Threat Modeling Report

Project: batavia-client-master

Property	Value
Project Name	batavia-client-master
Analysis Date	2025-10-18T21:45:23.210269
Methodology	STRIDE
Total Findings	16
Risk Level	MEDIUM

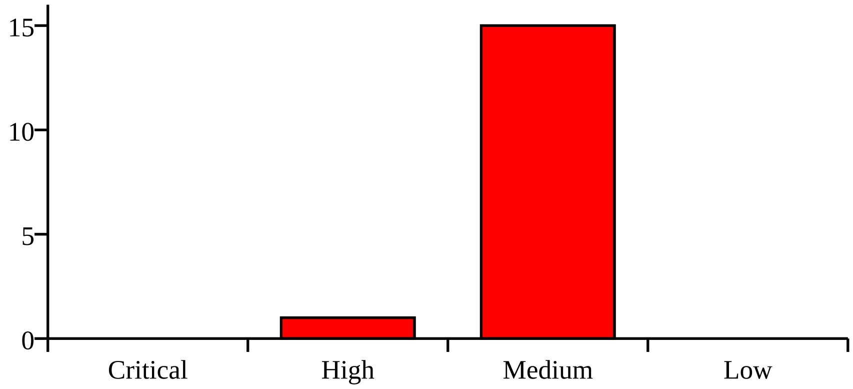
Executive Summary

This security assessment of **batavia-client-master** identified **16** potential security threats using the STRIDE methodology. The overall risk level is assessed as MEDIUM.

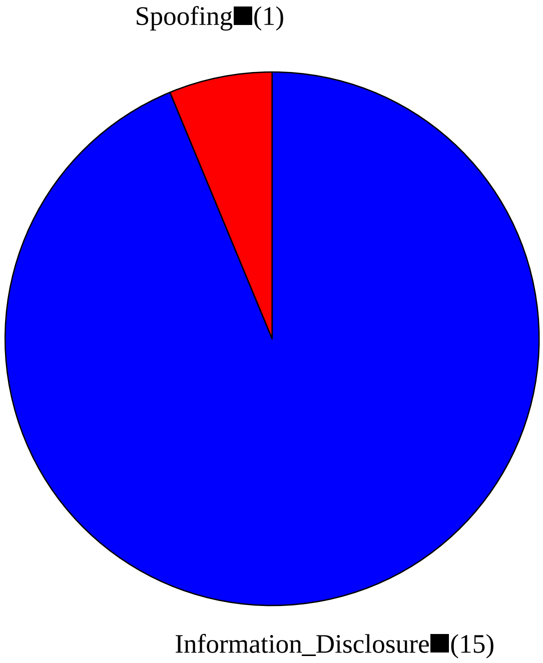
Key Findings:
- Critical vulnerabilities: 0
- High-severity issues: 1
- Medium-priority concerns: 15
- Low-priority items: 0

Immediate attention is required for all critical and high-severity vulnerabilities to prevent potential security breaches.

Threat Severity Distribution



STRIDE Category Distribution



STRIDE Methodology Overview

STRIDE is a threat modeling methodology developed by Microsoft that categorizes security threats into six main areas:

S - Spoofing Identity: Impersonating someone or something else to gain unauthorized access
T - Tampering with Data: Malicious modification of data or code
R - Repudiation: Users denying they performed an action without the system being able to prove otherwise
I - Information Disclosure: Exposure of information to individuals who shouldn't have access
D - Denial of Service: Attacks that deny or degrade service for legitimate users
E - Elevation of Privilege: A user gains capabilities without proper authorization

Each identified threat is categorized into one of these areas and assessed for severity and impact.

Project Architecture Analysis

Code Analysis Summary:
• Files analyzed: 3
• Programming languages: TypeScript
• Threat detection patterns: STRIDE-based security analysis
• Analysis depth: Source code static analysis with context awareness

Detailed Security Findings

Finding #1: Hardcoded password

Property	Details
Severity	High
STRIDE Category	Spoofing
CWE ID	CWE-798
Confidence Score	0.80
File Location	batavia-client-master/src/app/modules/login/login.component.ts:19
Attack Vector	Identity theft, credential compromise, session hijacking

Description:

Hardcoded password detected in TypeScript code

Code Evidence:

```
private ngUnsubscribe$ = new Subject<void>(); username = ''; >>> password =
''; showErrorMsg = false; returnUrl: string;
```

Proof of Concept:

Steps to Reproduce:
1. Review source code for hardcoded credentials
2. Extract username/password from code
3. Attempt authentication using discovered credentials
4. Verify unauthorized access to protected resources

Impact: Unauthorized system access, credential compromise

Remediation:

Use environment variables or secure credential management

Business Impact:

Unauthorized access, account takeover, service disruption

Finding #2: Insecure HTTP usage

Property	Details

Severity	Medium
STRIDE Category	Information_Disclosure
CWE ID	CWE-319
Confidence Score	0.70
File Location	batavia-client-master/src/polyfills.ts:33
Attack Vector	Data leakage, privacy violations, sensitive exposure

Description:

Insecure HTTP usage detected in TypeScript code

Code Evidence:

```
/** * Required to support Web Animations `@angular/animation`. >>> * Needed
for: All but Chrome, Firefox and Opera.
http://caniuse.com/#feat=web-animation **/
```

Proof of Concept:

Steps to Reproduce:
1. Identify information exposure point
2. Analyze data access controls
3. Attempt unauthorized data access
4. Extract sensitive information
5. Verify information disclosure

Impact: Data breach, privacy violation

Remediation:

Use HTTPS/TLS for all communications

Business Impact:

Minor data exposure, potential privacy concerns

Finding #3: Insecure HTTP usage

Property	Details
Severity	Medium
STRIDE Category	Information_Disclosure
CWE ID	CWE-319
Confidence Score	0.70
File Location	batavia-client-master/src/environments/environment.ts:12
Attack Vector	Data leakage, privacy violations, sensitive exposure

Description:

Insecure HTTP usage detected in TypeScript code

Code Evidence:

```
VERSION: require('../../package.json').version, // baseApiUrl:
'https://controlcenter.stage.halodoc.com', >>> baseApiUrl:
'http://localhost:4200', baseAuthUrl: '/api', googleMapApi: {
```

Proof of Concept:

Steps to Reproduce:
1. Identify information exposure point
2. Analyze data access controls
3. Attempt unauthorized data access
4. Extract sensitive information
5. Verify information disclosure

Impact: Data breach, privacy violation

Remediation:

Use HTTPS/TLS for all communications

Business Impact:

Minor data exposure, potential privacy concerns

Finding #4: Insecure HTTP usage

Property	Details
Severity	Medium

STRIDE Category	Information_Disclosure
CWE ID	CWE-319
Confidence Score	0.70
File Location	batavia-client-master/src/environments/environment.ts:29
Attack Vector	Data leakage, privacy violations, sensitive exposure

Description:

Insecure HTTP usage detected in TypeScript code

Code Evidence:

```
mfeConfig: { bataviaCmsMfe: { >>> remoteEntry:
'http://localhost:4200/cms-mfe/remoteEntry.js', exposedModule:
'CmsMfeWrapperModule', },
```

Proof of Concept:

Steps to Reproduce:
1. Identify information exposure point
2. Analyze data access controls
3. Attempt unauthorized data access
4. Extract sensitive information
5. Verify information disclosure

Impact: Data breach, privacy violation

Remediation:

Use HTTPS/TLS for all communications

Business Impact:

Minor data exposure, potential privacy concerns

Finding #5: Insecure HTTP usage

Property	Details
Severity	Medium
STRIDE Category	Information_Disclosure
CWE ID	CWE-319
Confidence Score	0.70
File Location	batavia-client-master/src/environments/environment.ts:33
Attack Vector	Data leakage, privacy violations, sensitive exposure

Description:

Insecure HTTP usage detected in TypeScript code

Code Evidence:

```
}, bataviaLabsMfe: { >>> remoteEntry:
'http://localhost:4200/labs-mfe/remoteEntry.js', exposedModule:
'LabsMfeWrapperModule', },
```

Proof of Concept:

Steps to Reproduce:
1. Identify information exposure point
2. Analyze data access controls
3. Attempt unauthorized data access
4. Extract sensitive information
5. Verify information disclosure

Impact: Data breach, privacy violation

Remediation:

Use HTTPS/TLS for all communications

Business Impact:

Minor data exposure, potential privacy concerns

Finding #6: Insecure HTTP usage

Property	Details
Severity	Medium

STRIDE Category	Information_Disclosure
CWE ID	CWE-319
Confidence Score	0.70
File Location	batavia-client-master/src/environments/environment.ts:37
Attack Vector	Data leakage, privacy violations, sensitive exposure

Description:

Insecure HTTP usage detected in TypeScript code

Code Evidence:

```
}, bataviaHospitalMfe: { >>> remoteEntry:
'http://localhost:4200/hospital-mfe/remoteEntry.js', exposedModule:
'HospitalMfeWrapperModule', },
```

Proof of Concept:

Steps to Reproduce:
1. Identify information exposure point
2. Analyze data access controls
3. Attempt unauthorized data access
4. Extract sensitive information
5. Verify information disclosure

Impact: Data breach, privacy violation

Remediation:

Use HTTPS/TLS for all communications

Business Impact:

Minor data exposure, potential privacy concerns

Finding #7: Insecure HTTP usage

Property	Details
Severity	Medium
STRIDE Category	Information_Disclosure
CWE ID	CWE-319
Confidence Score	0.70
File Location	batavia-client-master/src/environments/environment.ts:41
Attack Vector	Data leakage, privacy violations, sensitive exposure

Description:

Insecure HTTP usage detected in TypeScript code

Code Evidence:

```
}, bataviaSubscriptionsMfe: { >>> remoteEntry:
'http://localhost:4200/subscriptions-mfe/remoteEntry.js', exposedModule:
'SubscriptionsMfeWrapperModule', },
```

Proof of Concept:

Steps to Reproduce:
1. Identify information exposure point
2. Analyze data access controls
3. Attempt unauthorized data access
4. Extract sensitive information
5. Verify information disclosure

Impact: Data breach, privacy violation

Remediation:

Use HTTPS/TLS for all communications

Business Impact:

Minor data exposure, potential privacy concerns

Finding #8: Insecure HTTP usage

Property	Details
Severity	Medium

STRIDE Category	Information_Disclosure
CWE ID	CWE-319
Confidence Score	0.70
File Location	batavia-client-master/src/environments/environment.ts:45
Attack Vector	Data leakage, privacy violations, sensitive exposure

Description:

Insecure HTTP usage detected in TypeScript code

Code Evidence:

```
}, bataviaContactDoctorMfe: { >>> remoteEntry:
'http://localhost:4200/contact-doctor-mfe/remoteEntry.js', exposedModule:
'ContactDoctorMfeWrapperModule', },
```

Proof of Concept:

Steps to Reproduce:
1. Identify information exposure point
2. Analyze data access controls
3. Attempt unauthorized data access
4. Extract sensitive information
5. Verify information disclosure

Impact: Data breach, privacy violation

Remediation:

Use HTTPS/TLS for all communications

Business Impact:

Minor data exposure, potential privacy concerns

Finding #9: Insecure HTTP usage

Property	Details
Severity	Medium
STRIDE Category	Information_Disclosure
CWE ID	CWE-319
Confidence Score	0.70
File Location	batavia-client-master/src/environments/environment.ts:49
Attack Vector	Data leakage, privacy violations, sensitive exposure

Description:

Insecure HTTP usage detected in TypeScript code

Code Evidence:

```
}, bataviaFinanceMfe: { >>> remoteEntry:
'http://localhost:4200/finance-mfe/remoteEntry.js', exposedModule:
'FinanceMfeWrapperModule', },
```

Proof of Concept:

Steps to Reproduce:
1. Identify information exposure point
2. Analyze data access controls
3. Attempt unauthorized data access
4. Extract sensitive information
5. Verify information disclosure

Impact: Data breach, privacy violation

Remediation:

Use HTTPS/TLS for all communications

Business Impact:

Minor data exposure, potential privacy concerns

Finding #10: Insecure HTTP usage

Property	Details
Severity	Medium

STRIDE Category	Information_Disclosure
CWE ID	CWE-319
Confidence Score	0.70
File Location	batavia-client-master/src/environments/environment.ts:53
Attack Vector	Data leakage, privacy violations, sensitive exposure

Description:

Insecure HTTP usage detected in TypeScript code

Code Evidence:

```
}, bataviaMarketingMfe: { >>> remoteEntry:
'http://localhost:4200/marketing-mfe/remoteEntry.js', exposedModule:
'MarketingMfeWrapperModule', },
```

Proof of Concept:

Steps to Reproduce:
1. Identify information exposure point
2. Analyze data access controls
3. Attempt unauthorized data access
4. Extract sensitive information
5. Verify information disclosure

Impact: Data breach, privacy violation

Remediation:

Use HTTPS/TLS for all communications

Business Impact:

Minor data exposure, potential privacy concerns

Finding #11: Insecure HTTP usage

Property	Details
Severity	Medium
STRIDE Category	Information_Disclosure
CWE ID	CWE-319
Confidence Score	0.70
File Location	batavia-client-master/src/environments/environment.ts:57
Attack Vector	Data leakage, privacy violations, sensitive exposure

Description:

Insecure HTTP usage detected in TypeScript code

Code Evidence:

```
}, bataviaCustomersMfe: { >>> remoteEntry:
'http://localhost:4200/customers-mfe/remoteEntry.js', exposedModule:
'CustomersMfeWrapperModule', },
```

Proof of Concept:

Steps to Reproduce:
1. Identify information exposure point
2. Analyze data access controls
3. Attempt unauthorized data access
4. Extract sensitive information
5. Verify information disclosure

Impact: Data breach, privacy violation

Remediation:

Use HTTPS/TLS for all communications

Business Impact:

Minor data exposure, potential privacy concerns

Finding #12: Insecure HTTP usage

Property	Details
Severity	Medium

STRIDE Category	Information_Disclosure
CWE ID	CWE-319
Confidence Score	0.80
File Location	batavia-client-master/src/environments/environment.ts:61
Attack Vector	Data leakage, privacy violations, sensitive exposure

Description:

Insecure HTTP usage detected in TypeScript code

Code Evidence:

```
}, bataviaAdministrationMfe: { >>> remoteEntry:
'http://localhost:4200/users-mfe/remoteEntry.js', exposedModule:
'AdministrationMfeWrapperModule', },
```

Proof of Concept:

Steps to Reproduce:
1. Identify information exposure point
2. Analyze data access controls
3. Attempt unauthorized data access
4. Extract sensitive information
5. Verify information disclosure

Impact: Data breach, privacy violation

Remediation:

Use HTTPS/TLS for all communications

Business Impact:

Minor data exposure, potential privacy concerns

Finding #13: Insecure HTTP usage

Property	Details
Severity	Medium
STRIDE Category	Information_Disclosure
CWE ID	CWE-319
Confidence Score	0.70
File Location	batavia-client-master/src/environments/environment.ts:65
Attack Vector	Data leakage, privacy violations, sensitive exposure

Description:

Insecure HTTP usage detected in TypeScript code

Code Evidence:

```
}, bataviaEtoolsMfe: { >>> remoteEntry:
'http://localhost:4200/etools-mfe/remoteEntry.js', exposedModule:
'EtoolsMfeWrapperModule', },
```

Proof of Concept:

Steps to Reproduce:
1. Identify information exposure point
2. Analyze data access controls
3. Attempt unauthorized data access
4. Extract sensitive information
5. Verify information disclosure

Impact: Data breach, privacy violation

Remediation:

Use HTTPS/TLS for all communications

Business Impact:

Minor data exposure, potential privacy concerns

Finding #14: Insecure HTTP usage

Property	Details
Severity	Medium

STRIDE Category	Information_Disclosure
CWE ID	CWE-319
Confidence Score	0.70
File Location	batavia-client-master/src/environments/environment.ts:69
Attack Vector	Data leakage, privacy violations, sensitive exposure

Description:

Insecure HTTP usage detected in TypeScript code

Code Evidence:

```
}, bataviaInsuranceMfe: { >>> remoteEntry:
'http://localhost:4200/insurance-mfe/remoteEntry.js', exposedModule:
'InsuranceMfeWrapperModule', },
```

Proof of Concept:

Steps to Reproduce:
1. Identify information exposure point
2. Analyze data access controls
3. Attempt unauthorized data access
4. Extract sensitive information
5. Verify information disclosure

Impact: Data breach, privacy violation

Remediation:

Use HTTPS/TLS for all communications

Business Impact:

Minor data exposure, potential privacy concerns

Finding #15: Insecure HTTP usage

Property	Details
Severity	Medium
STRIDE Category	Information_Disclosure
CWE ID	CWE-319
Confidence Score	0.70
File Location	batavia-client-master/src/environments/environment.ts:73
Attack Vector	Data leakage, privacy violations, sensitive exposure

Description:

Insecure HTTP usage detected in TypeScript code

Code Evidence:

```
}, bataviaPharmacyMfe: { >>> remoteEntry:
'http://localhost:4200/pharmacy-mfe/remoteEntry.js', exposedModule:
'PharmacyMfeWrapperModule', },
```

Proof of Concept:

Steps to Reproduce:
1. Identify information exposure point
2. Analyze data access controls
3. Attempt unauthorized data access
4. Extract sensitive information
5. Verify information disclosure

Impact: Data breach, privacy violation

Remediation:

Use HTTPS/TLS for all communications

Business Impact:

Minor data exposure, potential privacy concerns

Finding #16: Insecure HTTP usage

Property	Details
Severity	Medium

STRIDE Category	Information_Disclosure
CWE ID	CWE-319
Confidence Score	0.70
File Location	batavia-client-master/src/environments/environment.ts:77
Attack Vector	Data leakage, privacy violations, sensitive exposure

Description:

Insecure HTTP usage detected in TypeScript code

Code Evidence:

```
}, medexDeliveryMfe: { >>> remoteEntry:
'http://localhost:4200/medex-mfe/remoteEntry.js', exposedModule:
'MedexMfeWrapperModule', },
```

Proof of Concept:

Steps to Reproduce:
1. Identify information exposure point
2. Analyze data access controls
3. Attempt unauthorized data access
4. Extract sensitive information
5. Verify information disclosure

Impact: Data breach, privacy violation

Remediation:

Use HTTPS/TLS for all communications

Business Impact:

Minor data exposure, potential privacy concerns

Remediation Summary

Remediation Priority Matrix

■ IMMEDIATE (0-7 days) - Critical Issues: 0
Critical vulnerabilities pose immediate risk to business operations and must be addressed urgently. Recommended actions: Emergency patches, temporary mitigations, incident response preparation.

■ HIGH PRIORITY (1-4 weeks) - High Severity: 1
High-severity issues should be addressed in the next sprint cycle. Recommended actions: Security patches, code reviews, testing validation.

■ MEDIUM PRIORITY (1-3 months) - Medium Severity: 15
Medium-severity issues can be addressed in regular development cycles. Recommended actions: Security improvements, best practice implementation, monitoring enhancement.

Implementation Guidelines:

- Establish security champion within development team
- Implement security testing in CI/CD pipeline
- Conduct regular security code reviews
- Provide security training for developers
- Monitor for new vulnerabilities and threat intelligence
- Regular penetration testing and security assessments