浅谈渗透测试中的逆向破解

随着越来越多的公司开发程序时都注意注重数据的安全了，很多时候会通过加密数据库连接，加密数据库部分敏感数据的方式保护数据不容易被窃取！因此我们经常在找

数据库连接的时候会找到一些加密过的连接字符串。对于不会有相关逆向的人来讲，可能就

会被止步在此！ 但是我们通常不能满足于此，于是需要我们对渗透测试过程中的逆向加解密有一些了解！下面我通过一些加解密的过程演示向大家展示下，是怎么样加密和怎么样解密的。

1. 数据库连接字符串加密（主要讲解在aspx中的加解密）

加密方式的多样化：

（1）Des加密（非对称加密）

<add name="democonn" connectionString="server=localhost;database=test;uid=sa;pwd=sa;"/>

<add name="democonndes" connectionString="fuWgz5qsA006DEV+G6ciq1XqAQEBs87717v8xEO7S8C1G3/WzkQPLQYyHlfsPSGb"/>

（2）aspnet\_regiis(.net Framework为数据库连接字符串提供的一种加密方式，只能在加密的机器上解密)

<connectionStrings>

<add name="mytest" connectionString="server=.;database=aa;uid=sa;pwd=sa" />

</connectionStrings>

connectionStrings configProtectionProvider="DataProtectionConfigurationProvider">

<EncryptedData>

<CipherData>

<CipherValue></CipherValue>

</CipherData>

</EncryptedData>

</connectionStrings>

1. 数据加密

数据库某些敏感数据的加密，比如密码等字段的加密，通常是md5，也可以是自己写的加密方式，通常自己写的加密方式。我们就要通过分析加密算法，写出解密的算法来解密；

1. 通常aspx程序中用的最多的加密就是des，一般程序里也会带有解密算法，这个时候就可以直接调用解密算法的方式来进行解密；
2. Java类的加密；

Java程序在通过编译之后源码中的.java就会对应编译成.class文件。此时这类文件

已经被加密了；直接打开是面目全非的；此时我们就可以通过反编译软件来进行逆向反编译；