

Basic-Auth

- Followed the instructions; this is what Burp Proxy shows after the interaction.

1	http://cs338.jeffondich.com	GET	/basicauth/	401	805	HTML	401 Authorization Required
2	http://cs338.jeffondich.com	GET	/basicauth/	200	666	HTML	Index of /basicauth/
3	http://cs338.jeffondich.com	GET	/favicon.ico	404	728	HTML	404 Not Found

Wireshark more in-depth view of queries + responses

68	5.359582064	10.0.2.15	172.233.221.124	HTTP	416	GET /basicauth/ HTTP/1.1
70	5.390269735	172.233.221.124	10.0.2.15	HTTP	457	HTTP/1.1 401 Unauthorized (text/html)
72	8.652775292	10.0.2.15	172.233.221.124	HTTP	459	GET /basicauth/ HTTP/1.1
74	8.683845448	172.233.221.124	10.0.2.15	HTTP	458	HTTP/1.1 200 OK (text/html)
76	8.757464185	10.0.2.15	172.233.221.124	HTTP	376	GET /favicon.ico HTTP/1.1
78	8.788315618	172.233.221.124	10.0.2.15	HTTP	383	HTTP/1.1 404 Not Found (text/html)

Steps

(Burp) First HTTP Request/Response

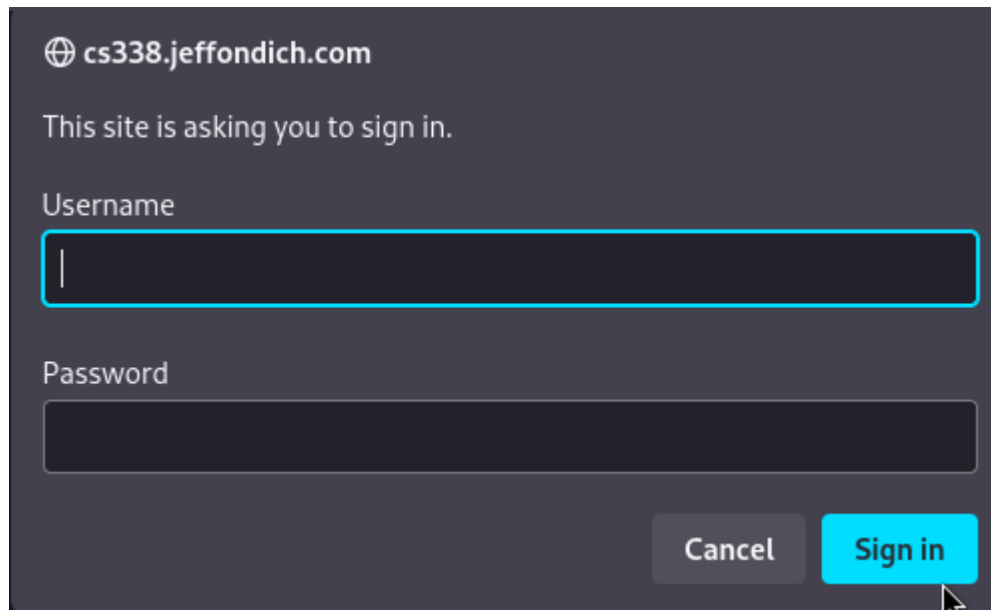
1	http://cs338.jeffondich.com	GET	/basicauth/	401	805	HTML	401 Authorization Required
---	-----------------------------	-----	-------------	-----	-----	------	----------------------------

Request
Pretty Raw Hex
1 GET /basicauth/ HTTP/1.1
2 Host: cs338.jeffondich.com
3 Accept-Language: en-US
4 Upgrade-Insecure-Requests: 1
5 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
6 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
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
9
10

Response
Pretty Raw Hex Render
1 HTTP/1.1 401 Unauthorized
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Thu, 26 Sep 2024 00:55:02 GMT
4 Content-Type: text/html
5 Content-Length: 590
6 Connection: keep-alive
7 WWW-Authenticate: Basic realm="Protected Area"
8
9 <html>
10 <head><title>401 Authorization Required</title></head>
11 <body>
12 <center><h1>401 Authorization Required</h1></center>
13 <hr><center>nginx/1.18.0 (Ubuntu)</center>
14 </body>
15 </html>
16 <!-- a padding to disable MSIE and Chrome friendly error page -->
17 <!-- a padding to disable MSIE and Chrome friendly error page -->
18 <!-- a padding to disable MSIE and Chrome friendly error page -->
19 <!-- a padding to disable MSIE and Chrome friendly error page -->
20 <!-- a padding to disable MSIE and Chrome friendly error page -->
21 <!-- a padding to disable MSIE and Chrome friendly error page -->
22

1. Browser sends a HTTP GET request for the page /basicauth/ on the server IP
2. Server sends back HTTP 401 Authorization Required as the response- essentially saying no, you must authenticate using Basic Authentication.

3. Displays the auth dialog with the basic little window in the browser that displays over the page before it even loads.



cs338.jeffondich.com

This site is asking you to sign in.

Username

Password

Cancel Sign in

4. I enter the username "cs338" and the password "password" and hit enter or click Sign in

(Burp) Second HTTP Request/Response

2	http://cs338.jeffondich.com	GET	/basicauth/	200	666	HTML	Index of /basicauth/
---	-----------------------------	-----	-------------	-----	-----	------	----------------------

Request

Pretty Raw Hex

```
1 GET /basicauth/ HTTP/1.1
2 Host: cs338.jeffondich.com
3 Cache-Control: max-age=0
4 Authorization: Basic Y3MzMzg6cGFzc3dvcmQ=
5 Accept-Language: en-US
6 Upgrade-Insecure-Requests: 1
7 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
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/
  avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
  ange;v=b3;q=0.7
9 Accept-Encoding: gzip, deflate, br
10 Connection: keep-alive
11
12
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Thu, 26 Sep 2024 00:55:20 GMT
4 Content-Type: text/html
5 Connection: keep-alive
6 Content-Length: 509
7
8 <html>
9 <head><title>Index of /basicauth/</title></head>
10 <body>
11 <h1>Index of /basicauth/</h1><hr><pre><a href="..">../</a>
12 <a href="amateurs.txt">amateurs.txt</a>
  04-Apr-2022 14:10
  75
13 <a href="armed-guards.txt">armed-guards.txt</a>
  04-Apr-2022 14:10
  161
14 <a href="dancing.txt">dancing.txt</a>
  04-Apr-2022 14:10
  227
15 </pre><hr></body>
16 </html>
17
```

5. Browser sends server a HTTP GET request for /basicauth/ that contains those credentials, encoded into base64, under the Authorization header.

(Wireshark view of the same thing)

10.0.2.15	172.233.221.124	HTTP	459 GET /basicauth/ HTTP/1.1
-----------	-----------------	------	------------------------------

```
▶ Frame 72: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits) on interface eth0, id 0
▶ Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.233.221.124
▶ Transmission Control Protocol, Src Port: 35726, Dst Port: 80, Seq: 363, Ack: 404, Len: 405
▼ Hypertext Transfer Protocol
  ▶ GET /basicauth/ 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
    DNT: 1\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
  ▼ Authorization: Basic Y3MzMzg6cGFzc3dvcmQ=\r\n
    Credentials: cs338:password
  \r\n
  [Full request URI: http://cs338.jeffondich.com/basicauth/]
  [HTTP request 2/3]
  [Prev request in frame: 68]
```

6. Server sends back HTTP 200 OK and the HTML for Index of /basicauth/ page as the response.

7. Page displays in browser.

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
