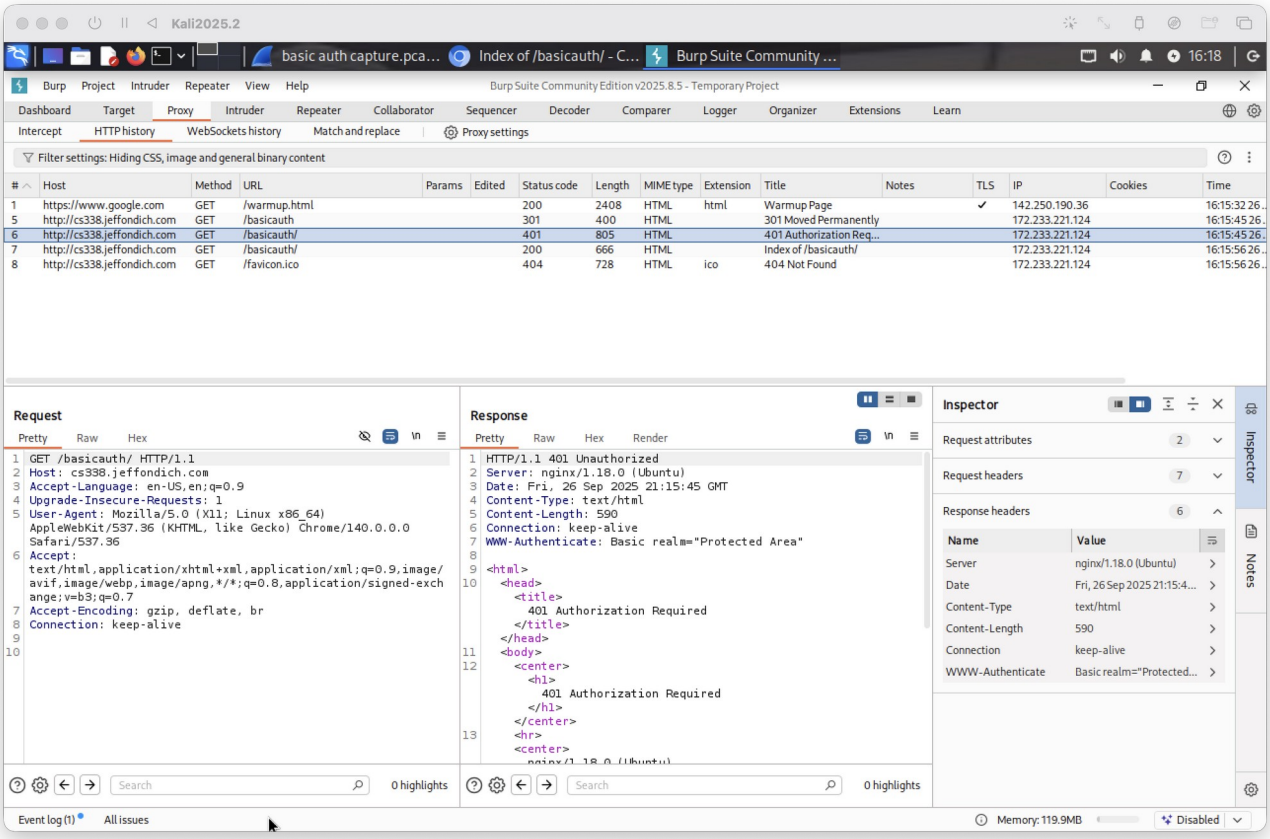
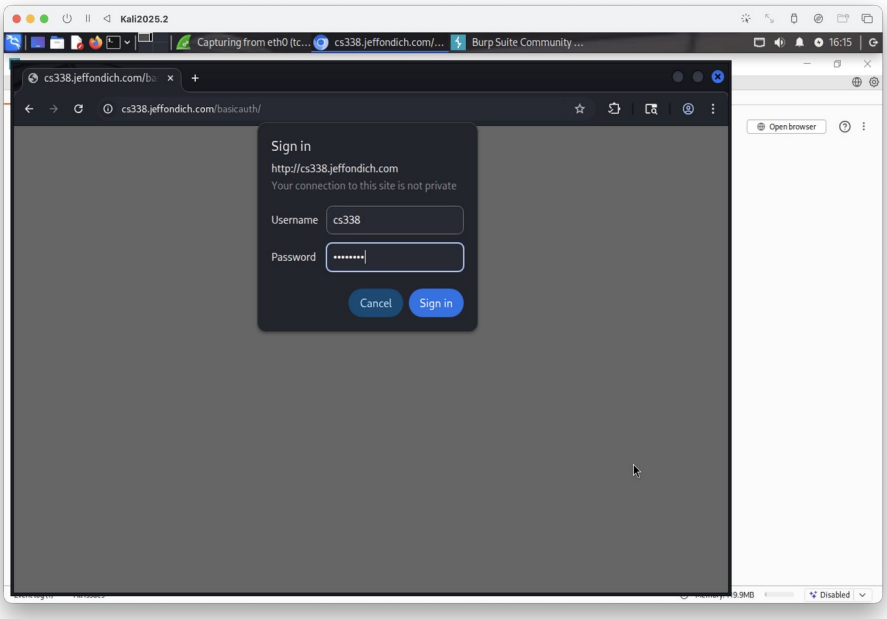
How Basic Auth Works

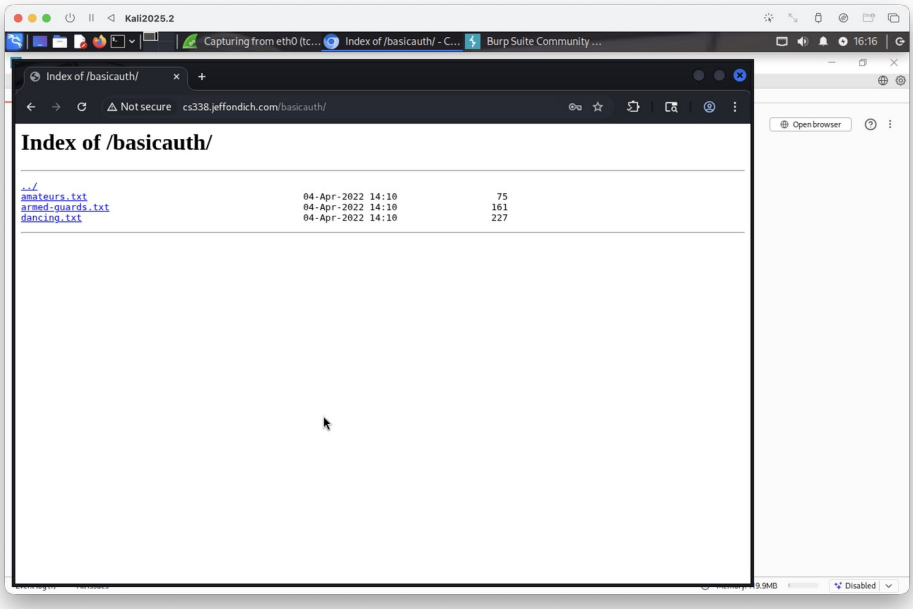
When we first try to connect to a website protected by HTML Basic Auth, the browser does not know that the page is password protected. After exchanging SYN and ACK packets with the server, the browser does a normal GET request, attempting to view the page. (In this case, I entered in the URL http://cs338.jeffondich.com/basicauth, and the server sent me to /basicauth/, which is what happened with #5 in the screenshot.)



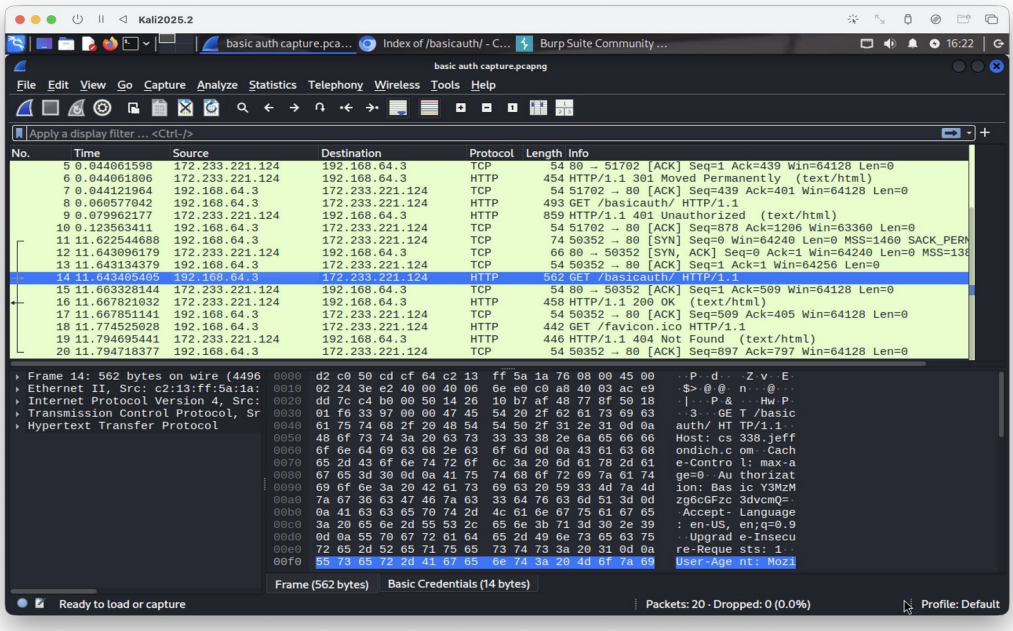
After the browser makes the GET request, the server then responds with the status code “401 Authorization Required.” Because of this, the browser knows that this is a password-protected page, so it asks for a username and password.



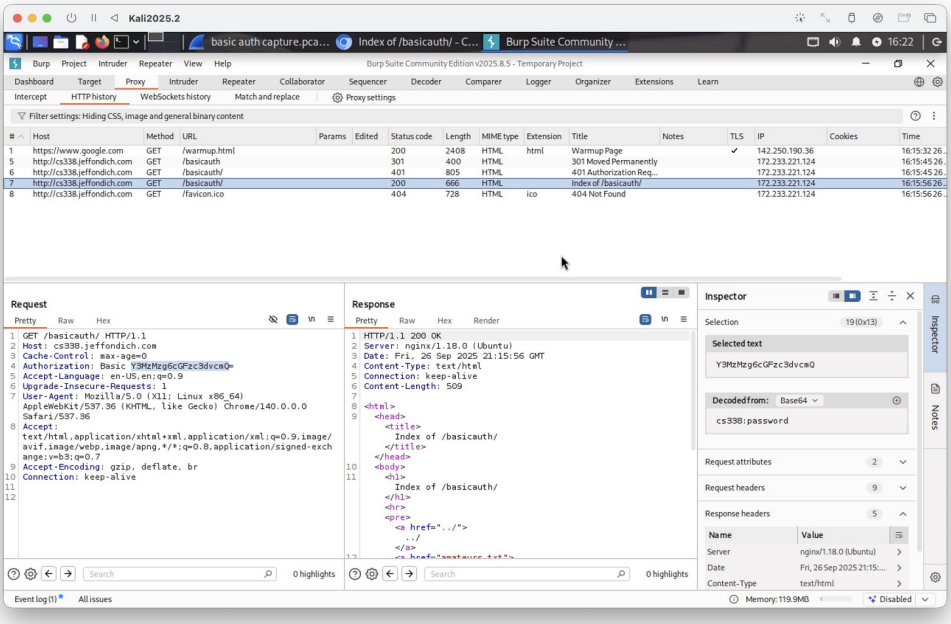
After we have entered our username and password, the page loads and we can view what was once password-protected. But how does this work?



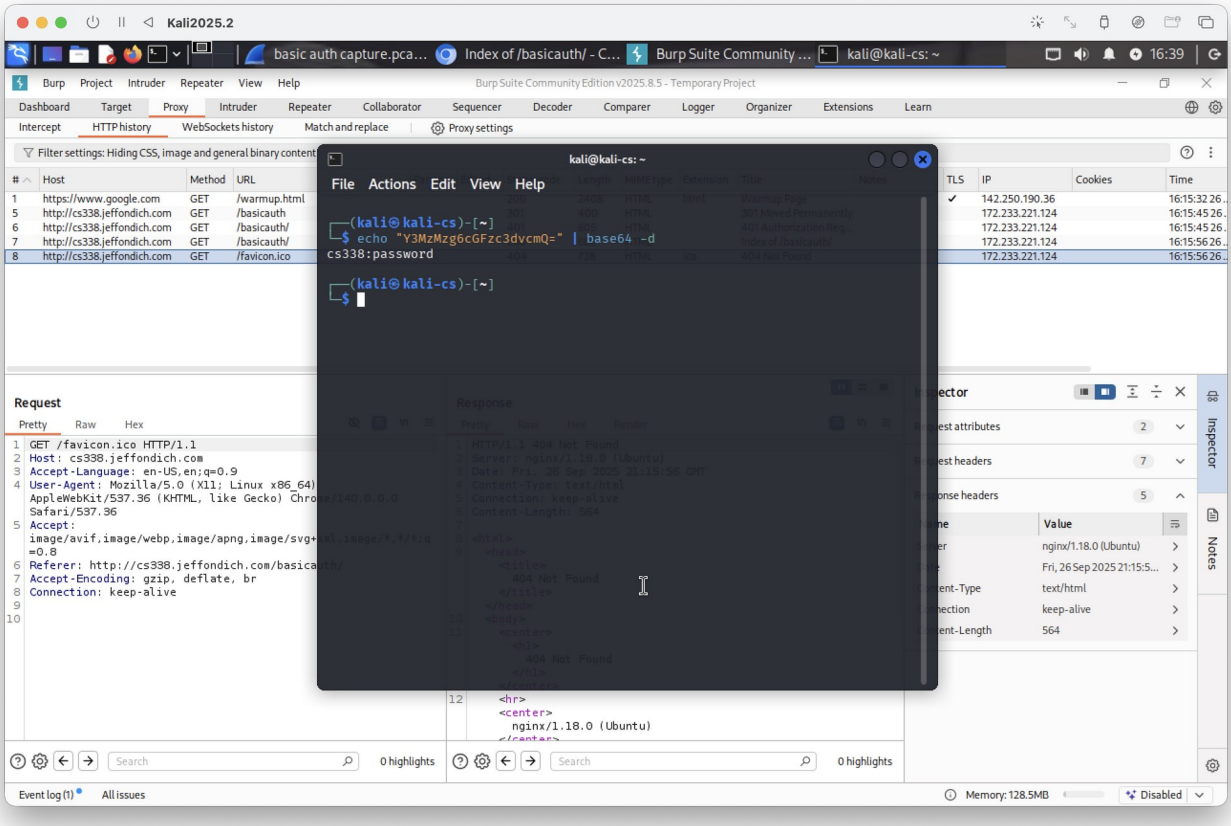
After we enter a username and password, the browser sends the server back the same GET request, but this time with an additional header, “Authorization: Basic Y3MzMzg6cGFzc3dvcmQ=”. After the browser sees this, it lets us in and responds with the page. On the surface, this looks pretty secure. Surely, we are sending the browser some kind of an encrypted version of the username and password.



But wait! As it turns out, the username and password aren’t encrypted at all! As Burp Suite conveniently tells us, this is just our username:our password encoded into base64!



We can verify this by using the base64 utility in the terminal.



So, HTTP Basic Auth is obviously pretty insecure and a great reason for why we should just be using HTTPS.