

Devin Dennis - HTTP's Basic Authentication: A Story

There once was a cs student trying to break into Jeff's website. Little did he know that he had left the username and password on a sticky note on his desk. The student found it and logged in. The student attempted to determine how he had gained access to the site.

I recorded all the traffic from logging on Wireshark and Burp Suite to see the HTTP and TCP requests being sent.

First, I looked at the Wireshark input to see what was going on

1	0.000000000	10.0.2.15	172.233.221.124	TCP	74	45152 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3547667222 TSecr=0 WS=128
2	0.021528864	172.233.221.124	10.0.2.15	TCP	60	80 → 45152 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
3	0.021598411	10.0.2.15	172.233.221.124	TCP	54	45152 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.024422593	10.0.2.15	172.233.221.124	HTTP	493	GET /basicauth/ HTTP/1.1
5	0.024907259	172.233.221.124	10.0.2.15	TCP	60	80 → 45152 [ACK] Seq=1 Ack=440 Win=65535 Len=0
6	0.044640201	172.233.221.124	10.0.2.15	HTTP	859	HTTP/1.1 401 Unauthorized (text/html)
7	0.044695764	10.0.2.15	172.233.221.124	TCP	54	45152 → 80 [ACK] Seq=440 Ack=800 Win=63435 Len=0
8	21.100318705	10.0.2.15	172.233.221.124	TCP	74	58438 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3547688322 TSecr=0 WS=128
9	21.116851498	172.233.221.124	10.0.2.15	TCP	60	80 → 58438 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
10	21.116920140	10.0.2.15	172.233.221.124	TCP	54	58438 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
11	21.120901221	10.0.2.15	172.233.221.124	HTTP	562	GET /basicauth/ HTTP/1.1
12	21.121536162	172.233.221.124	10.0.2.15	TCP	60	80 → 58438 [ACK] Seq=1 Ack=509 Win=65535 Len=0
13	21.140195661	172.233.221.124	10.0.2.15	HTTP	458	HTTP/1.1 200 OK (text/html)
14	21.140278097	10.0.2.15	172.233.221.124	TCP	54	58438 → 80 [ACK] Seq=509 Ack=405 Win=63036 Len=0
15	26.182383260	172.233.221.124	10.0.2.15	TLSv1.2	78	Application Data
16	26.182383704	172.233.221.124	10.0.2.15	TCP	60	443 → 39974 [FIN, ACK] Seq=25 Ack=1 Win=65535 Len=0
17	26.182417278	10.0.2.15	172.233.221.124	TCP	54	39974 → 443 [ACK] Seq=1 Ack=25 Win=65535 Len=0
18	26.226708138	10.0.2.15	172.233.221.124	TCP	54	39974 → 443 [ACK] Seq=1 Ack=26 Win=65535 Len=0

I see that an initial TCP connection was set up with the server. The browser then tried to make an HTTP GET request. Here's is the request:

```
▶ Frame 4: 493 bytes on wire (3944 bits), 493 bytes captured (3944 bits) on interface eth0, id
▼ Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
  ▶ Destination: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
  ▶ Source: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)
    Type: IPv4 (0x0800)
    [Stream index: 0]
  ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.233.221.124
  ▶ Transmission Control Protocol, Src Port: 45152, Dst Port: 80, Seq: 1, Ack: 1, Len: 439
  ▼ Hypertext Transfer Protocol
    ▶ GET /basicauth/ HTTP/1.1\r\n
      Host: cs338.jeffondich.com\r\n
      Accept-Language: en-US,en;q=0.9\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
      Accept-Encoding: gzip, deflate, br\r\n
      Connection: keep-alive\r\n
      \r\n
      [Response in frame: 6]
      [Full request URI: http://cs338.jeffondich.com/basicauth/]
```

The server sent back a response saying that you are not authorized to see this page with a HTTP/1.1 401 Unauthorized

```
▶ Frame 6: 859 bytes on wire (6872 bits), 859 bytes captured (6872 bits) on interface eth0, i
▼ Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)
  ▶ Destination: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)
  ▶ Source: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
    Type: IPv4 (0x0800)
    [Stream index: 0]
  ▶ Internet Protocol Version 4, Src: 172.233.221.124, Dst: 10.0.2.15
  ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 45152, Seq: 1, Ack: 440, Len: 805
  ▼ Hypertext Transfer Protocol
    ▶ HTTP/1.1 401 Unauthorized\r\n
      Server: nginx/1.18.0 (Ubuntu)\r\n
      Date: Thu, 25 Sep 2025 02:39:22 GMT\r\n
      Content-Type: text/html\r\n
      Content-Length: 590\r\n
      Connection: keep-alive\r\n
      WWW-Authenticate: Basic realm="Protected Area"\r\n
      \r\n
      [Request in frame: 4]
      [Time since request: 0.020217698 seconds]
      [Request URI: /basicauth/]
      [Full request URI: http://cs338.jeffondich.com/basicauth/]
```

This is when the browser prompts the user to enter the username and password. When I did so, it sent this HTTP request:

```
▶ Frame 11: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface eth0, i
▼ Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
  ▶ Destination: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
  ▶ Source: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)
    Type: IPv4 (0x0800)
    [Stream index: 0]
  ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.233.221.124
  ▶ Transmission Control Protocol, Src Port: 58438, Dst Port: 80, Seq: 1, Ack: 1, Len: 508
  ▼ Hypertext Transfer Protocol
    ▶ GET /basicauth/ HTTP/1.1\r\n
      Host: cs338.jeffondich.com\r\n
      Cache-Control: max-age=0\r\n
      Authorization: Basic Y3MzMzg6cGFzc3dvcmQ=\r\n
      Accept-Language: en-US,en;q=0.9\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome.
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image.
      Accept-Encoding: gzip, deflate, br\r\n
      Connection: keep-alive\r\n
      \r\n
      [Response in frame: 12]
```

This time, the GET request had the Authorization header inside the payload. But the confusing part is why it's just a bunch of characters. I figured out that it was in base64 and decoded it:

```
kali@kali: ~
Session Actions Edit View Help
(kali@kali)-[~]
$ echo "Y3MzMzg6cGFzc3dvcmQ=" | base64 -d
cs338:password
(kali@kali)-[~]
$
```

```

> Frame 13: 458 bytes on wire (3664 bits), 458 bytes captured (3664 bits) on interface eth0, id 0
> Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)
  > Destination: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)
  > Source: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 172.233.221.124, Dst: 10.0.2.15
> Transmission Control Protocol, Src Port: 80, Dst Port: 58438, Seq: 1, Ack: 509, Len: 404
> Hypertext Transfer Protocol, has 2 chunks (including last chunk)
  > HTTP/1.1 200 OK\r\n
    Server: nginx/1.18.0 (Ubuntu)\r\n
    Date: Thu, 25 Sep 2025 02:39:43 GMT\r\n
    Content-Type: text/html\r\n
    Transfer-Encoding: chunked\r\n
    Connection: keep-alive\r\n
    Content-Encoding: gzip\r\n
    \r\n
    [Request in frame: 11]
    [Time since request: 0.019294440 seconds]
    [Request URI: /basicauth/]
    [Full request URI: http://cs338.jeffondich.com/basicauth/]
  > HTTP chunked response
    Content-encoded entity body (gzip): 205 bytes -> 509 bytes
    File Data: 509 bytes
> Line-based text data: text/html (9 lines)
  <html>\r\n
  <head><title>Index of /basicauth/</title></head>\r\n
  <body>\r\n
  <h1>Index of /basicauth/</h1><hr><pre><a href="..">../</a>\r\n
  <a href="amateurs.txt">amateurs.txt</a>
  <a href="armed-guards.txt">armed-guards.txt</a>
  <a href="dancing.txt">dancing.txt</a>
  </pre><hr></body>\r\n
  </html>\r\n

```

Time

Type

Direction

Method

URL

21:59:51

24 S...

HTTP

→ Request

GET

http://cs338.jeffondich.com/basicauth/armed-guards.txt

Request

Pretty

Raw

Hex

1

GET /basicauth/armed-guards.txt HTTP/1.1

2

Host: cs338.jeffondich.com

3

Authorization: Basic Y3MzMzG6cFzc3dvcMq=

4

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

5

Upgrade-Insecure-Requests: 1

6

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/

7

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/

8

Referer: http://cs338.jeffondich.com/basicauth/

9

Accept-Encoding: gzip, deflate, br

10

Connection: keep-alive

11

12

←

→

×

Not secure

cs338.jeffondich.com/basicauth/

☆

🔄

🔍

🔒 Incognito

⋮

Index of /basicauth/

../		
amateurs.txt	04-Apr-2022 14:10	75
armed-guards.txt	04-Apr-2022 14:10	161
dancing.txt	04-Apr-2022 14:10	227

Hehehee, I have all Jeff's secrets.