Pentest Tools

Website Vulnerability Scanner Report

✓ **https://prod.kiss-demo.nl/**

KISS BFF

Summary

Overall risk level:

Low

Risk ratings:

High:	0
Medium:	0
Low:	2
Info:	66

Scan information:

Start time:	Jul 11, 2024 / 22:00:33
Finish time:	Jul 11, 2024 / 23:02:10
Scan duration:	1 hrs, 1 min, 37 sec
Tests performed:	70/70
Scan status:	Finished

Findings

Unsafe security header: Content-Security-Policy

CONFIRMED

URL	Evidence

https://prod.kiss-demo.nl/	Response headers include the HTTP Content-Security-Policy security header with the following security issues:
	`script-src:  'self' can be problematic if you host JSONP, Angular or user uploaded files.`
	`object-src:  We recommend restricting object-src to 'none'.`
	Request / Response

Details

Risk description:

For example, if the unsafe-inline directive is present in the CSP header, the execution of inline scripts and event handlers is allowed. This can be exploited by an attacker to execute arbitrary JavaScript code in the context of the vulnerable application.

Recommendation:

Remove the unsafe values from the directives, adopt nonces or hashes for safer inclusion of inline scripts if they are needed, and explicitly define the sources from which scripts, styles, images or other resources can be loaded.

References:

https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Classification:

CWE : CWE-693
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Exposure of Sensitive Information

UNCONFIRMED

URL	Method	Parameters	Evidence
https://prod.kiss-demo.nl/	GET		Email Address: info@utrecht.nl

Details

Risk description:

The risk exists that sensitive personal information within the application could be accessed by unauthorized parties. This could lead to privacy violations, identity theft, or other forms of personal or corporate harm.

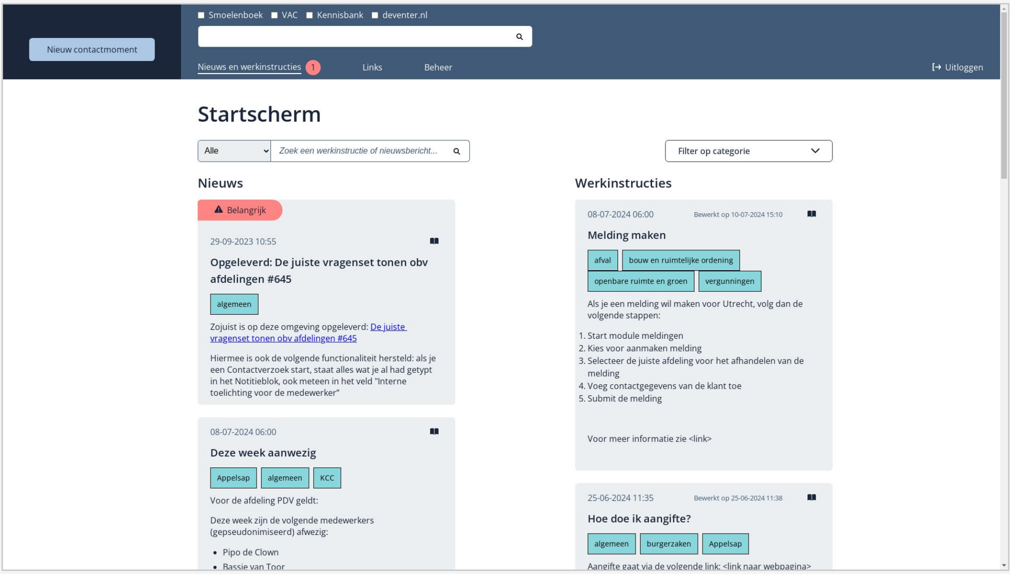
Recommendation:
Compartmentalize the application to have "safe" areas where trust boundaries can be unambiguously drawn. Do not allow sensitive data to go outside of the trust boundary and always be careful when interfacing with a compartment outside of the safe area.

Authentication complete: Recorded method.

URL
https://prod.kiss-demo.nl/

Details

Screenshot:



Nieuw contactmoment
■ Smoelenboek ■ VAC ■ Kennisbank ■ deventer.nl
Nieuws en werkinstructies 1
Links
Beheer
Uitloggen
Alle
Zoek een werkinstructie of nieuwsbericht...
Filter op categorie

Startscherm

Nieuws

Belangrijk

29-09-2023 10:55

Opgeleverd: De juiste vragenset tonen obv afdelingen #645

algemeen

Zojuist is op deze omgeving opgeleverd: De juiste vragenset tonen obv afdelingen #645

Hiermee is ook de volgende functionaliteit hersteld: als je een Contactverzoek start, staat alles wat je al had getypt in het Notitieblok, ook meteen in het veld "Interne toelichting voor de medewerker"

08-07-2024 06:00

Deze week aanwezig

Appelsap algemeen KCC

Voor de afdeling PDV geldt:

Deze week zijn de volgende medewerkers (gepseudonimiseerd) afwezig:

- Pipo de Clown
- Bassie van Toor

Werkinstructies

08-07-2024 06:00 Bewerkt op 10-07-2024 15:10

Melding maken

afval bouw en ruimtelijke ordening openbare ruimte en groen vergunningen

Als je een melding wil maken voor Utrecht, volg dan de volgende stappen:

1. Start module meldingen
2. Kies voor aanmaken melding
3. Selecteer de juiste afdeling voor het afhandelen van de melding
4. Voeg contactgegevens van de klant toe
5. Submit de melding

Voor meer informatie zie <link>

25-06-2024 11:35 Bewerkt op 25-06-2024 11:38

Hoe doe ik aangifte?

algemeen burgerzaken Appelsap

Aangifte gaat via de volgende link: <link naar webpagina>

Figure 1. Authentication sequence result

Spider results

URL	Method	Parameters	Page Title	Page Size	Status Code
https://prod.kiss-demo.nl/	GET		Klant Interactie Service Systeem	29.48 KB	200
https://prod.kiss-demo.nl/	GET	**Query:** page=2	Klant Interactie Service Systeem	9.87 KB	200
https://prod.kiss-demo.nl/	GET	**Query:** search=search type=Werkinstructie	Klant Interactie Service Systeem	11.05 KB	200
https://prod.kiss-demo.nl/	GET	**Query:** skillIds=16	Klant Interactie Service Systeem	11.25 KB	200
https://prod.kiss-demo.nl/api/KanalenContactmomentKeuzelijst	GET		Klant Interactie Service Systeem	9.87 KB	200
https://prod.kiss-demo.nl/api/afdelingen/api/v2/objects	GET	**Query:** ordering=record__data__naam	Klant Interactie Service Systeem	10.36 KB	200

https://prod.kiss-demo.nl/api/berichten/featuredcount	GET		Klant Interactie Service Systeem	10.36 KB	200
https://prod.kiss-demo.nl/api/berichten/published	GET	**Query:** page=1 pageSize=10 type=Nieuws	Klant Interactie Service Systeem	9.87 KB	200
https://prod.kiss-demo.nl/api/contactverzoekvragensets	GET		Klant Interactie Service Systeem	10.83 KB	200
https://prod.kiss-demo.nl/api/elasticsearch/search-smoelenboek,search-vac,enterprise-search-engine-engine-crawler,search-kennisbank	GET		Klant Interactie Service Systeem	11.73 KB	200
https://prod.kiss-demo.nl/api/groepen/api/v2/objects	GET	**Query:** ordering=record__data__naam	Klant Interactie Service Systeem	10.83 KB	200

Details

Risk description:
The table contains all the unique pages the scanner found. The duplicated URLs are not available here as scanning those is considered unnecessary

Recommendation:
We recommend to advanced users to make sure the scan properly detected most of the URLs in the application.

References:
All the URLs the scanner found, including duplicates (available for 90 days after the scan date)

Cloud Hosted URLs

URL	Cloud Provider	Found at URL
https://prod.kiss-demo.nl/api/contactverzoekvragensets	Azure	https://prod.kiss-demo.nl/

Website is accessible.

Nothing was found for vulnerabilities of server-side software.

Nothing was found for client access policies.

Nothing was found for robots.txt file.

Nothing was found for absence of the security.txt file.

Outdated JavaScript libraries were merged into server-side software vulnerabilities.

Nothing was found for CORS misconfiguration.

Nothing was found for use of untrusted certificates.

Nothing was found for enabled HTTP debug methods.

Nothing was found for sensitive files.

Nothing was found for administration consoles.

Nothing was found for interesting files.

Nothing was found for information disclosure.

Nothing was found for software identification.

Searching for URLs in Wayback Machine.

Nothing was found for enabled HTTP OPTIONS method.

Nothing was found for secure communication.

Nothing was found for directory listing.

Nothing was found for passwords submitted unencrypted.

Nothing was found for Cross-Site Scripting.

Nothing was found for SQL Injection.

Nothing was found for Local File Inclusion.

Nothing was found for OS Command Injection.

Nothing was found for error messages.

Nothing was found for debug messages.

Nothing was found for code comments.

- Nothing was found for missing HTTP header - Strict-Transport-Security.
- Nothing was found for missing HTTP header - Content Security Policy.
- Nothing was found for missing HTTP header - X-Content-Type-Options.
- Nothing was found for missing HTTP header - Referrer.
- Nothing was found for missing HTTP header - Feature.
- Nothing was found for XML External Entity Injection.
- Nothing was found for Insecure Direct Object Reference.
- Nothing was found for passwords submitted in URLs.
- Nothing was found for JWT weaknesses.
- Nothing was found for domain too loose set for cookies.
- Nothing was found for mixed content between HTTP and HTTPS.
- Nothing was found for cross domain file inclusion.
- Nothing was found for internal error code.
- Nothing was found for HttpOnly flag of cookie.
- Nothing was found for Secure flag of cookie.
- Nothing was found for login interfaces.
- Nothing was found for secure password submission.
- Nothing was found for Server Side Request Forgery.
- Nothing was found for Open Redirect.

Nothing was found for PHP Code Injection.

Nothing was found for JavaScript Code Injection.

Nothing was found for Broken Authentication.

Nothing was found for Ruby Code Injection.

Nothing was found for Python Code Injection.

Nothing was found for Perl Code Injection.

Nothing was found for Remote Code Execution through Log4j.

Nothing was found for Server Side Template Injection.

Nothing was found for Remote Code Execution through VIEWSTATE.

Nothing was found for Exposed Backup Files.

Nothing was found for Request URL Override.

Nothing was found for HTTP/1.1 Request Smuggling.

Nothing was found for CSRF

Nothing was found for NoSQL Injection.

Nothing was found for Insecure Deserialization.

Nothing was found for Session Fixation.

Nothing was found for OpenAPI files.

Nothing was found for file upload.

Scan coverage information

List of tests performed (70/70)

- ✓ Starting the scan...
- ✓ Trying to authenticate...
- ✓ Checking for unsafe HTTP header Content Security Policy...
- ✓ Checking for sensitive data...
- ✓ Checking for vulnerabilities of server-side software...
- ✓ Checking for client access policies...
- ✓ Checking for robots.txt file...
- ✓ Checking for absence of the security.txt file...
- ✓ Checking for outdated JavaScript libraries...
- ✓ Checking for CORS misconfiguration...
- ✓ Checking for use of untrusted certificates...
- ✓ Checking for enabled HTTP debug methods...
- ✓ Checking for sensitive files...
- ✓ Checking for administration consoles...
- ✓ Checking for interesting files... (this might take a few hours)
- ✓ Spidering target...
- ✓ Scanning for cloud URLs on target...
- ✓ Checking for information disclosure... (this might take a few hours)
- ✓ Checking for software identification...
- ✓ Searching for URLs in Wayback Machine...
- ✓ Checking for enabled HTTP OPTIONS method...
- ✓ Checking for secure communication...
- ✓ Checking for directory listing...
- ✓ Checking for passwords submitted unencrypted...
- ✓ Checking for Cross-Site Scripting...
- ✓ Checking for SQL Injection...
- ✓ Checking for Local File Inclusion...
- ✓ Checking for OS Command Injection...
- ✓ Checking for error messages...
- ✓ Checking for debug messages...
- ✓ Checking for code comments...
- ✓ Checking for missing HTTP header - Strict-Transport-Security...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ Checking for missing HTTP header - Feature...
- ✓ Checking for XML External Entity Injection...
- ✓ Checking for Insecure Direct Object Reference...
- ✓ Checking for passwords submitted in URLs...
- ✓ Checking for JWT weaknesses...
- ✓ Checking for domain too loose set for cookies...
- ✓ Checking for mixed content between HTTP and HTTPS...
- ✓ Checking for cross domain file inclusion...
- ✓ Checking for internal error code...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for Secure flag of cookie...
- ✓ Checking for login interfaces...
- ✓ Checking for secure password submission...
- ✓ Checking for Server Side Request Forgery...
- ✓ Checking for Open Redirect...
- ✓ Checking for PHP Code Injection...
- ✓ Checking for JavaScript Code Injection...
- ✓ Checking for Broken Authentication...
- ✓ Checking for Ruby Code Injection...
- ✓ Checking for Python Code Injection...
- ✓ Checking for Perl Code Injection...
- ✓ Checking for Remote Code Execution through Log4j...
- ✓ Checking for Server Side Template Injection...
- ✓ Checking for Remote Code Execution through VIEWSTATE...
- ✓ Checking for Exposed Backup Files...
- ✓ Checking for Request URL Override...
- ✓ Checking for HTTP/1.1 Request Smuggling...
- ✓ Checking for CSRF
- ✓ Checking for NoSQL Injection...
- ✓ Checking for Insecure Deserialization...
- ✓ Checking for Session Fixation...
- ✓ Checking for OpenAPI files...
- ✓ Checking for file upload...

Scan parameters

Target:	https://prod.kiss-demo.nl/
Scan type:	Deep_scan_default
Authentication:	True

Scan stats

Unique Injection Points Detected:	51
URLs spidered:	31
Total number of HTTP requests:	50603
Average time until a response was received:	103ms
Total number of HTTP request errors:	42