基础入门-加密编码算法

前言：在渗透测试中，常见的密码等敏感信息会采用加密处理，其中作为安全测试人员必须要了解常见的加密方式，才能为后续的安全测试做好准备，本次课程将讲解各种加密编码等知识，便于后期的学习和发展。

#常见加密编码等算法解析

MD5，SHA，ASC，进制，时间戳，URL，BASE64，Unescape，AES，DES 等

#常见加密形式算法解析

直接加密，带 salt，带密码，带偏移，带位数，带模式，带干扰，自定义组合等

#常见解密方式（针对）

枚举，自定义逆向算法，可逆向

#了解常规加密算法的特性
长度位数，字符规律，代码分析，搜索获取等

演示案例：

✧ 某 CTF 比赛题目解析

#脚本自定义算法组合逆向

✧ 某 CMS 密码加密解密

#MD5+salt
#部分 CMS 密码加密形式-wp,dz 等

✧ 某 URL 加密地址的漏洞测试

#AES+Base64+自定义
#观察参数值加密字符串，下载源代码分析，函数定义 AES 加密，涉及模式 CBC,128 位，加密密码，偏移量，两次 base64 减去常规一次，填充模式。（_mozhe）

ZUlJOGMzSmVMMHQwZHhNN3diM056Zz09
eII8c3JeL0t0dxM7wb3Nzg==

✧ 某实际应用 URL 地址参数加密

#搜素特定关键字加密字符串

涉及资源：

https://www.mozhe.cn

https://www.cmd5.com

http://tool.chacuo.net/cryptaes

https://ctf.bugku.com/challenges

https://www.cr173.com/soft/21692.html

https://gitee.com/ComsenzDiscuz/DiscuzX
