Task 8 - Security Tests
Tested application name: https://warsawsneakerstore.com/
Report creation date: 14.12.2022
Author: Kurzydło Paweł

1. Security Defects List:

- Lack of CAPTCHA during registration
- Lack of message when entering an incorrect password during login in the pop-up window (it only works from **https://warsawsneakerstore.com/login**)
- No response from the page instead of applying a time lock on login after entering an incorrect password several times in a row.
- Missing security headers such as Content-Security-Policy, X-Content-Type-Options, Permissions-Policy
- The Mobile Phone form during registration does not have a limit on the number of digits entered.

2. Security Improvement Suggestions:

- Additional confirmation of the password during registration
- Set a limit on the number of digits entered in the Mobile Phone form, e.g. up to 15 digits.
- A message when entering an incorrect password should also appear in the login pop-up window on the website.
- Add CAPTCHA to registration
- Complete the security headers Content-Security-Policy, X-Content-Type-Options, Permissions-Policy
- Add a time lock after three unsuccessful login attempts, for example, for 2 or 3 minutes.

3. Tools used for website security analysis:

https://www.virustotal.com - The tool used to check the application for viruses
https://securityheaders.com/ - The website used to check security headers
The third and last tool used was the developer tools in Safari browser, used to monitor the website's behavior.