

确定

共 14 条

5条/页

进程资产

软件资产

风险发现

安全日志管理

合规基线

课堂派-简单好用的互动课堂

Os Distribution Bar Chart

实训答疑 - Slidev

四川大学威胁感知平台

+

localhost:8080/page/index

☆

↓ ↻ 🔍 📄 📱 🎮 📺 🌐 📧 ☰

📁 archived

📁 ctf

📁 scu

📁 research

📁 language

📁 linux

📁 LLM

📁 self-learning

📁 android

四川大学威胁感知平台

🏠 主页

📊 基础数据

💰 资产管理

📋 主机列表

👤 账号资产

🔑 服务资产

🚀 进程资产

📦 软件资产

📁 风险发现

📉 安全日志管理

⚙️ 合规基线

☰ 搜索...

🔔 admin

⋮

⏪

🏠

修改密码

×

分析平台

×

用户管理

×

角色管理

×

主机列表

×

账号资产

×

服务资产

×

进程资产

×

⏩

⏴

⏵

主机名

所有主机

🔍

🗑️ 删除

<input type="checkbox"/>	ID	MAC地址	进程ID	父进程ID	进程名	命令行	优先级	描述	操作	
<input type="checkbox"/>	10295	F4:8E:38:EA:84:21	1	0	systemd	/sbin/init splash	0		查看详情 删除	
<input type="checkbox"/>	10296	F4:8E:38:EA:84:21	2	0	kthreadd		0		查看详情 删除	
<input type="checkbox"/>	10297	F4:8E:38:EA:84:21	3	2	pool_wo...		0		查看详情 删除	
<input type="checkbox"/>	10298	F4:8E:38:EA:84:21	4	2	kworker/...		-20		查看详情 删除	
<input type="checkbox"/>	10299	F4:8E:38:EA:84:21	5	2	kworker/...		-20		查看详情 删除	

⏪

1

2

3

...

90

⏩

到第

1

页

确定

共 447 条

5 条/页

⏴

课堂派-简单好用的互动课堂

Os Distribution Bar Chart

实训答疑 - Slidew

四川大学威胁感知平台

+

localhost:8080/page/index

☆

↓

📄

🔍

📺

🎮

🌐

📱

☰

archivedctfscuresearchlanguagelinuxLLMself-learningandroid

四川大学威胁感知平台

🏠 主页

📊 基础数据

💰 资产管理

📋 主机列表

👤 账号资产

🔄 服务资产

🖥️ 进程资产

📁 软件资产

📁 风险发现

📁 安全日志管理

⚙️ 合规基线

☰ 搜索...

🔔 admin

⋮

⏪

🏠

修改密码

×

分析平台

×

用户管理

×

角色管理

×

主机列表

×

账号资产

×

服务资产

×

进程资产

×

软件资产

×

⏩

⏴

主机名

所有主机

🔍

🗑️ 删除

<input type="checkbox"/>	ID	MAC地址	显示名称	安装地址	卸载命令	操作
<input type="checkbox"/>	1	F4:8E:38:EA:84:21	7zip	/usr/bin	apt-get remove 7zip	🔍 详情 🗑️ 删除
<input type="checkbox"/>	2	F4:8E:38:EA:84:21	accountsservice	/usr/bin	apt-get remove accountsservice	🔍 详情 🗑️ 删除
<input type="checkbox"/>	3	F4:8E:38:EA:84:21	acl	/usr/bin	apt-get remove acl	🔍 详情 🗑️ 删除
<input type="checkbox"/>	4	F4:8E:38:EA:84:21	adduser	/usr/bin	apt-get remove adduser	🔍 详情 🗑️ 删除
<input type="checkbox"/>	5	F4:8E:38:EA:84:21	adwaita-icon-theme	/usr/bin	apt-get remove adwaita-icon-the	🔍 详情 🗑️ 删除

⏪

1

2

3

...

1117

➡

到第

1

页

确定

共 5582 条

5 条/页

⏴

风险发现

课堂派-简单好用的互动课堂

Os Distribution Bar Chart

实训答疑 - Slidev

四川大学威胁感知平台

+

localhost:8080/page/index

archivedctfscuresearchlanguagelinuxLLMself-learningandroid

四川大学威胁感知平台

主页

基础数据

资产管理

风险发现

安全补丁

漏洞检测

弱密码

应用风险

系统风险

安全日志管理

合规基线

搜索...

admin

安全补丁

删除

账号名 请输入关键字

☐

序号

☐

3

☐

4

B8:81:98:C3:0E:7D

B8:81:98:C3:0E:7D

补丁编号

KB4480116

KB5037781

可能存在的CVE编号

CVE-2024-30049 CVE-2024-30040 CVE-2024-30039 CVE-2024-30038 ...

操作

详情删除

详情删除

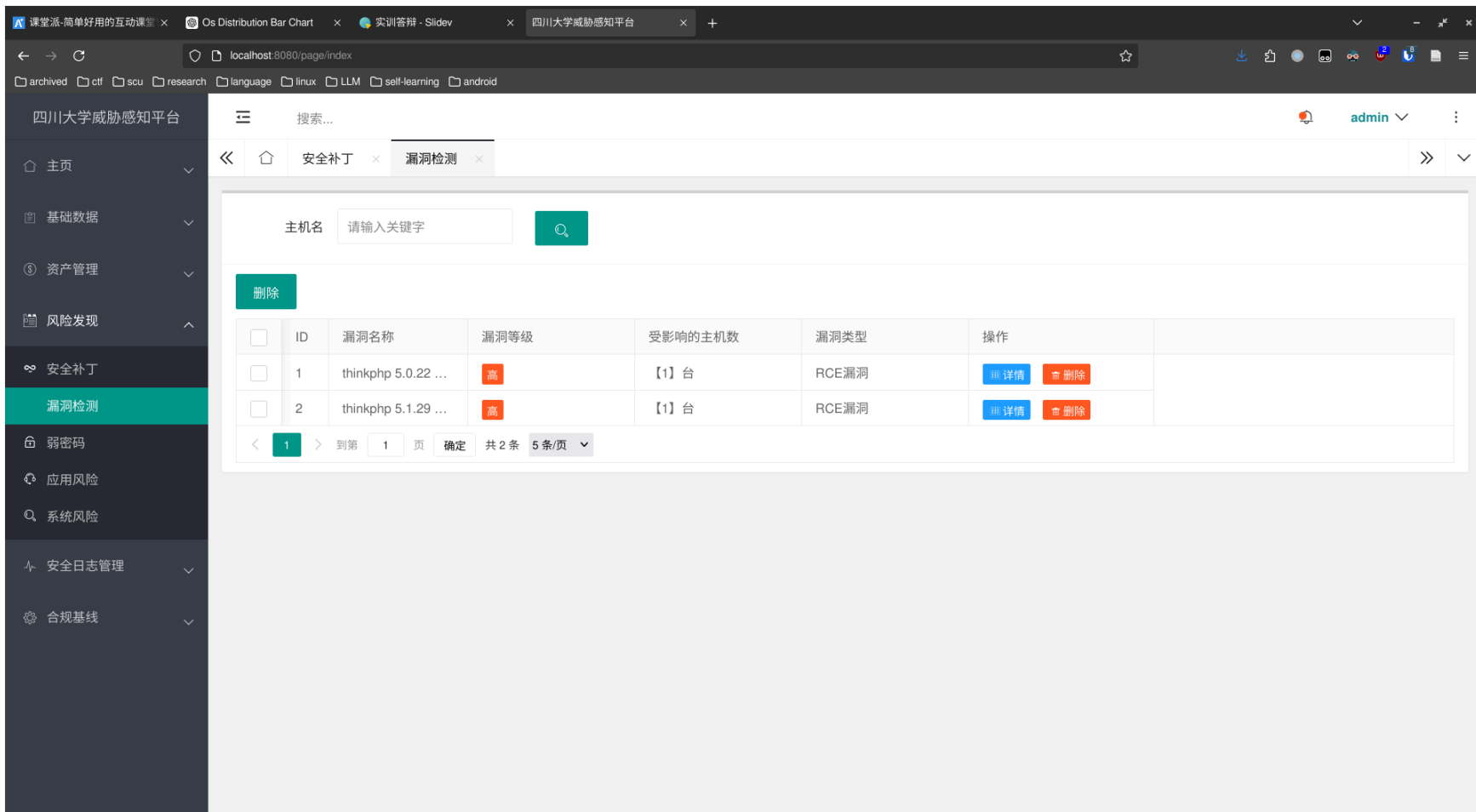
< 1 >

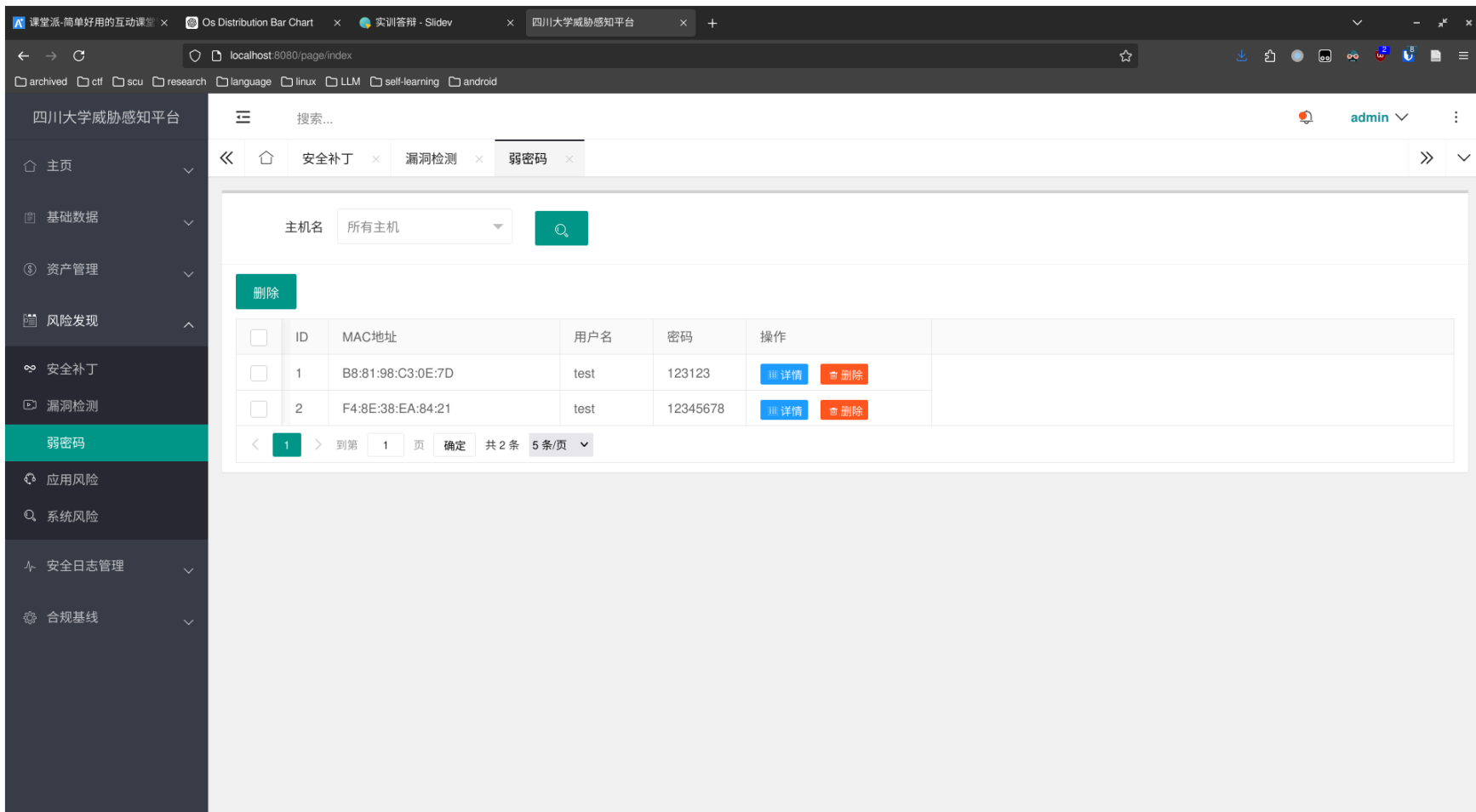
到第 1 页

确定

共 2 条

5 条/页





合规基线

课堂派-简单好用的互动课堂

Os Distribution Bar Chart

实训答疑 - Slidev

四川大学威胁感知平台

localhost:8080/page/index

archivedctfscuresearchlanguagelinuxLLMself-learningandroid

四川大学威胁感知平台

主页

基础数据

资产管理

风险发现

安全日志管理

合规基线

基线任务管理

基线检测结果

搜索...

安全补丁漏洞检测弱密码基线任务管理

admin

主机名 所有主机

删除添加

	ID	任务名称	任务时间	任务状态	主机名	操作
<input type="checkbox"/>	1	621任务	2024-06-21 15:53:00	已执行	B8:81:98:C3:0E:7D 00:0C:29:5F:88:69	查看详情 删除
<input type="checkbox"/>	5	test	2024-06-21 19:11:55	已执行	B8:81:98:C3:0E:7D 00:0C:29:5F:88:69	查看详情 删除

1

到第1页确定共2条5条/页

课堂派-简单好用的互动课堂 × Os Distribution Bar Chart × 实训答疑 - Slidew × 四川大学威胁感知平台 × +

localhost:8080/page/index

archived ctf scu research language linux LLM self-learning android

四川大学威胁感知平台

主页

基础数据

资产管理

风险发现

安全日志管理

合规基线

基线任务管理

基线检测结果

admin

安全补丁 × 漏洞检测 × 弱密码 × 基线任务管理 × 基线检测结果 ×

主机名 所有主机

删除

	ID	MAC地址	基线信息	操作
<input type="checkbox"/>	1	00:0C:29:5F:88:69	异常项 SysAccount [异常项]-系统中存在其他账号请检查: Administrator alice DefaultAccount Guest junyu33 sshd WDAG...	查看详情 删除
<input type="checkbox"/>	2	00:0C:29:5F:88:69	合格项 SysAccountPolicy::MinimumPa... [合格项][0 30]系统账号策略配置-密码最短留存期-【符合】等级保护标准.	查看详情 删除
<input type="checkbox"/>	3	00:0C:29:5F:88:69	合格项 SysAccountPolicy::MaximumPa... [合格项][1 90]系统账号策略配置-密码最长留存期-【符合】等级保护标准.	查看详情 删除
<input type="checkbox"/>	4	00:0C:29:5F:88:69	异常项 SysAccountPolicy::MinimumPa... [异常项][0 14]系统账号策略配置-密码长度最小值-【不符合】等级保护标准.	查看详情 删除
<input type="checkbox"/>	5	00:0C:29:5F:88:69	异常项 SysAccountPolicy::PasswordC... [异常项][0 1]系统账号策略配置-密码必须符合复杂性要求策略-【不符合】等级保...	查看详情 删除

< 1 2 3 ... 154 >

到第 1 页 确定 共 767 条 5条/页

登录token续期

在index.html引用一个自己写的js，检测用户活动以延长token有效期。

```
function extendSession() {  
    $.ajax({  
        url: "/user/extendSession",  
        type: "post",  
        headers: {  
            'Authorization': localStorage.getItem('token')  
        },  
        success: function(response) {  
            console.log("Session extended");  
        },  
        error: function(response) {  
            console.log("Error extending session: " + response);  
        }  
    });  
}  
  
$(document).on('click keydown', function() {  
    extendSession();  
});
```

后端代码：

```
@PostMapping("/user/extendSession")
public ResponseResult extendSession(@RequestHeader("Authorization") String token) throws Exception {
    // 从token中解析出uuid
    String uuid = JwtUtil.parseJWT(token).getId();
    // 获取redis中的用户信息
    String redisKey = "login_" + uuid;
    String userJson = redisCache.getCacheObject(redisKey);
    if (userJson != null) {
        // 重新设置redis中用户信息的过期时间
        redisCache.setCacheObject(redisKey, userJson, 60 * 60, TimeUnit.SECONDS);
        return new ResponseResult(200, "Session extended successfully");
    } else {
        return new ResponseResult(1001, "Session not found");
    }
}
```

效果：

课堂派-简单好用的互动课堂

Os Distribution Bar Chart

实训答疑 - Slidev

四川大学威胁感知平台

localhost:8080/page/index

archivedctfscuresearchlanguagelinuxLLMself-learningandroid

四川大学威胁感知平台

搜索...

admin

安全补丁

漏洞检测

弱密码

基线任务管理

基线检测结果

主机名

所有主机

删除

添加

	ID	任务名称	任务时间	任务状态	主机名	操作
<input type="checkbox"/>	1	621任务	2024-06-21 15:53:00	已执行	B8:81:98:C3:0E:7D 00:0C:29:5F:88:69	查看详情 删除
<input type="checkbox"/>	5	test	2024-06-21 19:11:55	已执行	B8:81:98:C3:0E:7D 00:0C:29:5F:88:69	查看详情 删除

1

到第 1 页

确定

共 2 条

5 条/页

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Accessibility

Application

Filter Output

Errors

Warnings

Logs

Info

Debug

CSS

XHR

Requests

Expected 'none', URL, or filter function but found 'alpha'. Error in parsing value for 'filter'. Declaration dropped.

Unknown property 'overflow:hidden'. Declaration dropped.

Expected declaration but found ';'. Skipped to next declaration.

Expected declaration but found ';'. Skipped to next declaration.

Unknown property 'blr'. Declaration dropped.

Expected 'none', URL, or filter function but found 'Alpha'. Error in parsing value for 'filter'. Declaration dropped.

Expected declaration but found ';'. Skipped to next declaration.

Expected declaration but found ';'. Skipped to next declaration.

Keyframe rule ignored due to bad selector.

Keyframe rule ignored due to bad selector.

Keyframe rule ignored due to bad selector.

Expected declaration but found ';'. Skipped to next declaration.

Source map error: Error: request failed with status 403

Resource URL: http://localhost:8080/js/jquery-2.0.3.min.js

Source Map URL: jquery-2.0.3.min.map

Session extended

POST http://localhost:8080/user/extendSession

Session extended

extend-session.js:12:21

HTTP/1.1 200 5ms

extend-session.js:12:21

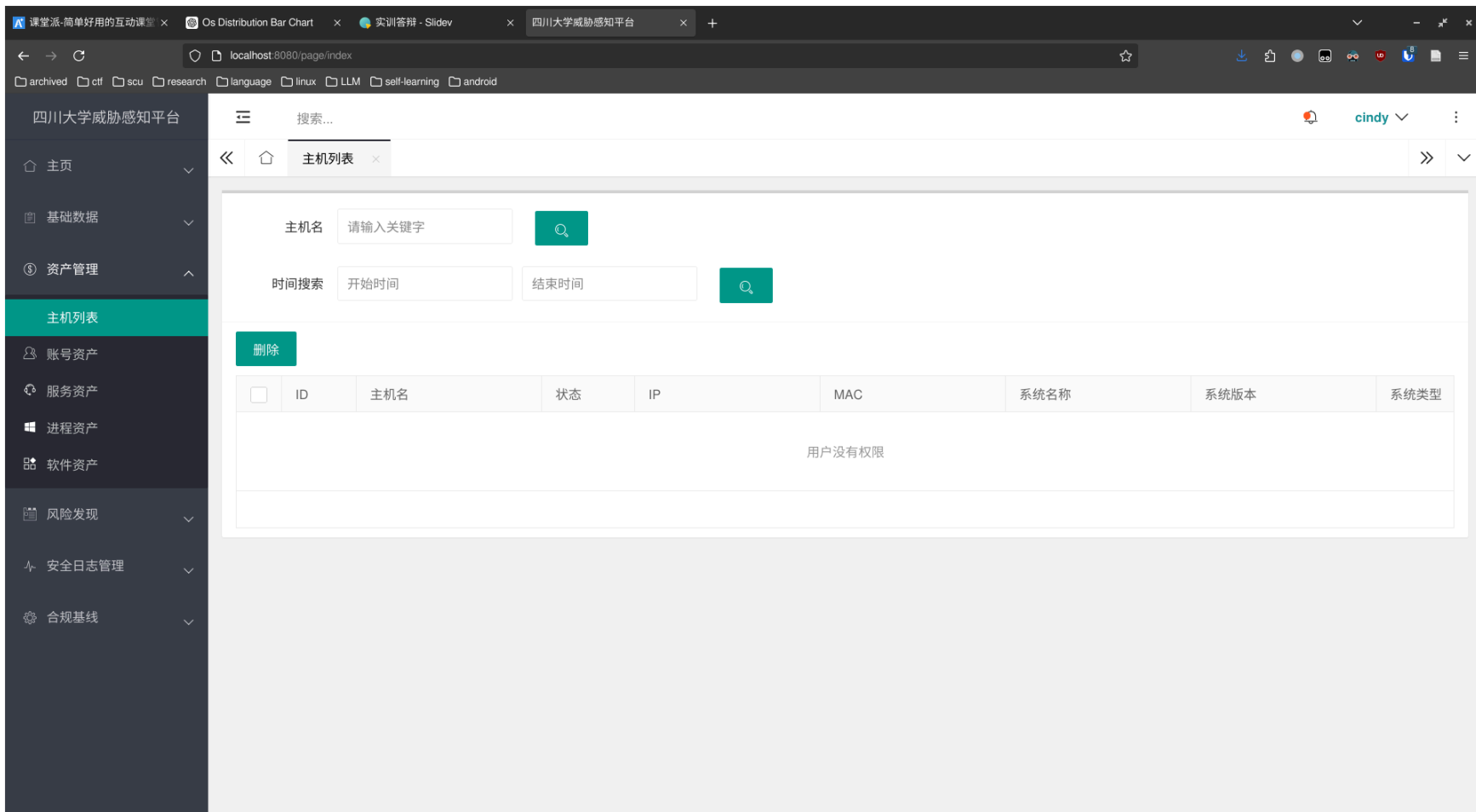
权限管理

我的权限设计是基于角色的访问控制，方案如下：

- Admin 可以修改任意用户的角色，其他用户不能修改。
- Admin 可以编辑角色对资产信息的访问权限，其他用户不能修改。
- 只有“权限管理”页面的角色名中“是否允许查看资产信息”被赋值为“是”的角色，可以查看资产管理的页面。

在本例中，超级管理员和资产管理员可以查看资产信息，而admin是超级管理员，alice和tomcat是资产管理员，因此他们三个人可以查看资产信息：

角色名 <input type="text" value="请输入角色名"/> 				
<div>删除 添加</div>				
<input type="checkbox"/>	ID	角色名	是否允许查看资产信息	操作
<input type="checkbox"/>	1	超级管理员	是	编辑 删除
<input type="checkbox"/>	2	资产管理员	是	编辑 删除
<input type="checkbox"/>	3	test	否	编辑 删除
<div>< 1 > 到第 <input type="text" value="1"/> 页 <input type="button" value="确定"/> 共 3 条 <div>5 条/页 v</div></div>				



后端实现：

```
@Override
public ResponseResult list(MyParam param) {
    Authentication authentication = SecurityContextHolder.getContext().getAuthentication();
    if (authentication == null || !authentication.isAuthenticated()) {
        return new ResponseResult(1004, "User not authenticated");
    }
    String username = authentication.getName();

    Long roleId = (long) userMapper.selectUserRoleByUserName(username);
    int allowed = permissionMapper.selectPermissionByRoleId(roleId);
    if (allowed != 1) { // 不是超级管理员或资产管理员，则返回错误
        return new ResponseResult(1009, "用户没有权限");
    }

    // 做分页
    PageHelper.startPage(param.getPage(), param.getLimit());
    // 做查询
    List<Host> data = hostMapper.findAll(param);
    // 构建分页数据
    PageInfo<Host> pageInfo = new PageInfo<>(data);
    return new ResponseResult(pageInfo.getTotal(), pageInfo.getList());
}
```

风险发现

课堂派-简单好用的互动课堂

Os Distribution Bar Chart

实训答疑 - Slides

四川大学威胁感知平台

localhost:8080/page/index

archived ctf scu research language linux LLM self-learning android

四川大学威胁感知平台

主页

基础数据

资产管理

风险发现

安全补丁

漏洞检测

弱密码

应用风险

系统风险

安全日志管理

合规基线

搜索...

alice

主机列表 应用风险

主机名 请输入关键字

删除

<input type="checkbox"/>	ID	漏洞名称	漏洞等级	受影响的主机数	漏洞类型	漏洞端口	操作
<input type="checkbox"/>	2	thinkphp/2-rce	高	【1】台	RCE	8080	查看详情 删除

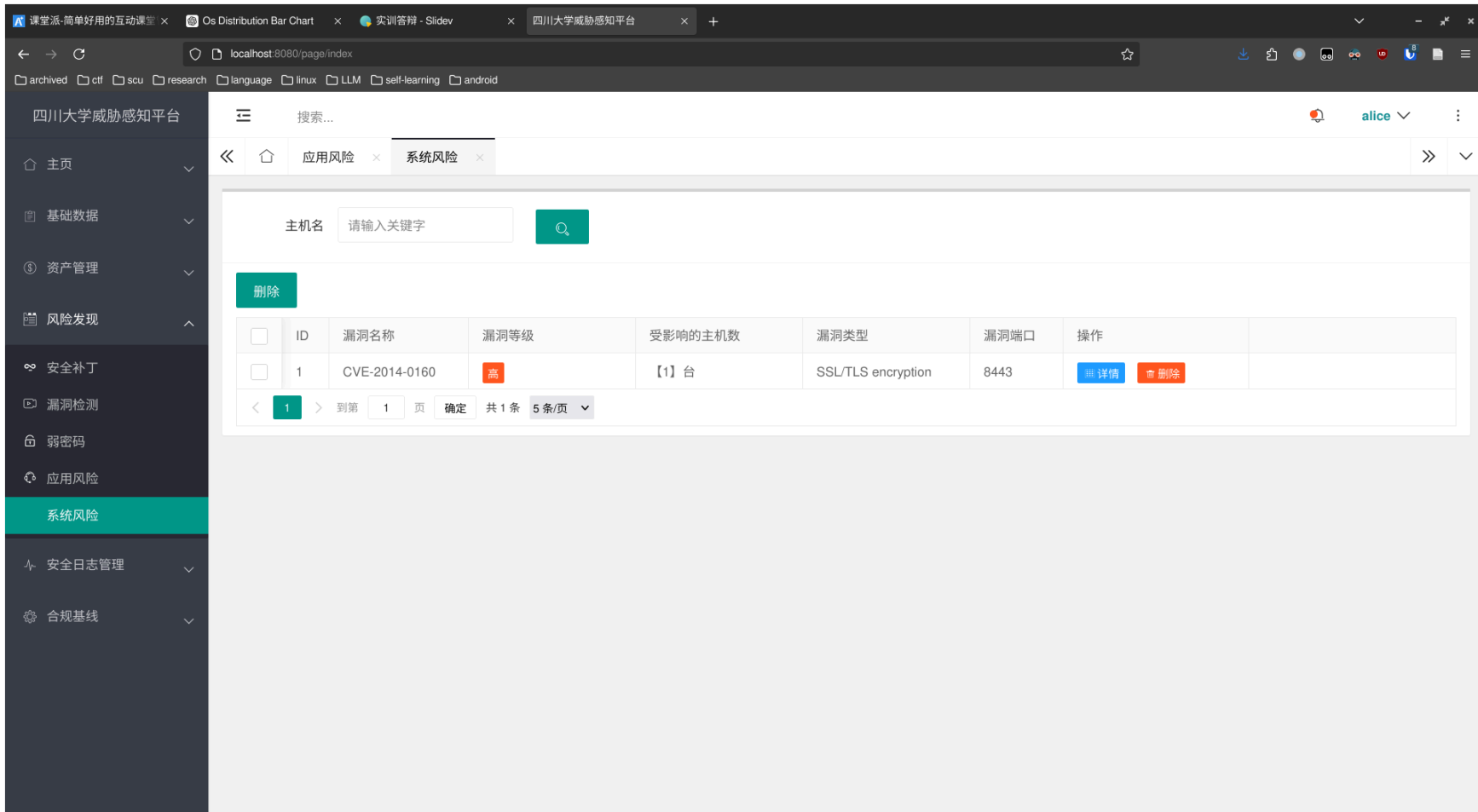
< 1 >

到第 1 页

确定

共 1 条

5 条/页



安全日志

课堂派-简单好用的互动课堂

Os Distribution Bar Chart

实训答疑 - Slidew

四川大学威胁感知平台

localhost:8080/page/index

archivedctfscuresearchlanguagelinuxLLMself-learningandroid

四川大学威胁感知平台

主页

基础数据

资产管理

风险发现

安全日志管理

审计日志

登录日志

账号变更日志

合规基线

搜索...

alice

应用风险系统风险审计日志

主机名所有主机

时间搜索开始时间结束时间

删除

	ID	MAC地址	事件ID	时间戳	进程名	操作
<input type="checkbox"/>	72950	B8:81:98:C3:0E:7D	4703	2024-06-20 16:32:16	C:\Windows\System32\svchost.exe	查看详情 删除
<input type="checkbox"/>	72951	B8:81:98:C3:0E:7D	4703	2024-06-20 16:32:16	C:\Windows\System32\svchost.exe	查看详情 删除
<input type="checkbox"/>	72952	B8:81:98:C3:0E:7D	4703	2024-06-20 16:32:16	C:\Windows\System32\svchost.exe	查看详情 删除
<input type="checkbox"/>	72953	B8:81:98:C3:0E:7D	4703	2024-06-20 16:32:16	C:\Windows\System32\svchost.exe	查看详情 删除
<input type="checkbox"/>	72954	B8:81:98:C3:0E:7D	4703	2024-06-20 16:32:16	C:\Windows\System32\svchost.exe	查看详情 删除

<123...2614>

到第1页

确定

共 13066 条

5条/页

课堂派-简单好用的互动课堂 × Os Distribution Bar Chart × 实训答疑 - Slidex × 四川大学威胁感知平台 × +

localhost:8080/page/index

archived ctf scu research language linux LLM self-learning android

四川大学威胁感知平台

搜索...

alice

应用风险 × 系统风险 × 审计日志 × 登录日志 ×

主机名

所有主机

时间搜索

开始时间

结束时间

删除

	ID	MAC地址	事件ID	时间戳	进程名	操作
<input type="checkbox"/>	73410	B8:81:98:C3:0E:7D	4624	2024-06-20 18:17:54		<div>查看详情</div> <div>删除</div>
<input type="checkbox"/>	73464	B8:81:98:C3:0E:7D	4624	2024-06-20 18:17:56	C:\Windows\System32\wininit.exe	<div>查看详情</div> <div>删除</div>
<input type="checkbox"/>	73467	B8:81:98:C3:0E:7D	4624	2024-06-20 18:17:56	C:\Windows\System32\winlogon.exe	<div>查看详情</div> <div>删除</div>
<input type="checkbox"/>	73472	B8:81:98:C3:0E:7D	4624	2024-06-20 18:17:56	C:\Windows\System32\services.exe	<div>查看详情</div> <div>删除</div>
<input type="checkbox"/>	73479	B8:81:98:C3:0E:7D	4624	2024-06-20 18:17:57	C:\Windows\System32\services.exe	<div>查看详情</div> <div>删除</div>

< 1 2 3 ... 9 >

到第 1 页

确定

共 44 条

5 条/页

首页

基础数据

资产管理

风险发现

安全日志管理

审计日志

登录日志

账号变更日志

合规基线

课堂派-简单好用的互动课堂

Os Distribution Bar Chart

实训答疑 - Slidew

四川大学威胁感知平台

localhost:8080/page/index

archivedctfscuresearchlanguagelinuxLLMself-learningandroid

四川大学威胁感知平台

搜索...

alice

应用风险

系统风险

审计日志

登录日志

账号变更日志

删除

	ID	MAC地址	事件ID	时间戳	进程名	操作
<input type="checkbox"/>	84289	B8:81:98:C3:0E:7D	4726	2024-06-20 19:51:03		<div>查看详情</div> <div>删除</div>
<input type="checkbox"/>	84313	B8:81:98:C3:0E:7D	4726	2024-06-20 19:51:05		<div>查看详情</div> <div>删除</div>
<input type="checkbox"/>	84326	B8:81:98:C3:0E:7D	4726	2024-06-20 19:51:08		<div>查看详情</div> <div>删除</div>

<

1

>

到第

1

页

确定

共 3 条

5 条/页

主页

基础数据

资产管理

风险发现

安全日志管理

审计日志

登录日志

账号变更日志

合规基线