

# Lab8. Native Code Reversing

STU ID: 20307130044

Your Flag: FLAG{29868659734356183824165126738494685273254614315275839}

## Analysis Process Breakdown:

首先 jeb 反编译一下, 没什么东西, 这里就不放截图了, 就是有一个 native 函数, 如果真就是 right, 如果假就是 wrong, 主要去看 native 里面的, 用 ida 反编译一下

这是第一部分

```
if ( (*env)->GetStringUTFLength(env, a3) == 59 )
{
    v3 = (*env)->GetStringUTFChars(env, a3, 0);
    if ( *v3 == 70 && v3[1] == 76 && v3[2] == 65 && v3[3] == 71 && v3[4] == 123 && v3[58] == 125 )
    {
        v4 = -53;
        while ( (unsigned __int8)(v3[v4 + 58] - 48) <= 9u )
        {
```

前两个判断表出了格式是 FLAG{xxxx}, 其中中间有 53 个 ascii 码小于等于 9 的字符, 这时候大概能猜到是一串数字了 (因为连下划线都不在范围内, 前面只有一些零散符号)

然后看下面一段, 用 x86 在 32 位里反编译的真的很怪, 感觉 dest 和最后的 mubiao 好像没关系, mubiao 基本没改过呢?

```
if ( !v4 )
{
    v19 = 0LL;
    v18 = 0LL;
    v17 = 0LL;
    *(_OWORD *)dest = 0LL;
    strncpy(dest, v3 + 5, 53u);
    v13 = 0LL;
    v12 = 0LL;
    v11 = 0LL;
    v10 = 0LL;
    *(_OWORD *)mubiao = 0LL;
    v14 = 0;
    v5 = 0;
    v6 = -81;
    do
    {
        v8 = *((_BYTE *)&ccc + v6 + 81);
        if ( !v8 )
            v8 = dest[v5++] - 48;
        v11[v6++] = v8;
    }
    while ( v6 );
    return bbb(mubiao);
}
```

也是我运气好, 想着换一个版本 x86-64 的反编译看看呢? 这里就看懂了

```
/* v11, v12, v13, v14, v15, v16, v17, v18, v19, v20, v21, v22, v23, v24, v25, v26, v27, v28, v29, v30, v31, v32, v33, v34, v35, v36, v37, v38, v39, v40, v41, v42, v43, v44, v45, v46, v47, v48, v49, v50, v51, v52, v53, v54, v55, v56, v57, v58, v59, v60, v61, v62, v63, v64, v65, v66, v67, v68, v69, v70, v71, v72, v73, v74, v75, v76, v77, v78, v79, v80, v81, v82, v83, v84, v85, v86, v87, v88, v89, v90, v91, v92, v93, v94, v95, v96, v97, v98, v99, v100, v101, v102, v103, v104, v105, v106, v107, v108, v109, v110, v111, v112, v113, v114, v115, v116, v117, v118, v119, v120, v121, v122, v123, v124, v125, v126, v127, v128, v129, v130, v131, v132, v133, v134, v135, v136, v137, v138, v139, v140, v141, v142, v143, v144, v145, v146, v147, v148, v149, v150, v151, v152, v153, v154, v155, v156, v157, v158, v159, v160, v161, v162, v163, v164, v165, v166, v167, v168, v169, v170, v171, v172, v173, v174, v175, v176, v177, v178, v179, v180, v181, v182, v183, v184, v185, v186, v187, v188, v189, v190, v191, v192, v193, v194, v195, v196, v197, v198, v199, v200, v201, v202, v203, v204, v205, v206, v207, v208, v209, v210, v211, v212, v213, v214, v215, v216, v217, v218, v219, v220, v221, v222, v223, v224, v225, v226, v227, v228, v229, v230, v231, v232, v233, v234, v235, v236, v237, v238, v239, v240, v241, v242, v243, v244, v245, v246, v247, v248, v249, v250, v251, v252, v253, v254, v255, v256, v257, v258, v259, v260, v261, v262, v263, v264, v265, v266, v267, v268, v269, v270, v271, v272, v273, v274, v275, v276, v277, v278, v279, v280, v281, v282, v283, v284, v285, v286, v287, v288, v289, v290, v291, v292, v293, v294, v295, v296, v297, v298, v299, v300, v301, v302, v303, v304, v305, v306, v307, v308, v309, v310, v311, v312, v313, v314, v315, v316, v317, v318, v319, v320, v321, v322, v323, v324, v325, v326, v327, v328, v329, v330, v331, v332, v333, v334, v335, v336, v337, v338, v339, v340, v341, v342, v343, v344, v345, v346, v347, v348, v349, v350, v351, v352, v353, v354, v355, v356, v357, v358, v359, v360, v361, v362, v363, v364, v365, v366, v367, v368, v369, v370, v371, v372, v373, v374, v375, v376, v377, v378, v379, v380, v381, v382, v383, v384, v385, v386, v387, v388, v389, v390, v391, v392, v393, v394, v395, v396, v397, v398, v399, v400, v401, v402, v403, v404, v405, v406, v407, v408, v409, v410, v411, v412, v413, v414, v415, v416, v417, v418, v419, v420, v421, v422, v423, v424, v425, v426, v427, v428, v429, v430, v431, v432, v433, v434, v435, v436, v437, v438, v439, v440, v441, v442, v443, v444, v445, v446, v447, v448, v449, v450, v451, v452, v453, v454, v455, v456, v457, v458, v459, v460, v461, v462, v463, v464, v465, v466, v467, v468, v469, v470, v471, v472, v473, v474, v475, v476, v477, v478, v479, v480, v481, v482, v483, v484, v485, v486, v487, v488, v489, v490, v491, v492, v493, v494, v495, v496, v497, v498, v499, v500, v501, v502, v503, v504, v505, v506, v507, v508, v509, v510, v511, v512, v513, v514, v515, v516, v517, v518, v519, v520, v521, v522, v523, v524, v525, v526, v527, v528, v529, v530, v531, v532, v533, v534, v535, v536, v537, v538, v539, v540, v541, v542, v543, v544, v545, v546, v547, v548, v549, v550, v551, v552, v553, v554, v555, v556, v557, v558, v559, v560, v561, v562, v563, v564, v565, v566, v567, v568, v569, v570, v571, v572, v573, v574, v575, v576, v577, v578, v579, v580, v581, v582, v583, v584, v585, v586, v587, v588, v589, v590, v591, v592, v593, v594, v595, v596, v597, v598, v599, v600, v601, v602, v603, v604, v605, v606, v607, v608, v609, v610, v611, v612, v613, v614, v615, v616, v617, v618, v619, v620, v621, v622, v623, v624, v625, v626, v627, v628, v629, v630, v631, v632, v633, v634, v635, v636, v637, v638, v639, v640, v641, v642, v643, v644, v645, v646, v647, v648, v649, v650, v651, v652, v653, v654, v655, v656, v657, v658, v659, v660, v661, v662, v663, v664, v665, v666, v667, v668, v669, v670, v671, v672, v673, v674, v675, v676, v677, v678, v679, v680, v681, v682, v683, v684, v685, v686, v687, v688, v689, v690, v691, v692, v693, v694, v695, v696, v697, v698, v699, v700, v701, v702, v703, v704, v705, v706, v707, v708, v709, v710, v711, v712, v713, v714, v715, v716, v717, v718, v719, v720, v721, v722, v723, v724, v725, v726, v727, v728, v729, v730, v731, v732, v733, v734, v735, v736, v737, v738, v739, v740, v741, v742, v743, v744, v745, v746, v747, v748, v749, v750, v751, v752, v753, v754, v755, v756, v757, v758, v759, v760, v761, v762, v763, v764, v765, v766, v767, v768, v769, v770, v771, v772, v773, v774, v775, v776, v777, v778, v779, v780, v781, v782, v783, v784, v785, v786, v787, v788, v789, v790, v791, v792, v793, v794, v795, v796, v797, v798, v799, v800, v801, v802, v803, v804, v805, v806, v807, v808, v809, v810, v811, v812, v813, v814, v815, v816, v817, v818, v819, v820, v821, v822, v823, v824, v825, v826, v827, v828, v829, v830, v831, v832, v833, v834, v835, v836, v837, v838, v839, v840, v841, v842, v843, v844, v845, v846, v847, v848, v849, v850, v851, v852, v853, v854, v855, v856, v857, v858, v859, v860, v861, v862, v863, v864, v865, v866, v867, v868, v869, v870, v871, v872, v873, v874, v875, v876, v877, v878, v879, v880, v881, v882, v883, v884, v885, v886, v887, v888, v889, v890, v891, v892, v893, v894, v895, v896, v897, v898, v899, v900, v901, v902, v903, v904, v905, v906, v907, v908, v909, v910, v911, v912, v913, v914, v915, v916, v917, v918, v919, v920, v921, v922, v923, v924, v925, v926, v927, v928, v929, v930, v931, v932, v933, v934, v935, v936, v937, v938, v939, v940, v941, v942, v943, v944, v945, v946, v947, v948, v949, v950, v951, v952, v953, v954, v955, v956, v957, v958, v959, v960, v961, v962, v963, v964, v965, v966, v967, v968, v969, v970, v971, v972, v973, v974, v975, v976, v977, v978, v979, v980, v981, v982, v983, v984, v985, v986, v987, v988, v989, v990, v991, v992, v993, v994, v995, v996, v997, v998, v999, v1000, v1001, v1002, v1003, v1004, v1005, v1006, v1007, v1008, v1009, v1010, v1011, v1012, v1013, v1014, v1015, v1016, v1017, v1018, v1019, v1020, v1021, v1022, v1023, v1024, v1025, v1026, v1027, v1028, v1029, v1030, v1031, v1032, v1033, v1034, v1035, v1036, v1037, v1038, v1039, v1040, v1041, v1042, v1043, v1044, v1045, v1046, v1047, v1048, v1049, v1050, v1051, v1052, v1053, v1054, v1055, v1056, v1057, v1058, v1059, v1060, v1061, v1062, v1063, v1064, v1065, v1066, v1067, v1068, v1069, v1070, v1071, v1072, v1073, v1074, v1075, v1076, v1077, v1078, v1079, v1080, v1081, v1082, v1083, v1084, v1085, v1086, v1087, v1088, v1089, v1090, v1091, v1092, v1093, v1094, v1095, v1096, v1097, v1098, v1099, v1100, v1101, v1102, v1103, v1104, v1105, v1106, v1107, v1108, v1109, v1110, v1111, v1112, v1113, v1114, v1115, v1116, v1117, v1118, v1119, v1120, v1121, v1122, v1123, v1124, v1125, v1126, v1127, v1128, v1129, v1130, v1131, v1132, v1133, v1134, v1135, v1136, v1137, v1138, v1139, v1140, v1141, v1142, v1143, v1144, v1145, v1146, v1147, v1148, v1149, v1150, v1151, v1152, v1153, v1154, v1155, v1156, v1157, v1158, v1159, v1160, v1161, v1162, v1163, v1164, v1165, v1166, v1167, v1168, v1169, v1170, v1171, v1172, v1173, v1174, v1175, v1176, v1177, v1178, v1179, v1180, v1181, v1182, v1183, v1184, v1185, v1186, v1187, v1188, v1189, v1190, v1191, v1192, v1193, v1194, v1195, v1196, v1197, v1198, v1199, v1200, v1201, v1202, v1203, v1204, v1205, v1206, v1207, v1208, v1209, v1210, v1211, v1212, v1213, v1214, v1215, v1216, v1217, v1218, v1219, v1220, v1221, v1222, v1223, v1224, v1225, v1226, v1227, v1228, v1229, v1230, v1231, v1232, v1233, v1234, v1235, v1236, v1237, v1238, v1239, v1240, v1241, v1242, v1243, v1244, v1245, v1246, v1247, v1248, v1249, v1250, v1251, v1252, v1253, v1254, v1255, v1256, v1257, v1258, v1259, v1260, v1261, v1262, v1263, v1264, v1265, v1266, v1267, v1268, v1269, v1270, v1271, v1272, v1273, v1274, v1275, v1276, v1277, v1278, v1279, v1280, v1281, v1282, v1283, v1284, v1285, v1286, v1287, v1288, v1289, v1290, v1291, v1292, v1293, v1294, v1295, v1296, v1297, v1298, v1299, v1300, v1301, v1302, v1303, v1304, v1305, v1306, v1307, v1308, v1309, v1310, v1311, v1312, v1313, v1314, v1315, v1316, v1317, v1318, v1319, v1320, v1321, v1322, v1323, v1324, v1325, v1326, v1327, v1328, v1329, v1330, v1331, v1332, v1333, v1334, v1335, v1336, v1337, v1338, v1339, v1340, v1341, v1342, v1343, v1344, v1345, v1346, v1347, v1348, v1349, v1350, v1351, v1352, v1353, v1354, v1355, v1356, v1357, v1358, v1359, v1360, v1361, v1362, v1363, v1364, v1365, v1366, v1367, v1368, v1369, v1370, v1371, v1372, v1373, v1374, v1375, v1376, v1377, v1378, v1379, v1380, v1381, v1382, v1383, v1384, v1385, v1386, v1387, v1388, v1389, v1390, v1391, v1392, v1393, v1394, v1395, v1396, v1397, v1398, v1399, v1400, v1401, v1402, v1403, v1404, v1405, v1406, v1407, v1408, v1409, v1410, v1411, v1412, v1413, v1414, v1415, v1416, v1417, v1418, v1419, v1420, v1421, v1422, v1423, v1424, v1425, v1426, v1427, v1428, v1429, v1430, v1431, v1432, v1433, v1434, v1435, v1436, v1437, v1438, v1439, v1440, v1441, v1442, v1443, v1444, v1445, v1446, v1447, v1448, v1449, v1450, v1451, v1452, v1453, v1454, v1455, v1456, v1457, v1458, v1459, v1460, v1461, v1462, v1463, v1464, v1465, v1466, v1467, v1468, v1469, v1470, v1471, v1472, v1473, v1474, v1475, v1476, v1477, v1478, v1479, v1480, v1481, v1482, v1483, v1484, v1485, v1486, v1487, v1488, v1489, v1490, v1491, v1492, v1493, v1494, v1495, v1496, v1497, v1498, v1499, v1500, v1501, v1502, v1503, v1504, v1505, v1506, v1507, v1508, v1509, v1510, v1511, v1512, v1513, v1514, v1515, v1516, v1517, v1518, v1519, v1520, v1521, v1522, v1523, v1524, v1525, v1526, v1527, v1528, v1529, v1530, v1531, v1532, v1533, v1534, v1535, v1536, v1537, v1538, v1539, v1540, v1541, v1542, v1543, v1544, v1545, v1546, v1547, v1548, v1549, v1550, v1551, v1552, v1553, v1554, v1555, v1556, v1557, v1558, v1559, v1560, v1561, v1562, v1563, v1564, v1565, v1566, v1567, v1568, v1569, v1570, v1571, v1572, v1573, v1574, v1575, v1576, v1577, v1578, v1579, v1580, v1581, v1582, v1583, v1584, v1585, v1586, v1587, v1588, v1589, v1590, v1591, v1592, v1593, v1594, v1595, v1596, v1597, v1598, v1599, v1600, v1601, v1602, v1603, v1604, v1605, v1606, v1607, v1608, v1609, v1610, v1611, v1612, v1613, v1614, v1615, v1616, v1617, v1618, v1619, v1620, v1621, v1622, v1623, v1624, v1625, v1626, v1627, v1628, v1629, v1630, v1631, v1632, v1633, v1634, v1635, v1636, v1637, v1638, v1639, v1640, v1641, v1642, v1643, v1644, v1645, v1646, v1647, v1648, v1649, v1650, v1651, v1652, v1653, v1654, v1655, v1656, v1657, v1658, v1659, v1660, v1661, v1662, v1663, v1664, v1665, v1666, v1667, v1668, v1669, v1670, v1671, v1672, v1673, v1674, v1675, v1676, v1677, v1678, v1679, v1680, v1681, v1682, v1683, v1684, v1685, v1686, v1687, v1688, v1689, v1690, v1691, v1692, v1693, v1694, v1695, v1696, v1697, v1698, v1699, v1700, v1701, v1702, v1703, v1704, v1705, v1706, v1707, v1708, v1709, v1710, v1711, v1712, v1713, v1714, v1715, v1716, v1717, v1718, v1719, v1720, v1721, v1722, v1723, v1724, v1725, v1726, v1727, v1728, v1729, v1730, v1731, v1732, v1733, v1734, v1735, v1736, v1737, v1738, v1739, v1740, v1741, v1742, v1743, v1744, v1745, v1746, v1747, v1748, v1749, v1750, v1751, v1752, v1753, v1754, v1755, v1756, v1757, v1758, v1759, v1760, v1761, v1762, v1763, v1764, v1765, v1766, v1767, v1768, v1769, v1770, v1771, v1772, v1773, v1774, v1775, v1776, v1777, v1778, v1779, v1780, v1781, v1782, v1783, v1784, v1785, v1786, v1787, v1788, v1789, v1790, v1791, v1792, v1793, v1794, v1795, v1796, v1797, v1798, v1799, v1800, v1801, v1802, v1803, v1804, v1805, v1806, v1807, v1808, v1809, v1810, v1811, v1812, v1813, v1814, v1815, v1816, v1817, v1818, v1819, v1820, v1821, v1822, v1823, v1824, v1825, v1826, v1827, v1828, v1829, v1830, v1831, v1832, v1833, v1834, v1835, v1836, v1837, v1838, v1839, v1840, v1841, v1842, v1843, v1844, v1845, v1846, v1847, v1848, v1849, v1850, v1851, v1852, v1853, v1854, v1855, v1856, v1857, v1858, v1859, v1860, v1861, v1862, v1863, v1864, v1865, v1866, v1867, v1868, v1869, v1870, v1871, v1872, v1873, v1874, v1875, v1876, v1877, v1878, v1879, v1880, v1881, v1882, v1883, v1884, v1885, v1886, v1887, v1888, v1889, v1890, v1891, v1892, v1893, v1894, v1895, v1896, v1897, v1898, v1899, v1900, v1901, v1902, v1903, v1904, v1905, v1906, v1907, v1908, v1909, v1910, v1911, v1912, v1913, v1914, v1915, v1916, v1917, v1918, v1919, v1920, v1921, v1922, v1923, v1924, v1925, v1926, v1927, v1928, v1929, v1930, v1931, v1932, v1933, v1934, v1935, v1936, v1937, v1938, v1939, v1940, v1941, v1942, v1943, v1944, v1945, v1946, v1947, v1948, v1949, v1950, v1951, v1952, v1953, v1954, v1955, v1956, v1957, v1958, v1959, v1960, v1961, v1962, v1963, v1964, v1965, v1966, v1967, v1968, v1969, v1970, v1971, v1972, v1973, v1974, v1975, v1976, v1977, v1978, v1979, v1980, v1981, v1982, v1983, v1984, v1985, v1986, v1987, v1988, v1989, v1990, v1991, v1992, v1993, v1994, v1995, v1996, v1997, v1998, v1999, v2000, v2001, v2002, v2003, v2004, v2005, v2006, v2007, v2008, v2009, v2010, v2011, v2012, v2013, v2014, v2015, v2016, v2017, v2018, v2019, v2020, v2021, v2022, v2023, v2024, v2025, v2026, v2027, v2028, v2029, v2030, v2031, v2032, v2033, v2034, v2035, v2036, v2037, v2038, v2039, v2040, v2041, v2042, v2043, v2044, v2045, v2046, v2047, v2048, v2049, v2050, v2051, v2052, v2053, v2054, v2055, v2056, v2057, v2058, v2059, v2060, v2061, v2062, v2063, v2064, v2065, v2066, v2067, v2068, v2069, v2070, v2071, v2072, v2073, v2074, v2075, v
```

首先，有一个常量 ccc，点进去能看到，是一个 81 元素长的数组

.data:00002000	public ccc	
.data:00002000 ccc	db 0	; DATA XREF: LOAD:00000
.data:00002000		; .got:ccc_ptr↑o
.data:00002001	db 0	
.data:00002002	db 1	
.data:00002003	db 4	
.data:00002004	db 3	
.data:00002005	db 0	
.data:00002006	db 7	
.data:00002007	db 5	
.data:00002008	db 0	
.data:00002009	db 0	
.data:0000200A	db 0	
.data:0000200B	db 0	
.data:0000200C	db 0	
.data:0000200D	db 1	
.data:0000200E	db 0	
.data:0000200F	db 0	
.data:00002010	db 4	
.data:00002011	db 2	
.data:00002012	db 0	
.data:00002013	db 7	
.data:00002014	db 0	
.data:00002015	db 0	
.data:00002016	db 0	

这段代码不断拷贝数据，分别从 ccc 和 flag 里面拷贝数字，用 python 写一下更清楚一点

```
while True:
    v10 = ccc[j-1]
    if (v10 == 0):
        v10 = ord(dest[v8]) - 48
        v8 += 1
    mubiao.append(v10)
    if j == 81:
        break
    v11 = ccc[j]
    if (v11 == 0):
        v11 = ord(dest[v8]) - 48
        v8 += 1
    mubiao.append(v11)
    j +=2
```

然后就送到 bbb 函数了

转战 bbb 函数

这里的分析要用到存放的知识了，我把这一段画了一下：

```

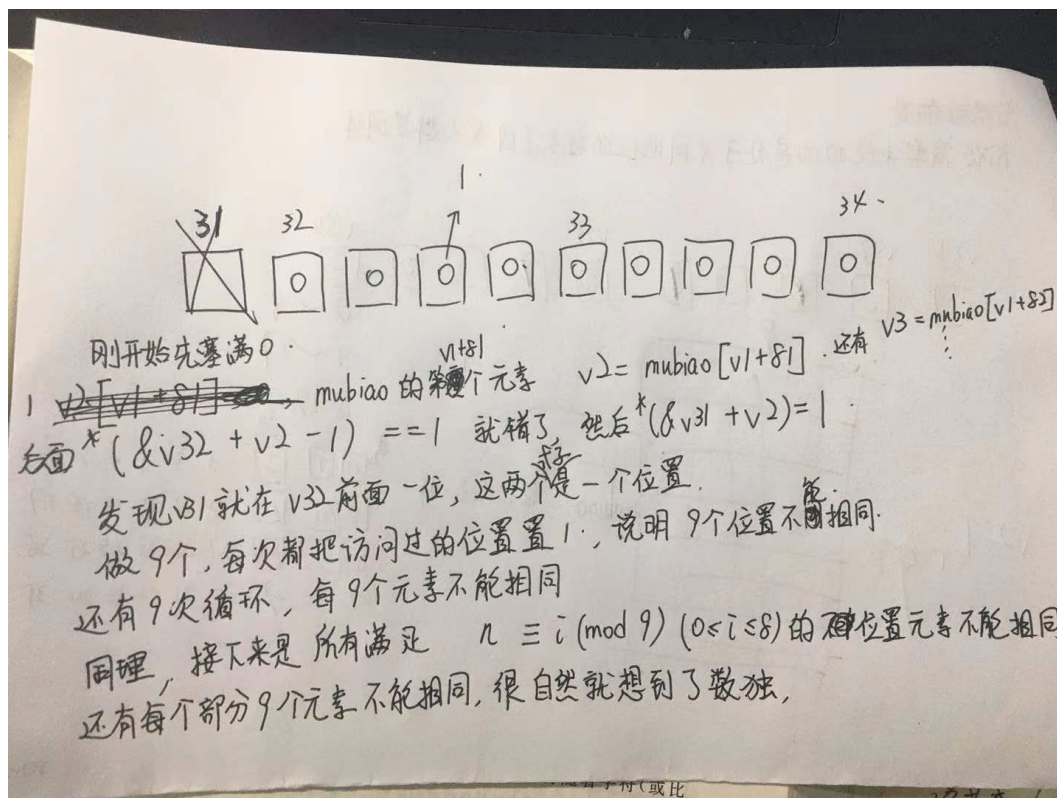
int result; // 00h
char v31; // [esp+8h] [ebp-21h]
int v32; // [esp+Ch] [ebp-20h] BYREF
int v33; // [esp+10h] [ebp-1Ch]
char v34; // [esp+14h] [ebp-18h]
unsigned int v35; // [esp+18h] [ebp-14h]

```

```

while ( 1 )
{
    v33 = 0;
    v32 = 0;
    v34 = 0;
    v2 = mubiao[v1 + 81];
    if ( *((_BYTE *)&v32 + v2 - 1) == 1 )
        return 0;
    *(&v31 + v2) = 1;
    v3 = mubiao[v1 + 82];
    if ( *((_BYTE *)&v32 + v3 - 1) == 1 )
        return 0;
    *(&v31 + v3) = 1;
    v4 = mubiao[v1 + 83];
    if ( *((_BYTE *)&v32 + v4 - 1) == 1 )
        return 0;
    *(&v31 + v4) = 1;
    v5 = mubiao[v1 + 84];
    if ( *((_BYTE *)&v32 + v5 - 1) == 1 )
        return 0;
    *(&v31 + v5) = 1;
    v6 = mubiao[v1 + 85];
    if ( *((_BYTE *)&v32 + v6 - 1) == 1 )
        return 0;
    *(&v31 + v6) = 1;
    v7 = mubiao[v1 + 86];
}

```



再回去看 ccc, 81 个元素, 有些有数字, 其余都是零, 太明显了就是数独, 然后找解数独的网站解了一下

## 数独求解器

		1	4	3		7	5	
				1			4	2
	7				2	9		
7					9			
	5						9	
			1					3
		9	7				8	
6	8			9				
	1	7		2	6	4		

## 数独求解器

2	9	1	4	3	8	7	5	6
8	6	5	9	1	7	3	4	2
4	7	3	5	6	2	9	1	8
7	3	8	2	4	9	1	6	5
1	5	2	6	7	3	8	9	4
9	4	6	1	8	5	2	7	3
3	2	9	7	5	4	6	8	1
6	8	4	3	9	1	5	2	7
5	1	7	8	2	6	4	3	9

把结果直接输入

## lab8\_task

FLAG{2986865973435618382416512  
6738494685273254614315275839}

CHECK

RIGHT!