PHP中使用crypt()实现用户身份验证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/62/2021_2022_PHP_E4_B8_AD_E4_BD_BF_E7_c40_62359.htm 在开发PHP应用中如果不想自己开发新的加密算法，还可以利用PHP提供的crypt()函数来完成单向加密功能。 了解crypt() 只要有一点使用非Windows平台经验的读者都可能对crypt()相当熟悉，这一函数完成被称作单向加密的功能，它可以加密一些明码，但不能反过来将密码重新转换为原来的明码。crypt()函数定义如下。 string crypt (string input_string [, string salt]) 其中，input_string参数是需要加密的明文字符串，第二个可选的salt是一个位字串，能够影响加密的暗码，进一步排除被破解的可能性。缺省情况下，PHP使用一个2个字符的DES干扰串，如果系统使用的是MD5(参考下一节内容)，PHP则会使用一个12个字符的干扰串。可以通过执行下面的命令发现系统将要使用的干扰串的长度。 print "My system salt size is: ". CRYPT_SALT_LENGTH. crypt()支持4种加密算法，表19.1显示了其支持的算法和相应的salt参数的长度。 表crypt()支持四种加密算法 算法 Salt长度 CRYPT_STD_DES 2-character (Default) CRYPT_EXT_DES 9-character CRYPT_MD5 12-character beginning with 1 CRYPT_BLOWFISH 16-character beginning with 2 从表面上看，crypt()的函数似乎没有什么用处，但该函数的确被广泛用来保证系统密码的完整性。因为，单向加密的口令即使落入第三方的手里，由于不能被还原为明文，也没有什么大用处。 用crypt()实现用户身份验证