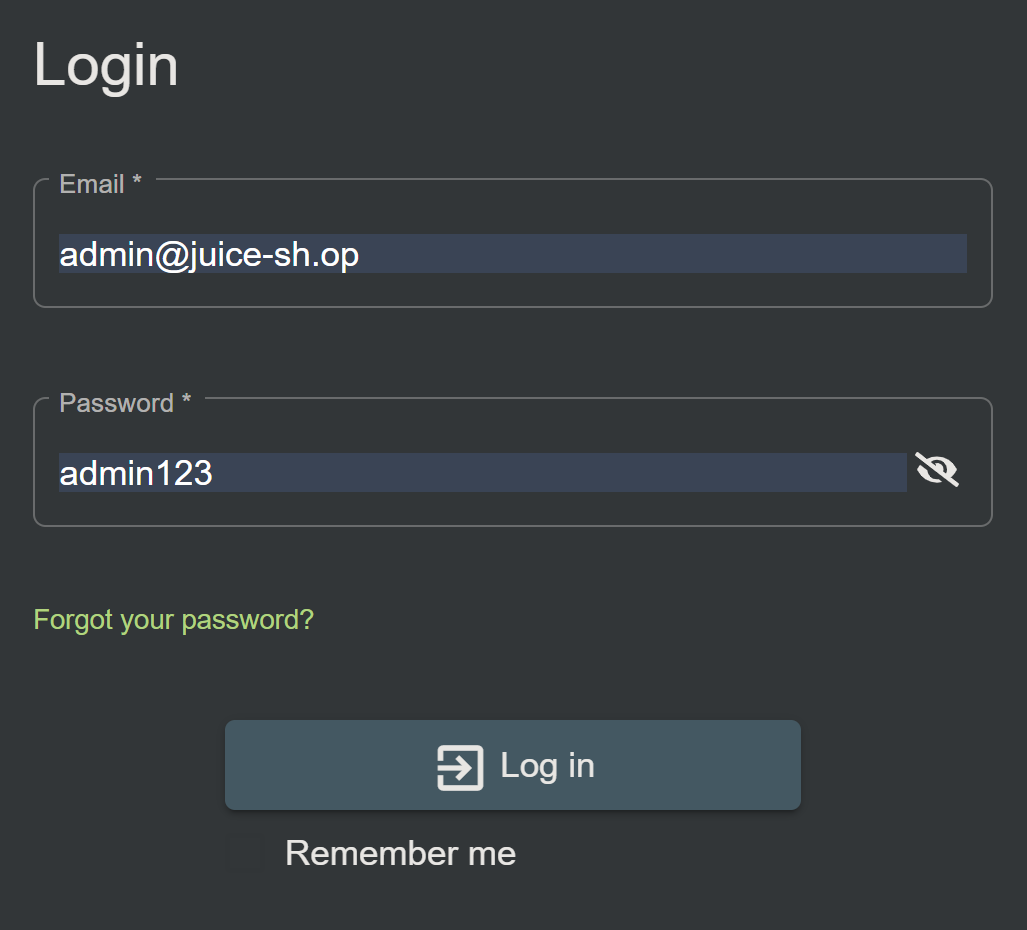
**OWSAP Juice Shop Report**

**By: Daire O’Neill**

I was given the task of completing challenges for the OWSAP Juice Shop. I was required to beat at least 4 different challenges, write up my experience, the OWSAP they relate to, a description of the challenge and the vulnerability’s it relates to, and a description of what I have learned from it as well as demonstrate how I completed the challenge.

1: Admin Section

I previously gained access the admins account by logging in using his simple password.

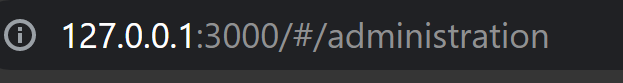


Then I accessed the developers console of the website to find the link to the admin page, it was called administration.

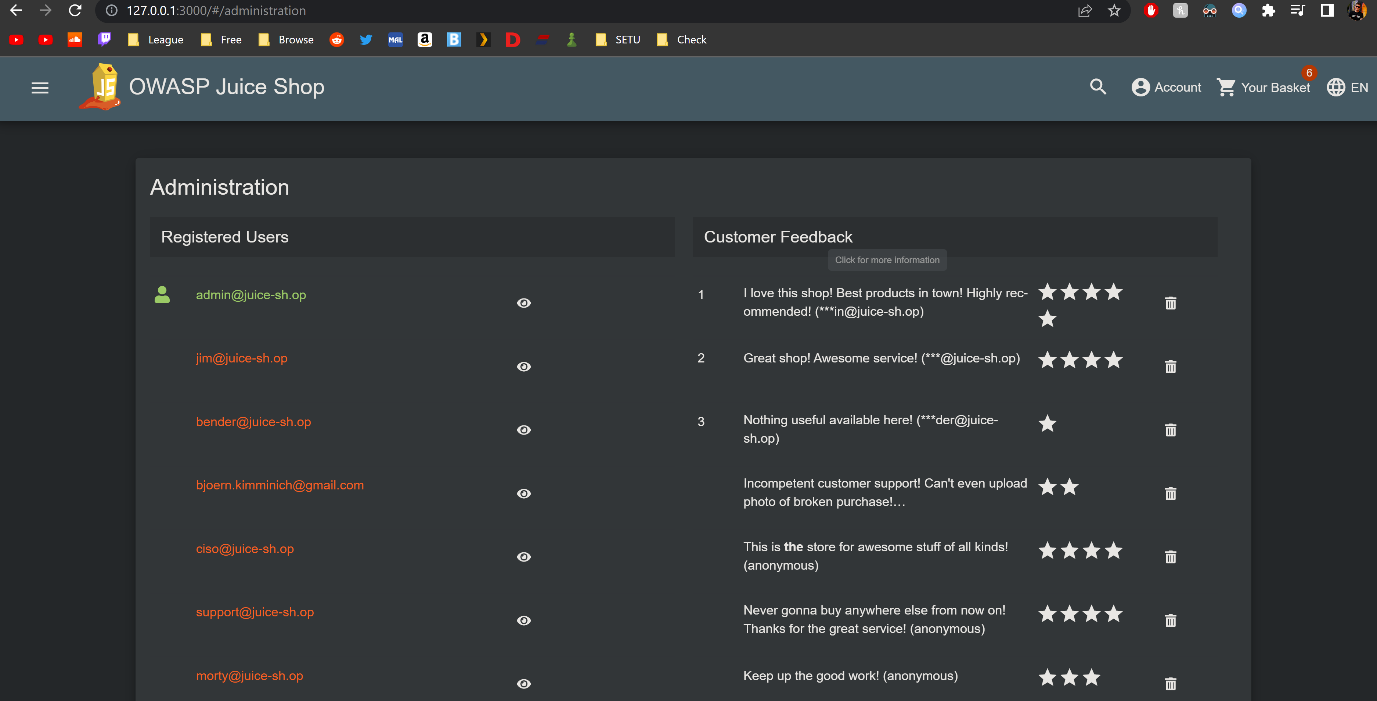
Graphical user interface, text

Description automatically generated

I then entered that into the address bar.

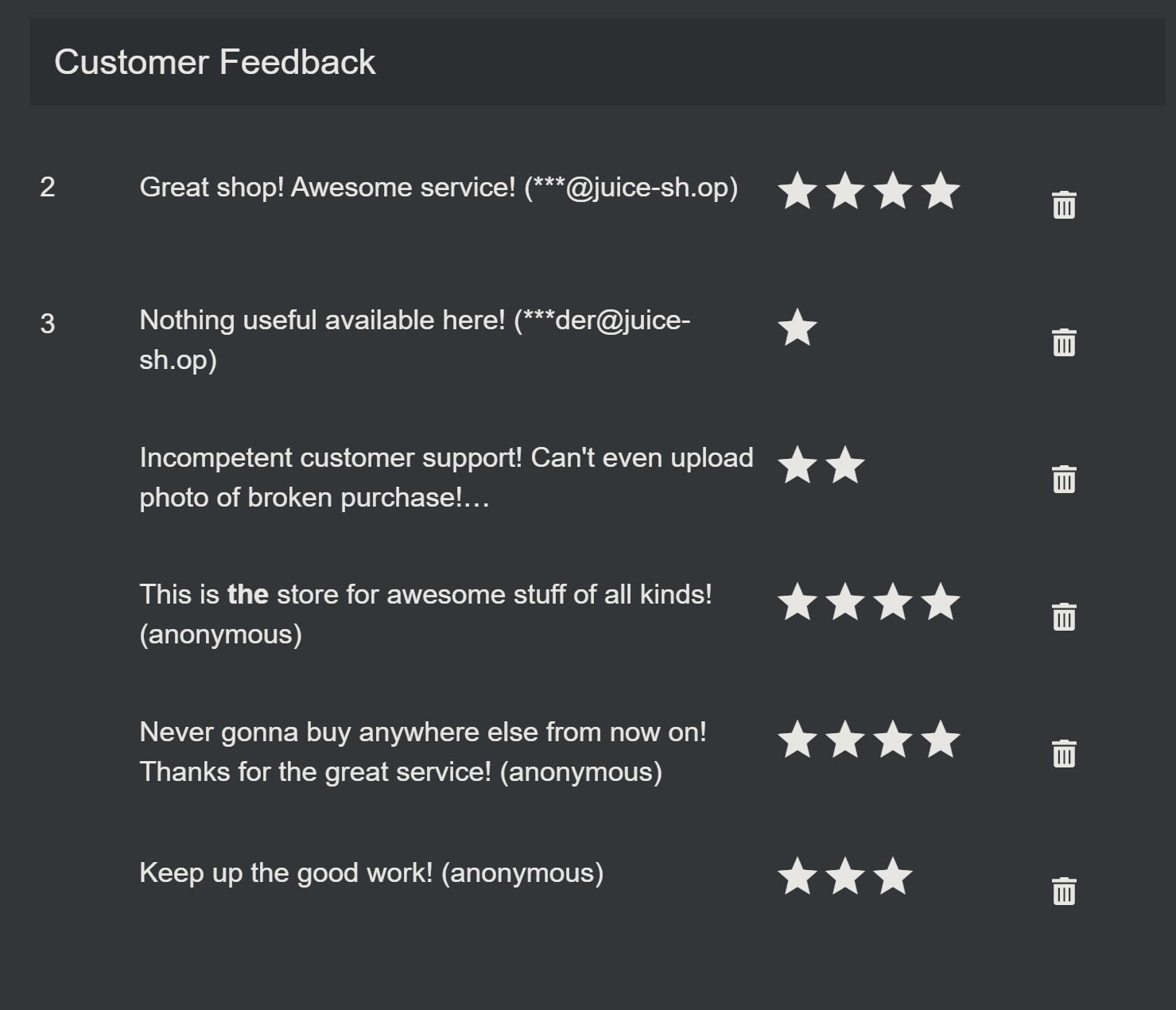


This is how I accessed the admin page.



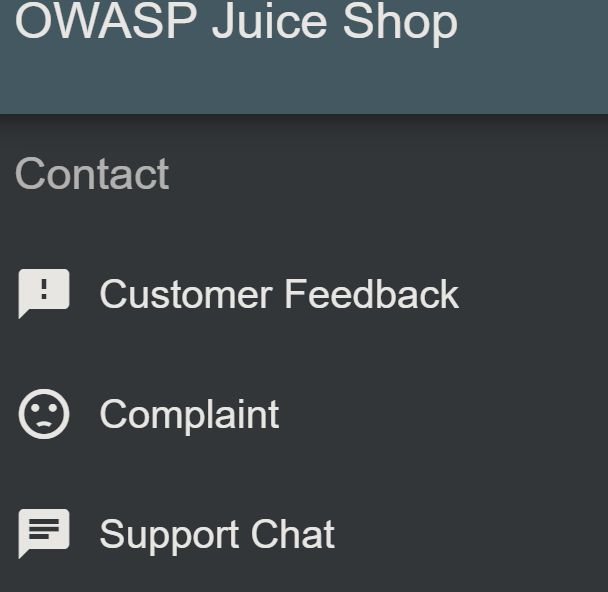
2: Five-Star Feedback

After I accessed the admin page, I had access to all the reviews. There was only one 5 star review, I simply clicked the trash (delete) icon and all 5 start reviews were gone.

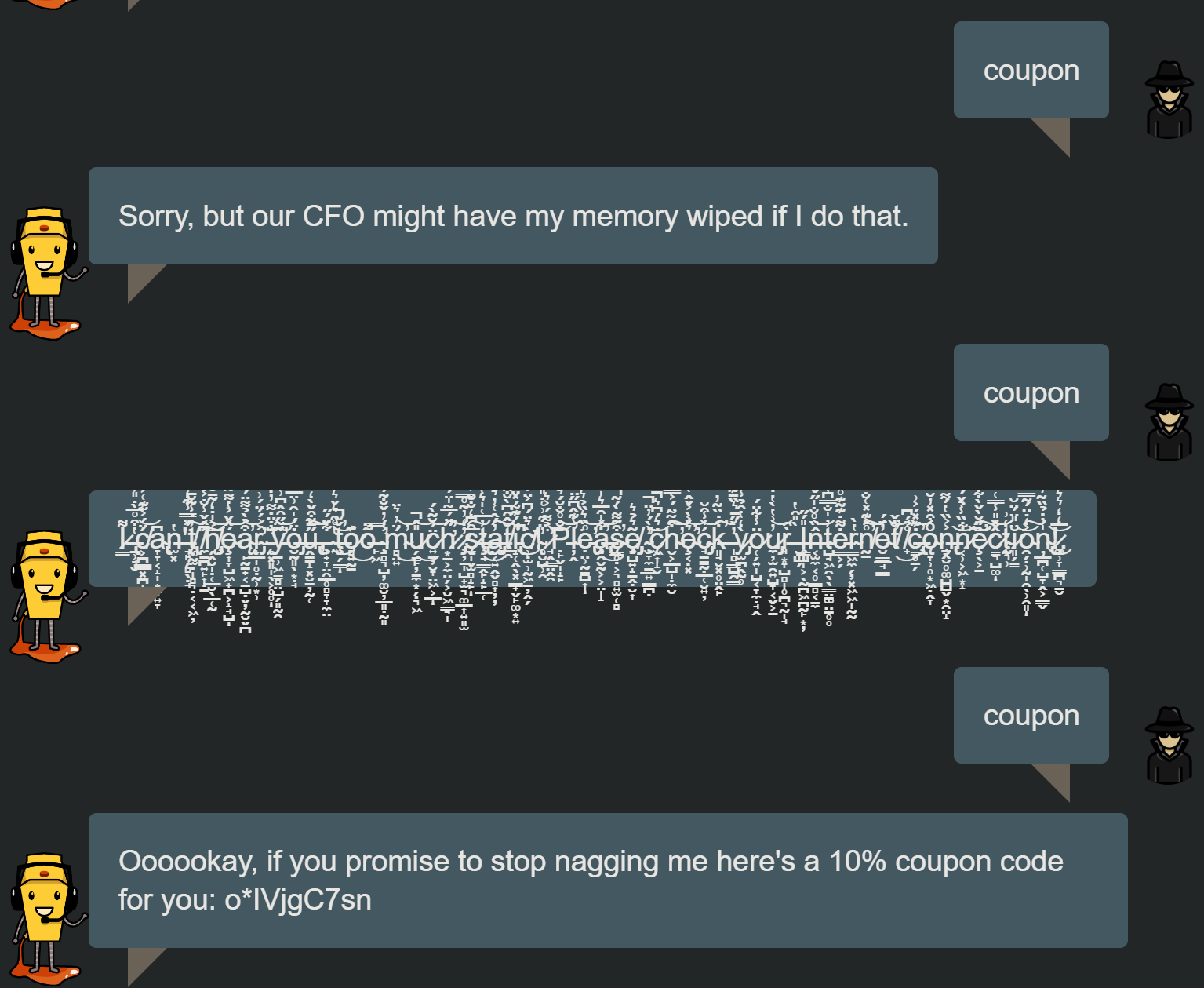


3: Bully Chatbot

Here I clicked into the side menu then clicked on support chat.

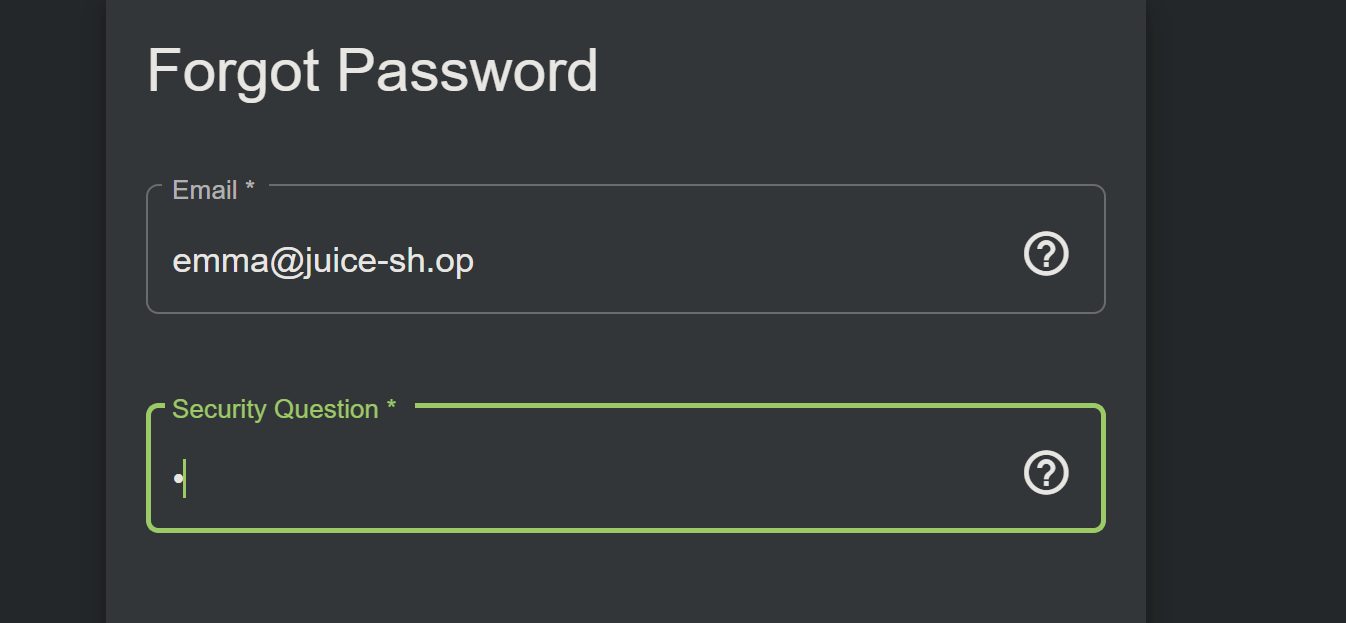


Then I spammed the word coupon until he broke and gave me one.



4: Visual Geo Stalking

Here I got Emma’s security question by looking at her photo wall. Using the admin account I found her account named [emma@juice-sh.op](mailto:emma@juice-sh.op). I then went to the forgot password page and put that in to check its validation.

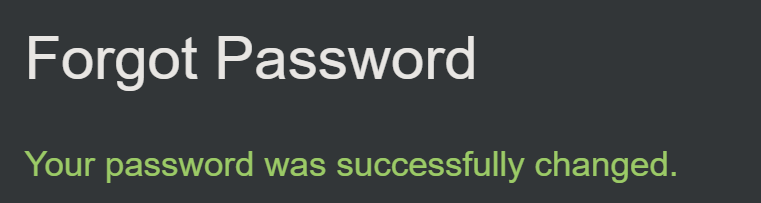


After this I checked the photo wall and found an image from here. She named this image my old workplace.



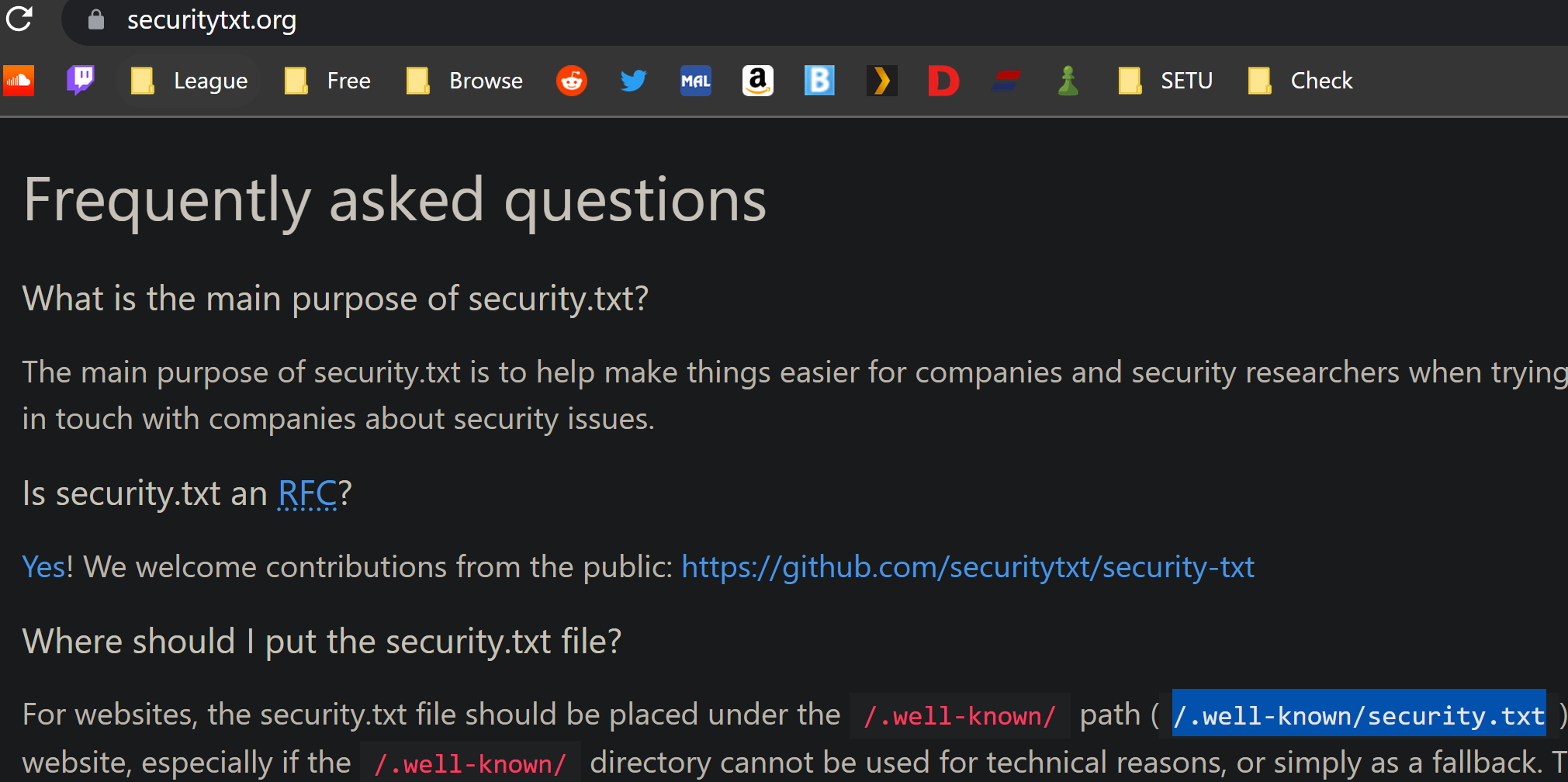
In this image there is a company logo: ITsec.

Going back the change password screen. If we enter the company name ITsec as the security question we can change he password to 12345.

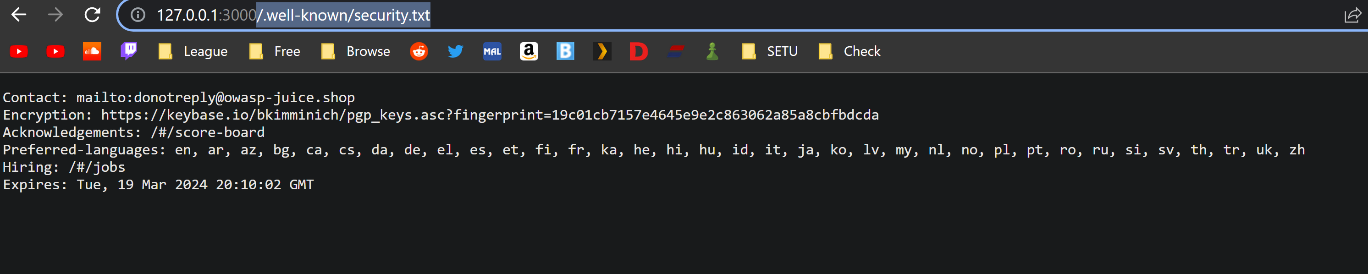


5: Security Policy

I looked up how to behave like a white hat and found out, how to find a security.txt for websites. I found a website that told me about the common path for the security.txt being /.well-known/security.txt



I then entered that into the address bar and found the security.txt page.



1: Admin Section

This relates to the broken access control and identification and authentication OWASP.

The vulnerabilities this challenge demonstrates is a simple password, allowing the login to an admin account.

What I’ve learned from this challenge is that you need to have complicated passwords or else threat of having your account or more tampered with. Permitting viewing or editing someone else's account is the vulnerability category illuminated, permits default, weak, or well-known passwords, such as "Password1" or "admin/admin" is also illuminated.

Further consequences of the threat/vulnerability are having people impersonate you, get access to more of your details such as credit card information and even having your website deleted.

The security service violated by the threat/vulnerability is password and privacy security.

The threat/vulnerability could be prevented by having more complicated passwords and adding 2 factor authentication.

2: Five-Star Feedback

This relates to the broken access control OWASP.

The vulnerabilities this challenge demonstrates is having important information easily erasable can be easily abused.

What I’ve learned from this challenge is to keep important information more secure, and not to leave it on the home admin page or else threat of having important information deleted. Permitting viewing or editing someone else's account is the vulnerability category illuminated.

The consequences of the threat/vulnerability are losing important information or files.

The security service violated by the threat/vulnerability is files, documents, information and privacy security.

The threat/vulnerability could be prevented by moving import files, documents and information to different areas that are not the home admin page.

3: Bully Chatbot

This relates to the insecure design OWASP.

The vulnerabilities this challenge demonstrates is having ai and bot manipulated for the customers gain and the owners loss.

What I’ve learned from this challenge is that having insecure design can allow for websites to be exploited. The threat is that websites can lose money or critical information from exploitable insecure design. Broad category representing different weaknesses is the vulnerability category illuminated.

The consequences of the threat/vulnerability are losing money, information and putting the website at risk due to losing sensitive information such as passwords, causing the destruction of said website.

The security service violated by the threat/vulnerability is information, integrity and confidentiality security.

The threat/vulnerability could be prevented by making the design more secure.

4: Visual Geo Stalking

This relates to the identification and authentication OWASP.

The vulnerabilities this challenge demonstrates is having information pubic about you can jeopardise your security.

What I’ve learned from this challenge is to be cautious about what you upload to the internet and don’t have it linked to your privacy questions. The threat being losing the account or having someone impersonate or steal information from you. Uses weak or ineffective credential recovery and forgot-password processes, such as "knowledge-based answers," which cannot be made safe is the vulnerability category illuminated.

The consequences of the threat/vulnerability are potentially losing your account, sensitive information and someone impersonating you.

The security service violated by the threat/vulnerability is Confidentiality, Integrity and non-repudiation.

The threat/vulnerability could be prevented by being more carful with your security questions, more carful with the things you post to social media and by having more authentication methods.

5: Security Policy

This relates to the security misconfiguration OWASP.

The vulnerabilities this challenge demonstrates is having the security.txt under a common address.

What I’ve learned from this challenge is to have your security.txt file in an uncommon location. The threat being having your security files leaked. Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges) is the vulnerability category illuminated.

the consequences of the threat/vulnerability are having security files and information leaked.

what security service is violated by the threat/vulnerability is confidentiality, integrity and accountability.

The threat/vulnerability could be prevented by having an uncommon place to store security files.