



OWASP TOP 10 2021

OnTrack Web (<http://localhost:4200>)**Description**

The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risk problem areas - and also provides guidance on where to go from here.

Disclaimer

This document or any of its content cannot account for, or be included in any form of legal advice. The outcome of a vulnerability scan (or security evaluation) should be utilized to ensure that diligent measures are taken to lower the risk of potential exploits carried out to compromise data.

Legal advice must be supplied according to its legal context. All laws and the environments in which they are applied, are constantly changed and revised. Therefore no information provided in this document may ever be used as an alternative to a qualified legal body or representative.

A portion of this report is taken from OWASP's Top Ten 2021 Project document, that can be found at <http://www.owasp.org>.

Scan Detail

Target	http://192.168.0.128:4200 - OnTrack Web
Scan Type	Full Scan
Start Time	Nov 30, 2024, 2:56:18 PM GMT+11
Scan Duration	2 minutes
Requests	7851
Average Response Time	1ms
Maximum Response Time	2684ms
Application Build	v24.1.240111130
Authentication Profile	-

Compliance at a Glance

CATEGORY

- | | |
|---|--|
| 3 | A01 Broken Access Control |
| 3 | A02 Cryptographic Failures |
| 0 | A03 Injection |
| 3 | A04 Insecure Design |
| 6 | A05 Security Misconfiguration |
| 7 | A06 Vulnerable and Outdated Components |
| 1 | A07 Identification and Authentication Failures |
| 0 | A08 Software and Data Integrity Failures |
| 0 | A09 Security Logging and Monitoring Failures |
| 0 | A10 Server-Side Request Forgery |

Detailed Compliance Report by Category

This section is a detailed report that explains each vulnerability found according to individual compliance categories.

A01 Broken Access Control

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

Clickjacking: X-Frame-Options header

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites.

CWE

CWE-1021

CVSS2

AV:N/AC:M/Au:N/C:N/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

The impact depends on the affected web application.

<http://192.168.0.128:4200/>

Paths without secure XFO header:

- http://192.168.0.128:4200/
- http://192.168.0.128:4200/assets/icons/
- http://192.168.0.128:4200/crossdomain.xml
- http://192.168.0.128:4200/sitemap.xml.gz
- http://192.168.0.128:4200/clientaccesspolicy.xml
- http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-italic.otf
- http://192.168.0.128:4200/sitemap.xml
- http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-regular.otf

- http://192.168.0.128:4200/assets/images/
- http://192.168.0.128:4200/assets/fonts/grotesk/
- http://192.168.0.128:4200/assets/
- http://192.168.0.128:4200/assets/fonts/
- http://192.168.0.128:4200/ws

Request

```
GET / HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

Clickjacking

<https://en.wikipedia.org/wiki/Clickjacking>

OWASP Clickjacking

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

Frame Buster Buster

<https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed>

Sensitive pages could be cached

One or more pages contain possible sensitive information (e.g. a password parameter) and could be potentially cached. Even in secure SSL channels sensitive data could be stored by intermediary proxies and SSL terminators. To prevent this, a Cache-Control header should be specified.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible sensitive information disclosure.

<http://192.168.0.128:4200/>

List of pages that could be cached:

- http://192.168.0.128:4200/?password=u]H[ww6KrA9F.x-F&username=eKJxcvFc

Request

```
GET /?password=u]H[ww6KrA9F.x-F&username=eKJxcvFc HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

Prevent caching by adding "Cache Control: No-store" and "Pragma: no-cache" to the HTTP response header.

Access-Control-Allow-Origin header with wildcard (*) value

Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the resource originated. The Access-Control-Allow-Origin header indicates whether a resource can be shared based on the value of the Origin request header, "*", or "null" in the response.

If a website responds with Access-Control-Allow-Origin: * the requested resource allows sharing with every origin. Therefore, any website can make XHR (XMLHttpRequest) requests to the site and access the responses.

CWE

CWE-284

CVSS2

AV:N/AC:H/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Any website can make XHR requests to the site and access the responses.

<http://192.168.0.128:4200/>

Affected paths (max. 25):

- /
- /assets/icons/
- /assets/
- /crossdomain.xml
- /sitemap.xml.gz

- /manifest.webmanifest
- /clientaccesspolicy.xml
- /assets/fonts/grotesk/grotesk-italic.otf
- /sitemap.xml
- /assets/fonts/grotesk/grotesk-regular.otf
- /assets/images/
- /assets/fonts/grotesk/
- /assets/fonts/
- /ws

Request

```
GET / HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

Check whether Access-Control-Allow-Origin: * is appropriate for the resource/response.

References

[Test Cross Origin Resource Sharing \(OTG-CLIENT-007\)](#)

[https://www.owasp.org/index.php/Test_Cross_Origin_Resource_Sharing_\(OTG-CLIENT-007\)](https://www.owasp.org/index.php/Test_Cross_Origin_Resource_Sharing_(OTG-CLIENT-007))

[Cross-origin resource sharing](#)

https://en.wikipedia.org/wiki/Cross-origin_resource_sharing

[Cross-Origin Resource Sharing](#)

<http://www.w3.org/TR/cors/>

[CrossOriginRequestSecurity](#)

<https://code.google.com/p/html5security/wiki/CrossOriginRequestSecurity>

[Cross-Origin Resource Sharing \(CORS\) and the Access-Control-Allow-Origin Header](#)

<https://www.acunetix.com/blog/web-security-zone/cross-origin-resource-sharing-cors-access-control-allow-origin-header/>

[PortSwigger Research on CORS misconfiguration](#)

<https://portswigger.net/research/exploiting-cors-misconfigurations-for-bitcoins-and-bounties>

A02 Cryptographic Failures

The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS).

Sensitive pages could be cached

One or more pages contain possible sensitive information (e.g. a password parameter) and could be potentially cached. Even in secure SSL channels sensitive data could be stored by intermediary proxies and SSL terminators. To prevent this, a Cache-Control header should be specified.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None

Integrity Impact	None
Availability Impact	None

Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible sensitive information disclosure.

<http://192.168.0.128:4200/>

List of pages that could be cached:

- http://192.168.0.128:4200/?password=u]H[ww6KrA9F.x-F&username=eKJxcvFc

Request

```
GET /?password=u]H[ww6KrA9F.x-F&username=eKJxcvFc HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

Prevent caching by adding "Cache Control: No-store" and "Pragma: no-cache" to the HTTP response header.

Javascript Source map detected

Client side Javascript source code can be combined, minified or compiled. A source map is a file that maps from the transformed source to the original source. Source map may help an attacker to read and debug Javascript.

CWE

CWE-16

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Access to source maps may help an attacker to read and debug Javascript code. It simplifies finding client-side vulnerabilities

URLs where links to SourceMaps were found:

- sourceMappingURL in JS body - http://192.168.0.128:4200/main.js
- sourceMappingURL in JS body - http://192.168.0.128:4200/polyfills.js
- sourceMappingURL in JS body - http://192.168.0.128:4200/runtime.js
- sourceMappingURL in JS body - http://192.168.0.128:4200/styles.js
- sourceMappingURL in JS body - http://192.168.0.128:4200/vendor.js

Request

```
GET /main.js HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

According to the best practices, source maps should not be accessible for an attacker. Consult web references for more information

References

[Using sourcemaps on production without exposing the source code](#)

<https://itnext.io/using-sourcemaps-on-production-without-revealing-the-source-code-%EF%B8%8F-d41e78e20c89>

[SPA source code recovery by un-Webpacking source maps](#)

<https://medium.com/@rarecoil/spa-source-code-recovery-by-un-webpacking-source-maps-ef830fc2351d>

SSL/TLS Not Implemented

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/V:L/VA:N/SC:N/SI:N/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

<http://192.168.0.128:4200/>

Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

A03 Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

No alerts in this category

A04 Insecure Design

Insecure design is a broad category representing different weaknesses, expressed as "missing or ineffective control design." Insecure design is not the source for all other Top 10 risk categories. There is a difference between insecure design and insecure implementation. We differentiate between design flaws and implementation defects for a reason, they have different root causes and remediation. A secure design can still have implementation defects leading to vulnerabilities that may be exploited. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks. One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.

Clickjacking: X-Frame-Options header

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites.

CWE

CWE-1021

CVSS2

AV:N/AC:M/Au:N/C:N/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

The impact depends on the affected web application.

http://192.168.0.128:4200/

Paths without secure XFO header:

- http://192.168.0.128:4200/
- http://192.168.0.128:4200/assets/icons/
- http://192.168.0.128:4200/crossdomain.xml
- http://192.168.0.128:4200/sitemap.xml.gz
- http://192.168.0.128:4200/clientaccesspolicy.xml
- http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-italic.otf
- http://192.168.0.128:4200/sitemap.xml
- http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-regular.otf
- http://192.168.0.128:4200/assets/images/
- http://192.168.0.128:4200/assets/fonts/grotesk/
- http://192.168.0.128:4200/assets/
- http://192.168.0.128:4200/assets/fonts/
- http://192.168.0.128:4200/ws

Request

```

GET / HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive

```

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

Clickjacking

<https://en.wikipedia.org/wiki/Clickjacking>

OWASP Clickjacking

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

Frame Buster Buster

<https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed>

Content Security Policy (CSP) Not Implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

Content-Security-Policy:

```
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

<http://192.168.0.128:4200/>

Paths without CSP header:

- <http://192.168.0.128:4200/>

- http://192.168.0.128:4200/assets/icons/
- http://192.168.0.128:4200/crossdomain.xml
- http://192.168.0.128:4200/sitemap.xml.gz
- http://192.168.0.128:4200/clientaccesspolicy.xml
- http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-italic.otf
- http://192.168.0.128:4200/sitemap.xml
- http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-regular.otf
- http://192.168.0.128:4200/assets/images/
- http://192.168.0.128:4200/assets/fonts/grotesk/
- http://192.168.0.128:4200/assets/
- http://192.168.0.128:4200/assets/fonts/
- http://192.168.0.128:4200/ws

Request

```
GET / HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy \(CSP\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

[Implementing Content Security Policy](#)

<https://hacks.mozilla.org/2016/02/implementing-content-security-policy/>

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None

Impact		Availability Impact	None
		Availability Impact to the Vulnerable System	None
		Confidentiality Impact to the Subsequent System	None
		Integrity Impact to the Subsequent System	None
		Availability Impact to the Subsequent System	None

Impact

<http://192.168.0.128:4200/>

Locations without Permissions-Policy header:

- http://192.168.0.128:4200/
- http://192.168.0.128:4200/assets/icons/
- http://192.168.0.128:4200/crossdomain.xml
- http://192.168.0.128:4200/sitemap.xml.gz
- http://192.168.0.128:4200/clientaccesspolicy.xml
- http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-italic.otf
- http://192.168.0.128:4200/sitemap.xml
- http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-regular.otf
- http://192.168.0.128:4200/assets/images/
- http://192.168.0.128:4200/assets/fonts/grotesk/
- http://192.168.0.128:4200/assets/
- http://192.168.0.128:4200/assets/fonts/
- http://192.168.0.128:4200/ws

Request

```
GET / HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

References

[Permissions-Policy / Feature-Policy \(MDN\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy>

[Permissions Policy \(W3C\)](#)

<https://www.w3.org/TR/permissions-policy-1/>

A05 Security Misconfiguration

Security misconfiguration is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.

Sensitive pages could be cached

One or more pages contain possible sensitive information (e.g. a password parameter) and could be potentially cached. Even in secure SSL channels sensitive data could be stored by intermediary proxies and SSL terminators. To prevent this, a Cache-Control header should be specified.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Access Vector	Network
Access	Low

Base Score	5.3
Attack Vector	Network

Base Score	6.9
Attack Vector	Network

Complexity	
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible sensitive information disclosure.

<http://192.168.0.128:4200/>

List of pages that could be cached:

- http://192.168.0.128:4200/?password=u]H[ww6KrA9F.x-F&username=eKJxcvFc

Request

```
GET /?password=u]H[ww6KrA9F.x-F&username=eKJxcvFc HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

Prevent caching by adding "Cache Control: No-store" and "Pragma: no-cache" to the HTTP response header.

Access-Control-Allow-Origin header with wildcard (*) value

Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the resource originated. The Access-Control-Allow-Origin header indicates whether a resource can be shared based on the value of the Origin request header, "*", or "null" in the response.

If a website responds with Access-Control-Allow-Origin: * the requested resource allows sharing with every origin. Therefore, any website can make XHR (XMLHttpRequest) requests to the site and access the responses.

CWE

CWE-284

CVSS2

AV:N/AC:H/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None

Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Any website can make XHR requests to the site and access the responses.

<http://192.168.0.128:4200/>

Affected paths (max. 25):

- /
- /assets/icons/
- /assets/
- /crossdomain.xml
- /sitemap.xml.gz
- /manifest.webmanifest
- /clientaccesspolicy.xml
- /assets/fonts/grotesk/grotesk-italic.otf
- /sitemap.xml
- /assets/fonts/grotesk/grotesk-regular.otf
- /assets/images/
- /assets/fonts/grotesk/
- /assets/fonts/
- /ws

Request

```
GET / HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

Check whether Access-Control-Allow-Origin: * is appropriate for the resource/response.

References

[Test Cross Origin Resource Sharing \(OTG-CLIENT-007\)](#)

[https://www.owasp.org/index.php/Test_Cross_Origin_Resource_Sharing_\(OTG-CLIENT-007\)](https://www.owasp.org/index.php/Test_Cross_Origin_Resource_Sharing_(OTG-CLIENT-007))

[Cross-origin resource sharing](#)

https://en.wikipedia.org/wiki/Cross-origin_resource_sharing

[Cross-Origin Resource Sharing](#)

[http://www.w3.org/TR/cors/](https://www.w3.org/TR/cors/)

[CrossOriginRequestSecurity](#)

<https://code.google.com/p/html5security/wiki/CrossOriginRequestSecurity>

[Cross-Origin Resource Sharing \(CORS\) and the Access-Control-Allow-Origin Header](#)

<https://www.acunetix.com/blog/web-security-zone/cross-origin-resource-sharing-cors-access-control-allow-origin-header/>

[PortSwigger Research on CORS misconfiguration](#)

<https://portswigger.net/research/exploiting-cors-misconfigurations-for-bitcoins-and-bounties>

Content Security Policy (CSP) Not Implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:  
default-src 'self';  
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

<http://192.168.0.128:4200/>

Paths without CSP header:

- <http://192.168.0.128:4200/>
- <http://192.168.0.128:4200/assets/icons/>
- <http://192.168.0.128:4200/crossdomain.xml>
- <http://192.168.0.128:4200/sitemap.xml.gz>
- <http://192.168.0.128:4200/clientaccesspolicy.xml>
- <http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-italic.otf>
- <http://192.168.0.128:4200/sitemap.xml>
- <http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-regular.otf>
- <http://192.168.0.128:4200/assets/images/>
- <http://192.168.0.128:4200/assets/fonts/grotesk/>
- <http://192.168.0.128:4200/assets/>
- <http://192.168.0.128:4200/assets/fonts/>
- <http://192.168.0.128:4200/ws>

Request

```
GET / HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy \(CSP\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

[Implementing Content Security Policy](#)

<https://hacks.mozilla.org/2016/02/implementing-content-security-policy/>

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/Vl:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

<http://192.168.0.128:4200/>

Locations without Permissions-Policy header:

- <http://192.168.0.128:4200/>
- <http://192.168.0.128:4200/assets/icons/>
- <http://192.168.0.128:4200/crossdomain.xml>
- <http://192.168.0.128:4200/sitemap.xml.gz>
- <http://192.168.0.128:4200/clientaccesspolicy.xml>
- <http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-italic.otf>
- <http://192.168.0.128:4200/sitemap.xml>
- <http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-regular.otf>
- <http://192.168.0.128:4200/assets/images/>
- <http://192.168.0.128:4200/assets/fonts/grotesk/>
- <http://192.168.0.128:4200/assets/>

- <http://192.168.0.128:4200/assets/fonts/>
- <http://192.168.0.128:4200/ws>

Request

```
GET / HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

References

[Permissions-Policy / Feature-Policy \(MDN\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy>

[Permissions Policy \(W3C\)](#)

<https://www.w3.org/TR/permissions-policy-1/>

Insecure HTTP Usage

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

CWE

CWE-16

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

<http://192.168.0.128:4200/>

Request

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

References

HTTP Redirections

https://infosec.mozilla.org/guidelines/web_security#http-redirections

Javascript Source map detected

Client side Javascript source code can be combined, minified or compiled. A source map is a file that maps from the transformed source to the original source. Source map may help an attacker to read and debug Javascript.

CWE

CWE-16

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Access to source maps may help an attacker to read and debug Javascript code. It simplifies finding client-side vulnerabilities

<http://192.168.0.128:4200/>

Confidence: 80%

URLs where links to SourceMaps were found:

- sourceMappingURL in JS body - http://192.168.0.128:4200/main.js
- sourceMappingURL in JS body - http://192.168.0.128:4200/polyfills.js
- sourceMappingURL in JS body - http://192.168.0.128:4200/runtime.js
- sourceMappingURL in JS body - http://192.168.0.128:4200/styles.js
- sourceMappingURL in JS body - http://192.168.0.128:4200/vendor.js

Request

```
GET /main.js HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

According to the best practices, source maps should not be accessible for an attacker. Consult web references for more information

References

[Using sourcemaps on production without exposing the source code](#)

<https://itnext.io/using-sourcemaps-on-production-without-revealing-the-source-code-%EF%B8%8F-d41e78e20c89>

[SPA source code recovery by un-Webpacking source maps](#)

<https://medium.com/@rarecoil/spa-source-code-recovery-by-un-webpacking-source-maps-ef830fc2351d>

A06 Vulnerable and Outdated Components

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

Sensitive pages could be cached

One or more pages contain possible sensitive information (e.g. a password parameter) and could be potentially cached. Even in secure SSL channels sensitive data could be stored by intermediary proxies and SSL terminators. To prevent this, a Cache-Control header should be specified.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible sensitive information disclosure.

<http://192.168.0.128:4200/>

List of pages that could be cached:

- [http://192.168.0.128:4200/?password=u\]H\[ww6KrA9F.x-F&username=eKJxcvFc](http://192.168.0.128:4200/?password=u]H[ww6KrA9F.x-F&username=eKJxcvFc)

Request

```
GET /?password=u]H[ww6KrA9F.x-F&username=eKJxcvFc HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

Prevent caching by adding "Cache Control: No-store" and "Pragma: no-cache" to the HTTP response header.

Access-Control-Allow-Origin header with wildcard (*) value

Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the resource originated. The Access-Control-Allow-Origin header indicates whether a resource can be shared based on the value of the Origin request header, "*", or "null" in the response.

If a website responds with Access-Control-Allow-Origin: * the requested resource allows sharing with every origin. Therefore, any website can make XHR (XMLHttpRequest) requests to the site and access the responses.

CWE

CWE-284

CVSS2

AV:N/AC:H/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Any website can make XHR requests to the site and access the responses.

<http://192.168.0.128:4200/>

Affected paths (max. 25):

- /
- /assets/icons/
- /assets/
- /crossdomain.xml
- /sitemap.xml.gz
- /manifest.webmanifest
- /clientaccesspolicy.xml
- /assets/fonts/grotesk/grotesk-italic.otf
- /sitemap.xml
- /assets/fonts/grotesk/grotesk-regular.otf
- /assets/images/
- /assets/fonts/grotesk/
- /assets/fonts/
- /ws

Request

```
GET / HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

Check whether Access-Control-Allow-Origin: * is appropriate for the resource/response.

References

[Test Cross Origin Resource Sharing \(OTG-CLIENT-007\)](#)

[https://www.owasp.org/index.php/Test_Cross_Origin_Resource_Sharing_\(OTG-CLIENT-007\)](https://www.owasp.org/index.php/Test_Cross_Origin_Resource_Sharing_(OTG-CLIENT-007))

[Cross-origin resource sharing](#)

https://en.wikipedia.org/wiki/Cross-origin_resource_sharing

[Cross-Origin Resource Sharing](#)

<http://www.w3.org/TR/cors/>

[CrossOriginRequestSecurity](#)

<https://code.google.com/p/html5security/wiki/CrossOriginRequestSecurity>

[Cross-Origin Resource Sharing \(CORS\) and the Access-Control-Allow-Origin Header](#)

<https://www.acunetix.com/blog/web-security-zone/cross-origin-resource-sharing-cors-access-control-allow-origin-header/>

[PortSwigger Research on CORS misconfiguration](#)

<https://portswigger.net/research/exploiting-cors-misconfigurations-for-bitcoins-and-bounties>

Content Security Policy (CSP) Not Implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

Content-Security-Policy:

```
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

<http://192.168.0.128:4200/>

Paths without CSP header:

- http://192.168.0.128:4200/
- http://192.168.0.128:4200/assets/icons/
- http://192.168.0.128:4200/crossdomain.xml
- http://192.168.0.128:4200/sitemap.xml.gz
- http://192.168.0.128:4200/clientaccesspolicy.xml
- http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-italic.otf
- http://192.168.0.128:4200/sitemap.xml
- http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-regular.otf
- http://192.168.0.128:4200/assets/images/
- http://192.168.0.128:4200/assets/fonts/grotesk/
- http://192.168.0.128:4200/assets/
- http://192.168.0.128:4200/assets/fonts/
- http://192.168.0.128:4200/ws

Request

```
GET / HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy \(CSP\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

[Implementing Content Security Policy](#)

<https://hacks.mozilla.org/2016/02/implementing-content-security-policy/>

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

CWE

CWE-1021

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active

Availability Impact	None
---------------------	------

Confidentiality Impact	None
Integrity Impact	None
Availability Impact	None

Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

<http://192.168.0.128:4200/>

Locations without Permissions-Policy header:

- http://192.168.0.128:4200/
- http://192.168.0.128:4200/assets/icons/
- http://192.168.0.128:4200/crossdomain.xml
- http://192.168.0.128:4200/sitemap.xml.gz
- http://192.168.0.128:4200/clientaccesspolicy.xml
- http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-italic.otf
- http://192.168.0.128:4200/sitemap.xml
- http://192.168.0.128:4200/assets/fonts/grotesk/grotesk-regular.otf
- http://192.168.0.128:4200/assets/images/
- http://192.168.0.128:4200/assets/fonts/grotesk/
- http://192.168.0.128:4200/assets/
- http://192.168.0.128:4200/assets/fonts/
- http://192.168.0.128:4200/ws

Request

```
GET / HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

References

[Permissions-Policy / Feature-Policy \(MDN\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy>

[Permissions Policy \(W3C\)](#)

<https://www.w3.org/TR/permissions-policy-1/>

Vulnerable JavaScript libraries

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

CWE

CWE-937

CVSS2

AV:N/AC:L/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Base Score	6.5
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None

Availability Impact	None
---------------------	------

Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Consult References for more information.

<http://192.168.0.128:4200/>

Confidence: 95%

- AngularJS 1.5.11
 - URL: <http://192.168.0.128:4200/>
 - Detection method: The library's name and version were determined based on its dynamic behavior.
 - CVE-ID: CVE-2020-7676
 - Description: Prototype pollution / Cross-Site Scripting.
 - References:
 - <https://github.com/angular/angular.js/commit/726f49dcf6c23106ddaf5cf5e2e592841db743a>
 - <https://github.com/angular/angular.js/blob/master/CHANGELOG.md#179-pollution-eradication-2019-11-19>
 - <https://nvd.nist.gov/vuln/detail/CVE-2020-7676>

Request

```
GET / HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

Outdated JavaScript libraries

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

CWE

CWE-937

CVSS2

AV:N/AC:H/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Consult References for more information.

<http://192.168.0.128:4200/>

Confidence: 95%

- D3.js 3.5.17
 - URL: <http://192.168.0.128:4200/>
 - Detection method: The library's name and version were determined based on its dynamic behavior.
 - References:
 - <https://github.com/d3/d3/releases>

Request

```
GET / HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

<http://192.168.0.128:4200/>

Confidence: 95%

- moment.js 2.29.1
 - URL: <http://192.168.0.128:4200/scripts.js>
 - Detection method: The library's name and version were determined based on the file's contents.
 - References:
 - <https://github.com/moment/moment/tags>

Request

```
GET /scripts.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

A07 Identification and Authentication Failures

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

SSL/TLS Not Implemented

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE

CWE-319

CVSS2

AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low

Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible information disclosure.

<http://192.168.0.128:4200/>

Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.0.128:4200/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Host: 192.168.0.128:4200
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

A08 Software and Data Integrity Failures

Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs). An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code, or system compromise. Lastly, many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application. Attackers could potentially upload their own updates to be distributed and run on all installations. Another example is where objects or data are encoded or serialized into a structure that an attacker can see and modify is vulnerable to insecure deserialization.

No alerts in this category

A09 Security Logging and Monitoring Failures

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

No alerts in this category

A10 Server-Side Request Forgery

SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

No alerts in this category

Coverage

http://192.168.0.128:4200

assets

fonts

grotesk

grotesk-bold.otf

grotesk-italic.otf

grotesk-regular.otf

icons

images

wav-worker.js

clientaccesspolicy.xml

crossdomain.xml

main.js

manifest.webmanifest

polyfills.js

robots.txt

runtime.js

scripts.js

sitemap.xml

styles.css

styles.js

vendor.js

ws