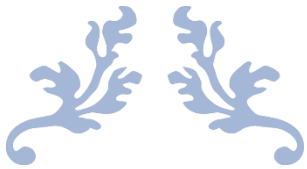

HELMET

Despliegue de Aplicaciones Web

3 DE DICIEMBRE DE 2023

PABLO VALLADARES GONZALEZ

1.-Instalar helmet

Para instalar helmet, lo primero que haremos será dentro de la rama develop, crear una nueva rama llamada feature/helmet

```
# Pez Ejecutivo @ Pecera-de-Negocios in ~\Desktop\Todo\github\API-REST on git:develop [11:28:49]
$ git checkout -b feature/helmet
Switched to a new branch 'feature/helmet'
# Pez Ejecutivo @ Pecera-de-Negocios in ~\Desktop\Todo\github\API-REST on git:feature/helmet [11:28:52]
$
```

Una vez dentro de la rama feature/helmet, instalaremos helmet usando el comando “npm install helmet”

```
$ npm install helmet

added 1 package, and audited 177 packages in 2s

34 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities
```

2.-Utilizar helmet

Una vez lo tenemos instalado, dentro del Código tendremos que importar helmet y usarlo, para esto utilizaremos los comandos:

const helmet = require("helmet"); - para importarlo

app.use(helmet()); - para usarlo

```
//importamos helmet
const helmet = require("helmet");

// Inicializamos la aplicación
const app = express();

//Usamos helmet
app.use(helmet());
```

3.-Configuración de helmet

Por defecto helmet trae las siguientes configuraciones:

Content-Security-Policy: Una potente lista de permisos que especifica qué puede ocurrir en tu página, lo que mitiga muchos tipos de ataques.

Cross-Origin-Opener-Policy: Ayuda a aislar el proceso de tu página.

Cross-Origin-Resource-Policy: Bloquea a otros sitios de cargar tus recursos desde un origen diferente.

Origin-Agent-Cluster: Cambia el aislamiento de procesos para basarse en el origen.

Referrer-Policy: Controla la cabecera Referer.

Strict-Transport-Security: Indica a los navegadores que prefieran HTTPS.

X-Content-Type-Options: Evita la detección de tipos MIME.

X-DNS-Prefetch-Control: Controla la precarga de DNS.

X-Download-Options: Obliga a que las descargas se guarden (solo en Internet Explorer).

X-Frame-Options: Encabezado antiguo que mitiga ataques de clickjacking.

X-Permitted-Cross-Domain-Policies: Controla el comportamiento entre dominios para productos de Adobe, como Acrobat.

X-Powered-By: Información sobre el servidor web. Se elimina porque podría ser utilizado en ataques simples.

X-XSS-Protection: Encabezado antiguo que intenta mitigar ataques XSS, pero empeora las cosas, por lo que Helmet lo deshabilita.

Pero cada apartado de helmet puede ser configurado específicamente por ti, para que cumpla tus requisitos, de la siguiente manera

```
app.use(
    helmet({
        contentSecurityPolicy: {
            directives: {
                "script-src": ["'self'", "example.com"],
            },
        },
    })
);
```

Cada apartado de helmet, además de ser posible de configurar por nuestra propia mano, también es posible de deshabilitar si queremos, de la siguiente manera:

```
app.use(
    helmet({
        contentSecurityPolicy: false,
        xDownloadOptions: false,
    })
);
```

Bibliografía:

-Toda la información obtenida para este trabajo ha sido sacada de la pagina: https://www.npmjs.com/package/helmet

-Las imágenes han sido tomadas desde mi propio VSCode utilizando la extensión Snapcode