09 用户与权限

账号分类

- 匿名账号：账号id为0，系统预建立的，代表灭有登录的匿名用户 ，即游客，所有匿名用户共享此账号。
- 维护账号：账号id为1，在系统安装过程中设置的账号，具备最高的管理权限，账号id如果为1，那么系统是不会进行权限判断的，用于系统维护人员，仅一个。
- 普通账号：除id为0和1以外的所有账号，可由用户自行注册，也可由系统管理员代为注册或批量生成。

权限

- 用于管控系统使用者的行为，识别能做什么、不能做什么。
- 在系统中，每一种权限，都有一个权限ID和说明，某个用户能不能执行某个动作，就看是否拥有该权限。
- 权限的检查是由检查器来完成的，检查的结果有三种状态：允许Allowed、中立Netral、禁止Forbidden；在中立状态时是否能够通过检查又涉及到严格还是宽松等问题，因此，权限的判断并不简单。

基于角色的控制访问（RBAC）

Drupal采用的是Role-Based Access Control，即权限不是直接关联到用户的，而是将所需的权限打包成一个权限集合，然后再将这个集合和用户进行关联，这个集合就是“角色”，这样的处理方式极具灵活性。在新增一个用户时，不需要一个一个的进行权限分配，只需要分配一个角色即可，用户还可以同时具备多种角色，这样就拥有多种权限集合。

用户、角色和权限的关系

- 权限和角色直接关联，多对多关系。一个权限可以被分配给多个角色，一个角色可以包含多个权限。

- 角色和账号直接关联，多对多关系。一个角色可以被分配到多个账户一，一个账户可以拥有多个角色。

系统中的权限、角色设置

- 系统中对权限和角色的更改在：People。
- List 的“状态”参数：“有效”指能够正常使用的账户；“阻止”指冻结账户。Action可以批量的修改人员信息（取消选中的用户账户 -> 指在系统中删除）。
- Roles：展示了系统中拥有的角色。匿名用户：所有未登录系统的游客，自动赋予；已登录用户：所有的注册用户，自动赋予；管理员：拥有最高权限，对系统进行管理的角色；Content editor：Drupal10新增的角色，可删除。
- Roles settings：设置哪个角色为管理员（默认管理员角色为管理员）。
- 系统中的“权限”设置文件：core/modules/user/user.permissions.yml（仅为核心自带的用户模块自定义的权限）。 当模块需要用到某一些权限时，就以这样的文件名的结构，静态的定义一些权限。当模块的程序需要去执行某些操作需要考虑到权限时，就会在该文件中先检查用户是否具备该权限，最后再执行操作。除了上述静态的定义文件外，还可以通过程序判断系统里面的情况环境动态的定义权限。更加复杂的权限，用户可以在底层更改权限检查器实现。
- 账户设置页：配置 -> People ->账户设置
    - 设置：联系设置（联系表：站内不同用户之间相互沟通的表单，类似于留言板）；匿名用户（匿名用户怎么在前台显示）；启用翻译（用户注册时，自己的资料界面是否需要多语言显示）；注册和取消注册（启用“访客，但须要管理员批准”之前，需要先对系统进行邮件方便的配置，让系统能够自行去发送邮件，推荐安装smtp的模块实现邮件的发送）。
    - 管理字段：存储和账户高度相关的信息，可根据需求重新添加字段。关于用户的资料储存推荐使用模块profile（该模块用于存放用户的各种资料，不同于用户字段信息，该模块可让单个用户存放多种类型的用户信息，且每种类型都可以有多条信息，权限控制也更加细致；其中"Allowed roles"如果不选择其中一个参数，则表示都可以使用；允许资料类型可版本化：修改后会形成新的版本，原来的版本还会保存）。Tips：当不知道模块的使用入口时，可以在启用模块的界面，找到相应模块，点击配置，即可直接到模块使用界面。

权限控制相关的模块

- 模块masquerade：用于临时切换为其他账户，以便管理员了解其配置情况，免去退出再登陆的麻烦，在不知道用户密码的情况下，使用此模块尤为方便。
- 模块admin_toolbar：过滤无权访问的菜单，使用体验更好、能进行菜单搜索等。

Drupal的账户密码

- 密码明文+干扰码哈希盐 -> 散列算法（如Sha512，MD5）-> 储存码
- 散列算法：又称哈希算法，可以将任意原文件（比如图片、文字、音乐、视频等）映射为一个固定长度的“字符串”，又称为散列值、哈希值、数字指纹等等，映射不是加密，是单向的，不可反推，即无法由哈希值得知原来的输入，相同的输入所计算出来的哈希值一定相同，反之则不一定。

- 实际情况更复杂。
- Drupal密码的特点：
  - 全世界只有自己知道密码；
  - 即使拿走代码和数据库也无法知道密码；
  - 密码相同的两个账户，内部存储也不相同；
  - 明文最长不超过512字节，可以是任意字符；
  - 密码存储算法是可以升级的，升级过程不影响系统使用。
  - （在《云客源码分析》的“密码储存”有忘记密码的各种处理办法）。
  - Drupal默认连续50次输错密码后，将会被暂时阻止登录（其中次数可以自行修改）；或者要求更加安全的话，也可以自行增加验证码。