

osint

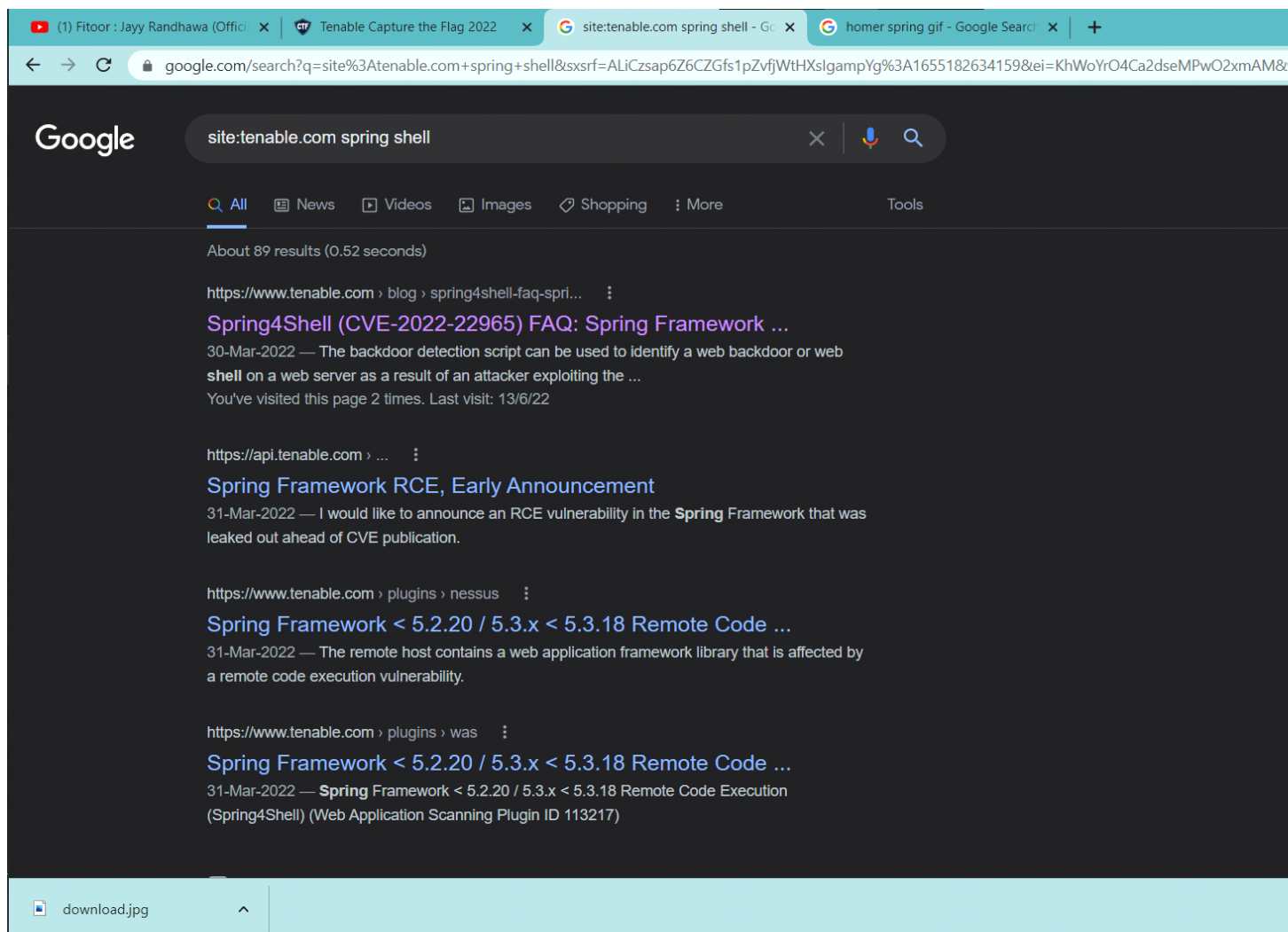
1. Find me if you can



(a) I start with googling homer gif and shell, but got nothing exciting there.

(b) I thought to add tenable website for searching.

(c) search related to spring4shell vulnerability pops up from tenable website www.tenable.com



(d)After opening website we can find flag inside source-code.

```
(1) Fitor: Jay Randhawa (Offici... x Tenable Capture the Flag 2022 x Spring4Shell (CVE-2022-22965) F x view-source:https://www.tenable.com/blog/spring4shell-faq-spring-framework-remote-code-execution-vulnerability x homer spring gif - Google Search x +
view-source:https://www.tenable.com/blog/spring4shell-faq-spring-framework-remote-code-execution-vulnerability
663 <p>Researchers at Praetorian <a href="https://www.praetorian.com/blog/spring-core-jdk9-rce/">have confirmed that Spring4Shell is a patch
664
665 <h5>Is Spring4Shell related to CVE-2022-22963?</h5>
666
667 <p>No, these are two completely unrelated vulnerabilities. <a href="https://www.tenable.com/cve/CVE-2022-22963">CVE-2022-22963</a> is a vulnerability in the Spring Cloud
668
669 <p>Because there was no CVE assigned for Spring4Shell at the time of its disclosure, Spring4Shell was erroneously associated with CVE-2022-22963.</p>
670
671 <h5>Is Proof of Concept exploit code available?</h5>
672
673 <p>Yes, there are multiple working proof-of-concept (PoC) exploits available for both <a href="https://github.com/search?q=Spring4Shell">Spring4Shell</a> and <a href="https://github.com/search?q=Spring4Shell">Spring4Shell</a> and <a href="https://github.com/search?q=Spring4Shell">Spring4Shell</a> and <a href="https://github.com/search?q=Spring4Shell">Spring4Shell</a>
674
675 <h5>Are Tenable products affected by Spring4Shell or CVE-2022-22963?</h5>
676
677 <p>Based on current information as of 4/1/2022 regarding Spring4Shell (CVE-2022-22965) and CVE-2022-22963, Tenable products are not affected.</p>
678
679 <h5>Apache Tomcat is listed as a prerequisite, has the Tomcat team released patches?</h5>
680
681 <p>Yes, they have. While CVE-2022-22965 resides in the Spring Framework, the Apache Tomcat team released new versions of Tomcat to <a href="https://spring.io/blog/2022/04/01/spring-framework-5-3-18-remote-code-execution-cve-2022-22965">https://spring.io/blog/2022/04/01/spring-framework-5-3-18-remote-code-execution-cve-2022-22965</a>
682
683 <h5>Does Tenable have any product coverage for Spring4Shell?</h5>
684
685 <p>Yes, please refer to the Identifying affected systems section below for details. If you would like to learn more about the plugins, please refer to <a href="https://community.tenable.com/t5/Plugins-and-Tools/Identifying-affected-systems-for-Spring4Shell/ba-p/159374">https://community.tenable.com/t5/Plugins-and-Tools/Identifying-affected-systems-for-Spring4Shell/ba-p/159374</a>
686 <!-- CTF: flag{si3L1 si0ck3D} -->
687
688 <h2>Identifying affected systems</h2>
689
690 <p>A list of Tenable plugins to identify this vulnerability can be found <a href="https://www.tenable.com/plugins/search?q=cves%3A%28%22CVE-2022-22965%22%29&sort=&page=1">https://www.tenable.com/plugins/search?q=cves%3A%28%22CVE-2022-22965%22%29&sort=&page=1</a>
691
692 <div class="table-responsive">
693 <table class="table">
694 <thead>
695 <tr>
696 <th><strong>Plugin ID</strong></th>
697 <th><strong>Name</strong></th>
698 <th><strong>Products</strong></th>
699 <th><strong>Requirements</strong></th>
700 </tr>
701 </thead>
702 <tbody>
703 <tr>
704 <td><a href="https://www.tenable.com/plugins/nessus/159374">159374</a></td>
705 <td>Spring Framework &lt; 5.2.20 / 5.3.x &lt; 5.3.18 Remote Code Execution (CVE-2022-22965)</td>
706 <td>Tenable.io, Tenable.sc, Nessus</td>
707 <td>Paranoid Mode, Thorough Tests</td>
708 </tr>
709 </tbody>
710 </table>
711
712 </div>
713
714 </div>
715
716 </div>
717
718 </div>
719
720 </div>
721
722 </div>
723
724 </div>
725
726 </div>
727
728 </div>
729
730 </div>
731
732 </div>
733
734 </div>
735
736 </div>
737
738 </div>
739
740 </div>
741
742 </div>
743
744 </div>
745
746 </div>
747
748 </div>
749
750 </div>
751
752 </div>
753
754 </div>
755
756 </div>
757
758 </div>
759
760 </div>
761
762 </div>
763
764 </div>
765
766 </div>
767
768 </div>
769
770 </div>
771
772 </div>
773
774 </div>
775
776 </div>
777
778 </div>
779
780 </div>
781
782 </div>
783
784 </div>
785
786 </div>
787
788 </div>
789
790 </div>
791
792 </div>
793
794 </div>
795
796 </div>
797
798 </div>
799
800 </div>
801
802 </div>
803
804 </div>
805
806 </div>
807
808 </div>
809
810 </div>
811
812 </div>
813
814 </div>
815
816 </div>
817
818 </div>
819
820 </div>
821
822 </div>
823
824 </div>
825
826 </div>
827
828 </div>
829
830 </div>
831
832 </div>
833
834 </div>
835
836 </div>
837
838 </div>
839
840 </div>
841
842 </div>
843
844 </div>
845
846 </div>
847
848 </div>
849
850 </div>
851
852 </div>
853
854 </div>
855
856 </div>
857
858 </div>
859
860 </div>
861
862 </div>
863
864 </div>
865
866 </div>
867
868 </div>
869
870 </div>
871
872 </div>
873
874 </div>
875
876 </div>
877
878 </div>
879
880 </div>
881
882 </div>
883
884 </div>
885
886 </div>
887
888 </div>
889
890 </div>
891
892 </div>
893
894 </div>
895
896 </div>
897
898 </div>
899
900 </div>
901
902 </div>
903
904 </div>
905
906 </div>
907
908 </div>
909
910 </div>
911
912 </div>
913
914 </div>
915
916 </div>
917
918 </div>
919
920 </div>
921
922 </div>
923
924 </div>
925
926 </div>
927
928 </div>
929
930 </div>
931
932 </div>
933
934 </div>
935
936 </div>
937
938 </div>
939
940 </div>
941
942 </div>
943
944 </div>
945
946 </div>
947
948 </div>
949
950 </div>
951
952 </div>
953
954 </div>
955
956 </div>
957
958 </div>
959
960 </div>
961
962 </div>
963
964 </div>
965
966 </div>
967
968 </div>
969
970 </div>
971
972 </div>
973
974 </div>
975
976 </div>
977
978 </div>
979
980 </div>
981
982 </div>
983
984 </div>
985
986 </div>
987
988 </div>
989
990 </div>
991
992 </div>
993
994 </div>
995
996 </div>
997
998 </div>
999
1000 </div>
1001
1002 </div>
1003
1004 </div>
1005
1006 </div>
1007
1008 </div>
1009
1010 </div>
1011
1012 </div>
1013
1014 </div>
1015
1016 </div>
1017
1018 </div>
1019
1020 </div>
1021
1022 </div>
1023
1024 </div>
1025
1026 </div>
1027
1028 </div>
1029
1030 </div>
1031
1032 </div>
1033
1034 </div>
1035
1036 </div>
1037
1038 </div>
1039
1040 </div>
1041
1042 </div>
1043
1044 </div>
1045
1046 </div>
1047
1048 </div>
1049
1050 </div>
1051
1052 </div>
1053
1054 </div>
1055
1056 </div>
1057
1058 </div>
1059
1060 </div>
1061
1062 </div>
1063
1064 </div>
1065
1066 </div>
1067
1068 </div>
1069
1070 </div>
1071
1072 </div>
1073
1074 </div>
1075
1076 </div>
1077
1078 </div>
1079
1080 </div>
1081
1082 </div>
1083
1084 </div>
1085
1086 </div>
1087
1088 </div>
1089
1090 </div>
1091
1092 </div>
1093
1094 </div>
1095
1096 </div>
1097
1098 </div>
1099
1100 </div>
1101
1102 </div>
1103
1104 </div>
1105
1106 </div>
1107
1108 </div>
1109
1110 </div>
1111
1112 </div>
1113
1114 </div>
1115
1116 </div>
1117
1118 </div>
1119
1120 </div>
1121
1122 </div>
1123
1124 </div>
1125
1126 </div>
1127
1128 </div>
1129
1130 </div>
1131
1132 </div>
1133
1134 </div>
1135
1136 </div>
1137
1138 </div>
1139
1140 </div>
1141
1142 </div>
1143
1144 </div>
1145
1146 </div>
1147
1148 </div>
1149
1150 </div>
1151
1152 </div>
1153
1154 </div>
1155
1156 </div>
1157
1158 </div>
1159
1160 </div>
1161
1162 </div>
1163
1164 </div>
1165
1166 </div>
1167
1168 </div>
1169
1170 </div>
1171
1172 </div>
1173
1174 </div>
1175
1176 </div>
1177
1178 </div>
1179
1180 </div>
1181
1182 </div>
1183
1184 </div>
1185
1186 </div>
1187
1188 </div>
1189
1190 </div>
1191
1192 </div>
1193
1194 </div>
1195
1196 </div>
1197
1198 </div>
1199
1200 </div>
1201
1202 </div>
1203
1204 </div>
1205
1206 </div>
1207
1208 </div>
1209
1210 </div>
1211
1212 </div>
1213
1214 </div>
1215
1216 </div>
1217
1218 </div>
1219
1220 </div>
1221
1222 </div>
1223
1224 </div>
1225
1226 </div>
1227
1228 </div>
1229
1230 </div>
1231
1232 </div>
1233
1234 </div>
1235
1236 </div>
1237
1238 </div>
1239
1240 </div>
1241
1242 </div>
1243
1244 </div>
1245
1246 </div>
1247
1248 </div>
1249
1250 </div>
1251
1252 </div>
1253
1254 </div>
1255
1256 </div>
1257
1258 </div>
1259
1260 </div>
1261
1262 </div>
1263
1264 </div>
1265
1266 </div>
1267
1268 </div>
1269
1270 </div>
1271
1272 </div>
1273
1274 </div>
1275
1276 </div>
1277
1278 </div>
1279
1280 </div>
1281
1282 </div>
1283
1284 </div>
1285
1286 </div>
1287
1288 </div>
1289
1290 </div>
1291
1292 </div>
1293
1294 </div>
1295
1296 </div>
1297
1298 </div>
1299
1300 </div>
1301
1302 </div>
1303
1304 </div>
1305
1306 </div>
1307
1308 </div>
1309
1310 </div>
1311
1312 </div>
1313
1314 </div>
1315
1316 </div>
1317
1318 </div>
1319
1320 </div>
1321
1322 </div>
1323
1324 </div>
1325
1326 </div>
1327
1328 </div>
1329
1330 </div>
1331
1332 </div>
1333
1334 </div>
1335
1336 </div>
1337
1338 </div>
1339
1340 </div>
1341
1342 </div>
1343
1344 </div>
1345
1346 </div>
1347
1348 </div>
1349
1350 </div>
1351
1352 </div>
1353
1354 </div>
1355
1356 </div>
1357
1358 </div>
1359
1360 </div>
1361
1362 </div>
1363
1364 </div>
1365
1366 </div>
1367
1368 </div>
1369
1370 </div>
1371
1372 </div>
1373
1374 </div>
1375
1376 </div>
1377
1378 </div>
1379
1380 </div>
1381
1382 </div>
1383
1384 </div>
1385
1386 </div>
1387
1388 </div>
1389
1390 </div>
1391
1392 </div>
1393
1394 </div>
1395
1396 </div>
1397
1398 </div>
1399
1400 </div>
1401
1402 </div>
1403
1404 </div>
1405
1406 </div>
1407
1408 </div>
1409
1410 </div>
1411
1412 </div>
1413
1414 </div>
1415
1416 </div>
1417
1418 </div>
1419
1420 </div>
1421
1422 </div>
1423
1424 </div>
1425
1426 </div>
1427
1428 </div>
1429
1430 </div>
1431
1432 </div>
1433
1434 </div>
1435
1436 </div>
1437
1438 </div>
1439
1440 </div>
1441
1442 </div>
1443
1444 </div>
1445
1446 </div>
1447
1448 </div>
1449
1450 </div>
1451
1452 </div>
1453
1454 </div>
1455
1456 </div>
1457
1458 </div>
1459
1460 </div>
1461
1462 </div>
1463
1464 </div>
1465
1466 </div>
1467
1468 </div>
1469
1470 </div>
1471
1472 </div>
1473
1474 </div>
1475
1476 </div>
1477
1478 </div>
1479
1480 </div>
1481
1482 </div>
1483
1484 </div>
1485
1486 </div>
1487
1488 </div>
1489
1490 </div>
1491
1492 </div>
1493
1494 </div>
1495
1496 </div>
1497
1498 </div>
1499
1500 </div>
1501
1502 </div>
1503
1504 </div>
1505
1506 </div>
1507
1508 </div>
1509
1510 </div>
1511
1512 </div>
1513
1514 </div>
1515
1516 </div>
1517
1518 </div>
1519
1520 </div>
1521
1522 </div>
1523
1524 </div>
1525
1526 </div>
1527
1528 </div>
1529
1530 </div>
1531
1532 </div>
1533
1534 </div>
1535
1536 </div>
1537
1538 </div>
1539
1540 </div>
1541
1542 </div>
1543
1544 </div>
1545
1546 </div>
1547
1548 </div>
1549
1550 </div>
1551
1552 </div>
1553
1554 </div>
1555
1556 </div>
1557
1558 </div>
1559
1560 </div>
1561
1562 </div>
1563
1564 </div>
1565
1566 </div>
1567
1568 </div>
1569
1570 </div>
1571
1572 </div>
1573
1574 </div>
1575
1576 </div>
1577
1578 </div>
1579
1580 </div>
1581
1582 </div>
1583
1584 </div>
1585
1586 </div>
1587
1588 </div>
1589
1590 </div>
1591
1592 </div>
1593
1594 </div>
1595
1596 </div>
1597
1598 </div>
1599
1600 </div>
1601
1602 </div>
1603
1604 </div>
1605
1606 </div>
1607
1608 </div>
1609
1610 </div>
1611
1612 </div>
1613
1614 </div>
1615
1616 </div>
1617
1618 </div>
1619
1620 </div>
1621
1622 </div>
1623
1624 </div>
1625
1626 </div>
1627
1628 </div>
1629
1630 </div>
1631
1632 </div>
1633
1634 </div>
1635
1636 </div>
1637
1638 </div>
1639
1640 </div>
1641
1642 </div>
1643
1644 </div>
1645
1646 </div>
1647
1648 </div>
1649
1650 </div>
1651
1652 </div>
1653
1654 </div>
1655
1656 </div>
1657
1658 </div>
1659
1660 </div>
1661
1662 </div>
1663
1664 </div>
1665
1666 </div>
1667
1668 </div>
1669
1670 </div>
1671
1672 </div>
1673
1674 </div>
1675
1676 </div>
1677
1678 </div>
1679
1680 </div>
1681
1682 </div>
1683
1684 </div>
1685
1686 </div>
1687
1688 </div>
1689
1690 </div>
1691
1692 </div>
1693
1694 </div>
1695
1696 </div>
1697
1698 </div>
1699
1700 </div>
1701
1702 </div>
1703
1704 </div>
1705
1706 </div>
1707
1708 </div>
1709
1710 </div>
1711
1712 </div>
1713
1714 </div>
1715
1716 </div>
1717
1718 </div>
1719
1720 </div>
1721
1722 </div>
1723
1724 </div>
1725
1726 </div>
1727
1728 </div>
1729
1730 </div>
1731
1732 </div>
1733
1734 </div>
1735
1736 </div>
1737
1738 </div>
1739
1740 </div>
1741
1742 </div>
1743
1744 </div>
1745
1746 </div>
1747
1748 </div>
1749
1750 </div>
1751
1752 </div>
1753
1754 </div>
1755
1756 </div>
1757
1758 </div>
1759
1760 </div>
1761
1762 </div>
1763
1764 </div>
1765
1766 </div>
1767
1768 </div>
1769
1770 </div>
1771
1772 </div>
1773
1774 </div>
1775
1776 </div>
1777
1778 </div>
1779
1780 </div>
1781
1782 </div>
1783
1784 </div>
1785
1786 </div>
1787
1788 </div>
1789
1790 </div>
1791
1792 </div>
1793
1794 </div>
1795
1796 </div>
1797
1798 </div>
1799
1800 </div>
1801
1802 </div>
1803
1804 </div>
1805
1806 </div>
1807
1808 </div>
1809
1810 </div>
1811
1812 </div>
1813
1814 </div>
1815
1816 </div>
1817
1818 </div>
1819
1820 </div>
1821
1822 </div>
1823
1824 </div>
1825
1826 </div>
1827
1828 </div>
1829
1830 </div>
1831
1832 </div>
1833
1834 </div>
1835
1836 </div>
1837
1838 </div>
1839
1840 </div>
1841
1842 </div>
1843
1844 </div>
1845
1846 </div>
1847
1848 </div>
1849
1850 </div>
1851
1852 </div>
1853
1854 </div>
1855
1856 </div>
1857
1858 </div>
1859
1860 </div>
1861
1862 </div>
1863
1864 </div>
1865
1866 </div>
1867
1868 </div>
1869
1870 </div>
1871
1872 </div>
1873
1874 </div>
1875
1876 </div>
1877
1878 </div>
1879
1880 </div>
1881
1882 </div>
1883
1884 </div>
1885
1886 </div>
1887
1888 </div>
1889
1890 </div>
1891
1892 </div>
1893
1894 </div>
1895
1896 </div>
1897
1898 </div>
1899
1900 </div>
1901
1902 </div>
1903
1904 </div>
1905
1906 </div>
1907
1908 </div>
1909
1910 </div>
1911
1912 </div>
1913
1914 </div>
1915
1916 </div>
1917
1918 </div>
1919
1920 </div>
1921
1922 </div>
1923
1924 </div>
1925
1926 </div>
1927
1928 </div>
1929
1930 </div>
1931
1932 </div>
1933
1934 </div>
1935
1936 </div>
1937
1938 </div>
1939
1940 </div>
1941
1942 </div>
1943
1944 </div>
1945
1946 </div>
1947
1948 </div>
1949
1950 </div>
1951
1952 </div>
1953
1954 </div>
1955
1956 </div>
1957
1958 </div>
1959
1960 </div>
1961
1962 </div>
1963
1964 </div>
1965
1966 </div>
1967
1968 </div>
1969
1970 </div>
1971
1972 </div>
1973
1974 </div>
1975
1976 </div>
1977
1978 </div>
1979
1980 </div>
1981
1982 </div>
1983
1984 </div>
1985
1986 </div>
1987
1988 </div>
1989
1990 </div>
1991
1992 </div>
1993
1994 </div>
1995
1996 </div>
1997
1998 </div>
1999
2000 </div>
2001
2002 </div>
2003
2004 </div>
2005
2006 </div>
2007
2008 </div>
2009
2010 </div>
2011
2012 </div>
2013
2014 </div>
2015
2016 </div>
2017
2018 </div>
2019
2020 </div>
2021
2022 </div>
2023
2024 </div>
2025
2026 </div>
2027
2028 </div>
2029
2030 </div>
2031
2032 </div>
2033
2034 </div>
2035
2036 </div>
2037
2038 </div>
2039
2040 </div>
2041
2042 </div>
2043
2044 </div>
2045
2046 </div>
2047
2048 </div>
2049
2050 </div>
2051
2052 </div>
2053
2054 </div>
2055
2056 </div>
2057
2058 </div>
2059
2060 </div>
2061
2062 </div>
2063
2064 </div>
2065
2066 </div>
2067
2068 </div>
2069
2070 </div>
2071
2072 </div>
2073
2074 </div>
2075
2076 </div>
2077
2078 </div>
2079
2080 </div>
2081
2082 </div>
2083
2084 </div>
2085
2086 </div>
2087
2088 </div>
2089
2090 </div>
2091
2092 </div>
2093
2094 </div>
2095
2096 </div>
2097
2098 </div>
2
```