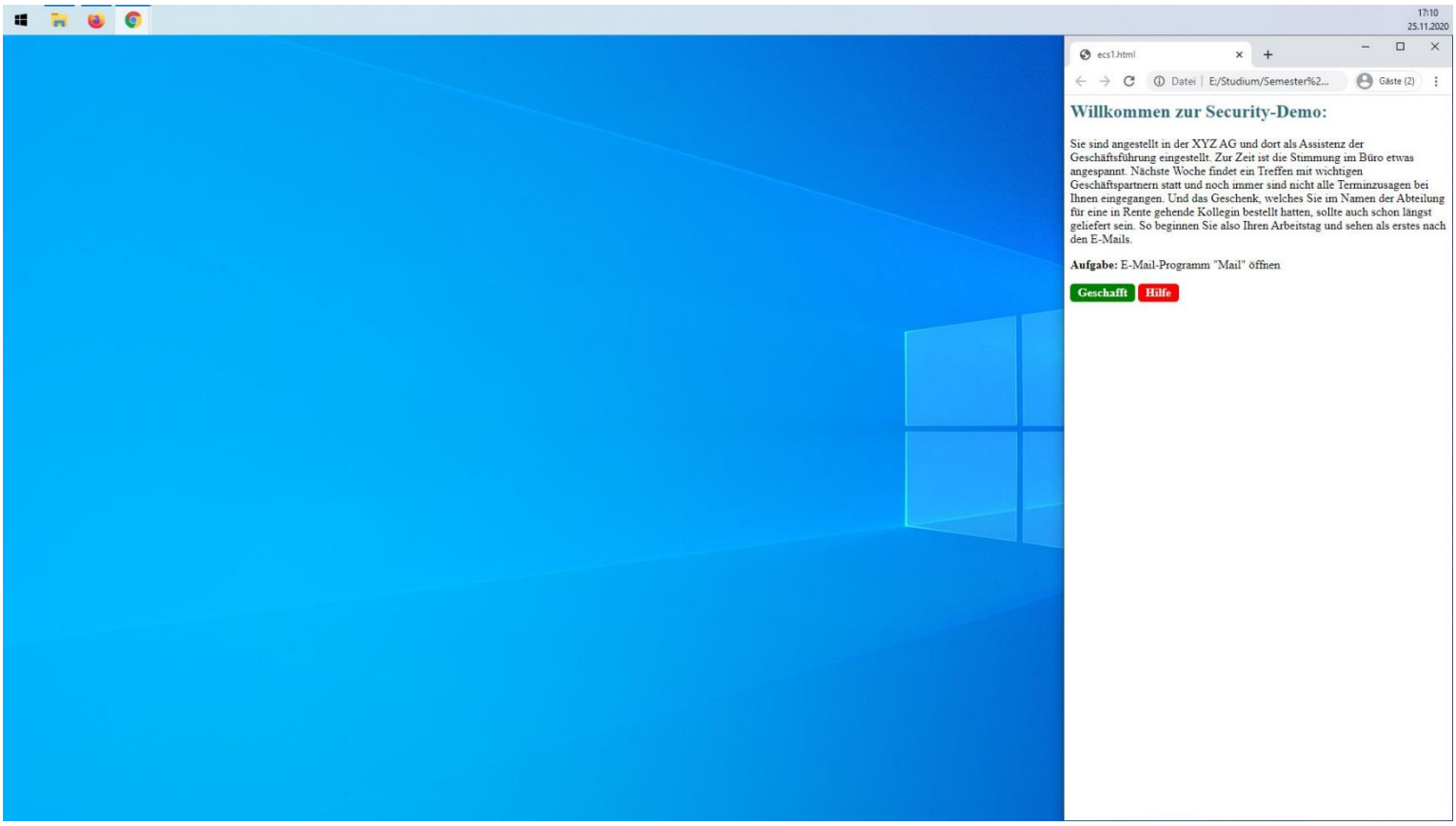
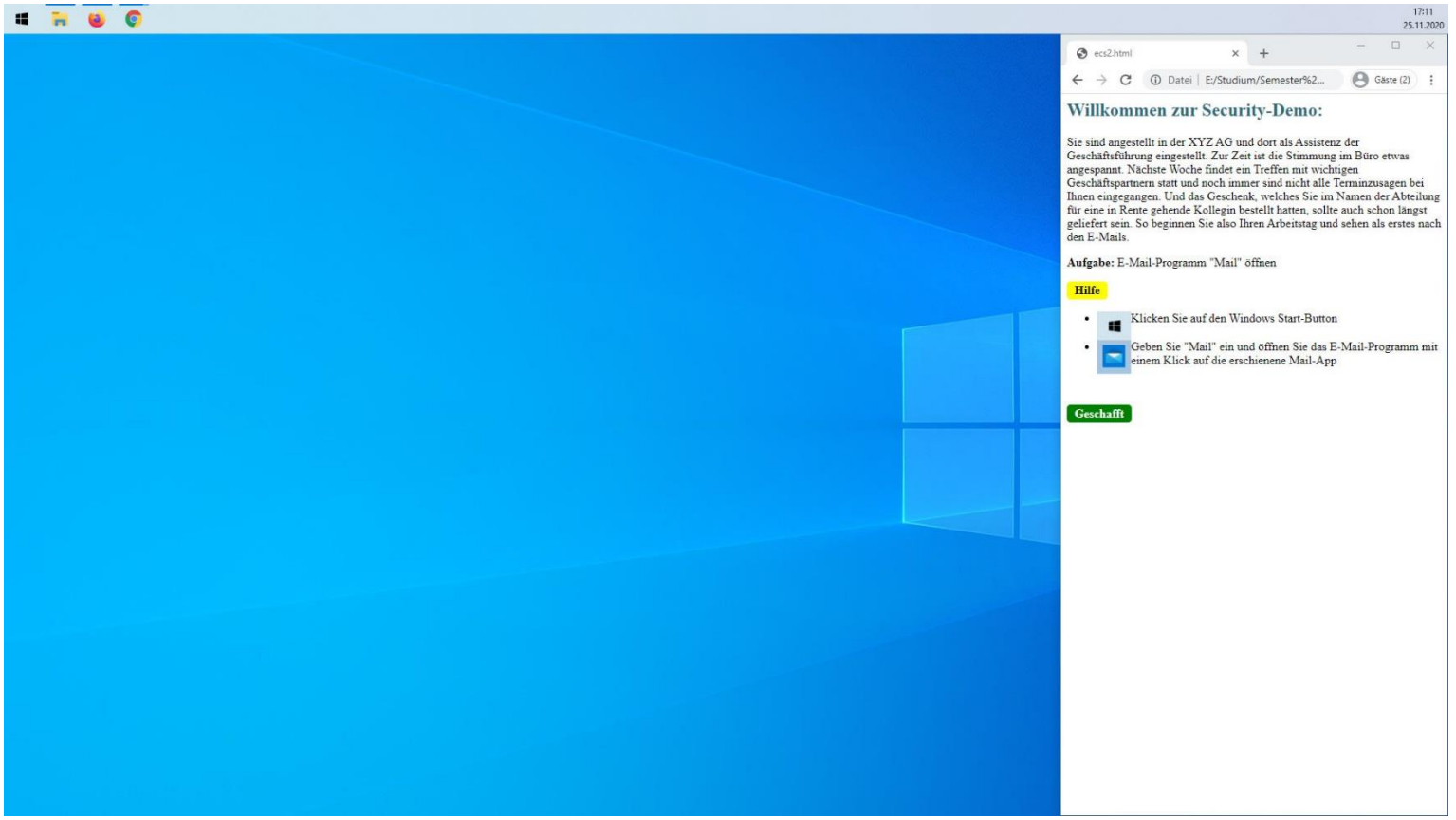
Phishing Demonstration

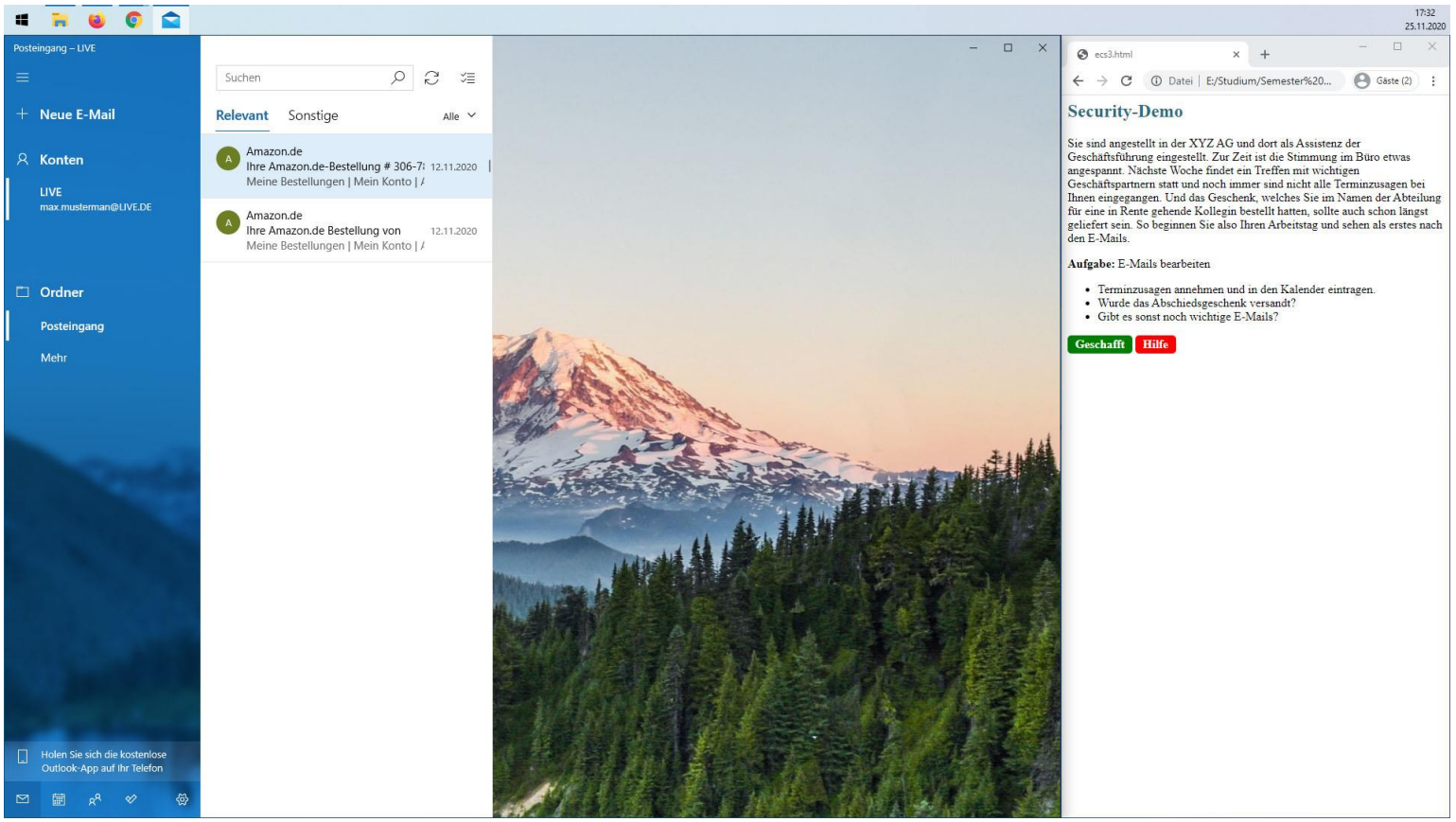
Start of the demo:



The user is greeted with a short introduction which also acts as a background story for this scenario. It is presented as a website. (The naming “Security”, not “Phishing”-Demo is intentional to not directly give a hint) The browser containing the website is located in the narrow right part of the screen. This way the main content of the demonstration gets the most space while background tory, navigation and help pages are always visible and accessible. Below the introduction there is one task the user has to follow. If help is needed it can be accessed via a button:



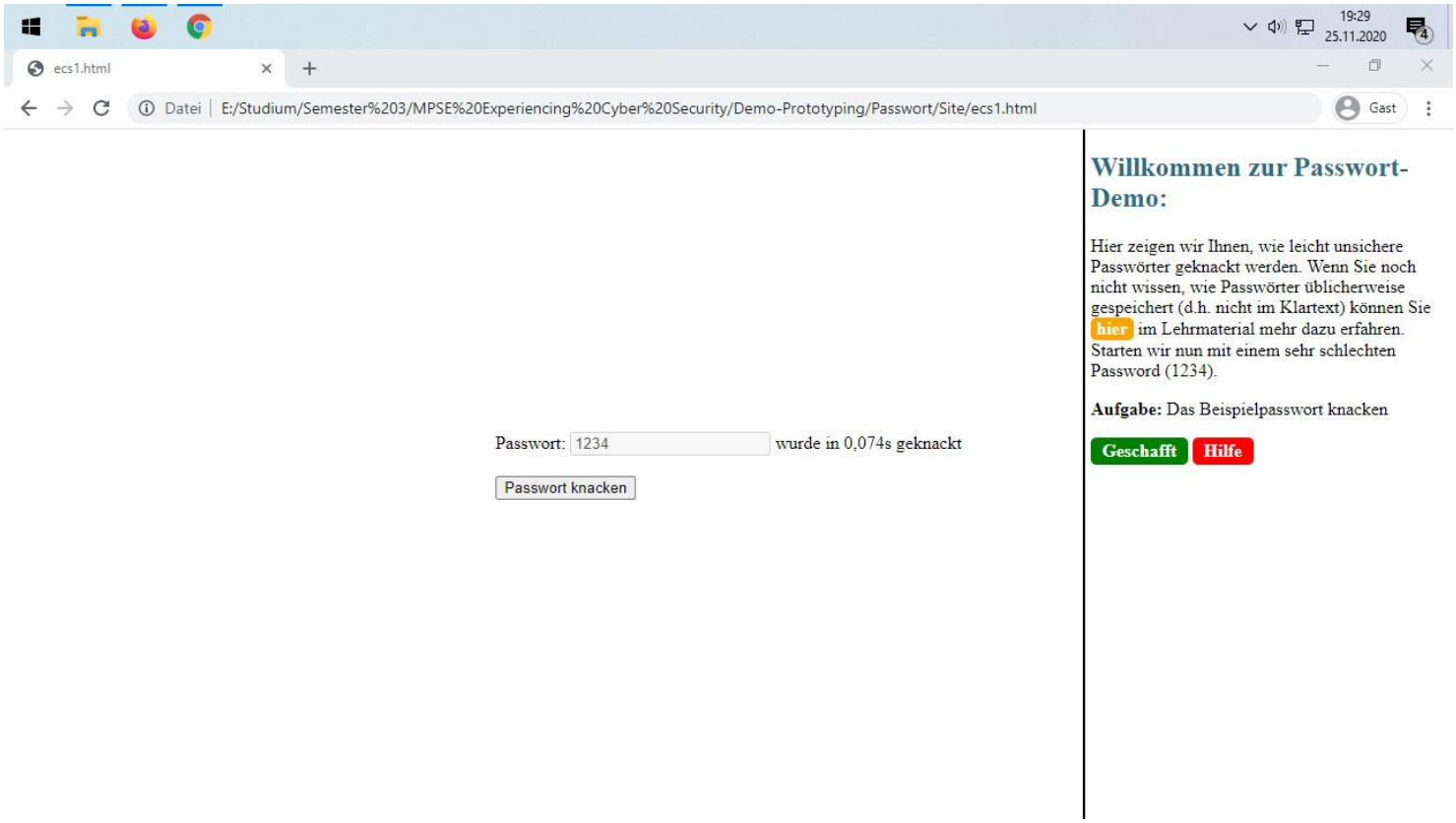
The introduction with the first task and the help page expanded.



The Screen after the user opened the mail app as ordered by the task. An email-account is already set up and the user has to process three tasks: To look for appointments and register them in a schedule, to check if an order was shipped already and to watch out for unexpected and important emails.

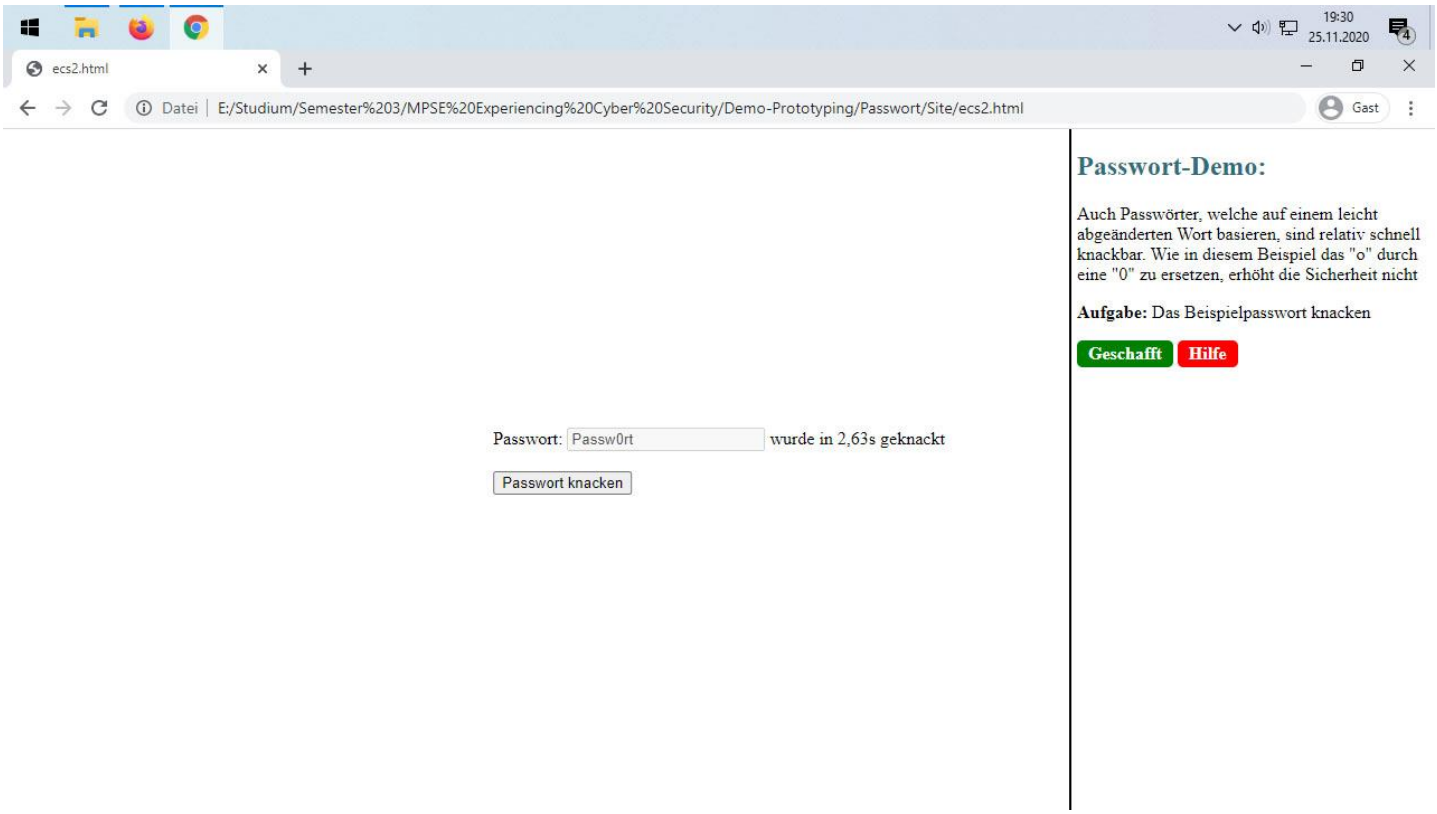
While most emails in the inbox are legitimate, some are phishing-mails who contain malicious links. Clicking on such a link will lead the user either to the forged version of a real website (e.g. an online bank) where the user is prompted to login with their credentials.
Another version will lead the user to a ransom website that tries to lock the user out, shows a warning and demands the payment of a ransom via e.g. bitcoin.

Password Demonstration

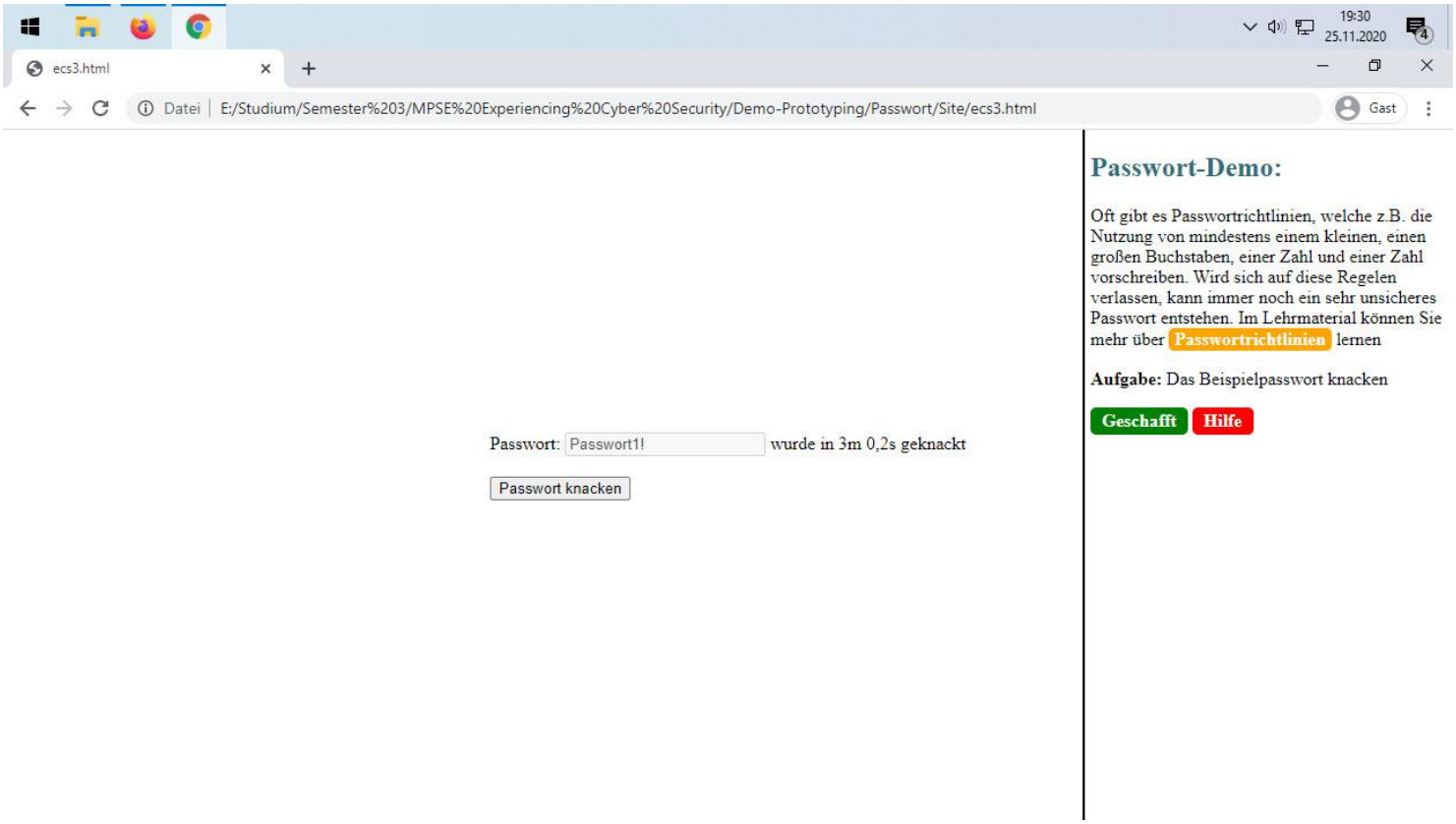


As this demonstration is running in the browser (at least the front-end), demonstration and navigation/help share the same website but are still separated.
In the first screen the user is presented the introduction of the demonstration and a first very weak password. The given task is to break this password (or at least initiate the process). Again, if help is needed there is a button expanding into a list of required steps. The yellow button is a link to a fitting part in the associated teaching material. (This time explaining the process of hashing a password before storing it)

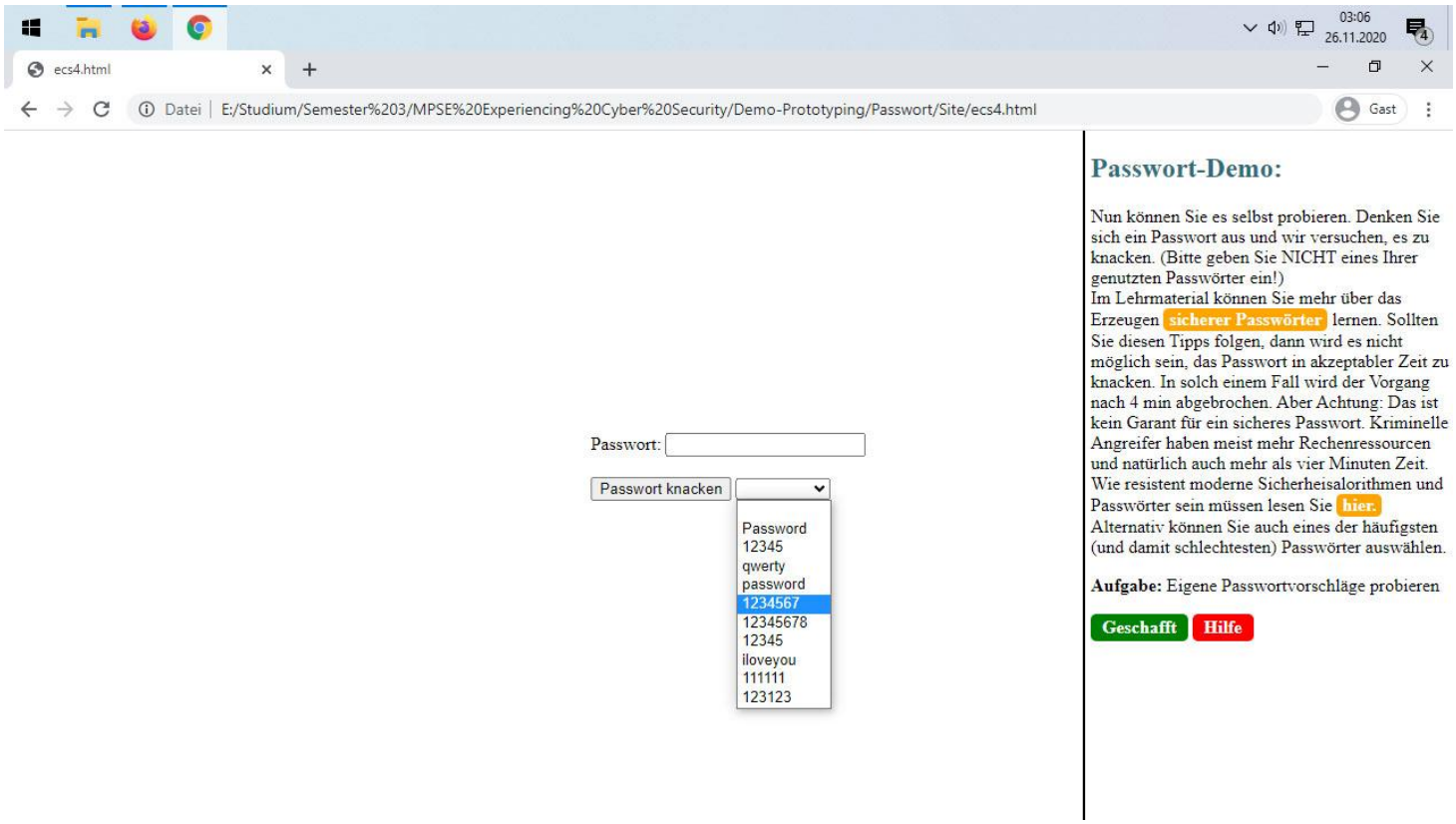
On a button press the password will be cracked by a password cracking tool (most probable John-the-Ripper). Afterwards the elapsed time is shown.



The next step shows that simple tries to “enhance” a password do not make it secure. Again, the password is predefined.



The third step refers to password policies and that following them does not necessarily results in a secure password. This is explained further in the linked teaching material.



Now on the last step the user can try own ideas for a password or, alternatively can choose out of a list with the top 10 most used passwords and see how fast they are cracked. There is opportunity for more learning about password related topics via the teaching material.