(A2) Broken Authentication and Some TryHackMe!

WebGoat - Authentication Bypasses

(Q) for Inspect, then find the security questions in HTML and edit them.

I added values, or answers to the questions so I could bypass the 2FA questions.

Before:

Text

Description automatically generated

After:

Tried this and it didn’t work:

Text

Description automatically generated

So, I tried this instead, with the help of <https://pvxs.medium.com/webgoat-authentication-bypass-2-4eeb8e8b502b> :

I probably could’ve left the values as secQuestion0 and secQuestion1 and fulfilled the field requirements by leaving the answers (the value field) as one word instead of words and characters like my previous answers.

Graphical user interface, text

Description automatically generated

I successfully bypassed the 2FA security question practice!

Text

Description automatically generated with medium confidence

TryHackMe

Intro to Offensive Security

I am rusty at hacking, so I am taking the introduction course to brush up on my skills.

I launched the machine and then the terminal and entered this command:

Text

Description automatically generated

The command gave me information on where I can find an admin login for Fake Bank (the highlighted selection)

Through that I entered the URL fakebank.com/bank-transfer and got this:

Graphical user interface, application

Description automatically generated

From here I transferred money from one account to my own.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

I successfully received the money.

Graphical user interface, text, application, chat or text message

Description automatically generated

Answer to question (BANK-HACKED):

Graphical user interface, text, application

Description automatically generated

I finished the first hacking room!

Background pattern

Description automatically generated

Web Fundamentals

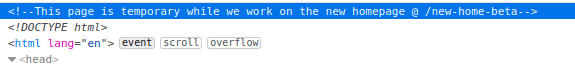
(I’m going to start it so I can work on it in other assignments)

Walking an Application

Go to this website: <https://10-10-70-236.p.thmlabs.com>

Inspect the page (Q):

Find flag from HTML comment:



Went to: <https://10-10-70-236.p.thmlabs.com/new-home-beta>

The flag that appeared:

Text

Description automatically generated

Find flag from secret link:



<https://10-10-70-236.p.thmlabs.com/secret-page>

Logo

Description automatically generated with medium confidence

Directory listing flag:

What is /assets?

Text

Description automatically generated

I found it, it’s the directory.

<https://10-10-70-236.p.thmlabs.com/assets/>

Text

Description automatically generated with low confidence

What about that flag.txt file? There we go.

Text

Description automatically generated

Framework flag:

This one was more difficult, I had to dig a little, but I found it.

I navigated to this website



<https://static-labs.tryhackme.cloud/sites/thm-web-framework>

Then clicked on the Change Log Tab:

Graphical user interface, text, application

Description automatically generated

And then navigated to this website:

<https://10-10-70-236.p.thmlabs.com/tmp.zip>

Which downloaded a .zip that I unzipped and read in Mousepad

Which gave me this tag:



Finished: Diagram

Description automatically generated

Notes:

**Graphical user interface, text, application, Word

Description automatically generated**

Walking an Application

Text

Description automatically generated