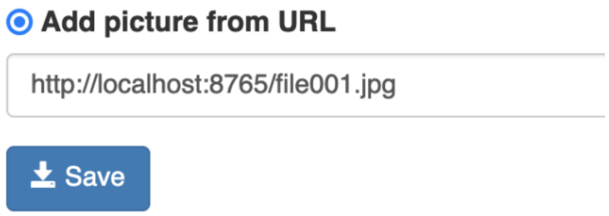
Description of the attack:
At first I checked the posts/reviews of other users and discovered that in one post there was a link instead of an image. When opening the link I got the the Error: “Not Found”, so I had a look at the url:
https://f0e2908c-e108-468a-afbe-9d33ccac86a6.idocker.vuln.land/post-images/**http://localhost:8765/file001.jpg**

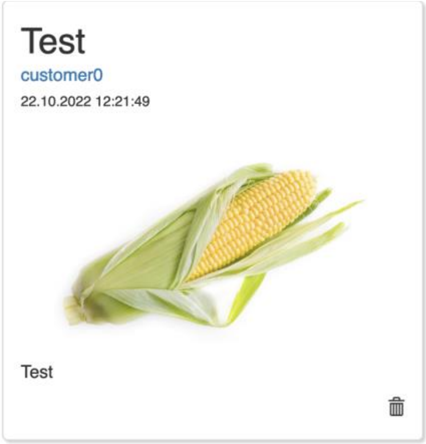
The last part of url looks interesting as it seems that http://localhost:8765/file001.jpg is probably referring to the place where the file001.jpg is stored on the server. In the next step I tried to access the resource by creating a Post and using the described url in the “Add picture from URL” functionality.



● Add picture from URL

http://localhost:8765/file001.jpg

It worked and I’ve got the following post as a result:



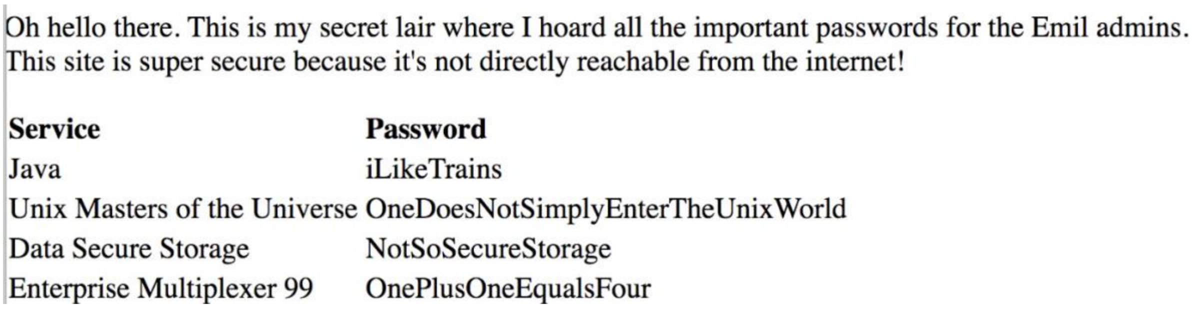
Test

customer0

22.10.2022 12:21:49

Test

Therefore, I assumed it is also possible to retrieve the file002.jpg in this manner. So, I added a second post and provided the following url: http://localhost:8765/file002.jpg, which resulted in the following post with the secret information we searched for:



Oh hello there. This is my secret lair where I hoard all the important passwords for the Emil admins. This site is super secure because it's not directly reachable from the internet!

Service	Password
Java	iLikeTrains
Unix Masters of the Universe	OneDoesNotSimplyEnterTheUnixWorld
Data Secure Storage	NotSoSecureStorage
Enterprise Multiplexer 99	OnePlusOneEqualsFour