10.7. 资源所有者密码凭据(10.7. Resource Owner Password Credentials)

10.7. 资源所有者密码凭据

资源所有者密码凭据许可类型通常用于遗留或迁移原因。它降低了由客户端存储用户名和密码的整体风险，但并没有消除泄露高度特权的凭证给客户端的需求。这种许可类型比其他许可类型承载了更高的风险，因为它保留了本协议寻求避免的密码反模式。客户端可能滥用密码或密码可能会无意中被泄露给攻击者（例如，通过客户端保存的日志文件或其他记录）。此外，由于资源拥有者对授权过程没有控制权（在转手它的凭据给客户端后资源所有者的参与结束），客户端可以获得比资源所有者预期的具有更大范围的访问令牌。授权服务器应该考虑由这种许可类型颁发的访问令牌的范围和寿命。授权服务器和客户端应该尽量减少这种许可类型的使用，并尽可能采用其他许可类型。

10.7. Resource Owner Password Credentials

```
   The resource owner password credentials grant type is often used for   legacy or migration
reasons.  It reduces the overall risk of storing   usernames and passwords by the client but
does not eliminate the need
   to expose highly privileged credentials to the client.
   This grant type carries a higher risk than other grant types because   it maintains the
password anti-pattern this protocol seeks to avoid.   The client could abuse the password, or
the password could
   unintentionally be disclosed to an attacker (e.g., via log files or   other records kept by
the client).
   Additionally, because the resource owner does not have control over   the authorization
process (the resource owner's involvement ends when   it hands over its credentials to the
client), the client can obtain   access tokens with a broader scope than desired by the
resource
   owner.  The authorization server should consider the scope and   lifetime of access tokens
issued via this grant type.
   The authorization server and client SHOULD minimize use of this grant   type and utilize
other grant types whenever possible.
```

Revision #1
Created Wed, Mar 25, 2020 11:22 PM by 爱异常
Updated Wed, Mar 25, 2020 11:23 PM by 爱异常