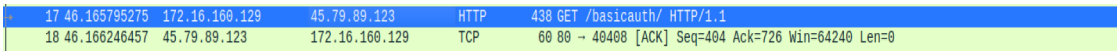
Emma Roskopf

Collaborators: Ashok Khare, Lily Haas (we're each submitting our own document but worked together to figure out what's going on) (we didn't all wanna boot up Kali)

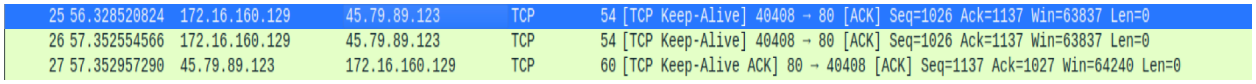
Introduction to nginx password protection

- Authentication is when the website is checking to make sure the user is who they say they are
    - Passwords are often the way that this works, enter the correct username and password and then the user is confirmed
- Authorization is checking that the user is allowed to access certain areas, information, folders, etc. Like a level of clearance
    - Here, the authorization is just being authenticated, certain users don't have more privileges than others

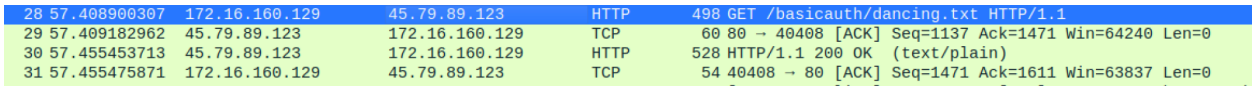
Wireshark Sniffing at the website

- We used the capture filter "host 45.79.89.123" because the basic auth site is on the same IP address as the other parts of the site, which we confirmed by running "wget http://cs338.jeffondich.com/basicauth/" on the terminal and it gave back the same IP
- The goal here is to get all communications between our computer, port 40408 and the server that we are requesting info from, running on port 80
- 

- So here you can see we're getting the main page of the website

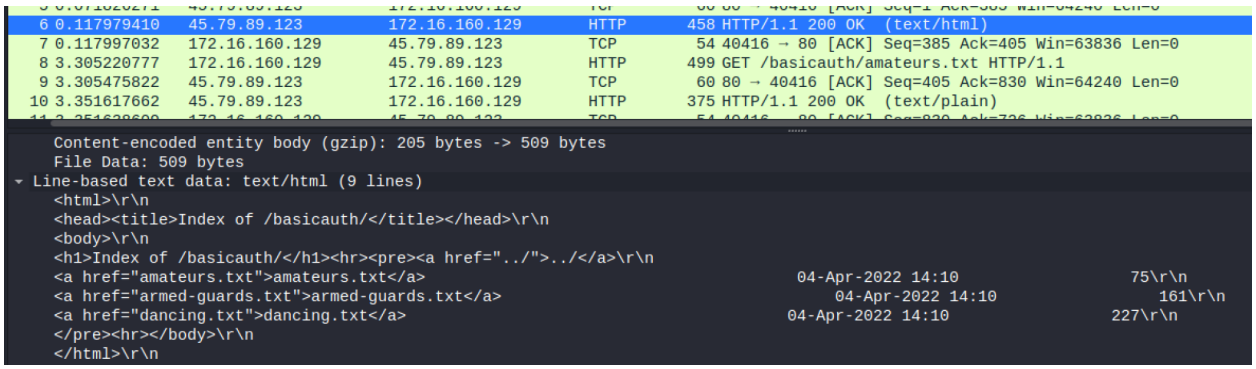
- 

- Here TCP is doing something, each frame has [TCP Keep-Alive]. We're think this is the client and server making sure each other is there
    - "Still alive over there" "Yep" "K"

- 

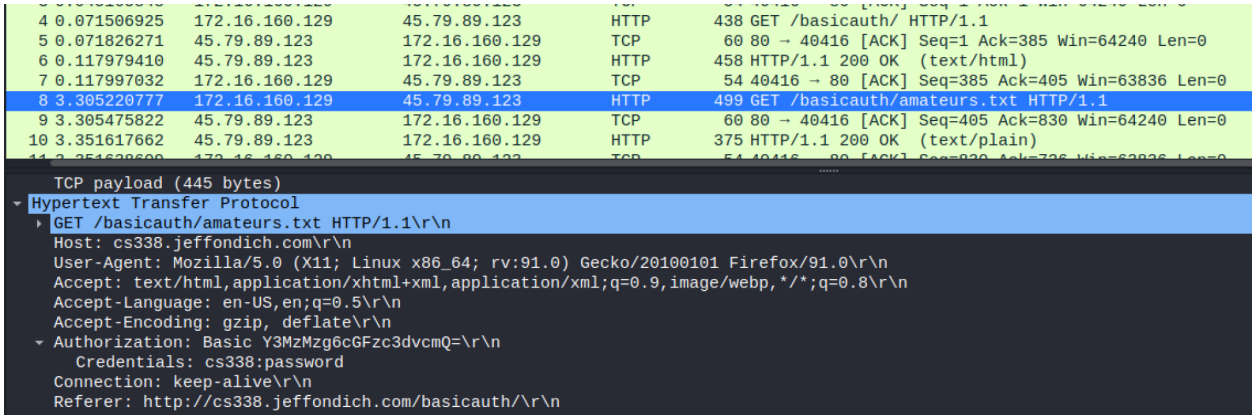
- Here we have gotten into the authentication password blocked area of the website
    - In Frame 28, we see the name of the file I accessed, /basicauth/dancing.txt
    - This seems wrong because this file and it's name was blocked but by sniffing I can see what the client is looking at, and see that is is being rendered in plain text
- That was a pretty good first pass, so now we're going to try to mess with it instead of following the regular order that things should be done

We found the HTML for the secure side of the website



- On the second pass, we realized that by expanding the HTTP messages we can get the line data, which tells us the HTML being rendered and gives the names of all the files
- These file names could be sensitive or private, and so being able to see them seems bad

We found the password and credential by dropdown menu underneath 'Authorization'

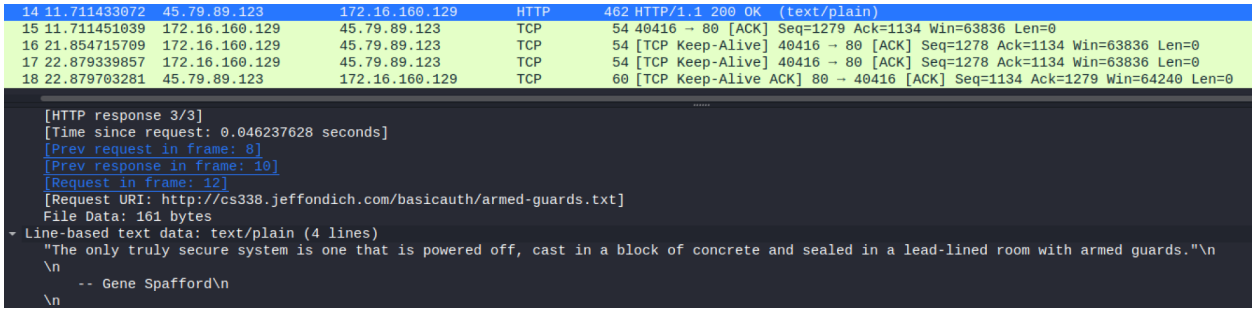


- "No one enters dropdown menus. They'll never find it here"

  ~the developers probably

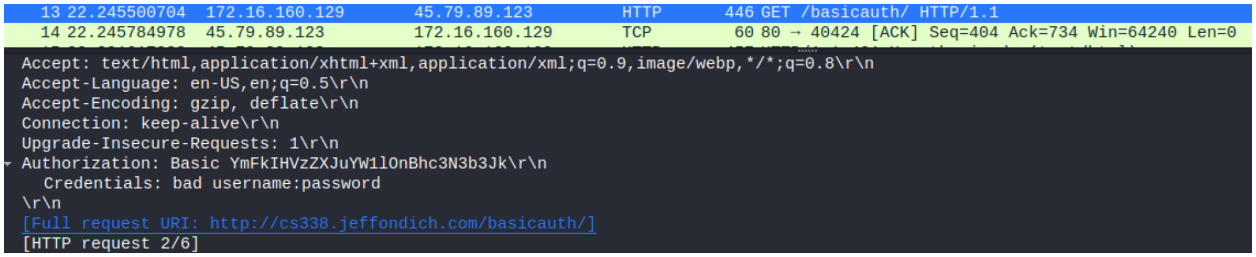
- This seems distinctly BAD
- We just sniffed someone who had accessed the website and now we have their identity
  - "Identity theft is not a joke Jim"
  - This seems like a pretty major problem. By knowing the credentials we can now just go back in as this person, and look at all the information and no one is going to know (we're gonna give them a name, this is Dwight). Unless Dwight has a particularly strong alibi for this exact moment where Jim hacked his account, now we just have a huge security breach that no one knows about. Also Jim signed up perfectly legally with Dwight's credentials, so you can't really trace this back to him at all.

Even better, we now have the whole file without even signing in as Dwight

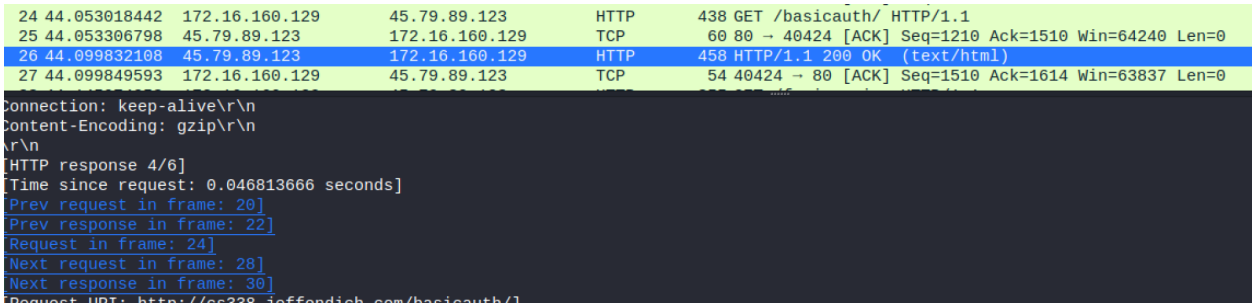


- Jim must be *thrilled* he doesn't even have to commit identity theft
    - He literally just needs to sniff Dwight's computer and the website that we know that Dwight is using
    - We may not get all of the files, like if Dwight didn't open them all, but we do just have the information without even signing in as another person

Out of curiosity we went back to see what fake passwords look like



- And yeah we get the fake passwords too, it's all stored in here



- Also even if there's a lot of fake passwords, once we get in Wireshark identifies where the correct credentials came from, and here we entered the correct username and

password at frame 24 and when we get in (get the message 200 OK, instead of a 400 Unauthorized) it references back to Frame 24, where we entered the correct password

Mastermind plan

1. Break target's computer
2. Install wireshark on loaner computer and hide the icon
3. Get target to sign in to the website and use their credentials
4. If they happen to use the file you want, great, we have everything from picking up the HTML
5. Otherwise sign in at some other point as them, with their credentials, like during lunch break or something so it isn't outside of business hours
6. Congratulations you have now seen Dwight's top secret diary (that he keeps in plain text files, idk ask him about that) or his bank account, your priorities are your own