proj2: Defense via Content Security Policy

Task1: CSP 2.0

For all levels, the same CSP policy header is included:

```
<meta http-equiv="Content-Security-Policy" content="default-src 'self'; script-src 'self'">
```

script-src 'self' prohibits <script> in html file (all scripts must be local), and for other possible inline scripting (ex: img src) that are not caught by script-src, **default-src 'self'** will handle them. Therefore, this header will force all inline-scripting to be external.

Task2: CSP 3.0

For all levels, the same CSP policy header is included:

```
<meta http-equiv="Content-Security-Policy" content="default-src 'self' 'nonce-2333'; script-src 'nonce-2333'">
```

The nonce-2333 for script-src force all script to have nonce == 2333. Other scripts not caught by script-src (ex: img-src) will be caught by default-src. Therefore, all script is either local or with nonce == 2333. (Note: the value of the nonce was chosen randomly)