Information Security with Helmet.js / Quality Assurance Testing with Chai

Securing Node.js Applications

What is Helmet.js

- Node.js module that helps secure HTTP headers
- HTTP headers provide important metadata about the HTTP, request and response, so the client (browser) & server can send additional information in one transaction.
- HTTP headers can leak sensitive information about your applications inadvertently.

How do we set up Helmet.js?

npm install helmet

```
1  const express = require('express');
2  const app = express();
3  const helmet = require('helmet');
4
5  app.use(helmet());
6
7  app.use(helmet.hidePoweredBy());
8
```

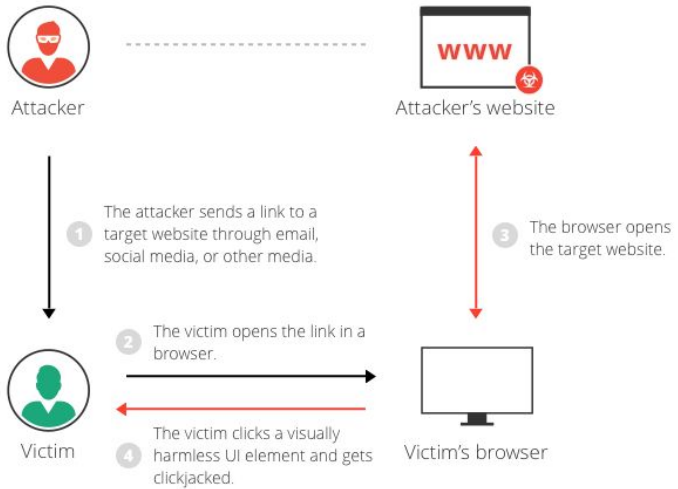
Security

- **helmet.hidePoweredBy()**
- Express leaks information through the X-Powered-By header, which informs the browser which server you're using.
  - X-Powered-By header: HTTP response header.
    - It can be *disabled* and/or *manipulated* by the server!
- Hackers cross reference that information with publicly disclosed known vulnerabilities. (Easily exploits).
- Removes the X-Powered-By header

Clickjacking

- **Clickjacking** is a technique of tricking the user into interacting with a page different from what the user thinks it is.
    - <iframe> placed in html, used to insert content from another source.
    - Ex: Advertisements
- **Frameguard:** Sets a header instructing the browser to keep an eye out for <iframe>. Helps eliminate clickjacking attacks.

```
app.use(helmet.frameguard({ action: 'deny' }));
```



MIME Type: noSniff

- **MIME sniffing** is a technique used by certain web browsers (Primarily *Internet Explorer*) to examine a websites file format.
    - helmet.noSniff()
    - Multipurpose Internet Mail Extension
- **X-Content-Type-Options:** A marker used to identify the MIME types advertised in the content-type.
    - Content-type: a header that tells the client what the content type of returned content actually is.

PreFetching, Caching, Bycript

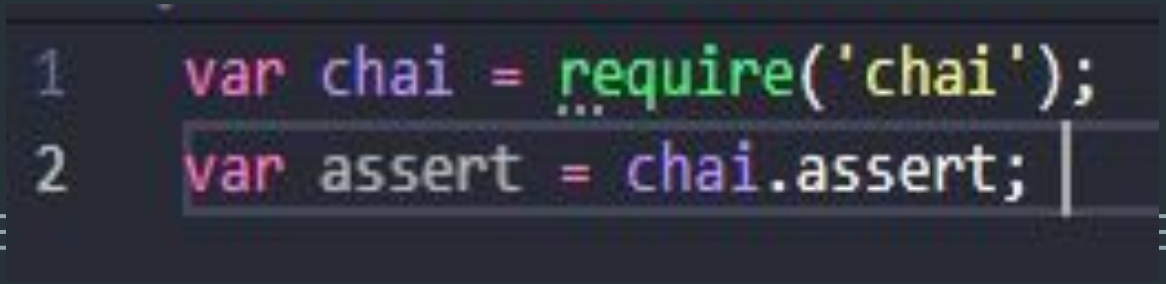
- DNS **prefetch**: boosts performance by fetching instructions/ data from their original storage in a slower memory to a faster local memory before it's needed.
    - Resolves a website IP address before the user clicks on its link.
    - dnsPrefetchControl() - stops DNS prefetch
- Using **noCache** helps boost performance and is useful in development.
- **Bycript** is a password-hashing function, which allows us to build secure and unique passwords.

What is Chai?

- Chai is a Javascript testing library that helps you confirm that your website/program still behaves the way you expect it to after you make changes to your code.
- You can write tests to describe your program's requirements and see if your program meets them.

How can we use Chai?

- npm install chai
- Styles - assert, expect, or should.
  - Assertion: assertions are particular to certain values. Assertions will fail if the expected value does not match the actual value. Uses dot notation to test!
  - Expect: Allows you to include random/your choice messages to prepend any failed assertions. Typically used with non-descript topics (booleans or numbers).
  - Should: Allows for chainable assertions, similar to *expect*. Although it extends each object with a *should* property. (Issues with internet explorer).




NOT SURE IF QUALITY IS REALLY GOOD
OR TESTING WAS REALLY LOUSY