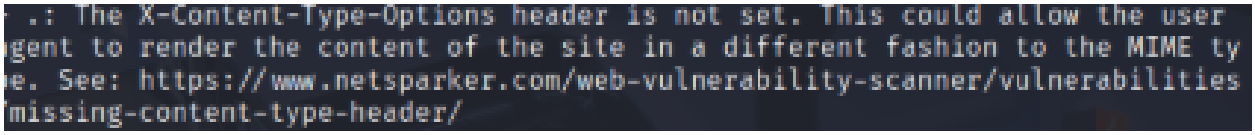
1.1.A05:2021-Security Misconfiguration
CWE ID(s): CWE-16, **CWE-693**

This category highlights security flaws due to improper configuration of the server, application, or related components.

- **Alert Type:** Missing Security Headers
- **Description of the Risk:** Critical HTTP security headers were not present on the web server. These headers provide crucial client-side protection against attacks like clickjacking and MIME-sniffing. Their absence forces browsers to rely on less secure default behaviors.
- **Severity:** Medium/High
- **Evidence:**
    - **Nikto Scan Output:** The scan explicitly reported the absence of key headers.
- 

Brief Description of Root Cause: Lack of explicit configuration on the web server or application framework to include these protective headers in HTTP responses.

Remediation Recommendation:

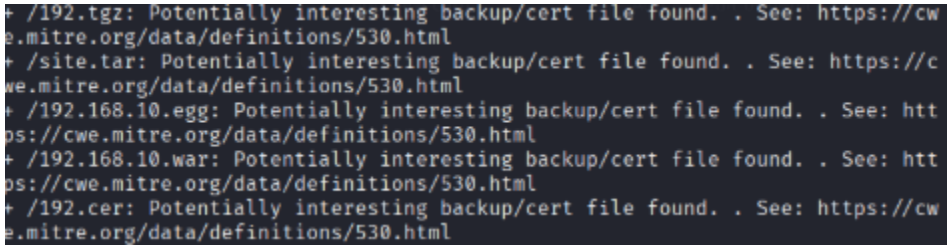
- Configure the web server (e.g., Express.js) to send these headers with every HTTP response. `X-Frame-Options: DENY` prevents clickjacking, `X-XSS-Protection: 1; mode=block` enables browser filters, and `X-Content-Type-Options: nosniff` prevents MIME-sniffing.

Reference:
https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

1.2. A02:2021-Cryptographic Failures (Sensitive Data Exposure)

CWE ID(s): CWE-200

This category relates to improper handling of sensitive data due to weak encryption or misconfigurations.

- **Alert Type:** Potentially Exposed Backup/Certificate Files
- **Description of the Risk:** Backup files, configuration files, and cryptographic key files were found publicly accessible on the web server. These files often contain sensitive information like source code, database credentials, API keys, or private cryptographic keys, which can lead to a full system compromise.
- **Severity:** High
- **Evidence:**
    - **Nikto Scan Output:** Numerous lines indicating "Potentially interesting backup/cert file found," often named after the IP address or common backup patterns.
        - 

Brief Description of Root Cause: Accidental deployment of development or backup files to the production web server, or misconfigured server rules that do not restrict access to these file types.

Remediation Recommendation:

- Remove all unnecessary files from public-facing web servers and implement a strict server policy to deny access to common backup file extensions.
- **Reference:** https://cheatsheetseries.owasp.org/cheatsheets/Sensitive_Data_Exposure_Cheat_Sheet.html

1.3. A07:2021-Identification and Authentication Failures

CWE ID(s): CWE-287

This category includes issues related to broken authentication or session management.

- **Alert Type:** Authentication Failure - 401 Unauthorized on Login Endpoint
- **Description of the Risk:** When attempting to log in with invalid credentials to the login endpoint, the server responded with an HTTP `401 Unauthorized` status code. The

response body provided a generic message: "Invalid email or password." This behavior, while seemingly benign, can indicate a misconfiguration in the application's handling of authentication failures.

- **Severity:** Medium
- **Evidence:**
    - **Burp Suite HTTP History/Repeater:**

32	http://192.168.10.10:3000	POST	/rest/user/login	✓	401	413	text
35	http://192.168.10.10:3000	POST	/rest/user/login	✓	401	413	text
38	http://192.168.10.10:3000	POST	/rest/user/login	✓	401	413	text
41	http://192.168.10.10:3000	POST	/rest/user/login	✓	401	413	text
44	http://192.168.10.10:3000	POST	/rest/user/login	✓	401	413	text
69	http://192.168.10.10:3000	POST	/rest/user/login	✓	401	413	text
72	http://192.168.10.10:3000	POST	/rest/user/login	✓	401	413	text
75	http://192.168.10.10:3000	POST	/rest/user/login	✓	401	413	text

Brief Description of Root Cause: The application's authentication API might be misconfigured to return `401` instead of a `200 OK` with a specific application-level error. This can lead to confusion and potential issues in how different parts of the application or external systems handle authentication failures.

Remediation Recommendation:

- Ensure consistent authentication error handling. For invalid email/password combinations, typically a `200 OK` with a generic application-level error in the response body is preferred over a `401` for simple login forms to avoid confusion with API token issues.

Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

1.4. A01:2021-Broken Access Control

CWE ID(s): CWE-639

This category addresses issues where a user can access resources they are not authorized to.

- **Alert Type: I**nsecure Direct Object Reference (IDOR) - Product Information Leakage
- **Description of the Risk:** The application is vulnerable to Insecure Direct Object References (IDORs), allowing an attacker to access information about different products by manipulating numerical IDs in GET requests without proper authorization checks.
- **Severity:** Medium/High
- **Evidence:**
    - **Burp Suite HTTP History/Repeater: When a `GET` request to a product detail URL (e.g., `http://192.168.10.10:3000/#/products/[ID]`) was**

intercepted and the `[ID]` parameter was tampered with (e.g., changed from 1 to 2), the application returned information about the other product.

-
```
GET /rest/basket/6 HTTP/1.1
```


```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 523
ETag: W/"20b-dNhAfswkbS2pHWBqetQnymhaSuo"
Vary: Accept-Encoding
Date: Sun, 03 Aug 2025 16:40:02 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
    "status":"success",
    "data":{
        "id":6,
        "coupon":null,
        "UserId":23,
        "createdAt":"2025-08-03T16:31:42.342Z",
        "updatedAt":"2025-08-03T16:31:42.342Z",
        "Products":[
            {
                "id":1,
                "name":"Apple Juice (1000ml)",
                "description":"The all-time classic.",
                "price":1.99,
                "deluxePrice":0.99,
                "image":"apple_juice.jpg",
                "createdAt":"2025-08-03T15:28:55.274Z",
                "updatedAt":"2025-08-03T15:28:55.274Z",
                "deletedAt":null,
                "BasketItem":{
                    "ProductId":1,
                    "BasketId":6,
                    "id":9,
                    "quantity":1,
                    "createdAt":
                    "2025-08-03T16:33:34.735Z",
                    "updatedAt":
                    "2025-08-03T16:33:34.735Z"
                }
            }
        ]
    }
}
```


-
-

-
```
1 GET /rest/basket/1 HTTP/1.1
```


```
"createdAt":"2025-08-03T15:28:55.989Z",
"updatedAt":"2025-08-03T15:28:55.989Z",
"Products":[
    {
        "id":1,
        "name":"Apple Juice (1000ml)",
        "description":"The all-time classic.",
        "price":1.99,
        "deluxePrice":0.99,
        "image":"apple_juice.jpg",
        "createdAt":"2025-08-03T15:28:55.274Z",
        "updatedAt":"2025-08-03T15:28:55.274Z",
        "deletedAt":null,
        "BasketItem":{
            "ProductId":1,
            "BasketId":1,
            "id":1,
            "quantity":2,
            "createdAt":
            "2025-08-03T15:28:56.184Z",
            "updatedAt":
            "2025-08-03T15:28:56.184Z"
        }
    },
    {
        "id":2,
        "name":"Orange Juice (1000ml)",
        "description":
        "Made from oranges hand-picked by Uncle
        ittmeyer.",
        "price":2.99,
        "deluxePrice":2.49,
        "image":"orange_juice.jpg",
        "createdAt":"2025-08-03T15:28:55.274Z",
        "updatedAt":"2025-08-03T15:28:55.274Z",
        "deletedAt":null,
        "BasketItem":{
            "ProductId":2,
            "BasketId":1,
            "id":2,
            "quantity":3,
            "createdAt":
            "2025-08-03T15:28:56.185Z",
            "updatedAt":
            "2025-08-03T15:28:56.185Z"
        }
    },
    {
        "id":3,
        "name":"Eggfruit Juice (500ml)",
        "description":
        "Now with even more exotic flavour.",
        "price":8.99,
        "deluxePrice":8.99,
        "image":"eggfruit_juice.jpg",
        "createdAt":"2025-08-03T15:28:55.274Z",
        "updatedAt":"2025-08-03T15:28:55.274Z",
        "deletedAt":null,
        "BasketItem":{
            "ProductId":3,
            "BasketId":1,
            "id":3,
            "quantity":1,
            "createdAt":
            "2025-08-03T15:28:56.185Z",
            "updatedAt":
            "2025-08-03T15:28:56.185Z"
        }
```


Brief Description of Root Cause: The application fails to perform authorization checks when retrieving objects based on user-supplied input. It directly uses the ID without verifying if the requesting user is authorized to view that specific product.

Remediation Recommendation:

- Implement robust, server-side access control checks for all direct object references. Before serving any data, verify that the authenticated user is explicitly authorized to access that specific resource.

Reference:

https://cheatsheetseries.owasp.org/cheatsheets/Access_Control_Cheat_Sheet.html

1.5. A08:2021-Software and Data Integrity Failures
CWE ID(s): CWE-829

- **Alert Type: Cross-Domain JavaScript Source File Inclusion**
- **Description of the Risk: The application includes JavaScript files from a third-party domain without using a Subresource Integrity (SRI) hash. This poses a risk because if the third-party domain were compromised, the attacker could modify the JavaScript file to execute malicious code on your site.**
- **Severity: Medium**
- **Evidence:**
    - **OWASP ZAP Scans: The passive scan flagged a "Cross-Domain JavaScript Source File Inclusion" alert.**

Brief Description of Root Cause: The application relies on a third-party source for a JavaScript file without validating its integrity.

Remediation Recommendation:

- Implement Subresource Integrity (SRI) for all cross-domain script and style files. The SRI hash ensures that the browser will only load the file if its content matches the expected hash.
- Reference:
    - **https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity**