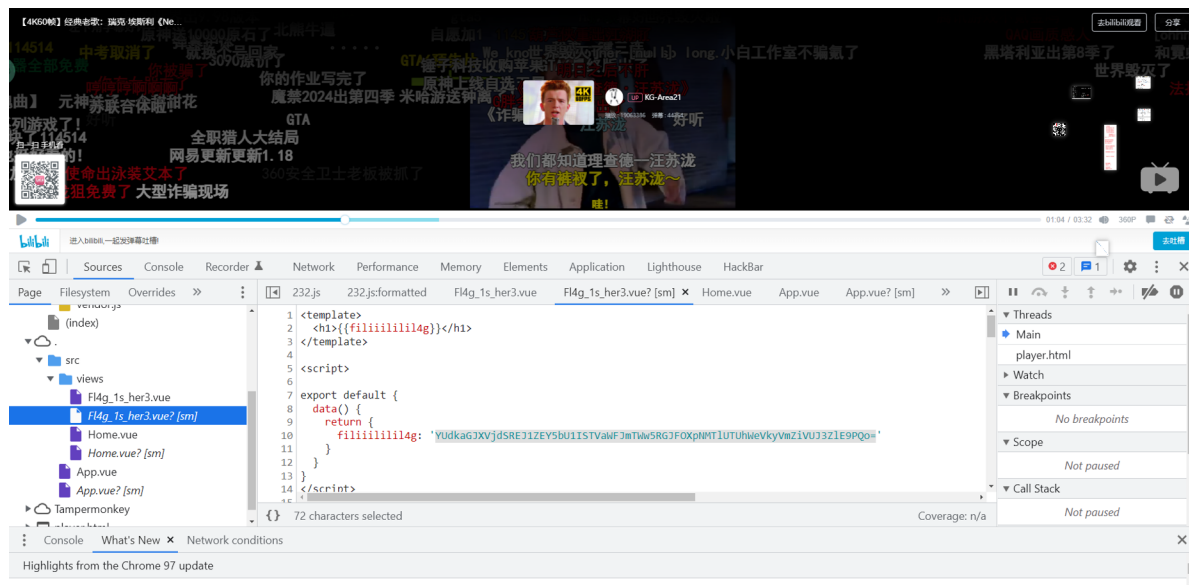


Web

1. Webpack

这一题没啥可说的，主要就是对b站某个页面进行了打包，网上查了一下，说打包的网页很可能会有Vue源码泄露，直接F12去控制台里查看一下，果然有



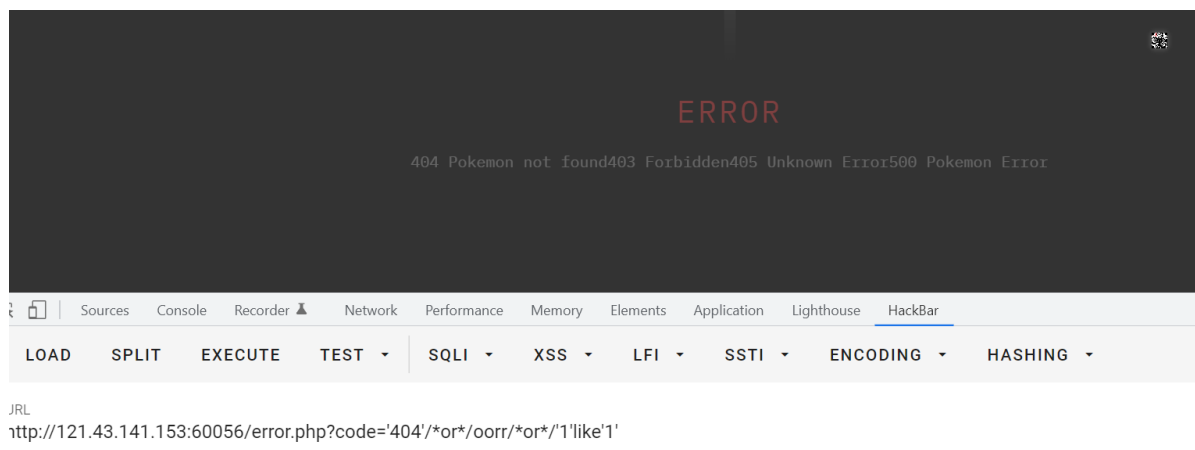
2. Pokeman

这道题主要考的是SQL注入，一开始打开网页源码说有一个注入点

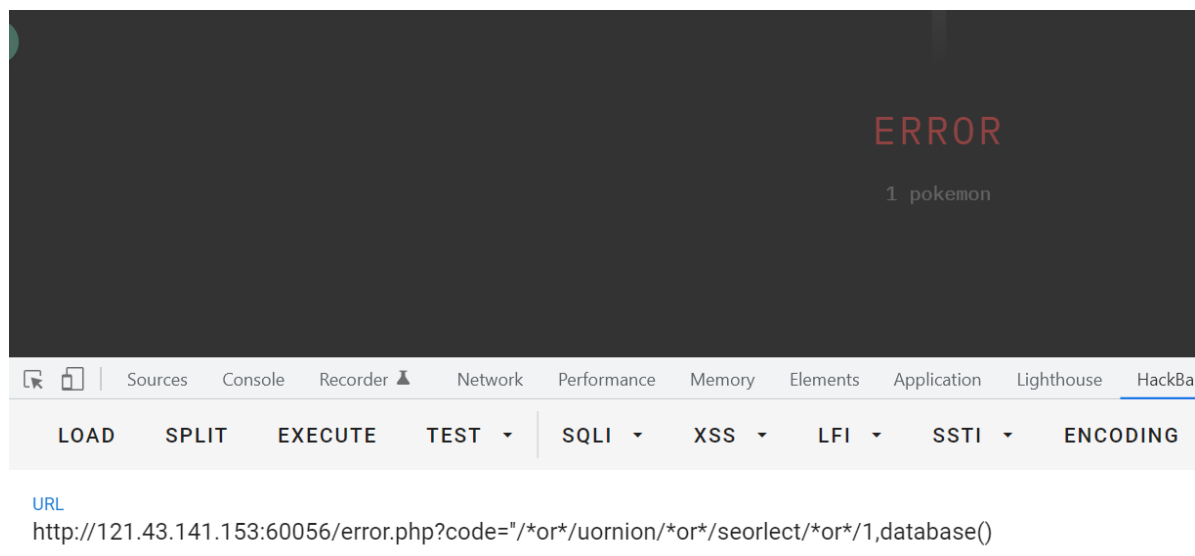
```
<html>
<head>
  <meta charset="UTF-8">
  <link rel="stylesheet" href="static/error.css">
</head>
<body>
  <div>
    <h1>Choose your Pokemon! </h1>
    <div>
      
      <p>Bulbasaur</p>
    </div>
  </div>
  <!-- /index.php?id=1 -->
</body>
</html>
```

那就注入呗，结果发现这个注入点只能注入数字，1、2、3等，其他都会进行一个302，这还注个锤子啊。。。

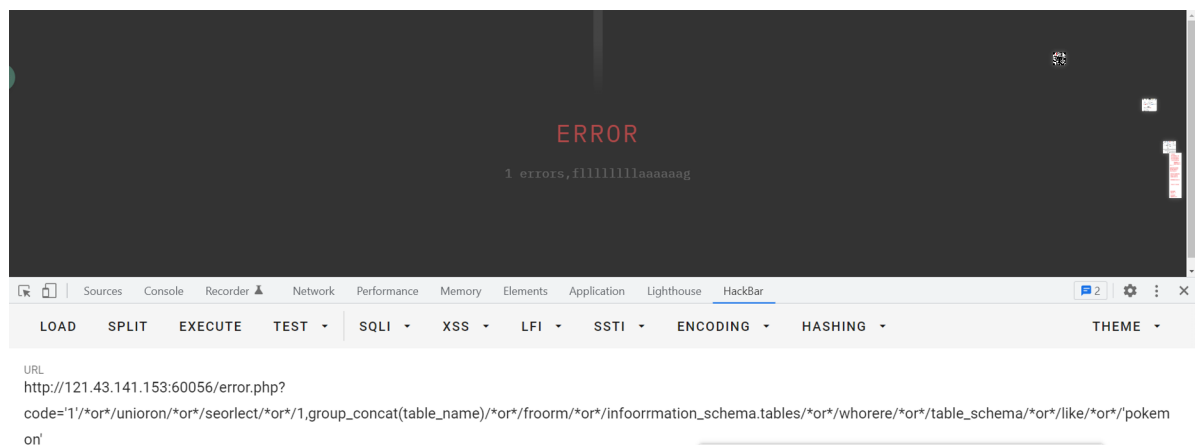
想了半天，看到302过去的地址里面有一个?code=404，唔，，会不会是在这个点进行注入呢？尝试一下爆出所有库



成功啦！接下去爆出现在的数据库：

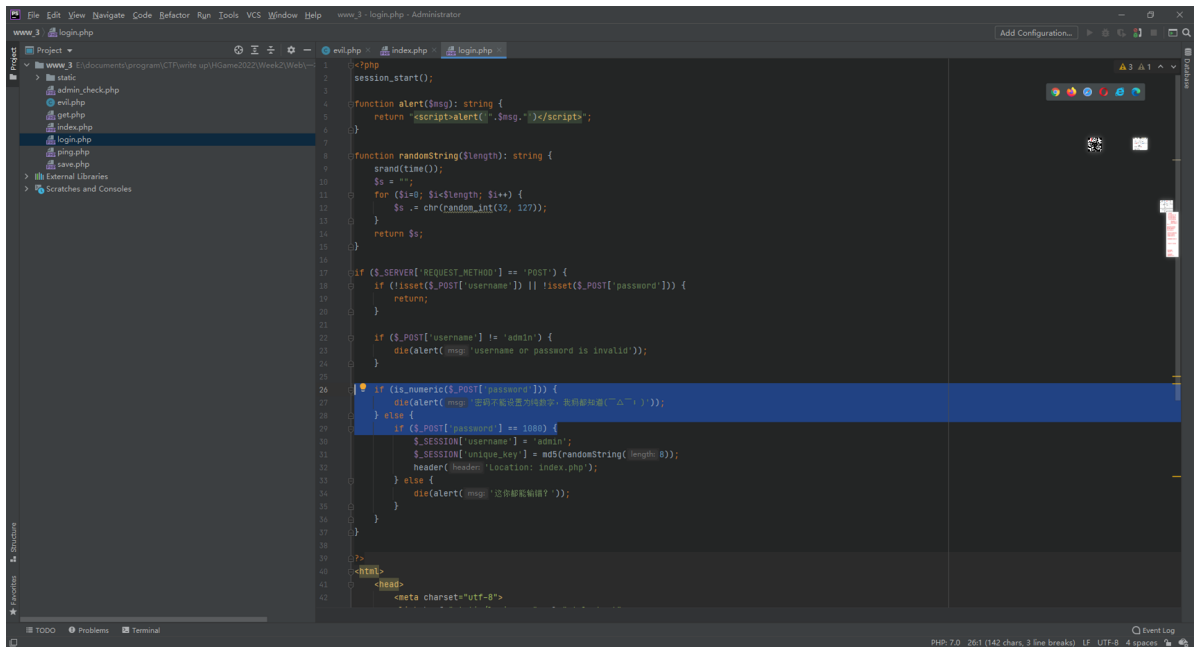


ok！接下来要在pokemon库 中找所有数据表：

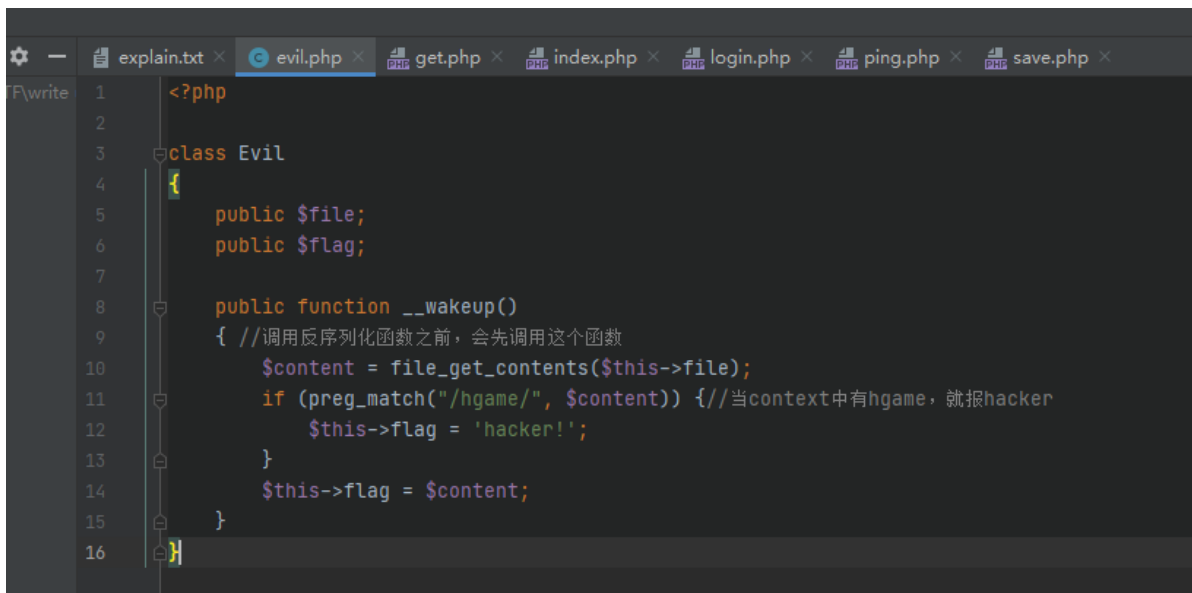


那么很明显flag在filllllllllaaaaaag表中， 进行一个查询字段

回到我们的题目中，题目一开始是要求我们登录，那么我们进行查看源码：



```
1 <?php
2 session_start();
3
4 function alert($msg): string {
5     return "<script>alert('$msg');</script>";
6 }
7
8 function randomString($length): string {
9     $s = '';
10    for ($i=0; $i<$length; $i++) {
11        $s .= chr(random_int(32, 127));
12    }
13    return $s;
14 }
15
16
17 if ($_SERVER['REQUEST_METHOD'] == 'POST') {
18     if (!isset($_POST['username']) || !isset($_POST['password'])) {
19         return;
20     }
21
22     if ($_POST['username'] != 'admin') {
23         die(alert('username or password is invalid'));
24     }
25
26     if (!is_numeric($_POST['password'])) {
27         die(alert('密码不能全是数字的哈，否则容易被猜出来'));
28     } else {
29         if ($_POST['password'] == '1080a') {
30             $_SESSION['username'] = 'admin';
31             $SESSION['unique_key'] = md5(randomString(100));
32             header(['Location: index.php']);
33         } else {
34             die(alert('密码输错了'));
35         }
36     }
37 }
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
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
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
2612
261
```



```
<?php
class Evil
{
    public $file;
    public $flag;

    public function __wakeup()
    { //调用反序列化函数之前，会先调用这个函数
        $content = file_get_contents($this->file);
        if (preg_match("/hgame/", $content)) { //当context中有hgame，就报hacker
            $this->flag = 'hacker!';
        }
        $this->flag = $content;
    }
}
```

通过查阅可得，当PHP在反序列化时，会自动执行这个方法，那么为什么之前我传入正常的字符串它没有给我返回呢？那是因为那就是正常的字符串，PHP在反序列化时检测不到这个方法，才没有调用。如果你让PHP反序列化时是这个Evil类，那么因为在get.php前include了evil.php，PHP检测的到这个方法，所以才会去调用。（这个地方建议搭建一个本地服务器测试一下，第一次接触这个玩意的小白（比如我）真的搞不明白）下面是我测试用的代码：

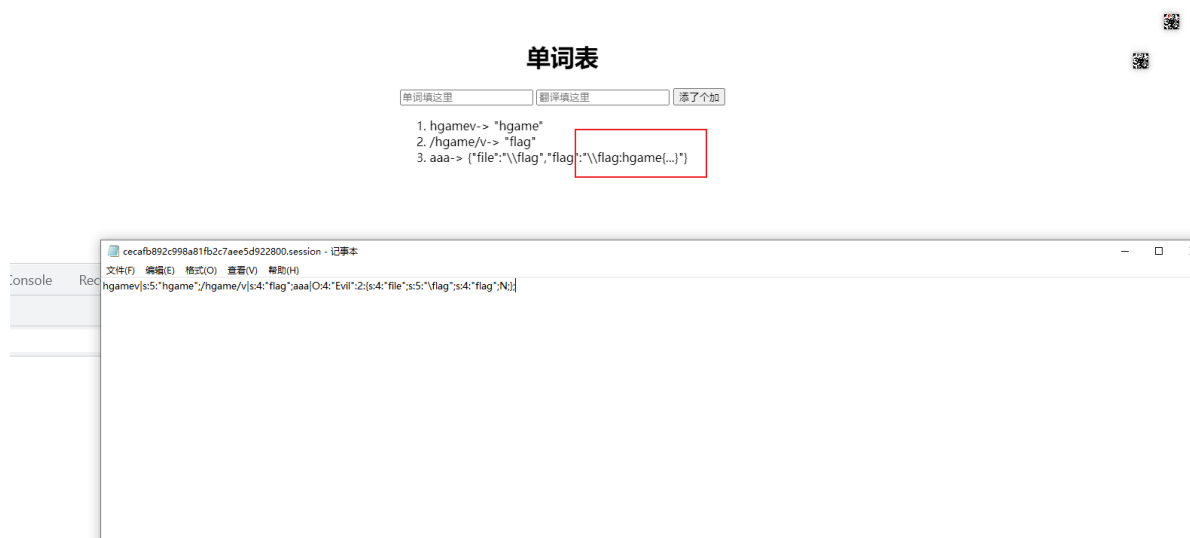
```
class Evil
{
    public $file;
    public $flag;

    function __wakeup()
    {
        echo ' __wake is working';
        $content = "hgame{...}";
        echo '</br>';
        if (preg_match("/hgame/", $content)) { //当context中有hgame，就报hacker
            $this->flag = 'hacker!';
        }
        $this->flag = $content;
    }
}

$Zhangsan = new Evil;
$Zhangsan->file = '\\flag';
$saveData = serialize($Zhangsan); //序列化后的字符串，可以保存在数据库或者文本文件中。
echo '这是序列化后的对象</br>';
var_dump($saveData);
echo '</br>';
echo '</br>';
echo '</br>';
$UnData = unserialize($saveData);
echo '这是反序列化后的序列化后的对象</br>';
print_r($UnData);
echo '</br>';
echo '</br>';
echo '</br>';
$saveData = serialize($Zhangsan); //序列化后的字符串，可以保存在数据库或者文本文件中。
echo '这是序列化后的反序列化后的序列化后的对象</br>';
var_dump($saveData);
```

这边再简单理解一下题目中的_wakeup方法，应该是你传入一个Evil类，里面带有file=/flag，然后PHP在反序列化这个类的时候会自动调用wakeup这个方法，读取这个file=/flag的文件到 \$this->flag里面，然后就可以传回来了 \$this->flag了，(但是我不理解为什么在这里要加一个/hgame/是否在 \$this->flag里的判断然后又到后面去把 \$this->flag再赋值一遍，，这不相当于没有判断吗？？难道是出题人故意留的，让我们知道这道题还可以更难？/doge)

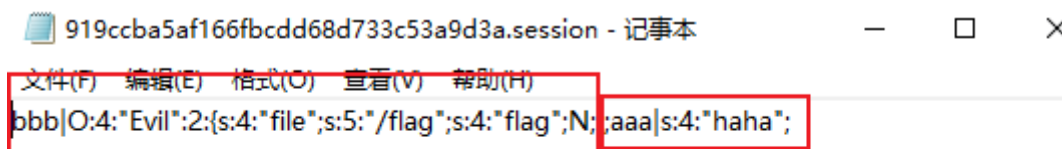
通过直接改本地session文件，我可以得到我预期得到的flag：



OK！那么现在我们还有最后一个问题，就是如何让PHP反序列化我们输入进去的Evil类呢？如果你直接传入value的话，PHP会把它当作字符串去序列化的呀！

我们通过之前的分析可以得到，代码是不会序列化key值的，那我们能不能在key中构造一个嵌套，输入一个k:v，但其实PHP读取的是两个k:v呢？

就比如说我输入key=bbb|O:4:"Evil":2:{s:4:"file";s:5:"/flag";s:4:"flag";N};aaa, value=hahaha，那么服务端存储的文件内容大致应该是这样的：



这样我们就成功把要让PHP反序列化的类输入进去啦！重新加载就可以看到flag啦！



下面是我查找PHP函数功能时记录的，也放在这里吧！

PS: 这应该是本题最长WP了吧，能不能赏点积分/doge

strstr:

查找 "Shanghai" 在 "I love Shanghai!" 中的第一次出现，并返回字符串的剩余部分：

```
echo strstr("I love Shanghai!","Shanghai");
```

strpos:

查找 "php" 在字符串中第一次出现的位置：

```
echo strpos("You love php, I love php too!","php");
```

substr:

从字符串中返回 "world":

```
echo substr("Hello world",6);
```

file_get_contents:

把整个文件读入一个字符串中

```
echo file_get_contents("test.txt");
```

file_put_contents()

函数把一个字符串写入文件中

```
echo file_put_contents("test.txt","Hello world. Testing!");
```

```
file_put_contents($filename, $str, FILE_APPEND);
```

使用 FILE_APPEND 可避免删除文件中已有的内容。

Apache!

这个题也是出自Summ3r大佬，着实让我从第一天看到了最后一天，，，，，，，

首先用dirresearch扫，发现有一个www.zip，里面是apache的配置文件

```
Target: http://httpd.summ3r.top:60010/
Output File: E:\documents\program\CTF\相关软件\dirsearch-master\reports\httpd.summ3r.top\_22-01-27_21-40-09.txt

[21:40:09] Starting:
[21:40:13] 403 - 199B - /.ht_wsr.txt
[21:40:13] 403 - 199B - /.htaccess.bak1
[21:40:13] 403 - 199B - /.htaccess.orig
[21:40:13] 403 - 199B - /.htaccess.save
[21:40:13] 403 - 199B - /.htaccess.sample
[21:40:13] 403 - 199B - /.htaccessBAK
[21:40:13] 403 - 199B - /.htaccessOLD2
[21:40:13] 403 - 199B - /.htaccess_extra
[21:40:13] 403 - 199B - /.htaccessOLD
[21:40:13] 403 - 199B - /.htaccess_orig
[21:40:13] 403 - 199B - /.htaccess_sc
[21:40:13] 403 - 199B - /.htm
[21:40:13] 403 - 199B - /.html
[21:40:13] 403 - 199B - /.htpasswd_test
[21:40:13] 403 - 199B - /.htpasswd
[21:40:13] 403 - 199B - /.httr-oauth
[21:40:31] 200 - 1KB - /cgi-bin/test-cgi
[21:40:38] 200 - 554B - /index.html
[21:40:45] 500 - 533B - /proxy
[21:40:45] 500 - 533B - /proxy/
[21:40:52] 200 - 8KB - /www.zip

Task Completed
```

首先说是要访问内网嘛，但是这个内网怎么个访问法，当时我也是查了很多资料，都是什么内网渗透、扫描端口、上传一句话，跟我们这个好像都没啥关系

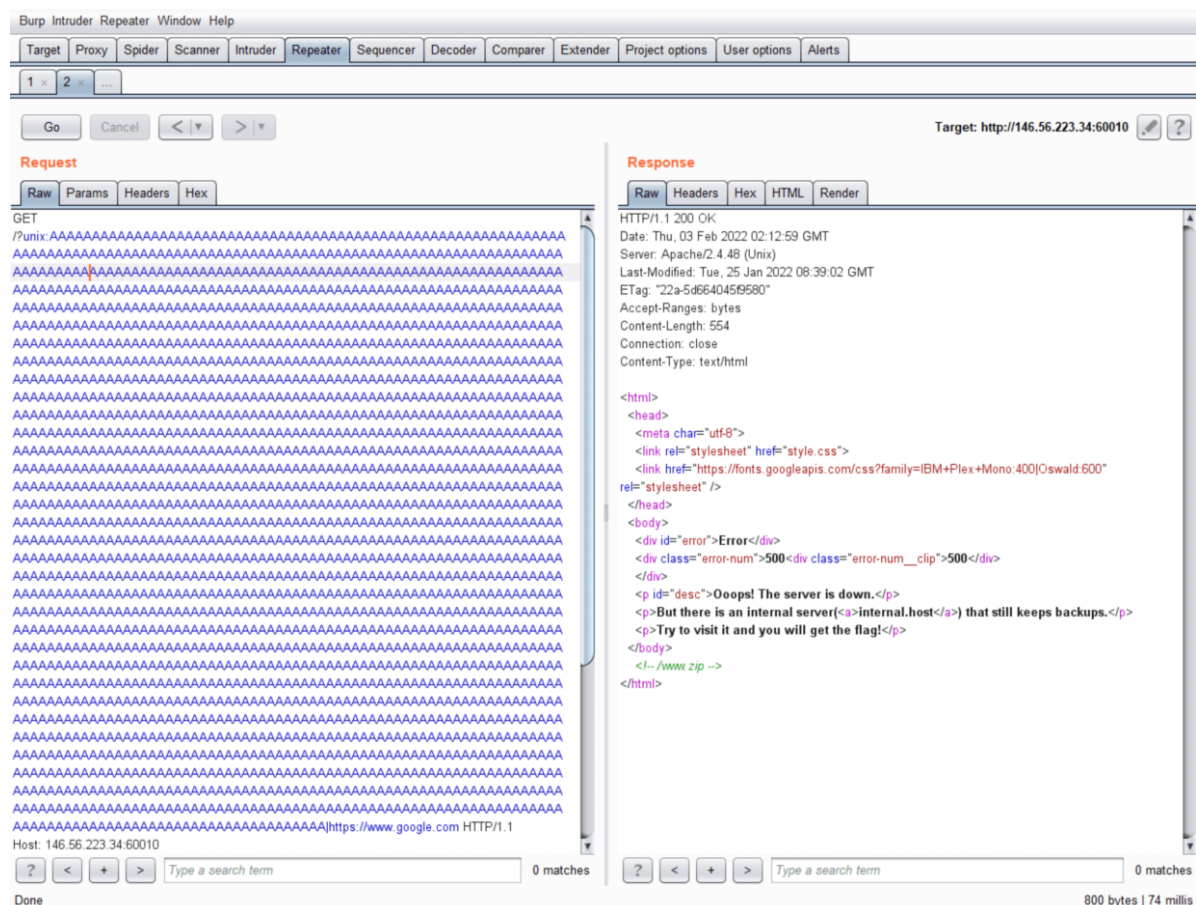
直到一天，有hint放出来说是利用Apache的CVE-2021-40438漏洞嘛。。

那就去查资料呗，查了半天资料，总结了以下几点：

主要就是利用了apache反向代理的漏洞，通过发送超长的请求信息比如

http://www.https.summer.top/?uni:A*5000 | <http://example.com> 这种请求。因为太长，代理服务器会忽略掉 | 前面的请求而直接把<http://example.com>请求发给内网主机。

但是我对着文章试了很多次，那个配置文件的压缩包我也看过了，但是就是做不到让代理服务器转发请求到内网，不知道是我漏掉了什么细节，，



直到后面看到了配置文件中的docker配置，好像懂了一点点

题目一直说让我们访问一个叫inernal,host的地方


```
docker-compose.yml - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
version: "3.8"
services:
  apache:
    image: httpd:2.4.48-alpine
    volumes:
      - ./static:/usr/local/apache2/htdocs
      - ./httpd.conf:/usr/local/apache2/conf/httpd.conf
      - ./httpd-vhosts.conf:/usr/local/apache2/conf/extra/httpd-vhosts.conf
    links:
      - internal.host
    depends_on:
      - internal.host
    ports:
      - 60010:80
  nginx:
    image: nginx:alpine
    container_name: internal.host
    volumes:
      - ./default.conf:/etc/nginx/conf.d/default.conf
```

要访问这个，它做了一个请求转发，从apache的60010端口转发到了nginx的80端口

而nginx的配置文件中有flag:

```
default.conf - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
server {
  listen 80;
  server_name localhost;
  #access_log /var/log/nginx/host.access.log main;

  location / {
    root /usr/share/nginx/html;
    index index.html index.htm;
  }

  #error_page 404 /404.html;

  # redirect server error pages to the static page /50x.html
  #
  error_page 500 502 503 504 /50x.html;
  location = /50x.html {
    root /usr/share/nginx/html;
  }

  location = /flag {
    return 200 "hgame{xxx}";
  }
}
```

监听80端口

servername=localhost

当路由为flag时，返回flag

好，那么现在问题就是如何让apache服务器将请求转发到内网的nginx服务器上，，

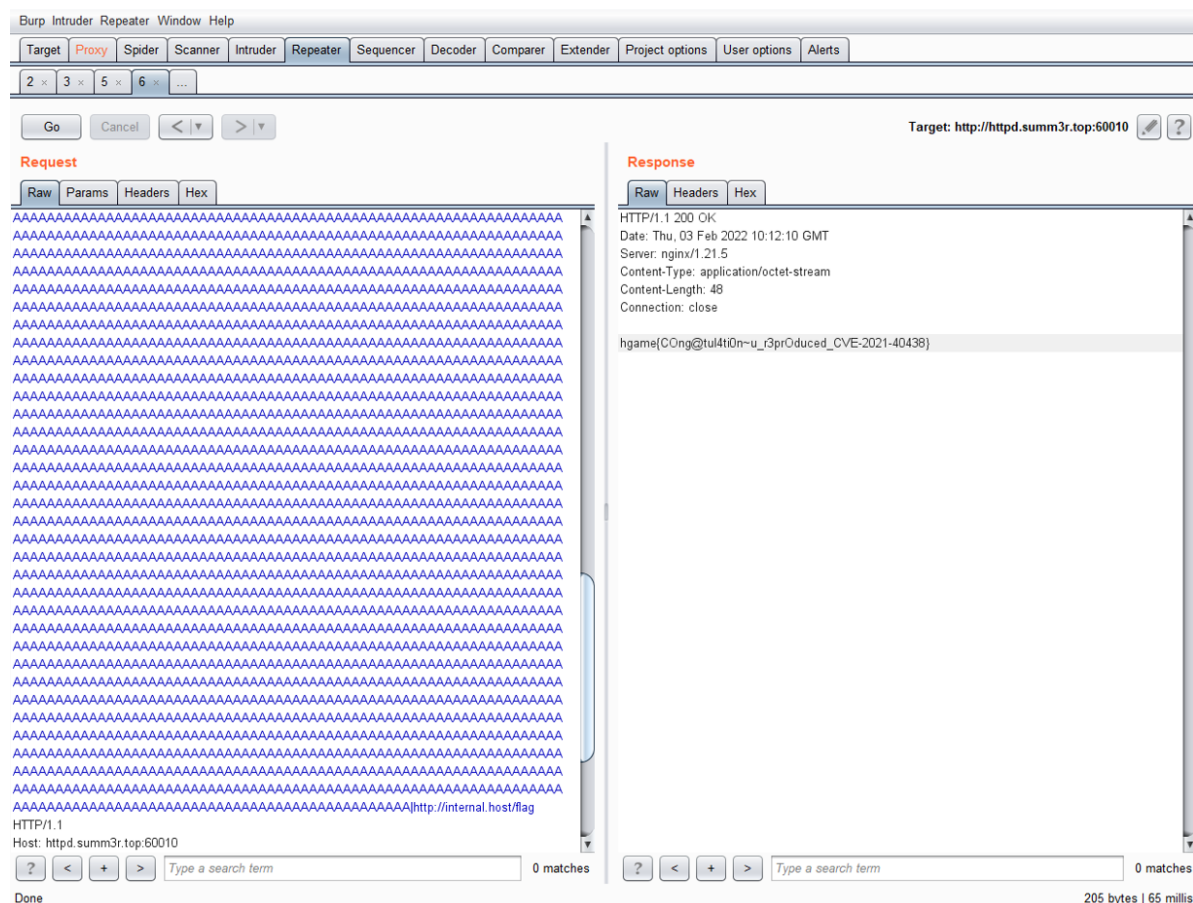
利用之前的那个漏洞，我用了千方百计，终于凑到了，需要向一个叫/proxy的路由发送请求带有<http://ocalhost/flag>的请求才能得到flag（说实话我现在还不知道为什么，连这个/proxy也是我用dirsearch扫出来的。。。)

```
Target: http://httpd.summ3r.top:60010/
Output File: E:\documents\program\CTF\相关软件\dirsearch-master\reports\httpd.summ3r.top\_22-01-27_21-40-09.txt

[21:40:09] Starting:
[21:40:13] 403 - 199B - /.ht_wsr.txt
[21:40:13] 403 - 199B - /.htaccess.bak1
[21:40:13] 403 - 199B - /.htaccess.orig
[21:40:13] 403 - 199B - /.htaccess.save
[21:40:13] 403 - 199B - /.htaccess.sample
[21:40:13] 403 - 199B - /.htaccessBAK
[21:40:13] 403 - 199B - /.htaccessOLD2
[21:40:13] 403 - 199B - /.htaccess_extra
[21:40:13] 403 - 199B - /.htaccessOLD
[21:40:13] 403 - 199B - /.htaccess_orig
[21:40:13] 403 - 199B - /.htaccess_sc
[21:40:13] 403 - 199B - /.htm
[21:40:13] 403 - 199B - /.html
[21:40:13] 403 - 199B - /.htpasswd_test
[21:40:13] 403 - 199B - /.htpasswd
[21:40:13] 403 - 199B - /.httr-oauth
[21:40:31] 200 - 1KB - /cgi-bin/test-cgi
[21:40:38] 200 - 554B - /index.html
[21:40:45] 500 - 533B - /proxy
[21:40:45] 500 - 533B - /proxy/
[21:40:52] 200 - 8KB - /www.zip

Task Completed
```

也是终于成功了（虽然是凑出来的



真的，7天了，几次三番想要放弃这个题，唉，，菜是原罪

CRYPTO

RSA Attack

简单的RSA攻击，直接上脚本吧

```
from Crypto.Util.number import *
from libnum import *
import gmpy2

p = 715800347513314032483037
q = 978782023871716954857211
e = 65537
n = 700612512827159827368074182577656505408114629807
c = 122622425510870177715177368049049966519567512708
s = (p - 1) * (q - 1)
d = gmpy2.invert(e, s)
print("dec: " + str(d))
# print("hex: " + hex(d))

m = pow(c, d, n)
print(m)
print(n2s(int(m)))
```

噫对了，这里的数不算很大，我还用到了一个分解质因数的工具叫yafu：我的p和q就是这样的得来的

```
Microsoft Windows [版本 10.0.19041.208]
(c) 2020 Microsoft Corporation. 保留所有权利。

E:\documents\program\CTF\相关软件\yafu-1.34(大数分解)>yafu-x64
factor(700612512827159827368074182577656505408114629807)

fac: factoring 700612512827159827368074182577656505408114629807
fac: using pretesting plan: normal
fac: no tune info: using qs/gnfs crossover of 95 digits

starting SIQS on c48: 700612512827159827368074182577656505408114629807

==== sieving in progress (1 thread): 1232 relations needed ====
==== Press ctrl-c to abort and save state      ====

SIQS elapsed time = 0.0399 seconds.
Total factoring time = 0.0459 seconds

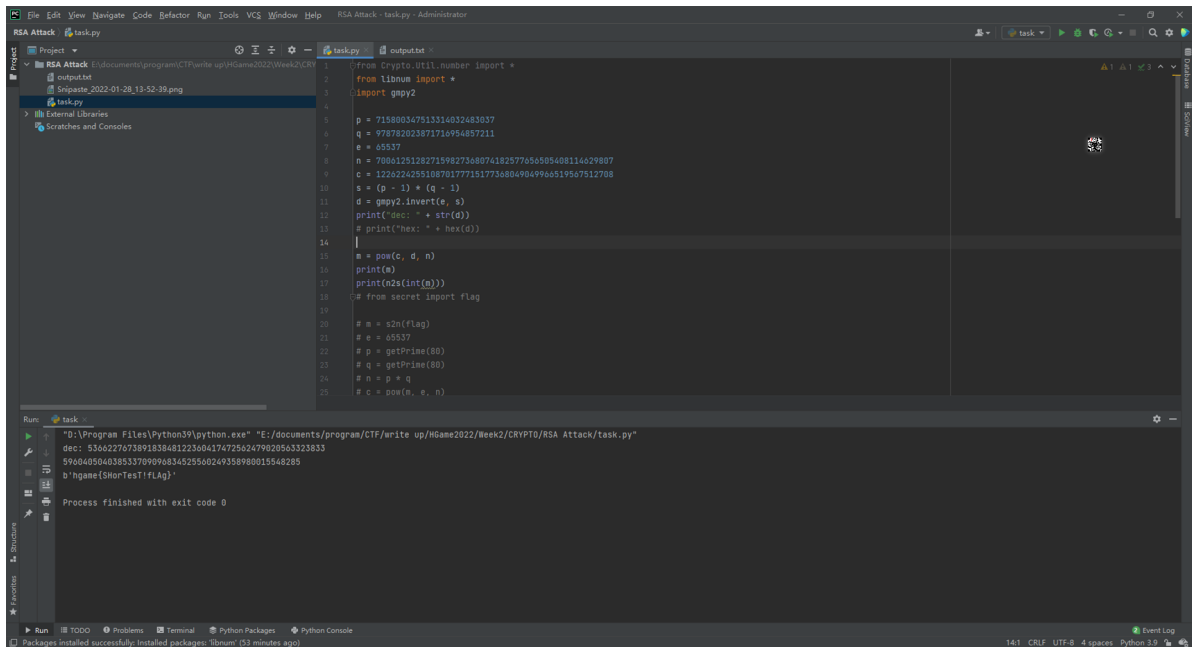
***factors found***
P24 = 715800347513314032483037
P24 = 978782023871716954857211

ans = 1

E:\documents\program\CTF\相关软件\yafu-1.34(大数分解)>
```

虽然后来得知网上也有在线工具/hhh

运行代码后得到flag:



RSA Attack 2

这题有点鬼，一个flag分了三种算法，不过还好都不算难，

第一种：知道两个n，而且两个n都有一个公因数，那就好办了，直接网上在线求公因数，再大的数都能求，直接可以把p、r、q求出来

求出来后就是老套路：

```
def pojie_tast1():
    e = 65537
    n1 =
14611545605107950827581005165327694782823188603151768169731431418361306231114985
03777591746143392530805439697080969080407398583537646462986060971029218136860061
86265904984918504045034434142414554873044483448923378774224657157091542386535051
41605904184985311873763495761345722155289457889686019746663293720106874227323699
28827779429220895717244652342059639111489155953781102947315012364162410810367651
6754449492805126642552751278309634846776360421141359905162459075173773201900914
00729277307636724890592155256437996566160995456743018225013851937593886086129131
351582958811003596445806061492952513851932238563627194553
    c1 =
9650758035549329886642718643918380232881201369420374132076310537603691258499503
16476723484681113104236808581019906700670653062375961216648843536799876895323054
37801346923070145524106271337770666947677115752724993307387122132705797012726237
07355066941911004630825740848453506351567806677768101721151098142927334692802297
11494110645562250012873991413061360817224710750324230796929083802671602141437205
16748000734987068685104675254411687005690312116824966036851568223828884335112144
63726809039715853293714112265407595273005233157398070113637821200295671929519273
3955673315234274064519957670199895100508623561838510479
```

```

n2 =
20937478725109983803079185450449616567464596961348727453817249035110047585580142
82355128957714595812712158679287850938608517845217111245589042947445779721920282
70308842622730613347524934967979353466315098066855891796183674539927497533182738
34113016237120686880514110415113673431170488958730203963489455418967544128619234
39491582039290842297407593275183801218554296884269182420320651779569389386394510
06619409884556959235117773065664193733940919073494316866464855163255754949026823
37518438042711296437513221448397034813099279203955535025939120139680604495486980
765910892438284945450733375156933863150808369796830892363

c2 =
11536506945313747180442473461658912307154460869003392732178457643224057969838224
60105983686088371845998600310697037577844372574860708562093878771408132131581714
44141155899522374924484834389103788653592395751693261166680304632758176098276260
48962304593324479546453471881099976644410889657248346038986836461779780183411686
26075677671172057705331950469137355010752529656093646743528381249339648667817802
02924333658980325970273388760451827434928318141756738341983453375140655963964777
09839868387265840430322983945906464646824470437783271607499089791869398590557314
713094674208261761299894705772513440948139429011425948090

q =
12371534352197068400012879987607104283057072321811693115146722024476505588941762
68065548681145255669784363239750834987038327945614932913120796913966712748373220
36085911028636844643698862533724625315331567014898932701977758733187411738771617
885153639118174062773966499612201555575923412045644028857989016603411

p =
11810617170951861319033738012072163909610943387175855148175055962860784152519993
33964010458573138419626670876810000779085753498562031979892801375181196104472650
22793158335778819939567162786340083036604758380394175830091289942677310940962706
354018362632488404102976344446903748276214668285468119214940392725123

r =
16923914309296392221334368692467736308896348563302709164550115138848256549023332
37968896916242726649851735258120023555304847414328471705113481770657043389787544
57533424010842217007432554862861949141613925946472939183705336155629494107050470
952474816647080432002189309272835581148740211208678012416960136441833

s1 = (p - 1) * (q - 1)
d1 = gmpy2.invert(e, s1)
# print("dec: " + str(d1))
m1 = pow(c1, d1, n1)
# print(m1)
# print(n2s(int(m1)))

s2 = (r - 1) * (q - 1)
d2 = gmpy2.invert(e, s2)
# print("dec: " + str(d2))
m2 = pow(c2, d2, n2)
# print(m2)
return n2s(int(m2))

```

第二种：可以发现e很小，这样的e可以直接凑出来，直接上代码：

```

def pojie_tast2():
    e = 7
    n =
14157878492255346300993349653813018105991884577529909522555551468374307942096214
96460417273438191305127374522829393083231448346692252924095899489769747593986702
55613480427259196635469490150246939526419364818415527514846041230971480718004166
08762258562797116583678332832015617217745966495992049762530373531163821979627361
20092154422357817071874134824201216411559377770090395440910311009292157882104893
33468932128050716822355758137241139783415928859577673775874922027401859708286297
67501662195356276862585025913615910839679860669917255271734413865211340126544199
760628445054131661484184876679626946360753009512634349537

    c =
10262871020519116406312674685238364023536657841034751572844570983750295909492149
10150086980641860373218135008257644759476658757235024667544550893157767015829555
86412195827293455816974482311163180804561125167007179847316559007263881858669059
89088504004805024490513718243036445638662260558477697146032055765285263446084259
81456019754901804409993515835193188515761652723528322906614539096409492900705694
6332051364474528453970904251050605631514869007890625

    for i in range(100):
        me = c - i * n
        result = gmpy2.iroot(me, e)
        if result[1]:
            return n2s(int(result[0]))

```

第三种：这里的特性是共模攻击（m，n相同；e，c不同，且e1和e2互质）

那么也是直接上代码：

```

def pojie_tast3():
    n =
18819509188106230363444813350468162056164434642729404632983082518225388069544777
3745441423176128584483453441373722298803336652808623663521375622781661086504592
43572321887689136421584486033463304625356961217396227022005403441054641266954320
11739181531217582949804939555720700457350512898322376591813135311921904580338340
20356958268188924345249536384955895594712497529373650942640046008398107884613874
00506349068244386897127483243368787916226769743418146910412622806042773578898922
11717124319329666052810029131172229930723477981468761369516771720250571713027972
064974999802168017946274736383148001865929719248159075729

    e1 = 2519901323
    c1 =
32307797262255448725314411690093070720737545787618883879834032063645484514967365
13905460381907928107310030086346589351105809028599650303539607581407627819797944
33739860140051056099246245504845132659399359508980015034299902187473474806669296
23626505400360020737487665093476498181393043639140838799189298735777063235996280
31618641793074018304521243460487551364823299685052518852685706687800209505277426
86914005105699624288213261625669518887078263431036297315376669828625894689686639
66708724518031142808467095727797805584822233937594759991036077045106183322537105
03857561025613632592682931552228150171423846203875344870

    e2 = 3676335737
    c2 =
94081859562227916143983671964170784679029465088879982233500738585416673645928312
94347690629951223710736367853718008576338413791397610918904261379811130875199348
54663776695944489430385663011713917022574342380155718317794204988626116362865144
12513662472278230945545225775880817241588440390984065155448536430923785388525187
69414770980086903896005443989986696359624959897360210207153964153758907203356975
04837045188626103142204474942751410819466379437091569610294575687793060945525108
98666085127747507999446647485911409264379741892764572643017592824747688487981703
4346652560116597965191204061051401916282814886688467861

    _, r, s = gmpy2.gcdext(e1, e2)
    # 根据数学关系(共模攻击)得
    m = pow(c1, r, n) * pow(c2, s, n) % n
    return n2s(int(m))

```

最后将三者合起来，就可以得到flag



```

116
117
118 print(pojie_tast1() + pojie_tast2() + pojie_tast3())
119

```

task (1) ×

"D:\Program Files\Python39\python.exe" "E:/documents/program/CTF/write up/HGame2022/Week2/CRYPTO/RSA Attack 2/task.py"

b'hgame{RsA@hAS!a&VArIETy?of.AttackK*mEthodS*whAT:other!AttACK|METHODS~do@you_KNOW}'

Process finished with exit code 0

