The chain of events starts with a query from the client to the server, requesting the http://cs338.jeffondich.com/basicauth/ page. The server replies with a status 401, unauthorized access, and requests authorization. Following that, the user inputs the information, and sends out a repeated query to the server, asking for the same page but also containing an authorization header, which is followed by a cryptographic hash 20 characters long. The response to that is the full page as expected if there was no authentication required. That is what burp suite gives as a general overview.

The status 401 reply:

```
HTTP/1.1 401 Unauthorized
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 24 Sep 2024 19:32:02 GMT
Content-Type: text/html
Content-Length: 590
Connection: keep-alive
WWW-Authenticate: Basic realm="Protected Area"

<html>
<head><title>401 Authorization Required</title></head>
<body>
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.18.0 (Ubuntu)</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

The Get request with authorization:

```
GET /basicauth/ HTTP/1.1
Host: cs338.jeffondich.com
Cache-Control: max-age=0
Authorization: Basic Y3MzMzg6cGFzc3dvcmQ=
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/126.0.6478.127 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
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Wireshark shows a slightly different story. A tcp handshake, followed by my computer trying to set up a TLS agreement automatically. The server responds, but since its http instead of https like my computer wants, mine tells it it needs to change cipher data. The server responds, with what I assume is a ‘no i don’t want to’ because nothing afterwards is encoded in TLS. They acknowledge and finish that discussion. They then have to sync up because something happened, but my computer then requests the page.

```
24	0.252409387	192.168.163.128	172.233.221.124	HTTP	416	GET /basicauth/ HTTP/1.1
```

The server then checks for the page, finds it is in a protected area, and responds with a 401 status unauthorized access response header.

```
30	0.293701168	172.233.221.124	192.168.163.128	HTTP	457	HTTP/1.1 401 Unauthorized  (text/html)
```

I then enter in the username and password, and the computer sends another get request for the page. This one also includes some information to get the necessary access: the authorization username, and the password (password).

```
4	0.095439340	192.168.163.128	172.233.221.124	HTTP	459	GET /basicauth/ HTTP/1.1
```

The authorization header:

```
  Authorization: Basic Y3MzMzg6cGFzc3dvcmQ=\r\n
     Credentials: cs338:password
  \r\n
```

The credentials are passed from the computer to the server as plain text.

The credentials:

```
63 73 33 33 38 3a 70 61 73 73 77 6f 72 64
```

Converted to text, that’s just cs338:password, or username:password.