



杭州2013.12.20

安全测试:

# 从传统移动客户端 到 移动网游客户端

---

卢彬良 @  盛大游戏™

L0ckhart .



<http://weibo.com/lockhartcn>

1 背景

2 传统移动客户端测试

3 移动游戏客户端测试

4 除了测试还能做什么

- 安全需求?
  - 1、金融（银行、券商）、运营商、ZF（气象、12306等）
  - 2、互联网、网游等（自己做）
- 现状
  - 1、移动应用只是包了一层壳的Web、PC应用（Wlan是包了一层壳的有线环境）
  - 2、大部分从客户端发现的严重问题都可以在服务端解决
- 引进类游戏的安全弊端
  - 1、本地化带来的安全问题
  - 2、漏洞、bug更新周期
  - 3、无法在服务端做更好的测试（协议、API）
  - 4、历史、组织问题
- 盲点？合作
  - 1、Web
  - \*2、逆向分析、调试
  - 3、脚本语言

# 传统客户端测试框架

## 客户端安全

源代码安全

重要函数、逻辑、加密算法、【是否开启PIE Flag】

数据存储安全

/data/data/\*(xml,plist,db)、sdcard、  
【/var/mobile/Applications/-GUID-/\*】

数据传输安全

传输加密、伪造、服务端验证

敏感信息安全

硬编码、日志、内存、调试信息、组件（Activity/Service/Receiver/Provider）、【Keychain、屏幕快照、键盘存储…】

异常处理

增强安全

权限、进程保护、内存修改、键盘劫持、第三方SDK、【URL schema、内购破解、Binary patch、Runtime attack】…

业务安全

支付...?聊天...?交友...?游戏...?

合规安全

行业合规、安全策略（密码、登陆、会话…）

# 阉割的Apk报告

Android 版 (v3.0.6)	安装包测试	安装包结构	安全	
		能否反编译出源代码	安全	
		安装包是否进行签名	安全	
	数据传输测试	关键数据是否加密	安全	
		客户端对服务器验证	安全	
	数据验证测试	程序是否对数据合法性校验	安全	
	数据存储测试	是否保存手机号、密码等敏感信息	不安全	高
		日志中是否存在敏感信息	安全	
		数据是否能被别的应用访问	安全	
	安全增强测试	手机验证码短信接口测试	不安全	中
		意见反馈接口测试	不安全	低
		键盘劫持测试	安全	
		静态密码测试	安全	
		进程保护测试	不安全	低
	安全策略测试	密码策略测试	不安全	低
		登陆次数限制	不安全	中
		界面切换清空表单	安全	
		会话超时重新登陆	不安全	中

检查代码**混淆**、**硬编码**信息

检查**加密**是否可逆、可篡改

检查文件、内存、日志**敏感**信息

根据业务功能项检查是否绕过正常**业务逻辑**

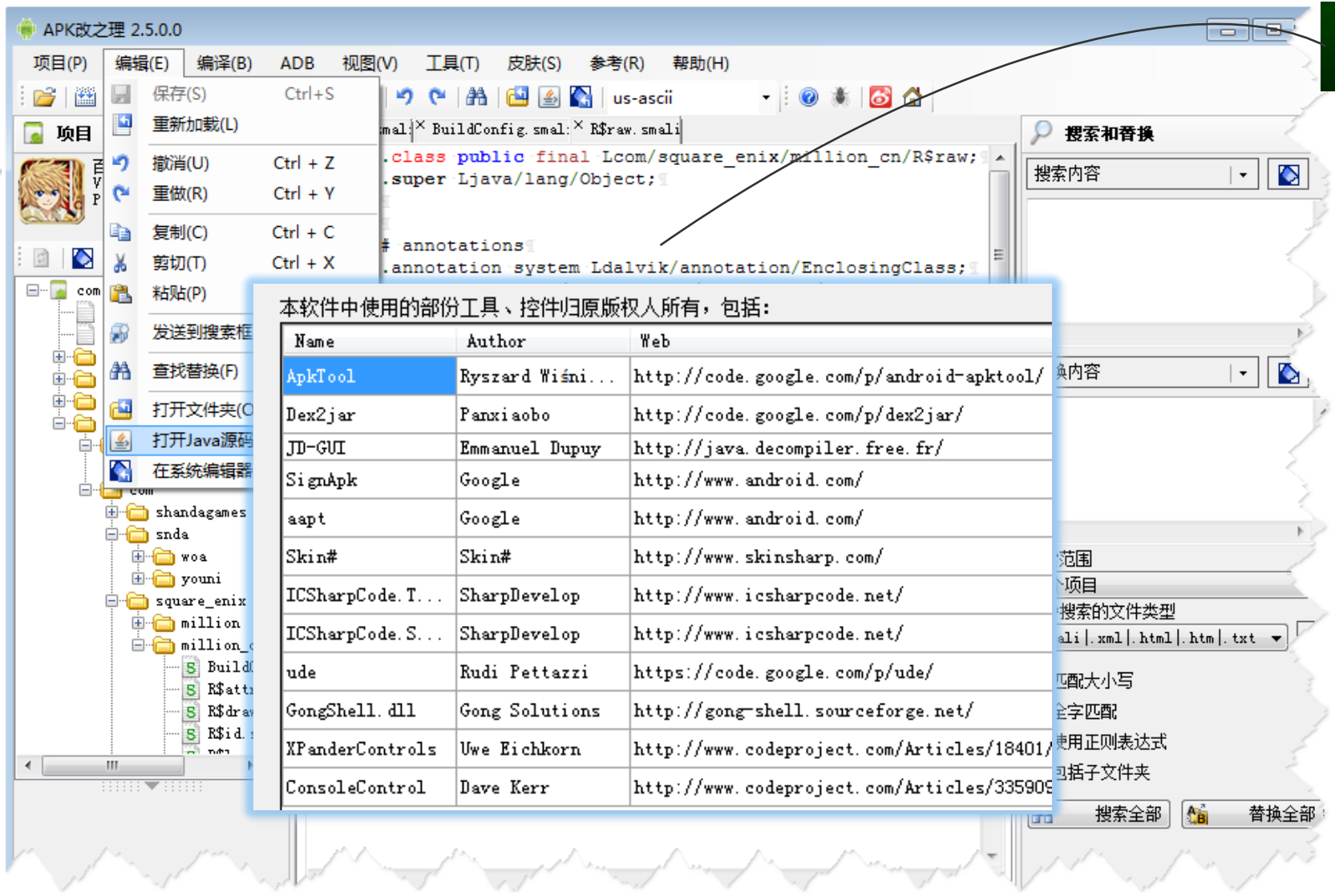
简单客户端的流水线测试  
--! 不看jar、不调试so，秒出

# Android-App测试工具

安装包测试	安装包结构	dex2jar、jd-gui、apktool、baksmali、keytool...
	能否反编译出源代码	
	安装包是否进行签名	
	权限设置是否合理	
数据传输测试	关键数据是否加密	tcpdump、"Hook"
数据验证测试	客户端对服务器验证	
	程序是否对数据合法性校验	
数据存储测试	是否保存账号、密码等敏感信息	adb logcat、SQLite、FileExplorer
	日志中是否存在敏感信息	
	数据能否被别的应用访问(目录及文件权限)	
安全增强测试	服务端安全测试	IDA
	键盘劫持测试	
	进程保护测试	
	第三方 SDK 安全测试	
	组件安全测试	
安全策略测试	密码策略测试	输入法劫持.apk、Web渗透测试、Drozer...
	登陆次数限制	
	密码保护机制	
	会话保护策略	
	系统保护策略	




# Android-App测试工具



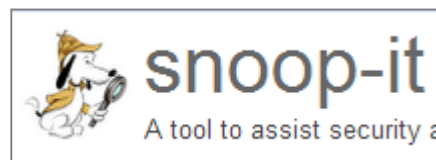
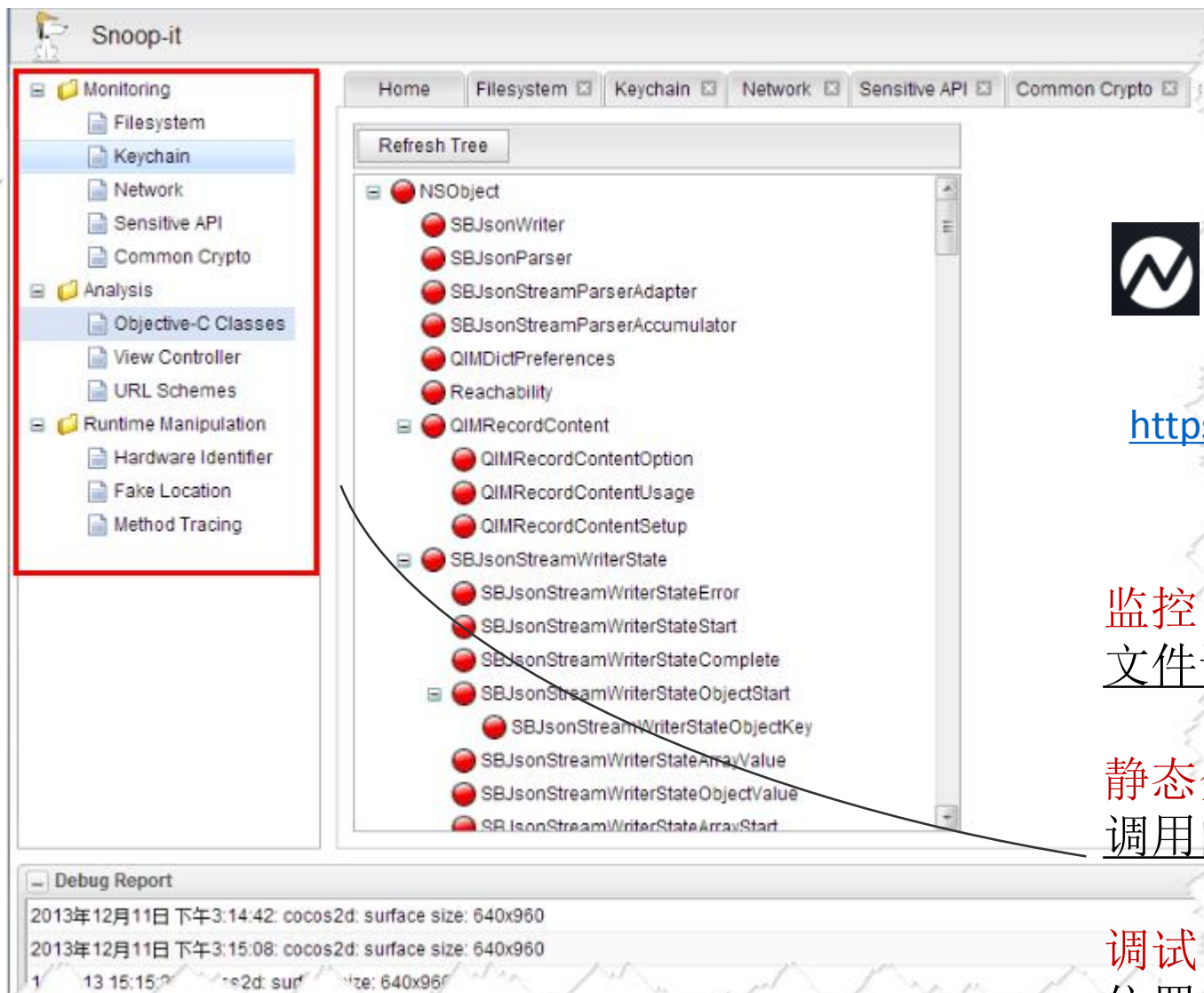
APK改之理  
www.xiaomiren.net

# iOS-App测试工具

安装包测试	安装包结构	otool、class-dump
	硬编码是否保存敏感信息	
	是否开启 <b>PIE Flag</b>	
数据传输测试	关键数据是否加密	tcpdump、" <b>Http Proxy</b> "
	客户端对服务器验证	
数据验证测试	程序是否对数据合法性校验	 <a href="#">Links:看雪论坛</a> <b>IDA + <a href="#">hexarm.dll</a>、(GDB)...</b>  iTools、iGameGuardian、KeyChainDump、SQLite
数据存储测试	是否保存账号、密码等敏感信息	
	日志中是否存在敏感信息	
	内存中是否存在敏感信息	
	<b>KeyChain</b> 中是否存在敏感信息	
	屏幕快照中是否保存敏感信息	
	键盘存储是否存在敏感信息	
安全增强测试	第三方 <b>SDK</b> 安全测试	IAPFree、cycrypt、snoopy (慎用iNalyzer,一堆bug)
	<b>URL schema</b> 漏洞检测	
	进程保护测试	
	内购破解保护测试	
	可否 <b>Binary patch</b> 、 <b>Runtime attack</b>	
	信息泄露检查	
安全策略测试		



# iOS-App测试工具



Cydia:

<http://repo.nesolabs.de/>

<https://code.google.com/p/snoop-it/>

监控:

文件读写、网络访问、敏感API...

静态分析:

调用的类、视图、URL Schemes

调试:

位置伪造、MAC伪造...

# 移动游戏测试



# 测试环境

Android:

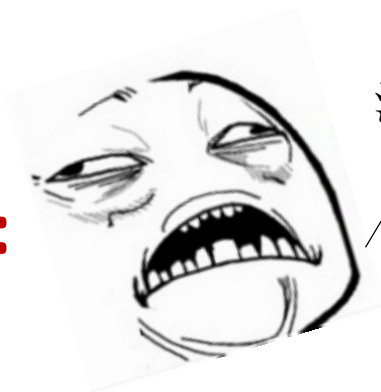


hookme  
TCP Proxy (Data tamper)



droidbox  
Android Application Sandbox

iOS:



没有虚拟机??!



Only http proxy...

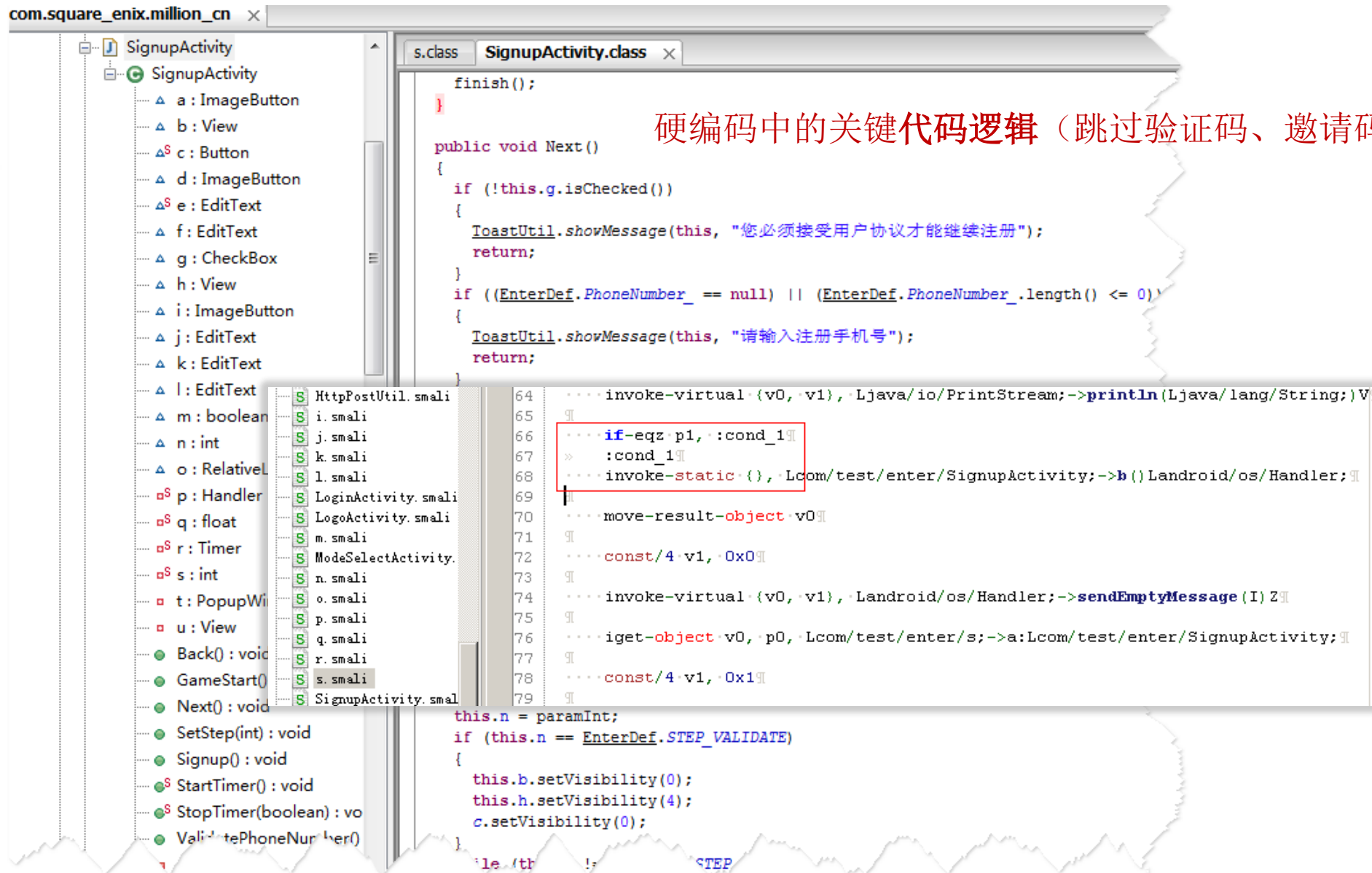


# 移动网游 常见缺陷

---



# 手游“硬伤”一：硬编码-99%





# 手游“硬伤”一：硬编码-99%

```
313 import org.apache.http.client.entity.UrlEncodedFormEntity;
314 ..
315 33 {
316 34
317 35: private static final String BASIC_PASS = "8KdtjVfX";
318 36 private static final String BASIC_USER = "iW7B5MWJ";
319 37 public static final int CONNECT_TASK BILLING = 0x186a1;
```

dex中的  
基础认证信息、加密Key、method

```
320 ..
321 228 Debug.log(">BASIC> BEGIN", new Object[0]);
322 229 URI uri = httpPost.getURI();
323 230:
```

```
324 231
325 232
326 233
327 234
328 235
329 236
330 237
331 238
332 239
333 240
334 241
335 242
336 243
337 244
338 245
339 246
340 247
341 248
342 249
343 250
344 251
345 252
346 253
347 254
348 255
349 256
350 257
351 258
352 259
353 260
354 261
355 262
356 263
357 264
358 265
359 266
360 267
361 268
362 269
363 270
364 271
365 272
366 273
367 274
368 275
369 276
370 277
371 278
372 279
373 280
374 281
375 282
376 283
377 284
378 285
379 286
380 287
381 288
382 289
383 290
384 291
385 292
386 293
387 294
388 295
389 296
390 297
391 298
392 299
393 300
394 301
395 302
396 303
397 304
398 305
399 306
400 307
401 308
402 309
403 310
404 311
405 312
406 313
407 314
408 315
409 316
410 317
411 318
412 319
413 320
414 321
415 322
416 323
417 324
418 325
419 326
420 327
421 328
422 329
423 330
424 331
425 332
426 333
427 334
428 335
429 336
430 337
431 338
432 339
433 340
434 341
435 342
436 343
437 344
438 345
439 346
440 347
441 348
442 349
443 350
444 351
445 352
446 353
447 354
448 355
449 356
450 357
451 358
452 359
453 360
454 361
455 362
456 363
457 364
458 365
459 366
460 367
461 368
462 369
463 370
464 371
465 372
466 373
467 374
468 375
469 376
470 377
471 378
472 379
473 380
474 381
475 382
476 383
477 384
478 385
479 386
480 387
481 388
482 389
483 390
484 391
485 392
486 393
487 394
488 395
489 396
490 397
491 398
492 399
493 400
494 401
495 402
496 403
497 404
498 405
499 406
500 407
501 408
502 409
503 410
504 411
505 412
506 413
507 414
508 415
509 416
510 417
511 418
512 419
513 420
514 421
515 422
516 423
517 424
518 425
519 426
520 427
521 428
522 429
523 430
524 431
525 432
526 433
527 434
528 435
529 436
530 437
531 438
532 439
533 440
534 441
535 442
536 443
537 444
538 445
539 446
540 447
541 448
542 449
543 450
544 451
545 452
546 453
547 454
548 455
549 456
550 457
551 458
552 459
553 460
554 461
555 462
556 463
557 464
558 465
559 466
560 467
561 468
562 469
563 470
564 471
565 472
566 473
567 474
568 475
569 476
570 477
571 478
572 479
573 480
574 481
575 482
576 483
577 484
578 485
579 486
580 487
581 488
582 489
583 490
584 491
585 492
586 493
587 494
588 495
589 496
590 497
591 498
592 499
593 500
594 501
595 502
596 503
597 504
598 505
599 506
600 507
601 508
602 509
603 510
604 511
605 512
606 513
607 514
608 515
609 516
610 517
611 518
612 519
613 520
614 521
615 522
616 523
617 524
618 525
619 526
620 527
621 528
622 529
623 530
624 531
625 532
626 533
627 534
628 535
629 536
630 537
631 538
632 539
633 540
634 541
635 542
636 543
637 544
638 545
639 546
640 547
641 548
642 549
643 550
644 551
645 552
646 553
647 554
648 555
649 556
650 557
651 558
652 559
653 560
654 561
655 562
656 563
657 564
658 565
659 566
660 567
661 568
662 569
663 570
664 571
665 572
666 573
667 574
668 575
669 576
670 577
671 578
672 579
673 580
674 581
675 582
676 583
677 584
678 585
679 586
680 587
681 588
682 589
683 590
684 591
685 592
686 593
687 594
688 595
689 596
690 597
691 598
692 599
693 600
694 601
695 602
696 603
697 604
698 605
699 606
700 607
701 608
702 609
703 610
704 611
705 612
706 613
707 614
708 615
709 616
710 617
711 618
712 619
713 620
714 621
715 622
716 623
717 624
718 625
719 626
720 627
721 628
722 629
723 630
724 631
725 632
726 633
727 634
728 635
729 636
730 637
731 638
732 639
733 640
734 641
735 642
736 643
737 644
738 645
739 646
740 647
741 648
742 649
743 650
744 651
745 652
746 653
747 654
748 655
749 656
750 657
751 658
752 659
753 660
754 661
755 662
756 663
757 664
758 665
759 666
760 667
761 668
762 669
763 670
764 671
765 672
766 673
767 674
768 675
769 676
770 677
771 678
772 679
773 680
774 681
775 682
776 683
777 684
778 685
779 686
780 687
781 688
782 689
783 690
784 691
785 692
786 693
787 694
788 695
789 696
790 697
791 698
792 699
793 700
794 701
795 702
796 703
797 704
798 705
799 706
800 707
801 708
802 709
803 710
804 711
805 712
806 713
807 714
808 715
809 716
810 717
811 718
812 719
813 720
814 721
815 722
816 723
817 724
818 725
819 726
820 727
821 728
822 729
823 730
824 731
825 732
826 733
827 734
828 735
829 736
830 737
831 738
832 739
833 740
834 741
835 742
836 743
837 744
838 745
839 746
840 747
841 748
842 749
843 750
844 751
845 752
846 753
847 754
848 755
849 756
850 757
851 758
852 759
853 760
854 761
855 762
856 763
857 764
858 765
859 766
860 767
861 768
862 769
863 770
864 771
865 772
866 773
867 774
868 775
869 776
870 777
871 778
872 779
873 780
874 781
875 782
876 783
877 784
878 785
879 786
880 787
881 788
882 789
883 790
884 791
885 792
886 793
887 794
888 795
889 796
890 797
891 798
892 799
893 800
894 801
895 802
896 803
897 804
898 805
899 806
900 807
901 808
902 809
903 810
904 811
905 812
906 813
907 814
908 815
909 816
910 817
911 818
912 819
913 820
914 821
915 822
916 823
917 824
918 825
919 826
920 827
921 828
922 829
923 830
924 831
925 832
926 833
927 834
928 835
929 836
930 837
931 838
932 839
933 840
934 841
935 842
936 843
937 844
938 845
939 846
940 847
941 848
942 849
943 850
944 851
945 852
946 853
947 854
948 855
949 856
950 857
951 858
952 859
953 860
954 861
955 862
956 863
957 864
958 865
959 866
960 867
961 868
962 869
963 870
964 871
965 872
966 873
967 874
968 875
969 876
970 877
971 878
972 879
973 880
974 881
975 882
976 883
977 884
978 885
979 886
980 887
981 888
982 889
983 890
984 891
985 892
986 893
987 894
988 895
989 896
990 897
991 898
992 899
993 900
994 901
995 902
996 903
997 904
998 905
999 906
1000 907
1001 908
1002 909
1003 910
1004 911
1005 912
1006 913
1007 914
1008 915
1009 916
1010 917
1011 918
1012 919
1013 920
1014 921
1015 922
1016 923
1017 924
1018 925
1019 926
1020 927
1021 928
1022 929
1023 930
1024 931
1025 932
1026 933
1027 934
1028 935
1029 936
1030 937
1031 938
1032 939
1033 940
1034 941
1035 942
1036 943
1037 944
1038 945
1039 946
1040 947
1041 948
1042 949
1043 950
1044 951
1045 952
1046 953
1047 954
1048 955
1049 956
1050 957
1051 958
1052 959
1053 960
1054 961
1055 962
1056 963
1057 964
1058 965
1059 966
1060 967
1061 968
1062 969
1063 970
1064 971
1065 972
1066 973
1067 974
1068 975
1069 976
1070 977
1071 978
1072 979
1073 980
1074 981
1075 982
1076 983
1077 984
1078 985
1079 986
1080 987
1081 988
1082 989
1083 990
1084 991
1085 992
1086 993
1087 994
1088 995
1089 996
1090 997
1091 998
1092 999
1093 1000
1094 1001
1095 1002
1096 1003
1097 1004
1098 1005
1099 1006
1100 1007
1101 1008
1102 1009
1103 1010
1104 1011
1105 1012
1106 1013
1107 1014
1108 1015
1109 1016
1110 1017
1111 1018
1112 1019
1113 1020
1114 1021
1115 1022
1116 1023
1117 1024
1118 1025
1119 1026
1120 1027
1121 1028
1122 1029
1123 1030
1124 1031
1125 1032
1126 1033
1127 1034
1128 1035
1129 1036
1130 1037
1131 1038
1132 1039
1133 1040
1134 1041
1135 1042
1136 1043
1137 1044
1138 1045
1139 1046
1140 1047
1141 1048
1142 1049
1143 1050
1144 1051
1145 1052
1146 1053
1147 1054
1148 1055
1149 1056
1150 1057
1151 1058
1152 1059
1153 1060
1154 1061
1155 1062
1156 1063
1157 1064
1158 1065
1159 1066
1160 1067
1161 1068
1162 1069
1163 1070
1164 1071
1165 1072
1166 1073
1167 1074
1168 1075
1169 1076
1170 1077
1171 1078
1172 1079
1173 1080
1174 1081
1175 1082
1176 1083
1177 1084
1178 1085
1179 1086
1180 1087
1181 1088
1182 1089
1183 1090
1184 1091
1185 1092
1186 1093
1187 1094
1188 1095
1189 1096
1190 1097
1191 1098
1192 1099
1193 1100
1194 1101
1195 1102
1196 1103
1197 1104
1198 1105
1199 1106
1200 1107
1201 1108
1202 1109
1203 1110
1204 1111
1205 1112
1206 1113
1207 1114
1208 1115
1209 1116
1210 1117
1211 1118
1212 1119
1213 1120
1214 1121
1215 1122
1216 1123
1217 1124
1218 1125
1219 1126
1220 1127
1221 1128
1222 1129
1223 1130
1224 1131
1225 1132
1226 1133
1227 1134
1228 1135
1229 1136
1230 1137
1231 1138
1232 1139
1233 1140
1234 1141
1235 1142
1236 1143
1237 1144
1238 1145
1239 1146
1240 1147
1241 1148
1242 1149
1243 1150
1244 1151
1245 1152
1246 1153
1247 1154
1248 1155
1249 1156
1250 1157
1251 1158
1252 1159
1253 1160
1254 1161
1255 1162
1256 1163
1257 1164
1258 1165
1259 1166
1260 1167
1261 1168
1262 1169
1263 1170
1264 1171
1265 1172
1266 1173
1267 1174
1268 1175
1269 1176
1270 1177
1271 1178
1272 1179
1273 1180
1274 1181
1275 1182
1276 1183
1277 1184
1278 1185
1279 1186
1280 1187
1281 1188
1282 1189
1283 1190
1284 1191
1285 1192
1286 1193
1287 1194
1288 1195
1289 1196
1290 1197
1291 1198
1292 1199
1293 1200
1294 1201
1295 1202
1296 1203
1297 1204
1298 1205
1299 1206
1300 1207
1301 1208
1302 1209
1303 1210
1304 1211
1305 1212
1306 1213
1307 1214
1308 1215
1309 1216
1310 1217
1311 1218
1312 1219
1313 1220
1314 1221
1315 1222
1316 1223
1317 1224
1318 1225
1319 1226
1320 1227
1321 1228
1322 1229
1323 1230
1324 1231
1325 1232
1326 1233
1327 1234
1328 1235
1329 1236
1330 1237
1331 1238
1332 1239
1333 1240
1334 1241
1335 1242
1336 1243
1337 1244
1338 1245
1339 1246
1340 1247
1341 1248
1342 1249
1343 1250
1344 1251
1345 1252
1346 1253
1347 1254
1348 1255
1349 1256
1350 1257
1351 1258
1352 1259
1353 1260
1354 1261
1355 1262
1356 1263
1357 1264
1358 1265
1359 1266
1360 1267
1361 1268
1362 1269
1363 1270
1364 1271
1365 1272
1366 1273
1367 1274
1368 1275
1369 1276
1370 1277
1371 1278
1372 1279
1373 1280
1374 1281
1375 1282
1376 1283
1377 1284
1378 1285
1379 1286
1380 1287
1381 1288
1382 1289
1383 1290
1384 1291
1385 1292
1386 1293
1387 1294
1388 1295
1389 1296
1390 1297
1391 1298
1392 1299
1393 1300
1394 1301
1395 1302
1396 1303
1397 1304
1398 1305
1399 1306
1400 1307
1401 1308
1402 1309
1403 1310
1404 1311
1405 1312
1406 1313
1407 1314
1408 1315
1409 1316
1410 1317
1411 1318
1412 1319
1413 1320
1414 1321
1415 1322
1416 1323
1417 1324
1418 1325
1419 1326
1420 1327
1421 1328
1422 1329
1423 1330
1424 1331
1425 1332
1426 1333
1427 1334
1428 1335
1429 1336
1430 1337
1431 1338
1432 1339
1433 1340
1434 1341
1435 1342
1436 1343
1437 1344
1438 1345
1439 1346
1440 1347
1441 1348
1442 1349
1443 1350
1444 1351
1445 1352
1446 1353
1447 1354
1448 1355
1449 1356
1450 1357
1451 1358
1452 1359
1453 1360
1454 1361
1455 1362
1456 1363
1457 1364
1458 1365
1459 1366
1460 1367
1461 1368
1462 1369
1463 1370
1464 1371
1465 1372
1466 1373
1467 1374
1468 1375
1469 1376
1470 1377
1471 1378
1472 1379
1473 1380
1474 1381
1475 1382
1476 1383
1477 1384
1478 1385
1479 1386
1480 1387
1481 1388
1482 1389
1483 1390
1484 1391
1485 1392
1486 1393
1487 1394
1488 1395
1489 1396
1490 1397
1491 1398
1492 1399
1493 1400
1494 1401
1495 1402
1496 1403
1497 1404
1498 1405
1499 1406
1500 1407
1501 1408
1502 1409
1503 1410
1504 1411
1505 1412
1506 1413
1507 1414
1508 1415
1509 1416
1510 1417
1511 1418
1512 1419
1513 1420
1514 1421
1515 1422
1516 1423
1517 1424
1518 1425
1519 1426
1520 1427
1521 1428
1522 1429
1523 1430
1524 1431
1525 1432
1526 1433
1527 1434
1528 1435
1529 1436
1530 1437
1531 1438
1532 1439
1533 1440
1534 1441
1535 1442
1536 1443
1537 1444
1538 1445
1539 1446
1540 1447
1541 1448
1542 1449
1543 1450
1544 1451
1545 1452
1546 1453
1547 1454
1548 1455
1549 1456
1550 1457
1551 1458
1552 1459
1553 1460
1554 1461
1555 1462
1556 1463
1557 1464
1558 1465
1559 1466
1560 1467
1561 1468
1562 1469
1563 1470
1564 1471
1565 1472
1566 1473
1567 1474
1568 1475
1569 1476
1570 1477
1571 1478
1572 1479
1573 1480
1574 1481
1575 1482
1576 1483
1577 1484
1578 1485
1579 1486
1580 1487
1581 1488
1582 1489
1583 1490
1584 1491
1585 1492
1586 1493
1587 1494
1588 1495
1589 1496
1590 1497
1591 1498
1592 1499
1593 1500
1594 1501
1595 1502
1596 1503
1597 1504
1598 1505
1599 1506
1600 1507
1601 1508
1602 1509
1603 1510
1604 1511
1605 1512
1606 1513
1607 1514
1608 1515
1609 1516
1610 1517
1611 1518
1612 1519
1613 1520
1614 1521
1615 1522
1616 1523
1617 1524
1618 1525
1619 1526
1620 1527
1621 1528
1622 1529
1623 1530
1624 1531
1625 1532
1626 1533
1627 1534
1628 1535
1629 1536
1630 1537
1631 1538
1632 1539
1633 1540
1634 1541
1635 1542
1636 1543
1637 1544
1638 1545
1639 1546
1640 1547
1641 1548
1642 1549
1643 1550
1644 1551
1645 1552
1646 1553
1647 1554
1648 1555
1649 1556
1650 1557
1651 1558
1652 1559
1653 1560
1654 1561
1655 1562
1656 1563
1657 1564
1658 1565
1659 1566
1660 1567
1661 1568
1662 1569
1663 1570
1664 1571
1665 1572
1666 1573
1667 1574
1668 1575
1669 1576
1670 1577
1671 1578
1672 
```

手游“硬伤”一：硬编码-99%

Address	Length	Type	String
.rodata:000...	00000041	C	1fcfcf823afccec9b5e45370496a5e3d89198ac3a
.rodata:000...	00000011	C	YsdADCKskKazKaMe
.rodata:000...	00000011	C	[GC@MajyuJiROU].
.rodata:000...	00000011	C	aDb-lh8l-PHk!Z9l
.rodata:000...	00000011	C	[__LazarUS__730]

so字符串中的Key



```
1 #coding=gbk
2 import os, sys, struct, binascii, urllib, threading, gzip,
3 from packetfilter import LogInfo, evtLog
4
5 import xml.dom.minidom as xdm
6 from pyaes import *
7
8 evtLog.log("load gcfilter ...")
9
10 class FILTER:
11     def __init__(self):
12         i_sendkey = "&lRrrN9/m372K.}"
13         i_recvkey = "XR<!OMO_)u-Z]u?5"
14         a_sendkey = "[__LazarUS__730]"
15         a_recvkey = "YsdADCKskKazKaMe"
16
17         self.keys = {
18             'iOS': {'S': i_sendkey,
19                     'R': i_recvkey,
20                     'And': '...', 'key': '...'}
```



安全增强  
测试

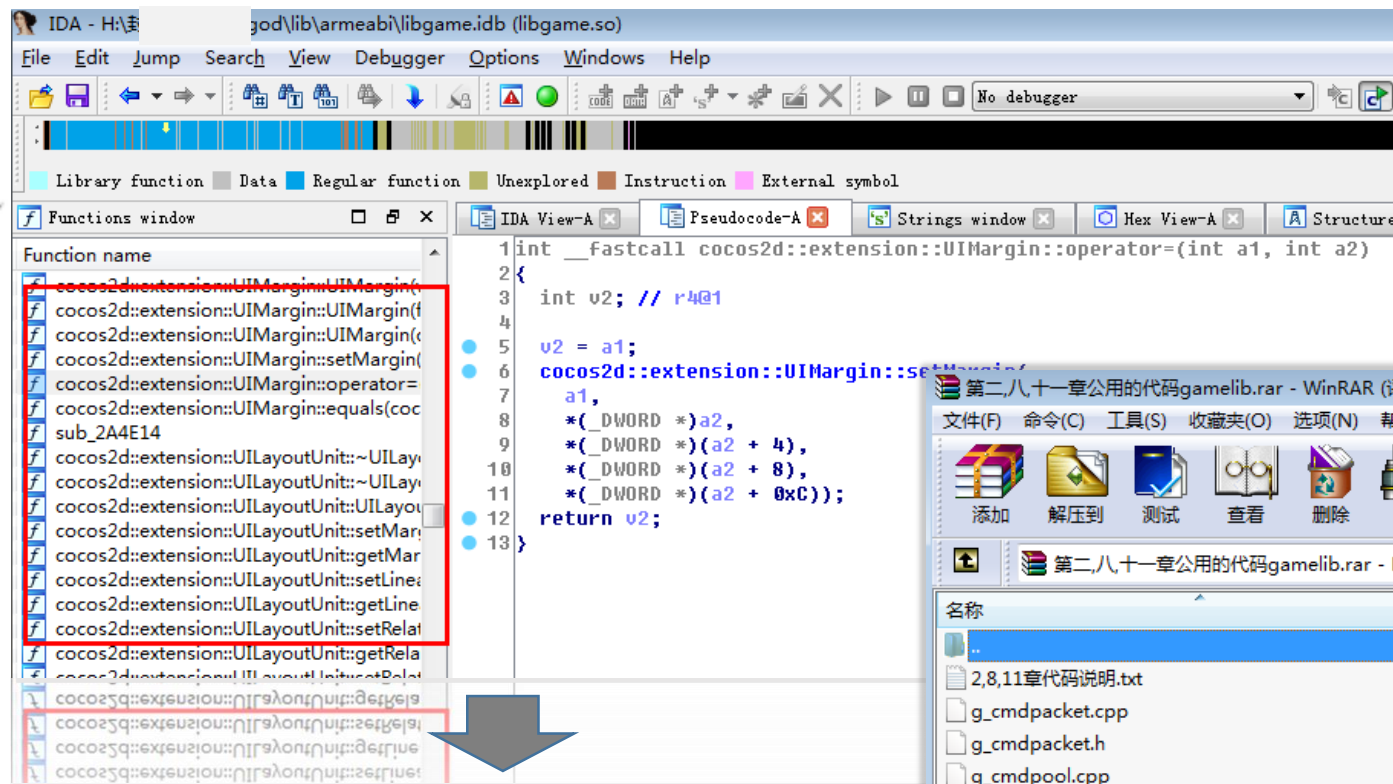
找回密码功能测试	不安全	高
账号登陆功能测试	不安全	高
修改游戏金钱测试	不安全	高
修改狩猎卷数量测试	不安全	高
修改斗兽场卷数量使用测试	不安全	高
修改角色经验等级测试	不安全	中
修改狩猎时间等限制测试	不安全	高
修改斗兽场不败测试	不安全	高
修改好友点数消耗测试	不安全	高
修改魔物强化测试	不安全	高
修改本地魔石数量和卡牌属性测试	不安全	高
修改本地魔石测试	不安全	低

```
3203 [5176] <message>0</message>
3203 [5176] <friend>0</friend>
3203 [5176] <trade>0</trade>
3203 [5176] <gift>1</gift>
3203 [5176] <send_message>30</send_message>
3203 [5176] <send_friend>0</send_friend>
3203 [5176] <send_trade>1</send_trade>
3203 [5176] <send_gift>30</send_gift>
3203 [5176] <battle>10</battle>
3203 [5176] <free_hunt>0</free_hunt>
3203 [5176] <point>0</point>
3203 [5176] <free_point>0</free_point>
3203 [5176] <hush_check>1</hush_check>
3203 [5176] <friend_point>90</friend_point>
3203 [5176] <guardian_r...t>0</...dian...t>
```

# 手游“硬伤”一：硬编码-99%

当我们再也找不到Key、  
看不懂什么加密时...

Google注释、特殊函数名



cocos2d::extension::UIMargin

网页

图片

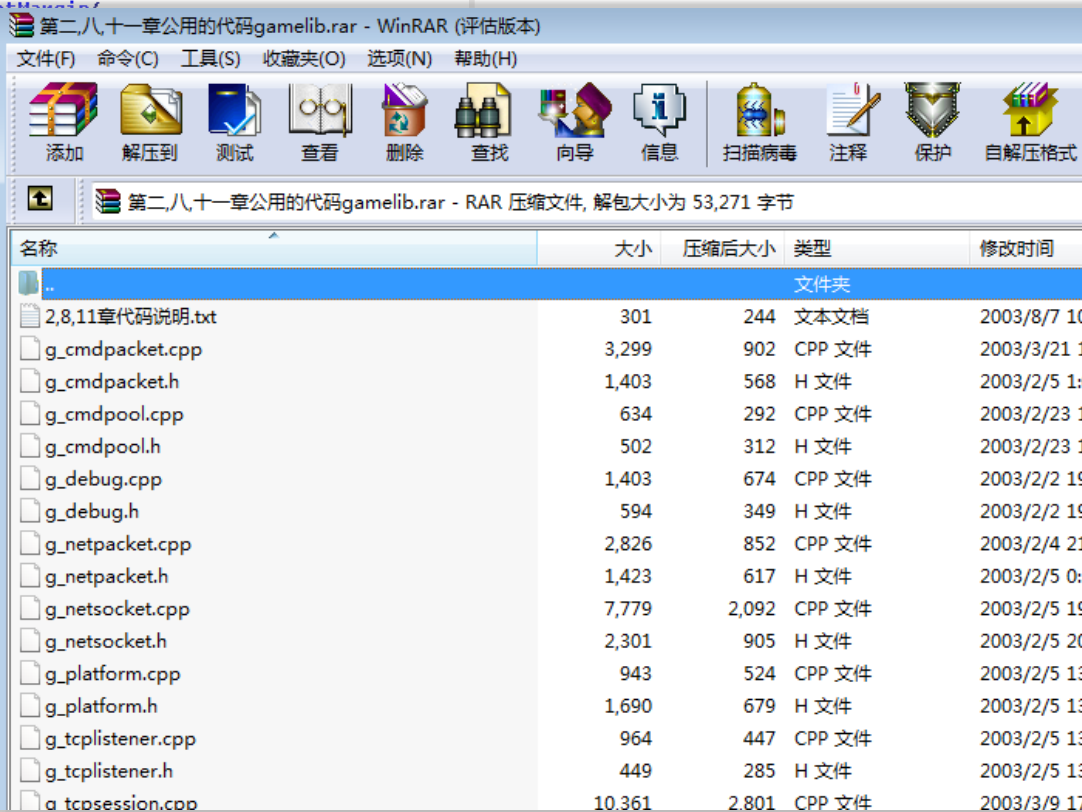
地图

视频

更多

搜索

找到约 34 条结果 (用时 0.17 秒)



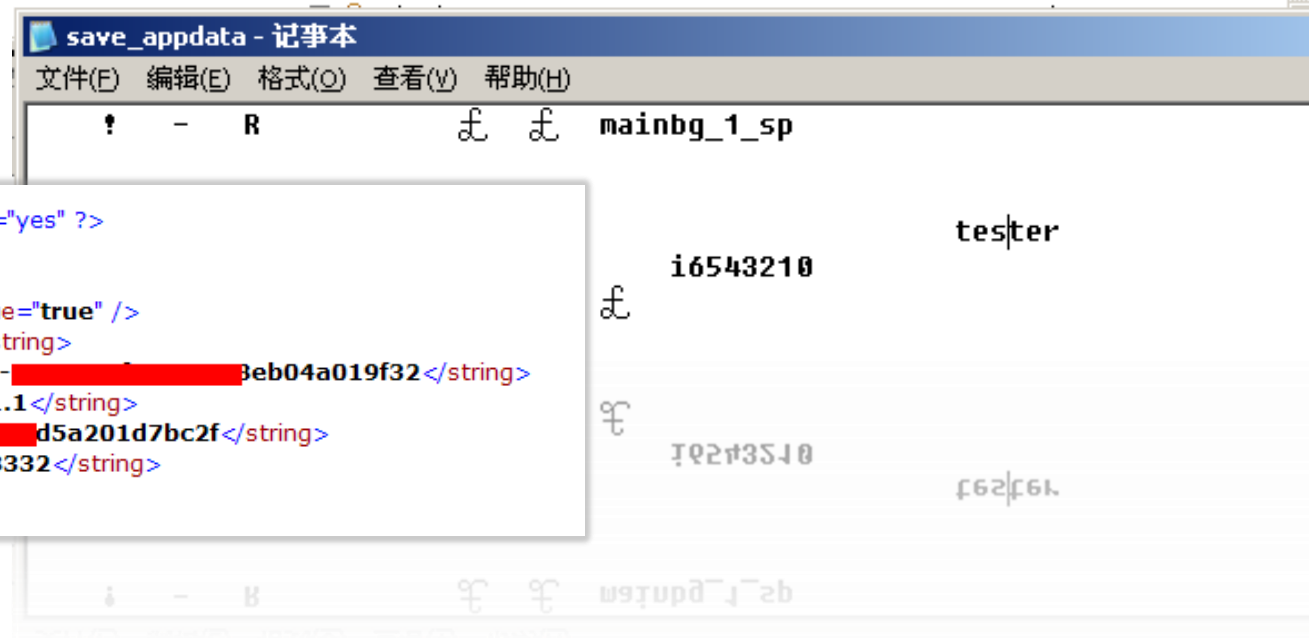


## 硬伤二：logcat、token存储-80%

账号密码输出、存储在  
**logcat**、xml、db、甚至SD card

token不过期、替换可登陆

mnt		2013-05-24	05:34	drwxrwxr-x
+ asec		2013-05-24	05:46	drwxr-xr-x
+ obb		2013-05-24	05:34	drwxr-xr-x
sdcard		2013-05-25	03:37	d---rwxr-x
Android		2013-05-24	05:48	d---rwxr-x
data		2013-05-24	05:48	d---rwxr-x
com.square_enix.million_cn		2013-05-24	05:48	d---rwxr-x
files		2013-05-24	05:48	d---rwxr-x
save		2013-05-24	05:48	d---rwxr-x
appdata		2013-05-24	06:01	d---rwxr-x
save_appdata	433	2013-05-24	11:38	----rwxr-x
save_version	2016	2013-05-24	06:37	----rwxr-x



# 硬伤三：服务端缺陷-50%

1、服务端对客户端的无厘头信任  
告诉你我有多少钱、多少牌、多少经验、我在哪里

2、WebService：API泄露、后台泄露、短信接口、统计数据、SQL注入、XSS、列目录...

3、人的问题



## 漏洞概要

缺陷编号：WooYun-2013-36826

Hush Framework  
hush framework sandbox

测试菜单

测试应用

系统管理	常用流程
测试接口调试	
AccountPage	
AccountPage -> statusAction	账号接口/验证账号
AccountPage -> codeverifyAction	账号接口/验证短信验
AccountPage -> registerAction	账号接口/注册并登录
AccountPage -> loginAction	账号接口/登录
AccountPage -> loginautoAction	账号接口/自动登录
AccountPage -> resetpasswdAction	账号接口/修改密码
AccountPage -> activeAction	账号接口/激活
AccountPage -> bindAction	账号接口/盛大通行证
AccountPage -> logoutAction	账号接口/登出账号
AccountPage -> sndastatusAction	账号接口/盛大通行证
AccountPage -> activatecheckAction	账号接口/用户激活码
AccountPage -> sendcaptchaAction	账号接口/注册验证码



## 硬伤四：内存修改-?%

在**网游**中鲜有案例...

(image display error)



多种修改方法....

移动业务的安全建设？

效仿Web安全建设

一、开发安全规范、安全测试指南

《OWASP Top 10 Mobile Risks》、  
《OWASP Mobile Threat Model》 ...

二、安全培训

测什么、怎么测、怎么写、什么问题

三、测试融入流程

引进前、对外前所有版本

四、平台、定制脚本的实现

Apk静态分析平台（检查混淆等）及  
相关测试脚本

ost:62745/analyse.aspx?sha1=5dcdbb8478affdc0d764e9ba21b1bb80b1a01eb1

文件名称: FruitNinja.apk  
SHA1: 5dcdbb8478affdc0d764e9ba21b1bb80b1a01eb1

文件大小: 26.44 MB  
上传时间: 2013/10/29 15:42:03 +08:00

基本信息

文件大小: 26.44 MB  
SHA1: 5dcdbb8478affdc0d764e9ba21b1bb80b1a01eb1  
MD5: 8526782485b7d41d70387c0ed910df14  
版本: 1.7.8  
上传时间: 2013/10/29 15:42:03 +08:00  
应用名称: 水果忍者

反编译

是否混淆: 至少有一部分源代码没有混淆

签名

是否签名: 是  
证书信息: CN=Huawei, OU=Company, O=Huawei, L=shenzhen, S=China, C=086  
颁发机构: CN=Huawei, OU=Company, O=Huawei, L=shenzhen, S=China, C=086

权限

安装应用程序

android.permission.INSTALL\_PACKAGES  

发送短信

android.permission.SEND\_SMS  

获取精确位置

android.permission.ACCESS\_FINE\_LOCATION  
访问网络 android.permission.INTERNET  
获取网络状态 android.permission.ACCESS\_NETWORK\_STATE  
写入外部存储 android.permission.WRITE\_EXTERNAL\_STORAGE  
读取电话状态 android.permission.READ\_PHONE\_STATE  
获取Wifi状态 android.permission.ACCESS\_WIFI\_STATE  
显示系统窗口 android.permission.SYSTEM\_ALERT\_WINDOW  
获取任务信息 android.permission.GET\_TASKS  
获取粗略位置 android.permission.ACCESS\_COARSE\_LOCATION  
改变配置 android.permission.CHANGE\_CONFIGURATION  
未知权限 android.permission.READ\_EXTERNAL\_STORAGE



# Thanks

---

Q&A