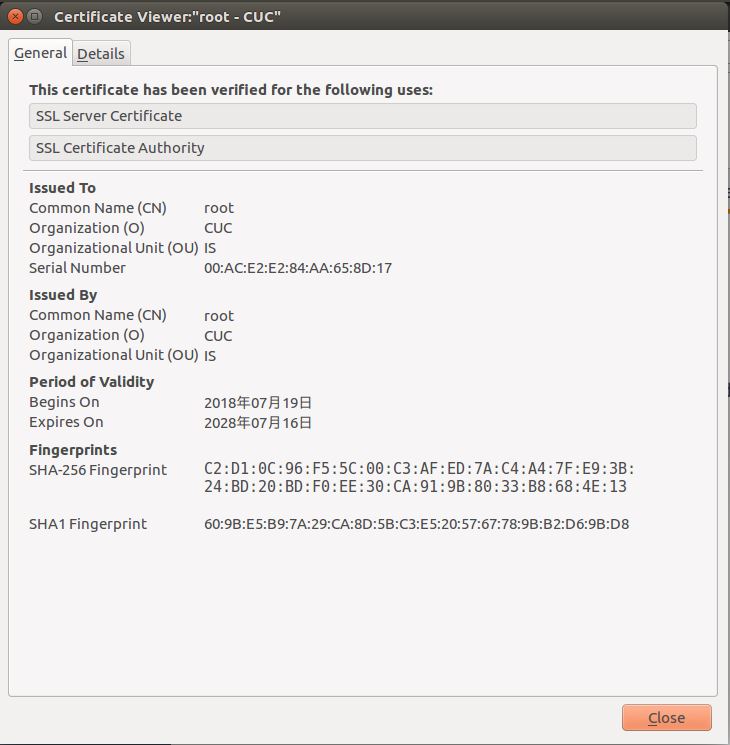
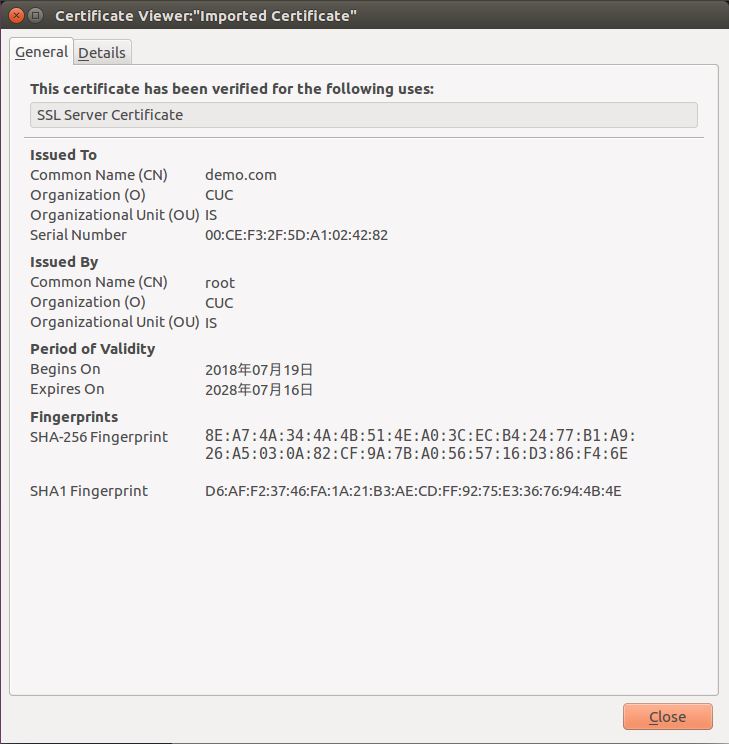
1. X.509证书中各个字段含义、用途解释说明。

由自签发证书可以得到：





x.509证书通常含有如下字段：

（1）公用名称：(Common Name)，一般为网站域名，本证书使用demo.com

（2）单位名称：(Organization)，本证书使用CUC

（3）所在城市：(Locality)，本证书使用Beijing

（4）所在省份：(State/Province)，本证书使用Beijing

（5）所在国家：(Country)，如中国CN

（6）电子邮件：(Email)

（7）多个姓名字段

1. WEB服务器使用的证书和CA使用的证书有什么区别和联系？

WEB服务器证书是用来保护数据加密传输的证书，CA证书是证书链证书，为了方便客户端验证服务器证书的有效性和给服务器证书提供兼容性的证书。

1. 简述你的口令安全存储策略。

禁止使用明文存储用户口令。利用libsodium库中的

string sodium\_crypto\_pwhash(int $output\_length, string $password, string $salt, int $opslimit, int $memlimit) 函数对用户的明文口令进行hash，将hash后的结果和过程中随机生成的盐值与对应的用户名一起存入数据库。

1. 你是如何实现弱口令检测的？

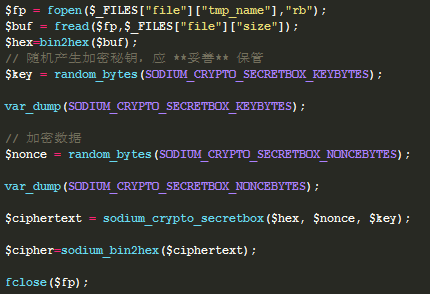
利用正则表达式，对于用户设置的口令，规定其长度为6~36之间，且口令不能只由字母或数字组成，即合法的口令必须满足：

* 1. 口令长度在6~36之间
  2. 口令必须同时含有数字和字母

1. 你是如何实现安全的文件上传的？
   1. 限制文件的大小：< 10MB
   2. 限制文件类型：office文档、常见图片类型
   3. 匿名用户禁止上传文件：即未登录的用户无法上传文件
   4. 对文件进行对称加密存储到文件系统，禁止明文存储文件
2. 请展示并说明你的文件加密代码片段

以只读模式打开文件，将文件内容以二进制读入变量$buf中，并转化为16进制$hex；生成随机加密密钥和加密数据

随后调用sodium\_crypto\_secretbox(message,nonce,key)函数对文件进行加密，转换为16进制存储，最后关闭文件



1. 简述RSA加密算法和RSA签名算法之间的关系？

RSA加密算法：A和B进行加密通信时,B首先要生成一对公私钥。公钥分发给A，而B自己持有私钥。A使用B的公钥加密要加密发送的内容，然后B再通过自己的私钥解密内容。

RSA签名算法：假设A要想B发送消息，A会先计算出消息的消息摘要，然后使用自己的私钥加密这段摘要加密，最后将加密后的消息摘要和消息一起发送给B，被加密的消息摘要就是“签名”。B收到消息后，也会使用和A相同的方法提取消息摘要，然后使用A的公钥解密A发送的来签名，并与自己计算出来的消息摘要进行比较。如果相同则说明消息是A发送给B的，同时，A也无法否认自己发送消息给B的事实。

1. 你是如何实现匿名用户禁止上传文件功能的？

在登陆成功时进行session\_start()函数的调用，记录某一用户访问该网站的cookie，并将用户名存入SESSION的系统常量中，以便后面文件上传时进行身份判别。

