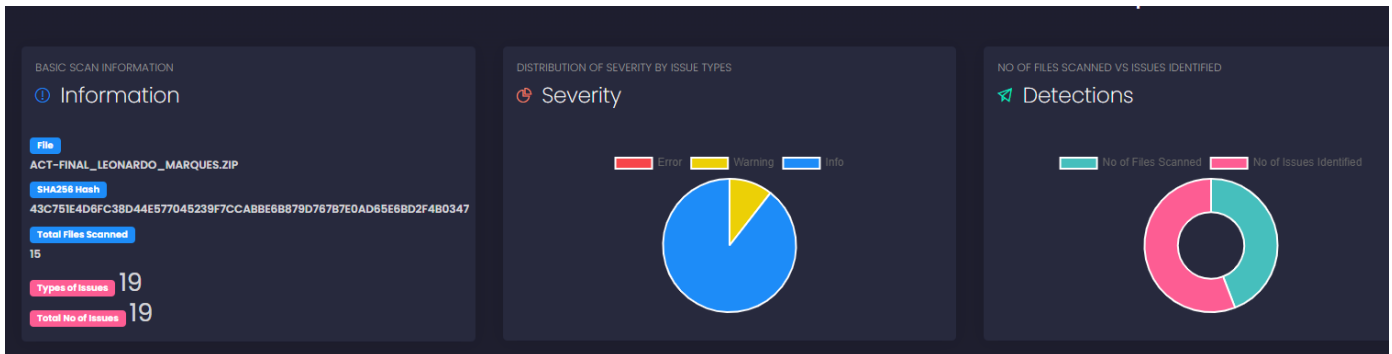
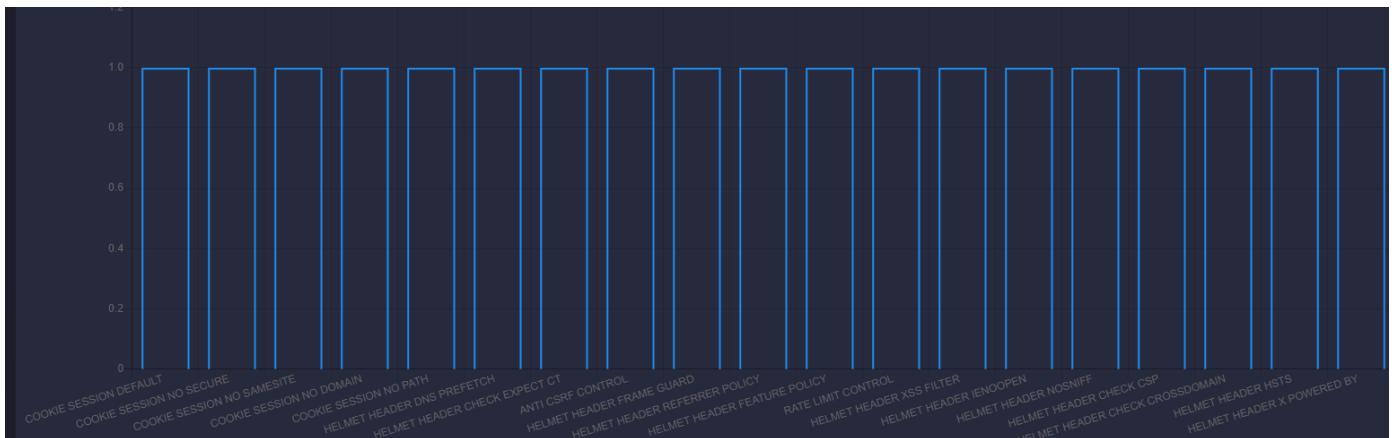


Para la segunda actividad he elegido la misma aplicación de la actividad uno y lo resultado es:

1. Nodejsscan



2. Report



Básicamente en el informe apunta las siguientes clases de Warning.

COOKIE SESSION NO SECURE	Default session middleware settings: `secure` not set. It ensures the browser only sends the cookie over HTTPS.	WARNING	cwe-614
COOKIE SESSION NO SAMESITE	Default session middleware settings: `sameSite` attribute is not configured to strict or lax. These configurations provides protection against Cross Site Request Forgery attacks.	WARNING	cwe-1275

Las issues reportadas están en el fichero: **act-final/config/session.config.js**

▼ COOKIE SESSION DEFAULT - 1

Description: Consider changing the default session cookie name. An attacker can use it to fingerprint the server and target attacks accordingly.

Severity: INFO

OWASP:

CWE: CWE-522: Insufficiently Protected Credentials

File: act-final/config/session.config.js

Lines: [5, 19]

Show Code

View File

Not Applicable

False Positive

✓ COOKIE SESSION NO SECURE - 1

Description: Default session middleware settings: `secure` not set. It ensures the browser only sends the cookie over HTTPS.

Severity: WARNING

OWASP:

CWE: cwe-614

File: act-final/config/session.config.js

Lines: [5, 19]

Show Code View File Not Applicable False Positive

La definición del CWE-614:

*“The **Secure** attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over an HTTP session.”*

En el código:

```
module.exports = session({
  secret: process.env.SESSION_SECRET || 'super secret (change it)',
  resave: true,
  saveUninitialized: false,
  cookie: {
    sameSite: "none",
    secure: process.env.SESSION_SECURE || false,
    httpOnly: true,
    maxAge: process.env.SESSION_MAX_AGE || 3600000,
  },
  store: new MongoStore({
    mongooseConnection: mongoose.connection,
    ttl: process.env.SESSION_MAX_AGE || 3600,
  })
});
```

Lo que se puede mirar que el parámetro está presente y tiene su valor de una variable de entorno, lo que creo que puede ser un false-positive.

▼ COOKIE SESSION NO SAMESITE - 1

Description: Default session middleware settings: `sameSite` attribute is not configured to strict or lax. These configurations provides protection against Cross Site Request Forgery attacks.

Severity: WARNING

OWASP:

CWE: cwe-1275

File: act-final/config/session.config.js

Lines: [5, 19]

Show CodeView FileNot ApplicableFalse Positive

La definición CWE-1275:

“The SameSite attribute controls how cookies are sent for cross-domain requests. This attribute may have three values: 'Lax', 'Strict', or 'None'. If the 'None' value is used, a website may create a cross-domain POST HTTP request to another website, and the browser automatically adds cookies to this request. This may lead to Cross-Site-Request-Forgery (CSRF) attacks if there are no additional protections in place (such as Anti-CSRF tokens).”

En el código:

```
module.exports = session({
  secret: process.env.SESSION_SECRET || 'super secret (change it)',
  resave: true,
  saveUninitialized: false,
  cookie: {
    sameSite: "none",
    secure: process.env.SESSION_SECURE || false,
    httpOnly: true,
    maxAge: process.env.SESSION_MAX_AGE || 3600000,
  },
  store: new MongoStore({
    mongooseConnection: mongoose.connection,
    ttl: process.env.SESSION_MAX_AGE || 3600,
  })
});
```

Un posible corrección puede ser el cambio del valor del parámetro sameSite para 'Lax', 'Strict'