原文地址:http://drops.wooyun.org/papers/506

0x00 前言

对于一个完善系统而言,无论是桌面还是web程序, 都会使用客户端保存数据如cookie,db文件等。为了不让外部获取或者控制,系统会对数据进行私有加密 例如qq密码,聊天记录,web程序中用户信息等。而对于开源程序而言,算法是公开的,对数据的加密只有依靠key来保护数据 ,一旦数据可控就可能造成某些安全问题,本文探讨web开源程序中对私有数据的使代码的安全性问题。

0x01 直捣黄龙:key可知

某些加密key可推算抑或可爆破情况下,私有数据数据完全可控,根据实际环境sql注入,xss,越权等攻击。

例如:

WooYun: Espcms v5.6 暴力注入

WooYun: dedecms sql injection

PHPCMS V9 sys_auth()设计缺陷导致多个SQL注入漏洞

0x02 隔山打牛:key不可知

为了数据和代码的统一,一套系统中数据的加密解密key一般是通用的,我们可以利用程序的某些功能来生成加密之后的数据,从而控制程序的私有数据,进行攻击。

类似的案例如:

WooYun: PHPCMS最新版(V9)SQL注入一枚

WooYun: espcms 二次注入一枚

WooYun: Espcms加密函数缺陷导致getshell

0x03 总结

当变量能控时,一切数据都是危险的,程序除了对输入输出的数据做严格过滤之外,对内部私有数据也要相应的过滤。