







SeMF 使用指南

1 账号体系：

本系统账号及权限遵循 RBAC 原则，可动态定义用户，角色和权限之间的管理，系统初始化时提供 安全管理员、运维管理员、网络管理员、业务负责人四级用户。如需变更角色权限，可前往 `ip:port/semf/` 页面进行设置：

RBAC		
Areas	+ 增加	 修改
Menus	+ 增加	 修改
Permissions	+ 增加	 修改
Profiles	+ 增加	 修改
Roles	+ 增加	 修改
User requests	+ 增加	 修改

修改角色可编辑 Roles，变更用户所属可编辑 Profiles，用户区域所属修改 Area，其他选项在定制化需求时使用，建议拥有 django 开发能力的团队自定义。

1.1 用户列表

该模块用于显示当前用户列表（默认不显示命令行创建的用户），管理员可在该页面禁用/启用用户账号。

1.2 用户审批

该模块用于前段对用户进行管理，考虑到该用户模块的特殊性，所有用户在注册页的申请均需管理员进行审批。可在用户审批页面进行处理。

每个邮箱最多可申请两次，两次过后将无法进行申请，针对特殊案例，可在 `/semf/` 页面删除邮箱的申请记录。

2 资产管理

该功能主要包含资产列表、资产审批以及资产交接审批三大模块，考虑到不同企业的资产划分不同，该模块在后台自定义资产类型及不同类型的资产属性，可前往 `ip:port/semf/` 页面进行设置：

ASSETMANAGE		
Asset type infos	+ 增加	✎ 修改
Asset types	+ 增加	✎ 修改
Assets	+ 增加	✎ 修改

彻底删除资产或便捷修改资产，可操作 Assets，修改资产类型可编辑 Asset types；修改每种资产的附加属性信息可编辑 Asset type info。系统初始化时提供的资产分类，初网段资产外，均可进行修改。

2.1 资产列表

该模块可实现当前系统内资产的直观展现，支持分类查询及模糊查询

删除资产：普通用户删除资产，仅将该资产从该用户名下移除，资产及其相关信息不进行删除；管理员用户删除资产，会将该资产状态设置为已销毁。如需彻底删除资产信息，请访问 `/semf/` 页面进行删除。

资产申请：该模块用户将系统内已有资产申请到当前用户名下，提交资产申请需要由管理员进行审批

新增资产：针对系统内不存在的资产，可使用该功能进行补充

批量导入：该模块主要针对资产初始化，用户可根据提供的模板初始化资产信息

端口扫描：选定服务器类资产，点击端口扫描，后台将自动执行端口扫描任务，该任务不进入任务列表中，扫描完成后，会提供消息通知给用户。

安全扫描：该模块主要针对多资产进行安全扫描，目前仅支持 nessus

资产发现：该功能用户针对 ip 地址段类资产进行扫描，检查该网段内存活的主

机，发现的资产除 ip 地址外，均需自行修改。（使用 nessus 对网段进行安全扫描时，也可以实现资产发现功能）

资产指定：该功能可批量将资产管理权限指定给特定用户，减少资产申请及审批

资产详情：针对指定资产的信息及附加属性的查阅，可在资产详情页面进行增删查改

2.2 资产审批:

该模块主要是针对用户申请资产库中存在的，防止敏感资产的错误认领

2.3 交接审批

对于非管路员用户，在用户设置页存在 资产交接功能，该功能可将当前用户的所有资产转交给其他账号。所有资产交接，需要管理员人工确认后审批，审批通过后，交接申请账号将被停用。

3 网络映射

针对大型企业，内网和外网之间的映射管理非常复杂，在进行日志分析以及对外业务管理时，安全部门可能因为信息不流通无法进行准确分析处理，预留该功能，可作为参考信息（后续会与其他功能进行配合）

4 漏洞管理

该模块分为漏洞列表和漏洞库，用于漏洞信息的集中管理，漏洞列表展现当前所有资产存在的安全风险及详细信息，漏洞库存储 cnvd 所有漏洞信息

4.1 漏洞列表：

用于展示当前系统中所有安全风险及修复状态，支持分类及模糊查询，支持批量更新操作

4.2 漏洞自定义

目前主流扫描器都存在一定的误报，整改方案也不详细，如果直接反馈给业务部门，很可能出现高误报，漏洞整改困难等问题，这里提供了统一的漏洞筛查模块，访问/semf/页面设置

VULNMANAGE		
Advance_vulnss	+ 增加	✎ 修改
Cnvdfiles	+ 增加	✎ 修改

编辑 Advance_vulns 针对常见的误报漏洞进行统一更新，在导入扫描结果时，会根据该模块的漏洞进行自动过滤。减少人工二次核对。

4.3 漏洞库

该模块对接 cnvd 漏洞库，可实现漏洞信息内网查询，支持漏洞信息更新及漏洞整改方案管理。（该模块当前仅做参考查询使用，后续会与其他功能关联使用，可在权限设置页取消该功能）

5 任务管理

该模块用于管理第三方扫描器对接的安全扫描任务，

5.1 任务列表：

支持分类及模糊查询

扫描同步：该模块当前可用于对于 Nessus 已完成的扫描任务的任务同步，扫描任务 id 可在 nessus api 接口查询，也可通过访问任务详情，在 url 中获取

新建任务：该模块用于单个资产的安全扫描，支持 nessus 和 awvs（配置方法参考安装指南）

5.2 任务审批：

普通用户提交扫描任务后，不会立刻获取执行权限，需要安全部门进行审批，审批通过后方可进行扫描（考虑到部分安全扫描会对网络或业务造成一定影响，该

功能用于统一调度，减少异常事件）

6 报表中心

该模块用于展示当前系统内存在的资产分类，漏洞分级以及漏洞状态的图表展示，当前提供了饼图、柱状图、以及折线图，需要自定义报表的可以根据需要进行修改。

7 知识库管理

这个模块主要指针对安全信息的共享，分为通告类和科普类，通告类会将文章推送给平台内所有用户，可用于漏洞预警；科普类主要用于记录安全相关知识积累，便于业务部门进行查找，同时也可以与漏洞修复方案进行关联。