

Jarvis OJ BASIC部分题目writeup

原创

dr0s3 于 2019-01-20 22:47:06 发布 1007 收藏 1

分类专栏: [其他](#) 文章标签: [Jarvis BASIC writeup](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/qq1045553189/article/details/86516990>

版权



[其他专栏收录该内容](#)

16 篇文章 0 订阅

订阅专栏

base64?

```
GUYDIMZVGQ2DMN3CGRQTONJXGM3TINLGG42DGMZXGM3TINLGGY4DGNBXYGTGNLGGY3DGNBWMU3WI===
```

base64后面最多可能出现两个=号, 只有base32可能出现3个等号

使用base32解码, 得到 `504354467b4a7573745f743373745f683476335f66346e7d`

猜测是hex编码的字符串, 使用hex解码得到FLAG

```
PCTF{Just_t3st_h4v3_f4n}
```

veryeasy

使用基本命令获取flag

使用strings命令, 输出所有可以显示的字符

```
[root@VM_0_7_centos /]# cd tmp
[root@VM_0_7_centos tmp]# ls
veryeasy.d944f0e9f8d5fe5b358930023da97d1a
[root@VM_0_7_centos tmp]# strings veryeasy.d944f0e9f8d5fe5b358930023da97d1a
__PAGEZERO
__TEXT
__text
__TEXT
__unwind_info
__TEXT
__DATA
__data
__DATA
__LINKEDIT
/usr/lib/dyld
/usr/lib/libSystem.B.dylib
PCTF{strings_is_3asy_isnt_17}
_mh_execute_header
$main
_mh_execute_header
main
dyld_stub_binder
[root@VM_0_7_centos tmp]#
```

<https://blog.csdn.net/qq1045553189>

strings命令

strings - print the strings of printable characters in files.

打印文件中可打印的字符。可以配合管道使用。

例如：

```
root@kali:~/Documents/tmp# strings t.py
from pwn import *
print asm('XCHG EAX,ESP\nRET\nMOV ECX,[EAX]\nMOV [EDX],ECX\nPOP EBX\nRET'.lower(
)).encode('hex').upper()
root@kali:~/Documents/tmp# strings t.py | grep from
from pwn import *
root@kali:~/Documents/tmp# strings * | grep from
<size from="%zu" t
o="%zu" total="%zu" count="%zu"/>
<unsorted from="%zu" to="%zu" total="%zu" count="%zu"/>
_nl_load_locale_from_archive
(%s from file %s)
failed to map segment from shared object
_dl_map_object_from_fd
base_from_object
base_from_cb_data
translit_from_idx
translit_from_tbl
_dl_map_object_from_fd
fromlimit
fromidx
froms
_nl_load_locale_from_archive
lit_from_idx
```

段子

请提交其中"锸斤拷"的十六进制编码。(大写)

查看"锸斤拷"的GBK编码

手贱

某天A君的网站被日，管理员密码被改，死活登不上，去数据库一看，啥，这密码md5不是和原来一样吗？为啥登不上咧？

d78b6f302l25cdc811adfe8d4e7c9fd34

请提交PCTF{原来的管理员密码}

md5128位，写成16进制是32个数，而不是33个数

将原来的md5减去一位（尝试每一位），使用md5解码，得到FLAG

美丽实验室logo

放到stegsolve里面浏览frame。拿到flag。

神秘的文件

使用wget命令下载

放到binwalk发现是可以挂载的文件

```
root@kali:~/tmp/mfile# binwalk haha.f38a74f55b4e193561d1b707211cf7eb
DECIMAL      HEXADECIMAL  DESCRIPTION
```

```

0          0x0          Linux EXT filesystem, rev 1.0, ext2 filesystem dat
a (mounted or unclean), UUID=8eecd08f-bae8-41ff-8497-8338f58af58a
35751     0x8BA7       mcrypt 2.2 encrypted data, algorithm: blowfish-448
, mode: CBC, keymode: 8bit
1058924   0x10286C      Unix path: /tmp/mfile/1/t.py
1573996   0x18046C      Unix path: /tmp/mfile/1/t.py
3146860   0x30046C      Unix path: /tmp/mfile/1/t.py

```

使用mount命令挂载

```

root@kali:/tmp/mfile# mkdir 1
root@kali:/tmp/mfile# cd 1
root@kali:/tmp/mfile/1# cd ..
root@kali:/tmp/mfile# mount haha.f38a74f55b4e193561d1b707211cf7eb ./1
root@kali:/tmp/mfile# cd 1
root@kali:/tmp/mfile/1# ls
0tools 113 129 144 16 175 190 205 220 236 251 39 54 7 85
1 114 13 145 160 176 191 206 221 237 252 4 55 70 86
10 115 130 146 161 177 192 207 222 238 253 40 56 71 87
100 116 131 147 162 178 193 208 223 239 26 41 57 72 88
101 117 132 148 163 179 194 209 224 24 27 42 58 73 89
102 118 133 149 164 18 195 21 225 240 28 43 59 74 9
103 119 134 15 165 180 196 210 226 241 29 44 6 75 90
104 12 135 150 166 181 197 211 227 242 3 45 60 76 91
105 120 136 151 167 182 198 212 228 243 30 46 61 77 92
106 121 137 152 168 183 199 213 229 244 31 47 62 78 93
107 122 138 153 169 184 2 214 23 245 32 48 63 79 94
108 123 139 154 17 185 20 215 230 246 33 49 64 8 95
109 124 14 155 170 186 200 216 231 247 34 5 65 80 96
11 125 140 156 171 187 201 217 232 248 35 50 66 81 97
110 126 141 157 172 188 202 218 233 249 36 51 67 82 98
111 127 142 158 173 189 203 219 234 25 37 52 68 83 99
112 128 143 159 174 19 204 22 235 250 38 53 69 84 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 1391 1392 1393 1394 1395 1396 1397 1398 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1690 1691 1692 1693 1694 1695 1696 1697 1698 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 2391 2392 2393 2394 2395 2396 2397 2398 2399 2400 2401 2402 2403 2404 2405 2406 2407 2408 2409 2410 2411 2412 2413 2414 2415 2416 2417 2418 2419 2420 2421 2422 2423 2424 2425 2426 2427 2428 2429 2430 2431 2432 2433 2434 2435 2436 2437 2438 2439 2440 2441 2442 2443 2444 2445 2446 2447 2448 2449 2450 2451 2452 2453 2454 2455 2456 2457 2458 2459 2460 2461 2462 2463 2464 2465 2466 2467 2468 2469 2470 2471 2472 2473 2474 2475 2476 2477 2478 2479 2480 2481 2482 2483 2484 2485 2486 2487 2488 2489 2490 2491 2492 2493 249
```

```
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         wifi.cap.      Linux EXT filesystem, rev 1.0, ext2 filesystem data, UUID=8eecd0
8f-bae8-41ff-8497-8338f58af58a
1160        0x48825bf0cc  Unix path: /root/Documents/tmp/1/2
35751      0x8BA72056ce  mcrypt 2.2 encrypted data, algorithm: blowfish-448, mode: CBC, k
eymode: 8bit
           8e

root@kali:~/Documents/tmp/1# ls
haha.f38a74f55b4e193561d1b707211cf7eb _haha.f38a74f55b4e193561d1b707211cf7eb.extracted
root@kali:~/Documents/tmp/1# cd _haha.f38a74f55b4e193561d1b707211cf7eb.extracted
root@kali:~/Documents/tmp/1/_haha.f38a74f55b4e193561d1b707211cf7eb.extracted# ls
0.ext  ext-root
root@kali:~/Documents/tmp/1/_haha.f38a74f55b4e193561d1b707211cf7eb.extracted# cd ext-root
root@kali:~/Documents/tmp/1/_haha.f38a74f55b4e193561d1b707211cf7eb.extracted/ext-root# ls
0      11  121 133 145 157 169 180 192 203 215 227 239 250 34 46 58 7 81 93
1      110 122 134 146 158 17 181 193 204 216 228 24 251 35 47 59 70 82 94
10     111 123 135 147 159 170 182 194 205 217 229 240 252 36 48 6 71 83 95
100    112 124 136 148 16 171 183 195 206 218 23 241 253 37 49 60 72 84 96
101    113 125 137 149 160 172 184 196 207 219 230 242 26 38 5 61 73 85 97
```

binwalk

做misc题的时候，一般都需要从某个网址下载一个文件，然后开始分析这个文件，最终从文件中得到flag。而查看下载的文件中是否包含其他文件的时候一般都需要binwalk这个神器。

[binwalk参考](#)

公倍数

t.py

```
1 sum = 0
2 for i in range(1000000000):
3     if (i%3==0 or i%5==0):
4         sum += i
5
6 print(sum)
7
```

Python - t.py:2 ✓

```
233333333166666668
[Finished in 108.1s]
233333333166666668
[Finished in 166.493s]
```

<https://blog.csdn.net/qq1045553189>

veryeasyRSA

```
import libnum
```

```
p = 3487583947589437589237958723892346254777
```

```
q = 8767867843568934765983476584376578389
```

```
e = 65537
```

```
phin = (p - 1) * (q - 1)
```

```
d = libnum.invmod(e, phin)
```

```
print(d)
```

```
# d=19178568796155560423675975774142829153827883709027717723363077606260717434369
```

[kali安装gmpy2教程](#)

Easy RSA

```
import libnum

c = 0xdc2eeeb2782c
n = 322831561921859
e = 23
q = 13574881
p = 23781539

d = libnum.invmod(e, (p - 1) * (q - 1))
m = pow(c, d, n)
print(libnum.n2s(m))
```

爱吃培根的出题人

密文:

```
bacon is one of aMerICA'S sWEethEartS. it's A dARlinG, SuCCulEnt fOoD tHAT PaIRs FlawLE
```

去掉无关符号:

```
baconisoneofaMerICaSsWEethEartSitsAdARlinGSuCCulEntfOoDtHATPaIRsFlawLE
```

大小写分别代表b和a:

```
aaaabaaaaaaaaabaabbababbbaabaabaabaabbbaabbbaabaabaababbababbababbbaabb
```

按照第二种方式解密得: baconisnotfood

取证

百度“内存取证”，即volatility

熟悉的声音

只有X、Y空格三种字符，猜测是摩斯密码

```
XYYY YXXX XYXX XXY XYY X XYY YX YYXX
.-... -... .-... ..- .-... .-... -... -... .....
```

解密得 **JBLUWEWNZ**

交上去不对，凯撒一下，得到flag: **PHRACKCTF**

Help!!

使用010Editor打开压缩包word.zip，其中deFlags字段标记是否加密。当该字段为偶数时含义是未加密，当该字段是奇数时，含义是已加密。打开word.zip后发现该字段是09，将其修改为00，即可正常解压。

The screenshot shows the 010 Editor interface. The main window displays the hex editor view of word.zip. The deFlags field is highlighted in red, and its value is 09. The Inspector panel on the right shows the deFlags field with a value of 0. The Template Results - ZIP.bt table is also visible, showing the deFlags field with a value of 0.

Name	Value	Start	Size	Color	Comment
struct ZIPFILEHEADER	word.docx	0h	12DA5h	Fg: Bg:	
struct ZIPDIRENTRY di	word.docx	12DA6h	5Bh	Fg: Bg:	
char deSignature[4]	PK	12DA6h	4h	Fg: Bg:	
ushort deVersionMade	31	12DA6h	2h	Fg: Bg:	
ushort deVersionNeeded	20	12DA6h	2h	Fg: Bg:	
ushort deFlags	0	12DA6h	2h	Fg: Bg:	
enum COMPRES_DECOM	COMP_DEFLATE	12DA6h	2h	Fg: Bg:	
DOSTIME deFileTime	00:17:04	12DA6h	2h	Fg: Bg:	
DOSDATE deFileDate	04/27/2016	12DA6h	2h	Fg: Bg:	
uint deCRC	44CAE8F6h	12DA6h	4h	Fg: Bg:	
uint deCompressedSize	77182	12DA6h	4h	Fg: Bg:	
uint deUncompressedSize	83392	12DA6h	4h	Fg: Bg:	
ushort deFileNameLen	9	12DA6h	2h	Fg: Bg:	
ushort deExtraFieldLen	36	12DA6h	2h	Fg: Bg:	
ushort deFileCommentLen	0	12DA6h	2h	Fg: Bg:	
ushort deDiskNumber	0	12DA6h	2h	Fg: Bg:	
ushort deInternalAttr	0	12DA6h	2h	Fg: Bg:	
uint deExternalAttr	32	12DA6h	4h	Fg: Bg:	
uint deHeaderOffset	0	12DA6h	4h	Fg: Bg:	
char deFileName[9]	word.docx	12DA6h	9h	Fg: Bg:	
uchar deExtraField[36]		12DA6h	36h	Fg: Bg:	
struct ZIPENDLOCATOR		12DA00h	16h	Fg: Bg:	

解压后打开word.docx，并没有看到flag

但是发现word文件首为PK开头，那说明是就一个压缩文件包了，尝试将该word文档的后缀改为.zip，然后用解压缩软件居然能够正常解压缩。

在 word\media 目录下发现flag

参考：

Help!!

ZIP伪加密

ZIP文件头协议

Word文件格式分析

ROPGadget

```
from pwn import *
print asm('XCHG EAX,ESP\nRET\nMOV ECX,[EAX]\nMOV [EDX],ECX\nPOP EBX\nRET'.lower()).encode('hex').upper()
```

Kali安装pwntools

a piece of cake

quipquip传送门

解得：

the word robot can refer to both physical robots and virtual software agents, but the latter are usually referred to as bots. there is no consensus on which machines qualify as robots but there is general agreement among experts, and the public, that robots tend to do some or all of the following: accept electronic programming, process data or physical perceptions electronically, operate autonomously to some degree, move around, operate physical parts of itself or physical processes, sense and manipulate their environment, and exhibit intelligent behavior - especially behavior which mimics humans or other animals. flag is substitutepassisveryeasygotit. closely related to the concept of a robot is the field of synthetic biology, which studies entities whose nature is more comparable to beings than to machines.

容易猜到?是b

Shellcode

文件中都是可见字符串，可能是经过处理得shellcode。

```
int main(void)
{
    int x;
    char a[] = "PYIIIIIIIIIIIIII7QZjAXP0A0AKAAQ2AB2BB0BBABXP8ABuJIYIhkmKzyCDq414FQyBlrRWEahI1tLKT16Pnk1ftLnkPv
wlnkW6fhNkan5pNkgF6XPOR8T5HsCivaN19okQSP1KRlVd6DNk3ue1NkpTthRXuQ9znk2jEHLK1Ja0FaXkhcTtBink4t1KUQhmvQYotqo0ylnLMT
00SDEWZah0tMwqhG8kXteksLwTdh1e8aLKsja4uQ8kavLkDlrk1K0ZeL7qjKlKUTLKuQM8k9bdvDeL1qiSnR5XVIXT0yjENikrphNnrnVnh1BrzH
ooK0Yoyok93u7t0KCnyHzBBSnguLgTcbyx1NKOYoYoMYaUTHphRL2LupQQ0htsFRtn541x3E2Se5T26PyKK8QLTddJlIZFBvyoSeUTLIkrv0oKy8
ORpMmlk7G16DBrm8Soyoioyoaxr0qh0XwP1xu1Qw1upBbHrmrED3T34qiKOxQLTdeZ0yZCaxQmRxgPUp0hpnPn4srRe8BDSo2PT7axq0CWROpoph
SYpnSo04u83K72Peu70hBpCsqDpF4qHIMXpLQ429k98aEaJr1BF3Ca3bIozp01IPf0Yof5GxAA";

    asm("jmp %0;"
        : "=a"(x)
        : "0"(a));
}
```

运行即可得到flag

参考：

[171115 杂项-可见字符组成的Shellcode](#)

Shellcode

Shellcode实际上就是汇编对应的机器码

但是由于机器码大部分都是不可见字符，所以无法直接显示出来

本题直接给了大段的乱码可见字符串，再结合机器码不可见，首先就想到了Base64编码-它的出现就是为了将不可见字符全部转为可见字符嘛

然而解b64发现不仅长度不符合，而且在最后添上等号以后解出来的值转汇编也并没有意义

Alpha2这个工程是专门将Shellcode编码成可见字符串的（甚至仅有字母和数字）

.-字符串

摩斯解码即可得到flag

[摩斯电码转换器](#)

德军的密码

解压后得到两个文件，一个加密程序和一个flag加密得到的密文。将加密程序丢到IDA中，可以看到关键的加密代码如下：

```
00000C2B 53
31 LODWORD(v6) = fopen(*(_QWORD *)&argc, argv, "rb+", v19[1]);
32 v16 = v6;
33 if ( v6 )
34 {
35     LODWORD(v7) = fopen(*(_QWORD *)&argc, argv, "wb+", "tmp");
36     v15 = v7;
37     while ( feof(*(_QWORD *)&argc, argv, v8, v16) == 0 )
38     {
39         v17 = fgetc(*(_QWORD *)&argc, argv, v9, v16);
40         if ( v17 != -1 && v17 )
41         {
42             if ( v17 > 47 && v17 <= 96 )
43             {
44                 v17 += 53;
45             }
46             else if ( v17 <= 46 )
47             {
48                 v17 += v17 % 11;
49             }
50             else
51             {
52                 v17 -= v17 % 61;
53             }
54             fputc(*(_QWORD *)&argc, argv, v15, (unsigned int)v17);
55         }
56     }
57     fclose(*(_QWORD *)&argc, argv, v9, v15);
58     fclose(*(_QWORD *)&argc, argv, v10, v16);
59     sprintf(*(_QWORD *)&argc, argv, "del %s", &v14, v19[1]);

```

暴力破解得到flag:

```
f = open("flag.enc", "rb+")
cypher = f.read()
flag = ''
print(cypher)

for i in range(len(cypher)):
    for j in range(256):
        t = j
        if t > 47 and t <= 96 :
            t += 53
        elif t <= 46 :
            t += t % 11
        else :
            t -= t % 61
        if t == cypher[i] :
            flag += chr(j)

print(flag)
print(bytearray.fromhex(flag))
f.close()
```

运行结果:

```
b'jeihjiiklwjnk{ljj{kflghhj{ilk{k{kij{ihlgkfkhhwhhjgly'
504354467B596F755F6172335F476F6F645F437261636B33527D
bytearray(b'PCTF{You_ar3_Good_Crack3R}')
```