CONTENT SECURITY POLICY

- ***1.1: your CSP policy***

1.1 CSP basic example

In this exercise I will assume you use Netlify to host simple HTML pages. Since CSP headers must be set by the server, we must find a way to tell the Netlify server to set the Content-Security-Policy header. It turns out there is a specific mechanism that Netlify uses which allows you to do exactly that. The folder that you will host on Netlify must contain two files:

- index.html (we already know this from previous exercises)
- _headers (a new file that allows us to configure HTTP headers)

A basic example of the contents of a _headers file that sets the content-security-policy header on Netlify-hosted applications is the following:

```
## the path for which the header must be set:
/*
## the actual header:
  Test-header: testvalue;
```

A basic example of a HTML file:

```
<!DOCTYPE html>
<html>
<body>
<h1>This is CSP 1 example</h1>
<a href="javascript:alert(8)"> test link </a>
</body>
</html>
```

Host the folder containing the two files above on Netlify and browse to the result. Click the 'test link' hyperlink. What happens?

Protect against this attack, not by context-sensitive output encoding (which would the better way to protect against this), but by using a CSP.