

## Active Information Gathering & Web Traffic Analysis

Target: OWASP Juice Shop

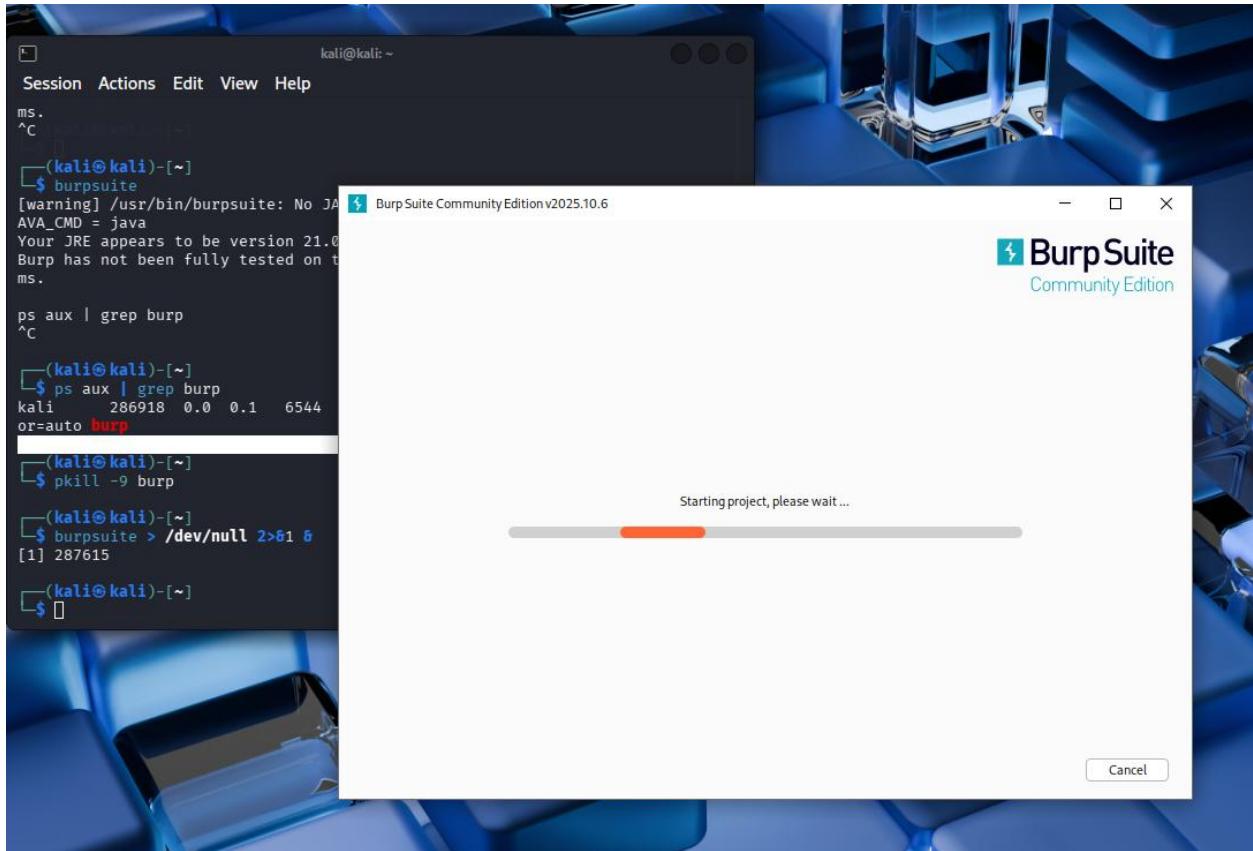
URL: <https://demo.owasp-juice.shop>

Reason for Selection:

OWASP Juice Shop is an intentionally vulnerable web application designed for legal security testing and learning purposes.

**Burp Suite was launched from the Kali Linux terminal to ensure proper integration with the system and browser traffic interception.**

```
(kali㉿kali)-[~]
$ burpsuite
[warning] /usr/bin/burpsuite: No JAVA_CMD set for run_java, falling back to J
AVA_CMD = java
Your JRE appears to be version 21.0.9 from Debian
Burp has not been fully tested on this platform and you may experience problem
ms.
```



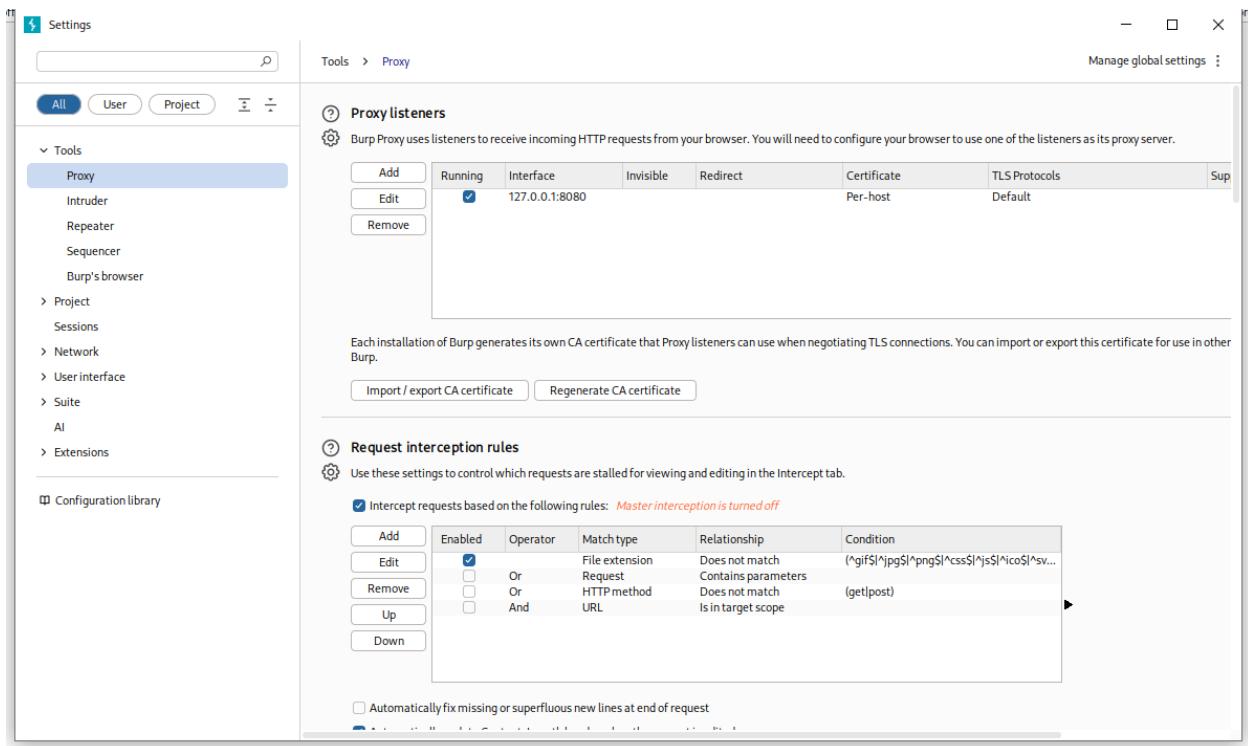


Figure 1 Burp proxy listener active on localhost (127.0.0.1) port 8080, ready to capture traffic from Firefox browser.

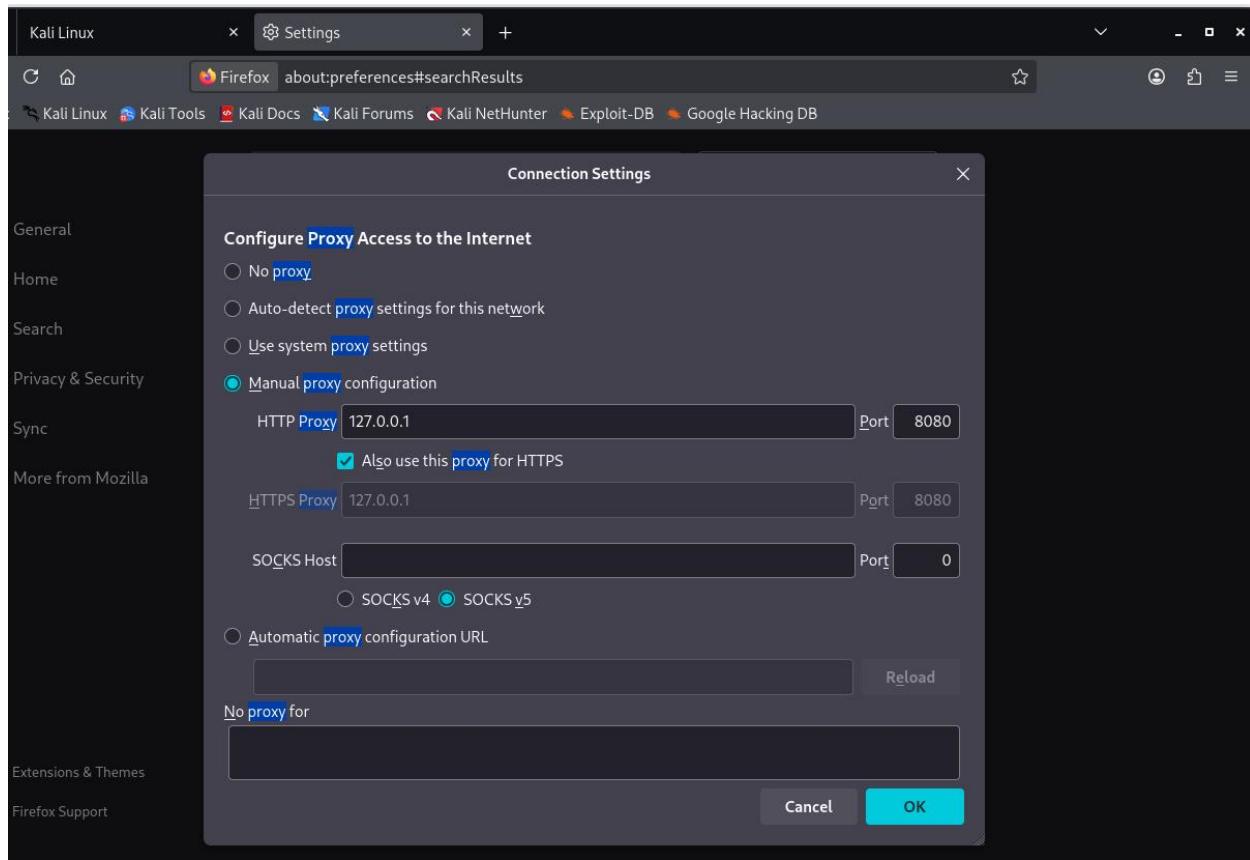


Figure 2 firefox\_proxy\_settings.png

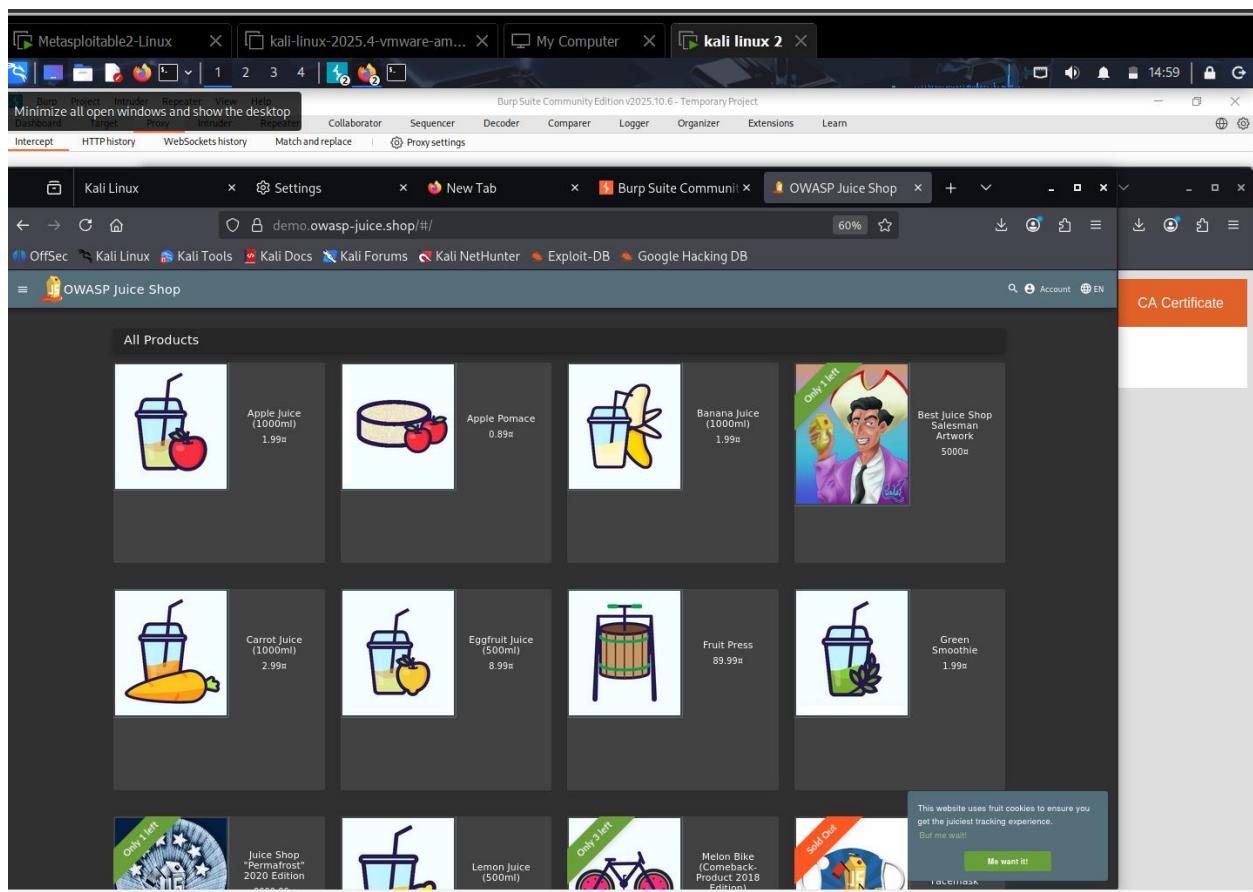


Figure 3 The OWASP Juice Shop website loading properly

Burp Suite Community Edition v2025.10.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS and image content; hiding specific extensions

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
1	https://demo.owasp-juice...	GET	/			200	76007	HTML		OWASP Juice Shop	
2	https://demo.owasp-juice...	GET	/			200	76007	HTML		OWASP Juice Shop	
9	https://demo.owasp-juice...	GET	/assets/i18n/en.json			503	1309	HTML	json	Application Error	
10	https://demo.owasp-juice...	GET	/socket.io/EIO=4&transport=polling...	✓		503	1309	HTML	io/	Application Error	
11	https://demo.owasp-juice...	GET	/rest/admin/application-configura...			503	1309	HTML		Application Error	
12	https://demo.owasp-juice...	GET	/rest/admin/application-version			503	1309	HTML		Application Error	
13	https://demo.owasp-juice...	GET	/api/challenged?name=Score%2e...			503	1289	HTML		Application Error	
14	https://demo.owasp-juice...	GET	/api/challenged?name=Score%2e...	✓		503	1289	HTML		Application Error	✓ 81.169.145.156
15	https://demo.owasp-juice...	GET	/rest/admin/application-version			503	1309	HTML		Application Error	✓ 81.169.145.156
16	https://demo.owasp-juice...	GET	/api/Challenged?name=Score%2e...	✓		503	1289	HTML		Application Error	✓ 81.169.145.156
17	https://demo.owasp-juice...	GET	/rest/admin/application-configura...			503	1289	HTML		Application Error	✓ 81.169.145.156
18	https://demo.owasp-juice...	GET	/rest/admin/application-configura...			503	1309	HTML		Application Error	✓ 81.169.145.156

Toggle your filter on or off  
Quickly compare filtered and unfiltered traffic without resetting your filter.

Learn more Got It

Start response

Burp Suite Community Edition v2025.10.6 - Temporary Project

Applications Dashboard Target Proxy Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS and image content; hiding specific extensions

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
123	https://demo.owasp-juice...	GET	/socket.io/EIO=4&transport=pollin...	✓		200	740	text	io/		
124	https://demo.owasp-juice...	POST	/socket.io/EIO=4&transport=pollin...	✓		200	721	HTML	io/		
125	https://demo.owasp-juice...	GET	/socket.io/EIO=4&transport=pollin...	✓		200	736	text	io/		
126	https://demo.owasp-juice...	GET	/socket.io/EIO=4&transport=pollin...	✓		200	744	text	io/		
127	https://demo.owasp-juice...	POST	/socket.io/EIO=4&transport=pollin...	✓		200	729	HTML	io/		
128	https://demo.owasp-juice...	POST	/socket.io/EIO=4&transport=pollin...	✓		200	721	HTML	io/		
129	https://demo.owasp-juice...	GET	/socket.io/EIO=4&transport=pollin...	✓		200	736	text	io/		
130	https://demo.owasp-juice...	GET	/socket.io/EIO=4&transport=pollin...	✓		200	827	text	io/		✓ 81.169.145.156
131	https://demo.owasp-juice...	POST	/socket.io/EIO=4&transport=pollin...	✓		200	717	HTML	io/		✓ 81.169.145.156
132	https://demo.owasp-juice...	GET	/socket.io/EIO=4&transport=pollin...	✓		200	740	text	io/		✓ 81.169.145.156
133	https://demo.owasp-juice...	POST	/socket.io/EIO=4&transport=pollin...	✓		200	725	HTML	io/		✓ 81.169.145.156
134	https://demo.owasp-juice...	GET	/socket.io/EIO=4&transport=pollin...	✓		200	827	text	io/		✓ 81.169.145.156

Toggle your filter on or off  
Quickly compare filtered and unfiltered traffic without resetting your filter.

Learn more Got It

Start response

Request

Pretty Raw Hex

Response

Pretty Raw Hex Render

Inspector

Request attributes 2

Request query parameters 4

Request body parameters 1

Request cookies 2

Request headers 18

Response headers 10

```

1 POST /socket.io/EIO=4&transport=polling&t=PmGVDb&sid=PyZgYUh05JcYW29ACUN HTTP/2
2 Host: demo.owasp-juice.shop
3 Accept-Language: en; q=0.5
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
5 Accept: /
6 Accept-Language: en-US; en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: text/plain;charset=UTF-8
9 Content-Length: 1
10 Origin: https://demo.owasp-juice.shop
11 Referer: https://demo.owasp-juice.shop
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 3
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
617
618
619
619
620
621
622
623
624
625
626
627
627
628
629
629
630
631
632
633
634
635
635
636
637
637
638
639
639
640
641
642
643
643
644
645
645
646
647
647
648
649
649
650
651
652
653
654
655
655
656
657
657
658
659
659
660
661
662
663
664
665
665
666
667
667
668
669
669
670
671
672
673
674
675
675
676
677
677
678
679
679
680
681
682
683
684
685
685
686
687
687
688
689
689
690
691
692
693
694
695
695
696
697
697
698
699
699
700
701
702
703
704
705
705
706
707
707
708
709
709
710
711
712
713
714
715
715
716
717
717
718
719
719
720
721
722
723
724
725
725
726
727
727
728
729
729
730
731
732
733
734
735
735
736
737
737
738
739
739
740
741
742
743
744
745
745
746
747
747
748
749
749
750
751
752
753
754
755
755
756
757
757
758
759
759
760
761
762
763
764
765
765
766
767
767
768
769
769
770
771
772
773
774
775
775
776
777
777
778
779
779
780
781
782
783
784
785
785
786
787
787
788
789
789
790
791
792
793
794
795
795
796
797
797
798
799
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
819
820
821
821
822
823
823
824
825
825
826
827
827
828
829
829
830
831
832
833
834
835
835
836
837
837
838
839
839
840
841
842
843
844
844
845
846
846
847
848
848
849
849
850
851
852
853
854
855
855
856
857
857
858
859
859
860
861
862
863
864
865
865
866
867
867
868
869
869
870
871
872
873
874
875
875
876
877
877
878
879
879
880
881
882
883
884
885
885
886
887
887
888
889
889
890
891
892
893
894
895
895
896
897
897
898
899
899
900
901
902
903
904
905
905
906
907
907
908
909
909
910
911
912
913
914
915
915
916
917
917
918
919
919
920
921
922
923
924
925
925
926
927
927
928
929
929
930
931
932
933
934
935
935
936
937
937
938
939
939
940
941
942
943
944
945
945
946
947
947
948
949
949
950
951
952
953
954
955
955
956
957
957
958
959
959
960
961
962
963
964
965
965
966
967
967
968
969
969
970
971
972
973
974
975
975
976
977
977
978
979
979
980
981
982
983
984
985
985
986
987
987
988
989
989
990
991
992
993
994
994
995
996
996
997
998
999
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1011
1012
1013
1013
1014
1015
1015
1016
1017
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1025
1026
1027
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1035
1036
1037
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1045
1046
1047
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1055
1056
1057
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1065
1066
1067
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1075
1076
1077
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1085
1086
1087
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1095
1096
1097
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1105
1106
1107
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1115
1116
1117
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1125
1126
1127
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1135
1136
1137
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1145
1146
1147
1147
1148
1149
1149
1150
1151
1152
1153
1154
1155
1155
1156
1157
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1165
1166
1167
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1175
1176
1177
1177
1178
1179
1179
1180
1181
1182
1183
1184
1185
1185
1186
1187
1187
1188
1189
1189
1190
1191
1192
1193
1194
1194
1195
1196
1196
1197
1198
1198
1199
1200
1201
1202
1203
1204
1205
1205
1206
1207
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1215
1216
1217
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1225
1226
1227
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1235
1236
1237
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1245
1246
1247
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1255
1256
1257
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1265
1266
1267
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1275
1276
1277
1277
1278
1279
1279
1280
1281
1282
1283
1284
1285
1285
1286
1287
1287
1288
1289
1289
1290
1291
1292
1293
1294
1294
1295
1296
1296
1297
1298
1298
1299
1300
1301
1302
1303
1304
1304
1305
1306
1306
1307
1308
1308
1309
1310
1311
1312
1313
1314
1314
1315
1316
1316
1317
1318
1318
1319
1320
1321
1322
1323
1324
1324
1325
1326
1326
1327
1328
1328
1329
1330
1331
1332
1333
1334
1334
1335
1336
1336
1337
1338
1338
1339
1340
1341
1342
1343
1344
1344
1345
1346
1346
1347
1348
1348
1349
1350
1351
1352
1353
1354
1354
1355
1356
1356
1357
1358
1358
1359
1360
1361
1362
1363
1364
1364
1365
1366
1366
1367
1368
1368
1369
1370
1371
1372
1373
1374
1374
1375
1376
1376
1377
1378
1378
1379
1380
1381
1382
1383
1384
1384
1385
1386
1386
1387
1388
1388
1389
1390
1391
1392
1393
1394
1394
1395
1396
1396
1397
1398
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
15310
15311
15312
15313
15314
15315
15316
15317
15318
15319
15320
15321
15322
15323
15324
15325
15326
15327
15328
15329
15330
15331
15332
15333
15334
15335
15336
15337
15338
15339
153310
153311
153312
153313
153314
153315
153316
153317
153318
153319
153320
153321
153322
153323
153324
153325
153326
153327
153328
153329
153330
153331
153332
153333
153334
153335
153336
153337
153338
153339
1533310
1533311
1533312
1533313
1533314
1533315
1533316
1533317
1533318
1533319
1533320
1533321
1533322
1533323
1533324
1533325
1533326
1533327
1533328
1533329
1533330
1533331
1533332
1533333
1533334
1533335
1533336
1533337
1533338
1533339
15333310
15333311
15333312
15333313
15333314
15333315
15333316
15333317
15333318
15333319
15333320
15333321
15333322
15333323
15333324
15333325
15333326
15333327
15333328
15333329
15333330
15333331
15333332
15333333
15333334
15333335
15333336
15333337
15333338
15333339
153333310
153333311
153333312
153333313
153333314
153333315
153333316
153333317
153333318
153333319
153333320
153333321
153333322
153333323
153333324
153333325
153333326
153333327
153333328
153333329
153333330
153333331
153333332
153333333
153333334
153333335
153333336
153333337
153333338
153333339
1533333310
1533333311
1533333312
1533333313
1533333314
1533333315
1533333316
1533333317
1533333318
1533333319
1533333320
1533333321
1533333322
1533333323
1533333324
1533333325
1533333326
1533333327
1533333328
1533333329
1533333330
1533333331
1533333332
1533333333
1533333334
1533333335
1533333336
1533333337
1533333338
1533333339
15333333310
15333333311
15333333312
15333333313
1533333
```

Burp Suite Community Edition v2025.10.6 - Temporary Project

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start respon.
223	https://demo.owasp.juice... 224 https://demo.owasp.juice... 225 https://demo.owasp.juice... 226 https://demo.owasp.juice... 227 https://demo.owasp.juice... 228 https://demo.owasp.juice... 229 https://demo.owasp.juice... 230 https://demo.owasp.juice... 231 https://demo.owasp.juice... 232 https://demo.owasp.juice... 233 https://demo.owasp.juice... 234 https://demo.owasp.juice...	GET POST GET GET POST POST GET GET POST GET POST GET POST	/socket.io/?EIO=4&transport=polling /socket.io/?EIO=4&transport=polling /socket.io/?EIO=4&transport=polling /socket.io/?EIO=4&transport=polling /socket.io/?EIO=4&transport=polling /socket.io/?EIO=4&transport=polling /socket.io/?EIO=4&transport=polling /socket.io/?EIO=4&transport=polling /socket.io/?EIO=4&transport=polling /socket.io/?EIO=4&transport=polling /socket.io/?EIO=4&transport=polling /socket.io/?EIO=4&transport=polling		✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	200 200 200 200 200 200 200 200 200 200 200 200	740 721 690 736 721 736 827 717 740 725	text HTML text text text text text text text text text text	io/ io/ io/ io/ io/ io/ io/ io/ io/ io/ io/ io/		✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	81.169.145.156 81.169.145.156 81.169.145.156 81.169.145.156 81.169.145.156 81.169.145.156 81.169.145.156 81.169.145.156 81.169.145.156 81.169.145.156 81.169.145.156		14:58:36 ... 14:59:01 ... 14:59:27 ... 14:59:52 ... 14:59:52 ... 14:59:52 ... 15:00:18 ... 15:00:18 ... 15:00:30 ... 15:00:43 ... 15:00:43 ...	8080 8080 8080 8080 8080 8080 8080 8080 8080 8080 8080 8080	25409 415 25416 384 25380 11940 482 13588 452 1768	

**Request**

Pretty Raw Hex

```
1 GET /socket.io/?EIO=4&transport=polling&t=PmGV05f&sid=PyZpkyUpS1cYWZACUN HTTP/2
2 Host: demo.owasp.juice.shop
3 Cookie: language=en; welcomebanner_status=dissmiss
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://demo.owasp.juice.shop/
9 Sec-Fetch-Dest: empty
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Access-Control-Allow-Origin: http://localhost:4200
3 Content-Length: 1
4 Content-Type: text/plain; charset=UTF-8
5 Date: Fri, 30 Jan 2026 19:59:26 GMT
6 Nel:
{"report_to": "heroku-nel", "response_headers": [{"Via": "3600", "success_fraction": 0.01, "failure_fraction": 0.1}}
7 Reporting-To:
{"group": "heroku-nel", "endpoints": [{"url": "https://nel.herokuapp.com/reports?seOLrawFDduquOp%2FPMmgwOrp1PomcGhFECracyMNxA7kE53D0u0026sid=812dcc77-0bd0-43b1-a5f1-b257503b2959.u0026ts=17698093141"}], "max_age": 3600}
8 Reporting-Endpoints:
heroku-nel="https://nel.herokuapp.com/reports?s=0LrawFXDduquOp%2FPMmgwOrp1PomcGhFECracyMNxA7kE53D0u0026sid=812dcc77-0bd0-43b1-a5f1-b257503b2959&ts=17698093141"
9 Server: Heroku
10 Vary: Origin
11 Via: 1.1 heroku-router
12
13 2
14
```

**Inspector**

Request attributes  
Request query parameters  
Request cookies  
Request headers  
Response headers

Figure 4 GET SS

Burp Suite Community Edition v2025.10.6 - Temporary Project

#	Host	Met...	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response
652	https://analytics.google.com	POST	/g/collect/?=2&tid=G-GGXCHR15...	✓	204	828	text				✓	216.239.34.181			15:37:52 30 ...	8080	169
653	https://www.google-analyt...	POST	/g/collect/?=2&tid=G-7RM05BDG...	✓	204	828	text				✓	142.250.202.46			15:37:52 30 ...	8080	167
654	https://www.google-analyt...	POST	/g/collect/?=2&tid=G-PTKGSY2K...	✓	204	828	text				✓	142.250.202.46			15:37:52 30 ...	8080	208
655	https://bat.bing.com	POST	/action?0=15071104&tmgtm...	✓	204	735					✓	150.171.28.10			MUID=3FP9CB4E...		172
670	https://demo.oswasp.juice...	POST	/socket.io/?EIO=4&transport=poll...	✓	200	725	HTML	io/			✓	81.169.145.156			15:37:52 30 ...	8080	299
689	https://demo.oswasp.juice...	POST	/socket.io/?EIO=4&transport=poll...	✓	200	729	HTML	io/			✓	81.169.145.156			15:38:12 30 ...	8080	480
690	https://demo.oswasp.juice...	POST	/socket.io/?EIO=4&transport=poll...	✓	200	721	HTML	io/			✓	81.169.145.156			15:38:17 30 ...	8080	392
692	https://demo.oswasp.juice...	POST	/socket.io/?EIO=4&transport=poll...	✓	200	721	HTML	io/			✓	81.169.145.156			15:38:37 30 ...	8080	365
695	https://demo.oswasp.juice...	POST	/socket.io/?EIO=4&transport=poll...	✓	200	721	HTML	io/			✓	81.169.145.156			15:38:45 30 ...	8080	418
699	https://demo.oswasp.juice...	POST	/rest/user/login	✓	401	923	HTML				✓	81.169.145.156			15:38:56 30 ...	8080	389
700	https://demo.oswasp.juice...	POST	/socket.io/?EIO=4&transport=poll...	✓	200	725	HTML	io/			✓	81.169.145.156			15:39:02 30 ...	8080	385
704	https://demo.oswasp.juice...	POST	/rest/user/login	✓	401	923	HTML				✓	81.169.145.156			15:39:03 30 ...	8080	402

Request		Response		Notes	
Pretty	Raw	Hex	Render	Pretty	Raw
1	POST /rest/user/login HTTP/2			1	HTTP/2 204 Unauthorized
2	Host: demo.oswasp.juice.shop			2	Access-Control-Allow-Origin: *
3	Cookie: language=en; welcomebanner_status=dismiss; continueCode=zvvo3yQBVApMK9V5Nm2XLQayfwXCT50qJxGe0027nix4kxrnbgl7ZL...			3	Content-Length: 26
4	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0			4	Content-Type: text/html; charset=utf-8
5	Accept: application/json, text/plain, */*			5	Date: Fri, 30 Jan 2024 20:09:03 GMT
6	Accept-Language: en-US;q=0.5			6	Expires: W/1a-ARUjVxK+smzAF3Q0vex2uDSG+3Eus"
7	Accept-Encoding: gzip, deflate, br			7	Feature-Policy: payment 'self';
8	X-User-Email: test@test.com			8	Nel:
9	Content-Type: application/json			9	f'>report_to': 'heroku-nel', >response_headers': {'Via': 'max_age': 3600, >success_fraction': 0.01, >'failure_fraction': 0.1}
10	Content-Length: 52			10	Report-To:
11	Content-Type: application/json			11	f'>heroku-nel', >endpoints': [{>"url": "https://nel.herokuapp.com/report...s=176905545", >'max_age': 3600}]
12	Referer: https://demo.oswasp.juice.shop/			12	Reporting-Endpoints:
13	Sec-Fetch-Dest: empty			13	heroku-nel=>https://nel.herokuapp.com/reports?>s=wA9u1E8L1Rgn0n2FzeUECJSLFq...
14	Sec-Fetch-Mode: cors			14	Server: Heroku
15	Sec-Fetch-Site: same-origin			15	Via: / Access-Encoding
16	Priority: u0			16	Via: / heroku-router
17	Te: trailers			17	X-Content-Type-Options: nosniff
18				18	X-FRAME-Options: SAMEORIGIN
19					X-Recruiting: #/jobs
					19
					Invalid email or password.

*Figure 5 unauthorized access*

The screenshot displays the Burp Suite interface with the following details:

- Network Tab:** Shows a list of captured requests and responses. The requests list includes entries for various URLs like `/rest/user/login`, `/rest/user/logout`, and `/socket.io/4/transport-polling`. The responses pane shows detailed headers and bodies for selected requests, such as the `HTTP/2 200 OK` response for `/rest/user/login`.
- Decoding Tab:** A sidebar showing the current decoding settings.
- Response Tab:** Displays the raw response body for the selected request, which includes JSON data and various HTTP headers.
- Notes Tab:** A sidebar for adding notes to specific items.

The interface is highly customizable with numerous toolbars, status bars, and a comprehensive help section.

*Figure 6 SUCCESSFUL Login*

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace ⚙ Proxy settings

Filter settings: Hiding CSS and image content; hiding specific extensions

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
1022	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	732	text	io/		✓	81.169.145.156			15:46:37 30...
1024	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	736	text	io/		✓	81.169.145.156			15:46:46 30...
1026	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	740	text	io/		✓	81.169.145.156			15:47:02 30...
1027	https://demo.owasp.juice...	GET	/rest/user/whoami			304	810				✓	81.169.145.156			15:47:10 30...
1028	https://demo.owasp.juice...	GET	/rest/products/42/reviews			200	1279	JSON			✓	81.169.145.156			15:47:10 30...
1029	https://demo.owasp.juice...	GET	/rest/products/42/reviews			200	1279	JSON			✓	81.169.145.156			15:47:10 30...
1030	https://demo.owasp.juice...	GET	/rest/products/42/reviews			304	819				✓	81.169.145.156			15:47:11 30...
1032	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	736	text	io/		✓	81.169.145.156			15:47:12 30...
1034	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	740	text	io/		✓	81.169.145.156			15:47:28 30...
1035	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	732	text	io/		✓	81.169.145.156			15:47:37 30...
1038	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	732	text	io/		✓	81.169.145.156			15:47:53 30...
1040	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	736	text	io/		✓	81.169.145.156			15:48:02 30...

Request Response Notes

```

1 GET /rest/user/whoami HTTP/1.1
2 Host: demo.owasp.juice.shop
3 Cookie: language=en; welcomebanner_status=dismiss; continueCode=xE80n25RLx7JDPWp4w6BGmfz; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGFyOSI
eyJpZC16MswidXNLc5hbWU0iIiLCJ1bwFpbG16mFkbWluOgplawnlLNxhmcIiIwicGF
ze3dvcn0i0i1wMTkyMDIzYtDyQ3M6i1MDuNxNyNj1kZjE4YjUwMCisInvbGljoiJzG1
phbisInRlLbhv42Vpva2Ui0i1iwbGFzdxEvZ2lSXAx0i1iLCjcm9mawh1SW1hZ2U0i1j
hc3NlDhvNvChibGjL2ltYWdlcy9lcGxvYWRzL2RlZm1fBHZGlpbiswmcilCJ0b3RwU2v
jcmVOi0i1iwiiaXNBY3RpdmU0iOnRduUsInY2ZGF0ZWR8dC16jIwMjYtMDEtMzAgMjAGMj
cGNDYuMjMSICswMdowMCisInwZGF0ZWR8dC16mVsbtHosImhdC16MtC20TgwNTc4Mn0.awfn5lJ43ZXq2jv
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101
5 Firefox/140.0
6 Accept: application/json, text/plain, */*
7 Accept-Language: en-US;en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Authorization: Bearer [REDACTED]
10 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGFyOSI
eyJpZC16MswidXNLc5hbWU0iIiLCJ1bwFpbG16mFkbWluOgplawnlLNxhmcIiIwicGF
ze3dvcn0i0i1wMTkyMDIzYtDyQ3M6i1MDuNxNyNj1kZjE4YjUwMCisInvbGljoiJzG1
phbisInRlLbhv42Vpva2Ui0i1iwbGFzdxEvZ2lSXAx0i1iLCjcm9mawh1SW1hZ2U0i1j
hc3NlDhvNvChibGjL2ltYWdlcy9lcGxvYWRzL2RlZm1fBHZGlpbiswmcilCJ0b3RwU2v
11 s=Opfse0MN9bchza9KiszZTP%2FvpMD10p900BXRes%3D&u0026sid=812dcc77-0
12 b0d-43b1-a5f1-b25750382959,u0026ts=1769806030";max_age:3600
13 Reporting-Endpoints: heroku.com: "https://heroku.com/reports?s=Opfse0MN9bchza9KiszZTP%2FvpMD10p900BXRes%3D&id=812dcc77-0b0d-43b1-a5f1-b25750382959&t=1769806030"
14 Nel: {"group": "heroku-nel", "endpoints": [{"url": "https://nel.herokuapp.com/report?g=s=Opfse0MN9bchza9KiszZTP%2FvpMD10p900BXRes%3D&id=812dcc77-0b0d-43b1-a5f1-b25750382959,u0026ts=1769806030"}, "max_age": 3600}
15 Report-To: {"group": "heroku-nel", "endpoints": [{"url": "https://nel.herokuapp.com/report?g=s=Opfse0MN9bchza9KiszZTP%2FvpMD10p900BXRes%3D&id=812dcc77-0b0d-43b1-a5f1-b25750382959,u0026ts=1769806030"}]

```

Figure 7 session persistence

Filter settings: Hiding CSS and image content; hiding specific extensions

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	
1022	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	732	text	io/		✓	81.169.145.156			
1024	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	736	text	io/		✓	81.169.145.156			
1026	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	740	text	io/		✓	81.169.145.156			
1027	https://demo.owasp.juice...	GET	/rest/user/whoami			304	810				✓	81.169.145.156			
1028	https://demo.owasp.juice...	GET	/rest/products/42/reviews			200	1279	JSON			✓	81.169.145.156			
1029	https://demo.owasp.juice...	GET	/rest/products/42/reviews			200	1279	JSON			✓	81.169.145.156			
1030	https://demo.owasp.juice...	GET	/rest/products/42/reviews			304	819				✓	81.169.145.156			
1032	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	736	text	io/		✓	81.169.145.156			
1034	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	740	text	io/		✓	81.169.145.156			
1035	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	732	text	io/		✓	81.169.145.156			
1038	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	732	text	io/		✓	81.169.145.156			
1040	https://demo.owasp.juice...	GET	/socket.io/?EIO=4&transport=polling	✓		200	736	text	io/		✓	81.169.145.156			

Request Response Notes

```

1 GET /rest/products/42/reviews HTTP/1.1
2 Host: demo.owasp.juice.shop
3 Cookie: language=en; welcomebanner_status=dismiss; continueCode=xE80n25RLx7JDPWp4w6BGmfz; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGFyOSI
eyJpZC16MswidXNLc5hbWU0iIiLCJ1bwFpbG16mFkbWluOgplawnlLNxhmcIiIwicGF
ze3dvcn0i0i1wMTkyMDIzYtDyQ3M6i1MDuNxNyNj1kZjE4YjUwMCisInvbGljoiJzG1
phbisInRlLbhv42Vpva2Ui0i1iwbGFzdxEvZ2lSXAx0i1iLCjcm9mawh1SW1hZ2U0i1j
hc3NlDhvNvChibGjL2ltYWdlcy9lcGxvYWRzL2RlZm1fBHZGlpbiswmcilCJ0b3RwU2v
jcmVOi0i1iwiiaXNBY3RpdmU0iOnRduUsInY2ZGF0ZWR8dC16jIwMjYtMDEtMzAgMjAGMj
cGNDYuMjMSICswMdowMCisInwZGF0ZWR8dC16mVsbtHosImhdC16MtC20TgwNTc4Mn0.awfn5lJ43ZXq2jv
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101
5 Firefox/140.0
6 Accept: application/json, text/plain, */*
7 Accept-Language: en-US;en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Authorization: Bearer [REDACTED]
10 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGFyOSI
eyJpZC16MswidXNLc5hbWU0iIiLCJ1bwFpbG16mFkbWluOgplawnlLNxhmcIiIwicGF
ze3dvcn0i0i1wMTkyMDIzYtDyQ3M6i1MDuNxNyNj1kZjE4YjUwMCisInvbGljoiJzG1
phbisInRlLbhv42Vpva2Ui0i1iwbGFzdxEvZ2lSXAx0i1iLCjcm9mawh1SW1hZ2U0i1j
hc3NlDhvNvChibGjL2ltYWdlcy9lcGxvYWRzL2RlZm1fBHZGlpbiswmcilCJ0b3RwU2v
11 s=Opfse0MN9bchza9KiszZTP%2FvpMD10p900BXRes%3D&u0026sid=812dcc77-0
12 b0d-43b1-a5f1-b25750382959,u0026ts=1769806030";max_age:3600
13 Reporting-Endpoints: heroku.com: "https://nel.herokuapp.com/reports?s=Opfse0MN9bchza9KiszZTP%2FvpMD10p900BXRes%3D&id=812dcc77-0b0d-43b1-a5f1-b25750382959&t=1769806030"
14 Nel: {"group": "heroku-nel", "endpoints": [{"url": "https://nel.herokuapp.com/report?g=s=Opfse0MN9bchza9KiszZTP%2FvpMD10p900BXRes%3D&id=812dcc77-0b0d-43b1-a5f1-b25750382959,u0026ts=1769806030"}, "max_age": 3600}
15 Report-To: {"group": "heroku-nel", "endpoints": [{"url": "https://nel.herokuapp.com/report?g=s=Opfse0MN9bchza9KiszZTP%2FvpMD10p900BXRes%3D&id=812dcc77-0b0d-43b1-a5f1-b25750382959,u0026ts=1769806030"}]

```

Figure 8 cookies

Cookie attributes were not explicitly visible in captured responses; however, secure session handling was observed via token-based authentication

#	Host	Met...	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
003	https://demo.owasp-juice... GET	/api/Challenges/?name=Score%2...	✓			200	1341	JSON			✓	81.169.145.156			15:46
005	https://demo.owasp-juice... GET	/api/Quantity/				304	812				✓	81.169.145.156			15:46
006	https://demo.owasp-juice... GET	/rest/products/search?q=	✓			304	812				✓	81.169.145.156			15:46
008	https://demo.owasp-juice... GET	/socket.io/?EIO=4&transport=polling	✓			200	768	text	io/		✓	81.169.145.156			15:46
009	https://demo.owasp-juice... GET	/socket.io/?EIO=4&transport=websocket	✓			400	787	JSON	io/		✓	81.169.145.156			15:46
022	https://demo.owasp-juice... GET	/socket.io/?EIO=4&transport=polling	✓			200	732	text	io/		✓	81.169.145.156			15:46
024	https://demo.owasp-juice... GET	/socket.io/?EIO=4&transport=polling	✓			200	736	text	io/		✓	81.169.145.156			15:46
026	https://demo.owasp-juice... GET	/socket.io/?EIO=4&transport=polling	✓			200	740	text	io/		✓	81.169.145.156			15:47
027	https://demo.owasp-juice... GET	/rest/user/whoami				304	810				✓	81.169.145.156			15:47
028	https://demo.owasp-juice... GET	/rest/products/42/reviews				200	1279	JSON			✓	81.169.145.156			15:47
029	https://demo.owasp-juice... GET	/rest/products/42/reviews				200	1279	JSON			✓	81.169.145.156			15:47
030	https://demo.owasp-juice... GET	/rest/products/42/reviews				304	819				✓	81.169.145.156			15:47

Figure 9 few status codes column

## Conclusion

This assignment demonstrated active information gathering and web traffic analysis using **Burp Suite** on the **OWASP Juice Shop** application. HTTP/HTTPS requests and responses were captured to analyze headers, cookies, session tokens, and status codes. Login behavior and session persistence were successfully observed using token-based authentication. The exercise improved practical understanding of web communication and ethical security testing.