10.2. 客户端仿冒(10.2. Client Impersonation)

10.2. 客户端仿冒

如果被仿冒的客户端不能，或无法保持其客户端凭据保密。恶意客户端可能冒充其他客户端，并获得对受保护资源的访问权限。授权服务器任何可能的时候必须验证客户端身份。如果授权服务器由于客户端的性质无法对客户端进行身份验证，授权服务器必须要求注册任何用于接收授权响应的重定向URI并且应该利用其他手段保护资源所有者防止这样的潜在仿

授权服务器应该实施显式的资源所有者身份验证并且提供给资源所有者有关客户端及其请求的授权范围和生命周期的信息。由资源所有者在当前客户端上下文中审查信息并授权或拒绝该请求。授权服务器未对客户端进行身份验证（没有活动的资源所有者交互）或未依靠其他手段确保重复的请求来自于原始客户端而非冒充者时，不应该自动处理重复的授权请求。

10.2. Client Impersonation

```
   A malicious client can impersonate another client and obtain access   to protected resources
if the impersonated client fails to, or is   unable to, keep its client credentials
confidential.
   The authorization server MUST authenticate the client whenever   possible.  If the
authorization server cannot authenticate the client   due to the client's nature, the
authorization server MUST require the   registration of any redirection URI used for receiving
authorization
   responses and SHOULD utilize other means to protect resource owners   from such potentially
malicious clients.  For example, the   authorization server can engage the resource owner to
assist in
   identifying the client and its origin.
   The authorization server SHOULD enforce explicit resource owner   authentication and provide
the resource owner with information about   the client and the requested authorization scope and
lifetime.  It is
   up to the resource owner to review the information in the context of   the current client and
to authorize or deny the request.
   The authorization server SHOULD NOT process repeated authorization   requests automatically
(without active resource owner interaction)   without authenticating the client or relying on
other measures to
   ensure that the repeated request comes from the original client and
```

```
   not an impersonator.
```

Revision #1
Created Wed, Mar 25, 2020 11:19 PM by □□□
Updated Wed, Mar 25, 2020 11:19 PM by □□□