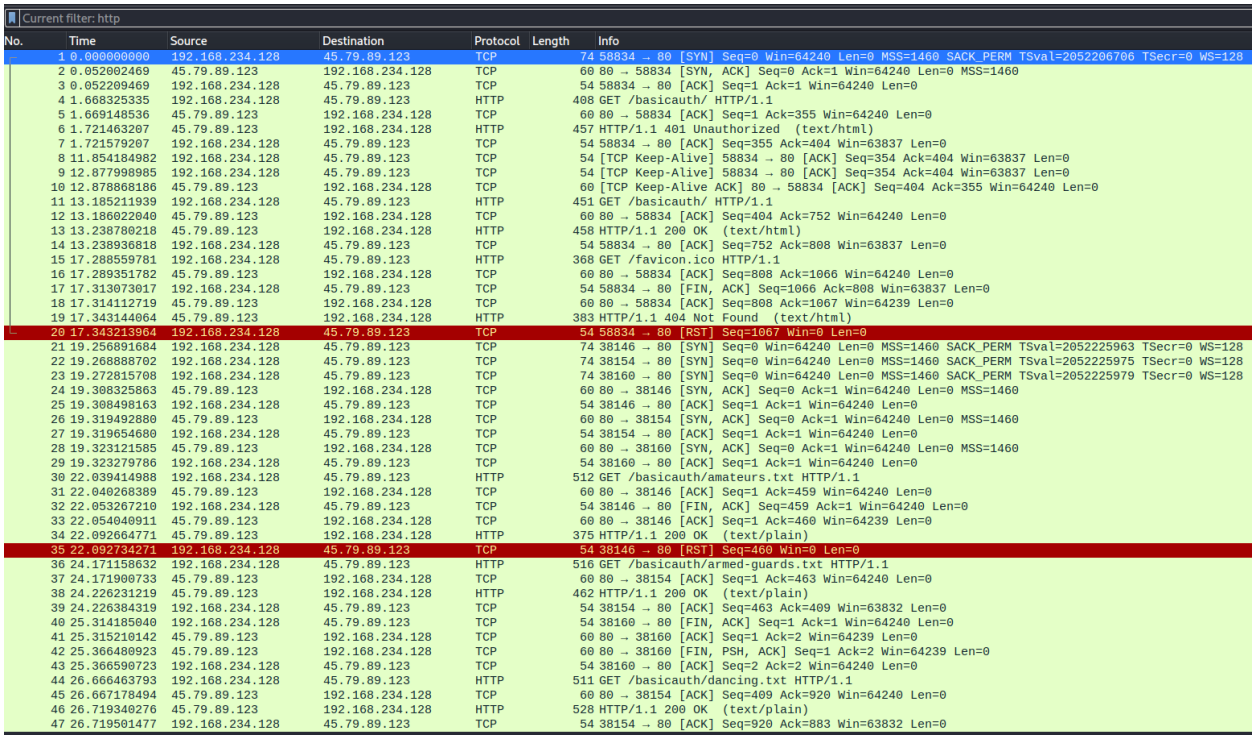
Basic-Authentication

Kyle Machalec



Current filter: http

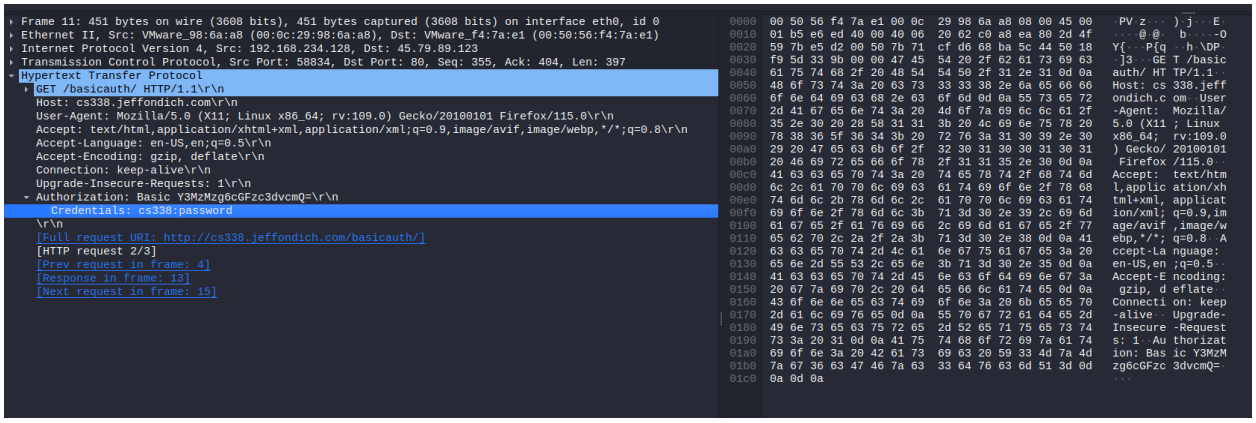
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 192.168.234.128 | 45.79.89.123 | TCP | 74 | 58834 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2052206706 TSecr=0 WS=128 |
| 2 | 0.052002469 | 45.79.89.123 | 192.168.234.128 | TCP | 60 | 80 → 58834 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 3 | 0.052209469 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | 58834 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 4 | 1.668325335 | 192.168.234.128 | 45.79.89.123 | HTTP | 408 | GET /basicauth/ HTTP/1.1 |
| 5 | 1.669148536 | 45.79.89.123 | 192.168.234.128 | TCP | 60 | 80 → 58834 [ACK] Seq=1 Ack=355 Win=64240 Len=0 |
| 6 | 1.721463207 | 45.79.89.123 | 192.168.234.128 | HTTP | 457 | HTTP/1.1 401 Unauthorized (text/html) |
| 7 | 1.721579207 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | 58834 → 80 [ACK] Seq=355 Ack=404 Win=63837 Len=0 |
| 8 | 11.854184982 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | [TCP Keep-Alive] 58834 → 80 [ACK] Seq=354 Ack=404 Win=63837 Len=0 |
| 9 | 12.877998985 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | [TCP Keep-Alive] 58834 → 80 [ACK] Seq=354 Ack=404 Win=63837 Len=0 |
| 10 | 12.878868186 | 45.79.89.123 | 192.168.234.128 | TCP | 60 | [TCP Keep-Alive ACK] 80 → 58834 [ACK] Seq=404 Ack=355 Win=64240 Len=0 |
| 11 | 13.185211939 | 192.168.234.128 | 45.79.89.123 | HTTP | 451 | GET /basicauth/ HTTP/1.1 |
| 12 | 13.186022040 | 45.79.89.123 | 192.168.234.128 | TCP | 60 | 80 → 58834 [ACK] Seq=404 Ack=752 Win=64240 Len=0 |
| 13 | 13.238780218 | 45.79.89.123 | 192.168.234.128 | HTTP | 458 | HTTP/1.1 200 OK (text/html) |
| 14 | 13.238936818 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | 58834 → 80 [ACK] Seq=752 Ack=808 Win=63837 Len=0 |
| 15 | 17.288559781 | 192.168.234.128 | 45.79.89.123 | HTTP | 368 | GET /favicon.ico HTTP/1.1 |
| 16 | 17.289351782 | 45.79.89.123 | 192.168.234.128 | TCP | 60 | 80 → 58834 [ACK] Seq=808 Ack=1066 Win=64240 Len=0 |
| 17 | 17.313073017 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | 58834 → 80 [FIN, ACK] Seq=1066 Ack=808 Win=63837 Len=0 |
| 18 | 17.314112719 | 45.79.89.123 | 192.168.234.128 | TCP | 60 | 80 → 58834 [ACK] Seq=808 Ack=1067 Win=64239 Len=0 |
| 19 | 17.343144064 | 45.79.89.123 | 192.168.234.128 | HTTP | 383 | HTTP/1.1 404 Not Found (text/html) |
| 20 | 17.343213964 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | 58834 → 80 [RST] Seq=1067 Win=0 Len=0 |
| 21 | 19.256891684 | 192.168.234.128 | 45.79.89.123 | TCP | 74 | 38146 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2052225963 TSecr=0 WS=128 |
| 22 | 19.268888702 | 192.168.234.128 | 45.79.89.123 | TCP | 74 | 38154 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2052225975 TSecr=0 WS=128 |
| 23 | 19.272815708 | 192.168.234.128 | 45.79.89.123 | TCP | 74 | 38160 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2052225979 TSecr=0 WS=128 |
| 24 | 19.308325863 | 45.79.89.123 | 192.168.234.128 | TCP | 60 | 80 → 38146 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 25 | 19.308498163 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | 38146 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 26 | 19.319492880 | 45.79.89.123 | 192.168.234.128 | TCP | 60 | 80 → 38154 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 27 | 19.319654680 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | 38154 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 28 | 19.323121585 | 45.79.89.123 | 192.168.234.128 | TCP | 60 | 80 → 38160 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 29 | 19.323279786 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | 38160 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 30 | 22.039414988 | 192.168.234.128 | 45.79.89.123 | HTTP | 512 | GET /basicauth/amateurs.txt HTTP/1.1 |
| 31 | 22.040268389 | 45.79.89.123 | 192.168.234.128 | TCP | 60 | 80 → 38146 [ACK] Seq=1 Ack=459 Win=64240 Len=0 |
| 32 | 22.053267210 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | 38146 → 80 [FIN, ACK] Seq=459 Ack=1 Win=64240 Len=0 |
| 33 | 22.054040911 | 45.79.89.123 | 192.168.234.128 | TCP | 60 | 80 → 38146 [ACK] Seq=1 Ack=460 Win=64239 Len=0 |
| 34 | 22.092664771 | 45.79.89.123 | 192.168.234.128 | HTTP | 375 | HTTP/1.1 200 OK (text/plain) |
| 35 | 22.092734271 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | 38146 → 80 [RST] Seq=460 Win=0 Len=0 |
| 36 | 24.171158632 | 192.168.234.128 | 45.79.89.123 | HTTP | 516 | GET /basicauth/armed-guards.txt HTTP/1.1 |
| 37 | 24.171900733 | 45.79.89.123 | 192.168.234.128 | TCP | 60 | 80 → 38154 [ACK] Seq=1 Ack=463 Win=64240 Len=0 |
| 38 | 24.226231219 | 45.79.89.123 | 192.168.234.128 | HTTP | 462 | HTTP/1.1 200 OK (text/plain) |
| 39 | 24.226384319 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | 38154 → 80 [ACK] Seq=463 Ack=409 Win=63832 Len=0 |
| 40 | 25.314185040 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | 38160 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 41 | 25.315210142 | 45.79.89.123 | 192.168.234.128 | TCP | 60 | 80 → 38160 [ACK] Seq=1 Ack=2 Win=64239 Len=0 |
| 42 | 25.366480923 | 45.79.89.123 | 192.168.234.128 | TCP | 60 | 80 → 38160 [FIN, PSH, ACK] Seq=1 Ack=2 Win=64239 Len=0 |
| 43 | 25.366590723 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | 38160 → 80 [ACK] Seq=2 Ack=2 Win=64240 Len=0 |
| 44 | 26.666463793 | 192.168.234.128 | 45.79.89.123 | HTTP | 511 | GET /basicauth/dancing.txt HTTP/1.1 |
| 45 | 26.667178494 | 45.79.89.123 | 192.168.234.128 | TCP | 60 | 80 → 38154 [ACK] Seq=409 Ack=920 Win=64240 Len=0 |
| 46 | 26.719340276 | 45.79.89.123 | 192.168.234.128 | HTTP | 528 | HTTP/1.1 200 OK (text/plain) |
| 47 | 26.719501477 | 192.168.234.128 | 45.79.89.123 | TCP | 54 | 38154 → 80 [ACK] Seq=920 Ack=883 Win=63832 Len=0 |

Above is the list of all frames recorded when visiting the website http://cs338.jeffondich.com/basicauth/.

The first 3 frames make up the TCP handshake, which includes an initial [SYN] request, followed by the server responding with [SYN, ACK], and ending with the client sending [ACK].

Frame 4 is where the client requests access to the page with “GET /basicauth/ HTTP/1.1”. The server acknowledges the client’s request in frame 5 and challenges the client’s access to the page with “Unauthorized (text/html)” in frame 6, which the client acknowledges in frame 7. Before a username and password is given, the client requests to keep the TCP connection active in frames 8 and 9, to which the server acknowledges in frame 10.

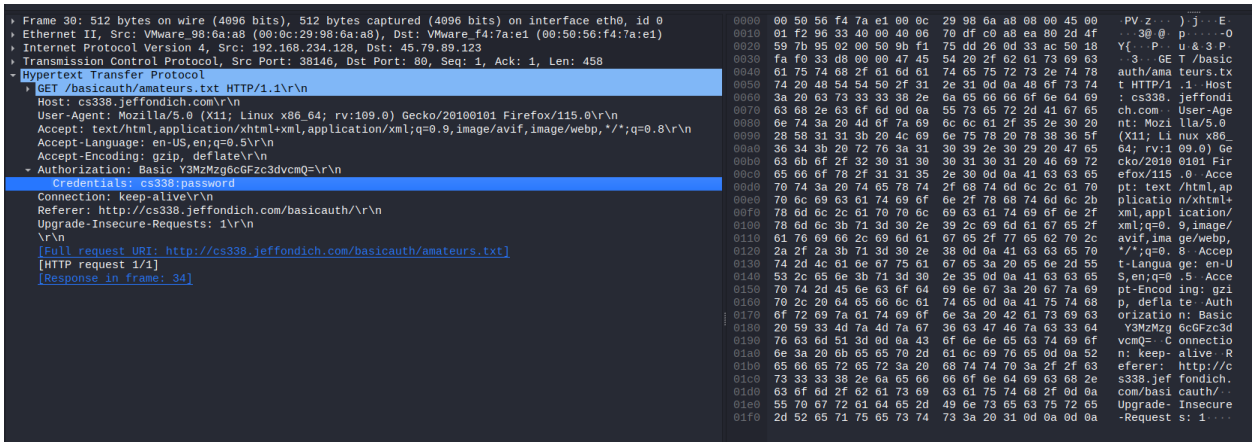
At this point, the user (me) finally finished typing in the username and password, pressing “sign in". As a result, the client once again requests the page from the server in frame 11 – this time with the proper credentials.




As can be seen in the image above, the username and password are found under the “Authorization” header. Although they are encoded in base64 (not encrypted because no key was used), Wireshark was able to figure out that “Y3MzMzg6cGFzc3dvcmQ=” can be read as plain text, revealing the entered credentials. The fact that the credentials are encoded using base64 in the format *username:password* matches my expectations from the HTTP Basic Authentication’s documentation. Base64 encoding is described in RFC 4648, Section 4 (https://datatracker.ietf.org/doc/html/rfc4648#section-4). If a malicious third party were able to intercept this HTTP request, they would have no trouble gaining the information needed to access the super secret files on the page.

Once the correct credentials are sent, either by the intended user or the malicious third party, the server responds with [ACK], followed by OK (text/html). This means that the server is satisfied with the authentication of the client, and the client is now free to access the page’s contents.

The rest of the frames are standard TCP and HTTP communication. I was able to access all 3 files on the page, such as armed-guards.txt, and soak up all the wisdom stored inside. As shown below, any HTTP request from the client for any of the 3 files contains the username and password under the same “Authorization” header, so a malicious third party could gain access to the page by intercepting any of these requests as well.


Frame 30: 512 bytes on wire (4096 bits), 512 bytes captured (4096 bits) on interface eth0, id 0
Ethernet II, Src: VMware_98:6a:a8 (00:0c:29:98:6a:a8), Dst: VMware_f4:7a:e1 (00:50:56:f4:7a:e1)
Internet Protocol Version 4, Src: 192.168.234.128, Dst: 45.79.89.123
Transmission Control Protocol, Src Port: 38146, Dst Port: 80, Seq: 1, Ack: 1, Len: 458
Hypertext Transfer Protocol
GET /basicauth/amateurs.txt HTTP/1.1\r\n
Host: cs338.jeffondich.com\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Authorization: Basic Y3MzMzg6cGFzc3dvcmQ=\r\n
Credentials: cs338:password
Connection: keep-alive\r\n
Referer: http://cs338.jeffondich.com/basicauth/\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://cs338.jeffondich.com/basicauth/amateurs.txt]
[HTTP request 1/1]
[Response in frame: 34]
0000 00 50 56 f4 7a e1 00 0c 29 98 6a a8 08 00 45 00
0010 01 f2 96 33 40 00 40 06 70 df c0 a8 ea 80 2d 4f
0020 59 7b 95 02 00 50 9b f1 75 dd 26 0d 33 ac 50 18
0030 fa f0 33 d8 00 00 47 45 54 20 2f 62 61 73 69 63
0040 61 75 74 68 2f 61 6d 61 74 65 75 72 73 2e 74 78
0050 74 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74
0060 3a 20 63 73 33 33 38 2e 6a 65 66 66 6f 6e 64 69
0070 63 68 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65
0080 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20
0090 28 58 31 31 3b 20 4c 69 6e 75 78 20 78 38 36 5f
00a0 36 34 3b 20 72 76 3a 31 30 39 2e 30 29 20 47 65
00b0 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72
00c0 65 66 6f 78 2f 31 31 35 2e 30 0d 0a 41 63 63 65
00d0 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70
00e0 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b
00f0 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f
0100 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f
0110 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c
0120 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70
0130 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55
0140 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65
0150 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69
0160 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 75 74 68
0170 6f 72 69 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63
0180 20 59 33 4d 7a 4d 7a 67 36 63 47 46 7a 63 33 64
0190 76 63 6d 51 3d 0d 0a 43 6f 6e 6e 65 63 74 69 6f
01a0 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 52
01b0 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 63
01c0 73 33 33 38 2e 6a 65 66 66 6f 6e 64 69 63 68 2e
01d0 63 6f 6d 2f 62 61 73 69 63 61 75 74 68 2f 0d 0a
01e0 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65
01f0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 0d 0a