Aggregated Scan Result

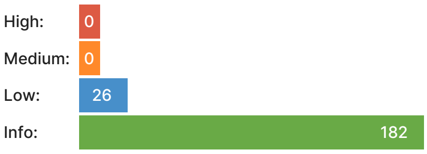
Vulnerability Scan Results

Summary

Overall risk level:

Low

Risk ratings:



Scan information:

This is an aggregated report from 4 scans.

Start time: 2022-12-16 15:54:21 UTC+02

Finish time: 2022-12-16 16:09:29 UTC+02

Findings (by target)

1. Target: https://kissdevelopment-frontend.commonground.nu/

Missing security header: X-Content-Type-Options CONFIRMED

URL	Evidence
https://kissdevelopment-frontend.commonground.nu/	Response headers do not include the X-Content-Type-Options HTTP security header

Details

Risk description:
The HTTP header `X-Content-Type-Options` is addressed to the Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation:
We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff` .

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

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

Missing security header: X-Frame-Options CONFIRMED

URL	Evidence
https://kissdevelopment-frontend.commonground.nu/	Response headers do not include the HTTP X-Frame-Options security header

Details

Risk description:
Because the `X-Frame-Options` header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:

https://owasp.org/www-community/attacks/Clickjacking

Recommendation:
We recommend you to add the `X-Frame-Options` HTTP header with the values `DENY` or `SAMEORIGIN` to every page that you want to be protected against Clickjacking attacks.

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

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

Missing security header: X-XSS-Protection CONFIRMED

URL	Evidence
https://kissdevelopment-frontend.commonground.nu/	Response headers do not include the HTTP X-XSS-Protection security header

Details

Risk description:
The `X-XSS-Protection` HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.

Recommendation:
We recommend setting the X-XSS-Protection header to `X-XSS-Protection: 1; mode=block`.

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

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

Missing security header: Content-Security-Policy CONFIRMED

URL	Evidence
https://kissdevelopment-frontend.commonground.nu/	Response headers do not include the HTTP Content-Security-Policy security header

Details

Risk description:
The Content-Security-Policy (CSP) header activates a protection mechanism implemented in web browsers which prevents exploitation of Cross-Site Scripting vulnerabilities (XSS). If the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Recommendation:
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

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

Missing security header: Referrer-Policy CONFIRMED

URL	Evidence
https://kissdevelopment-frontend.commonground.nu/	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response.

Details

Risk description:
The Referrer-Policy HTTP header controls how much referrer information the browser will send with each request originated from the current web application.
For instance, if a user visits the web page "http://example.com/pricing/" and it clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:
The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

References:
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

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

Server software and technology found UNCONFIRMED

Software / Version	Category
HSTS	Security

Details

Risk description:
An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Screenshot:

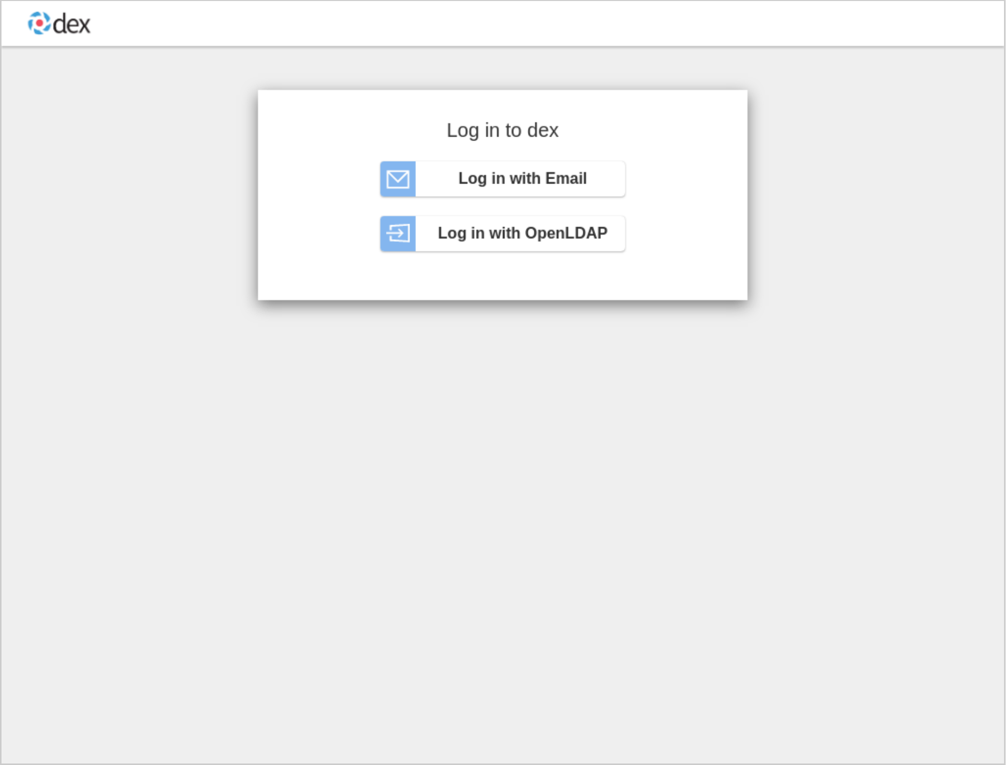


Figure 1. Website Screenshot

🟩 Website is accessible.

🟩 Spider results

URL	Method	Parameters
https://kissdevelopment-frontend.commonground.nu/	GET	Headers: User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36
https://kissdevelopment-frontend.commonground.nu/assets/	GET	Headers: User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36

🟩 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.

🟩 Nothing was found for outdated JavaScript libraries.

- 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.
- 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 - Feature.

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 sensitive data.

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 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.

2. Target: https://kissdevelopment-dimpact-gatewayui.commonground.nu/

Missing security header: Referrer-Policy CONFIRMED

URL	Evidence
https://kissdevelopment-dimpact-gatewayui.commonground.nu/	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response.

Details

Risk description:

The Referrer-Policy HTTP header controls how much referrer information the browser will send with each request originated from the current web application.
For instance, if a user visits the web page "http://example.com/pricing/" and it clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:

The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

References:

https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

Classification:

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

Missing security header: Content-Security-Policy CONFIRMED

URL	Evidence
https://kissdevelopment-dimpact-gatewayui.commonground.nu/	Response headers do not include the HTTP Content-Security-Policy security header

Details

Risk description:

The Content-Security-Policy (CSP) header activates a protection mechanism implemented in web browsers which prevents exploitation of Cross-Site Scripting vulnerabilities (XSS). If the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Recommendation:
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

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

Missing security header: X-Content-Type-Options CONFIRMED

URL	Evidence
https://kissdevelopment-dimpact-gatewayui.commonground.nu/	Response headers do not include the X-Content-Type-Options HTTP security header

Details

Risk description:
The HTTP header `X-Content-Type-Options` is addressed to the Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation:
We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff` .

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

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

Missing security header: X-Frame-Options CONFIRMED

URL	Evidence
https://kissdevelopment-dimpact-gatewayui.commonground.nu/	Response headers do not include the HTTP X-Frame-Options security header

Details

Risk description:
Because the `X-Frame-Options` header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:
https://owasp.org/www-community/attacks/Clickjacking

Recommendation:
We recommend you to add the `X-Frame-Options` HTTP header with the values `DENY` or `SAMEORIGIN` to every page that you want to be protected against Clickjacking attacks.

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

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

Missing security header: X-XSS-Protection CONFIRMED

URL	Evidence
https://kissdevelopment-dimpact-gatewayui.commonground.nu/	Response headers do not include the HTTP X-XSS-Protection security header

Details

Risk description:
The `X-XSS-Protection` HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.

Recommendation:
We recommend setting the X-XSS-Protection header to `X-XSS-Protection: 1; mode=block` .

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

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

Server software and technology found UNCONFIRMED

Software / Version	Category
webpack	Miscellaneous
Module Federation	Miscellaneous
React	JavaScript frameworks
Gatsby 4.24.8	Static site generator, JavaScript frameworks
Font Awesome	Font scripts
core-js 3.26.1	JavaScript libraries
HSTS	Security

Details

Risk description:
An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Screenshot:

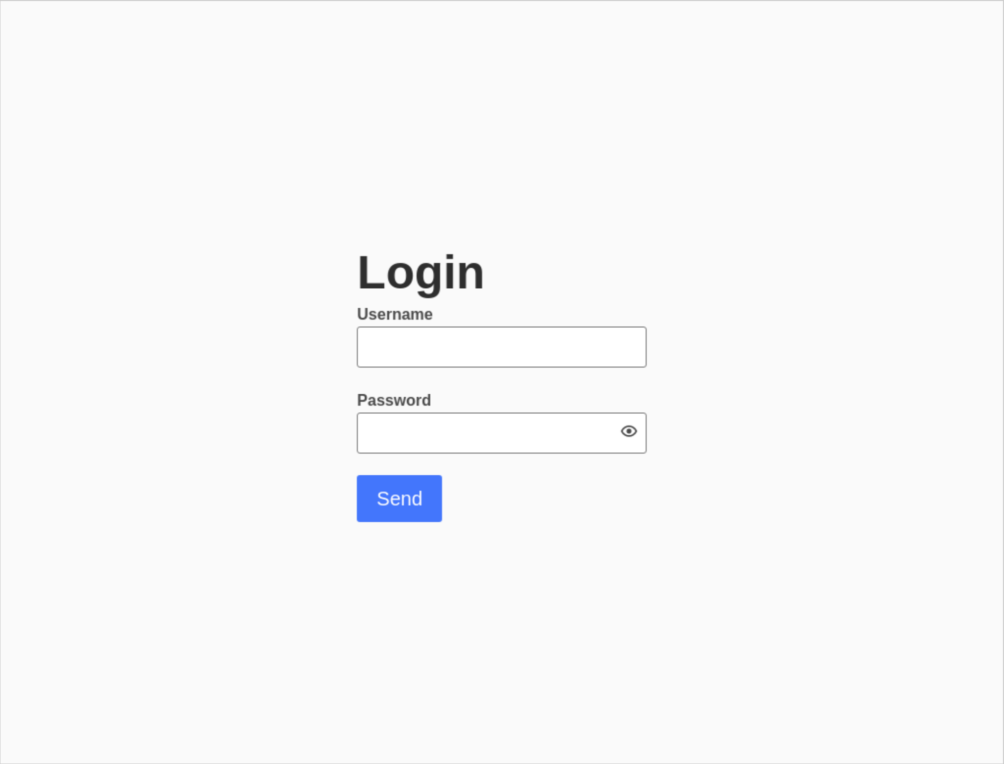


Figure 2. Website Screenshot

Interesting files found UNCONFIRMED

URL	Summary
https://kissdevelopment-dimpact-gatewayui.commonground.nu/logs/	This might be interesting...

Details

Risk description:
These files/folders usually contain sensitive information which may help attackers to mount further attacks against the server. Manual validation is required.

Recommendation:
We recommend you to analyze if the mentioned files/folders contain any sensitive information and restrict their access according to the business purposes of the application.

Classification:
CWE : CWE-200
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Website is accessible.

Login Interface Found CONFIRMED

URL	Evidence
https://kissdevelopment-dimpact-gatewayui.commonground.nu/	<input class="denhaag-textfield__input" name="username" type="text"/> <input class="denhaag-textfield__input" icon="[object Object]" name="password" type="password"/> <button class="denhaag-button denhaag-button--large" type="submit"><span class="denhaag-button__label">Send</span></button>

Details

Risk description:
An attacker could use this interface to mount brute force attacks against known passwords and usernames combinations leaked throughout the web.

Recommendation:
Ensure each interface is not bypassable using common knowledge of the application or leaked credentials using occasional password audits.

References:
https://pentest-tools.com/network-vulnerability-scanning/password-auditor
http://capec.mitre.org/data/definitions/16.html

Screenshot:

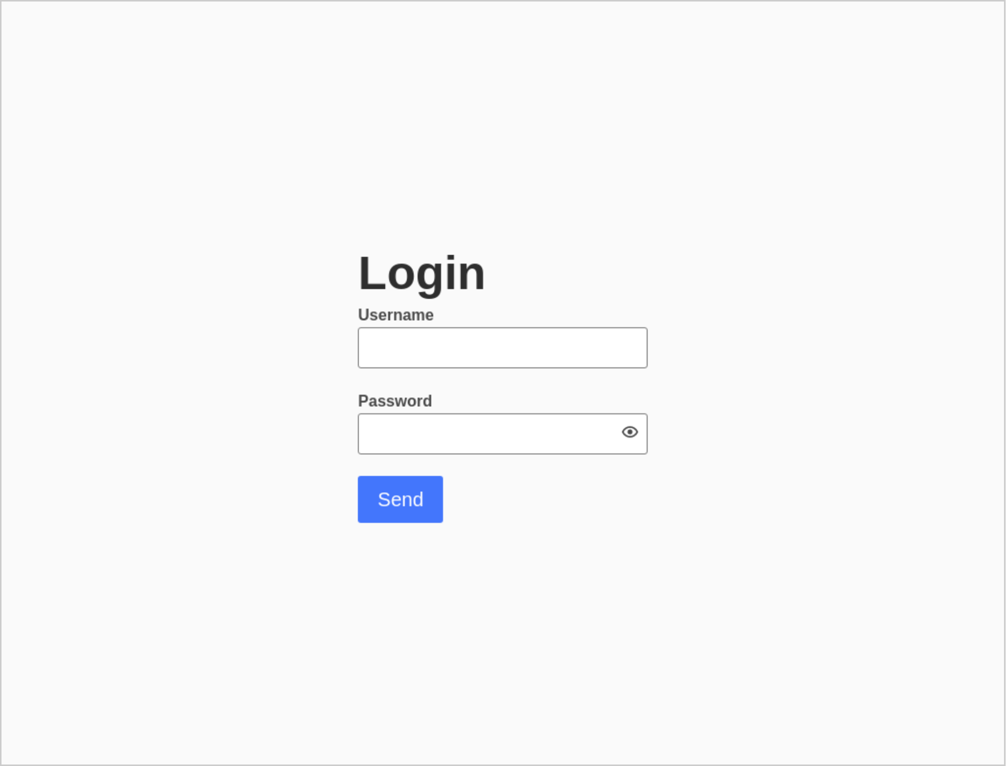


Figure 3. Login Interface

Spider results

URL	Method	Parameters
https://kissdevelopment-dimpact-gatewayui.commonground.nu/	GET	Headers: User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36

https://kissdevelopment-dimpact-gatewayui.commonground.nu/	GET	Query:
		password=Secure123456$
		username=1d3d2d231d2dd4
		Headers:
		User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36

https://kissdevelopment-dimpact-gatewayui.commonground.nu/logs/	GET	Headers: User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36

Nothing was found for vulnerabilities of server-side software.

Nothing was found for client access policies.

Nothing was found for robots.txt file.

Security.txt file is missing CONFIRMED

URL
Missing: https://kissdevelopment-dimpact-gatewayui.commonground.nu/.well-known/security.txt

Details

Risk description:
We have detected that the server is missing the security.txt file. There is no particular risk in not creating a valid Security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation:
We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

References:
https://securitytxt.org/

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Nothing was found for outdated JavaScript libraries.

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 information disclosure.

Nothing was found for software identification.

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 - Feature.

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 secure password submission.

Nothing was found for sensitive data.

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 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.

3. Target: https://kiss-dev.commonground.nu/

Missing security header: Content-Security-Policy CONFIRMED

URL	Evidence
https://kiss-dev.commonground.nu/	Response headers do not include the HTTP Content-Security-Policy security header

⌄ Details

Risk description:
The Content-Security-Policy (CSP) header activates a protection mechanism implemented in web browsers which prevents exploitation of Cross-Site Scripting vulnerabilities (XSS). If the target application is vulnerable to XSS, lack of this header makes it easily exploitable

by attackers.

Recommendation:
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

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

Missing security header: Referrer-Policy CONFIRMED

URL	Evidence
https://kiss-dev.commonground.nu/	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response.

Details

Risk description:
The Referrer-Policy HTTP header controls how much referrer information the browser will send with each request originated from the current web application.
For instance, if a user visits the web page "http://example.com/pricing/" and it clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:
The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

References:
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

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

Missing security header: X-Content-Type-Options CONFIRMED

URL	Evidence
https://kiss-dev.commonground.nu/	Response headers do not include the X-Content-Type-Options HTTP security header

Details

Risk description:
The HTTP header `X-Content-Type-Options` is addressed to the Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation:
We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff` .

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

Classification:
CWE : CWE-693

OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Missing security header: X-Frame-Options CONFIRMED

URL	Evidence
https://kiss-dev.commonground.nu/	Response headers do not include the HTTP X-Frame-Options security header

Details

Risk description:
Because the `X-Frame-Options` header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:
https://owasp.org/www-community/attacks/Clickjacking

Recommendation:
We recommend you to add the `X-Frame-Options` HTTP header with the values `DENY` or `SAMEORIGIN` to every page that you want to be protected against Clickjacking attacks.

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

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

Missing security header: X-XSS-Protection CONFIRMED

URL	Evidence
https://kiss-dev.commonground.nu/	Response headers do not include the HTTP X-XSS-Protection security header

Details

Risk description:
The `X-XSS-Protection` HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.

Recommendation:
We recommend setting the X-XSS-Protection header to `X-XSS-Protection: 1; mode=block` .

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

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

Server software and technology found UNCONFIRMED

Software / Version	Category
HSTS	Security

Details

Risk description:
An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Screenshot:

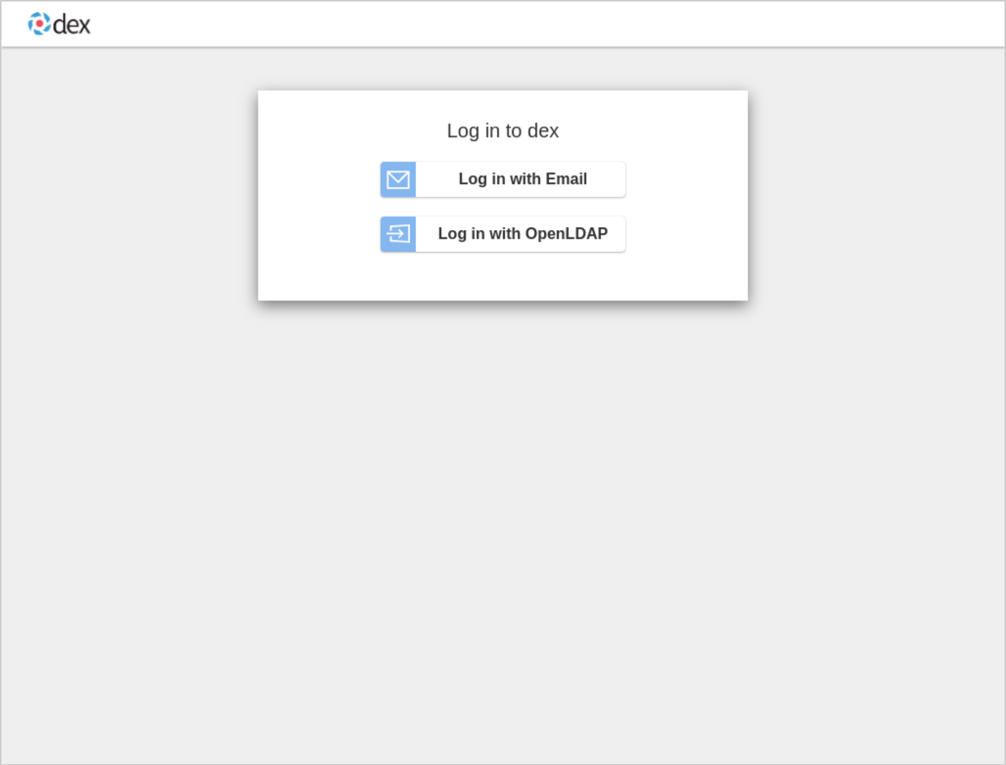


Figure 4. Website Screenshot

Website is accessible.

Spider results

URL	Method	Parameters
https://kiss-dev.commonground.nu/	GET	Headers: User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36
https://kiss-dev.commonground.nu/assets/	GET	Headers: User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36

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.

Nothing was found for outdated JavaScript libraries.

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.

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 - Feature.
- 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 sensitive data.
- 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 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.

4. Target: https://kissdevelopment-gatewayui.commonground.nu/

Missing security header: Content-Security-Policy CONFIRMED

URL	Evidence
https://kissdevelopment-gatewayui.commonground.nu/	Response headers do not include the HTTP Content-Security-Policy security header

Details

Risk description:
The Content-Security-Policy (CSP) header activates a protection mechanism implemented in web browsers which prevents exploitation of Cross-Site Scripting vulnerabilities (XSS). If the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Recommendation:
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

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

Missing security header: Referrer-Policy CONFIRMED

URL	Evidence
https://kissdevelopment-gatewayui.commonground.nu/	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response.

Details

Risk description:
The Referrer-Policy HTTP header controls how much referrer information the browser will send with each request originated from the current web application.
For instance, if a user visits the web page "http://example.com/pricing/" and it clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:
The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

References:
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

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

Missing security header: X-Content-Type-Options CONFIRMED

URL	Evidence
https://kissdevelopment-gatewayui.commonground.nu/	Response headers do not include the X-Content-Type-Options HTTP security header

Details

Risk description:
The HTTP header `X-Content-Type-Options` is addressed to the Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation:
We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff` .

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

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

Missing security header: X-XSS-Protection CONFIRMED

URL	Evidence
https://kissdevelopment-gatewayui.commonground.nu/	Response headers do not include the HTTP X-XSS-Protection security header

Details

Risk description:
The `X-XSS-Protection` HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.

Recommendation:
We recommend setting the X-XSS-Protection header to `X-XSS-Protection: 1; mode=block` .

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

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

Missing security header: X-Frame-Options CONFIRMED

URL	Evidence
https://kissdevelopment-gatewayui.commonground.nu/	Response headers do not include the HTTP X-Frame-Options security header

Details

Risk description:
Because the `X-Frame-Options` header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:
https://owasp.org/www-community/attacks/Clickjacking

Recommendation:
We recommend you to add the `X-Frame-Options` HTTP header with the values `DENY` or `SAMEORIGIN` to every page that you want to be protected against Clickjacking attacks.

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

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

Server software and technology found UNCONFIRMED

Software / Version	Category
webpack	Miscellaneous
Module Federation	Miscellaneous
React	JavaScript frameworks
Gatsby 4.24.8	Static site generator, JavaScript frameworks
Font Awesome	Font scripts
core-js 3.26.1	JavaScript libraries
HSTS	Security

Details

Risk description:
An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Screenshot:

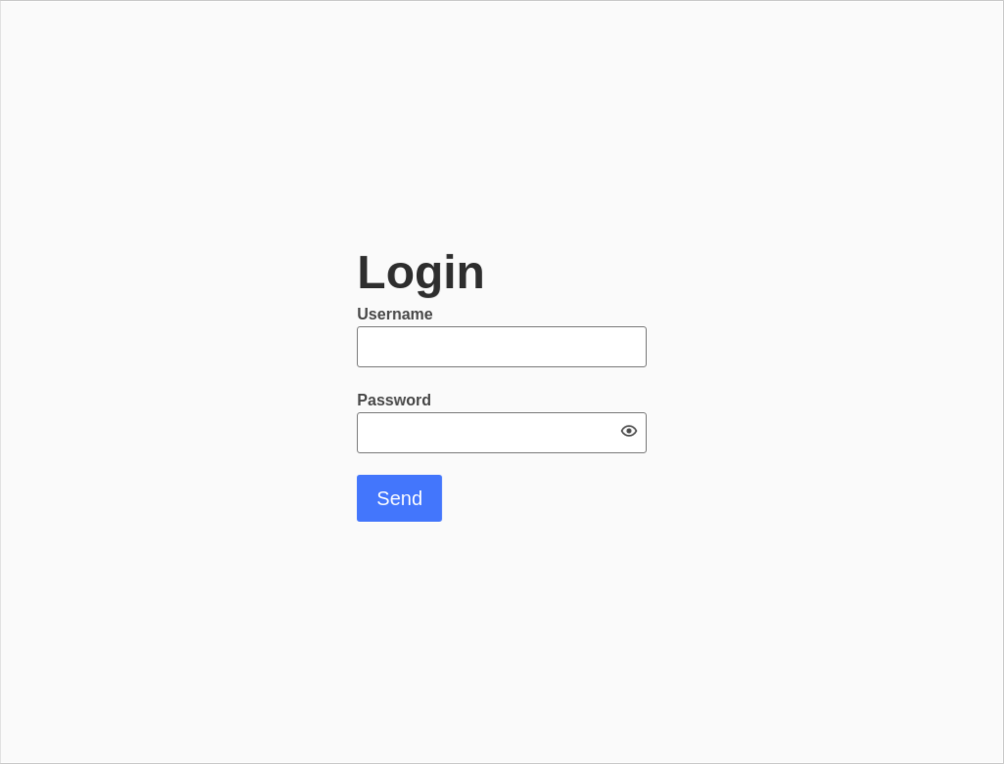


Figure 5. Website Screenshot

Interesting files found UNCONFIRMED

URL	Summary
https://kissdevelopment-gatewayui.commonground.nu/logs/	This might be interesting...

Details

Risk description:
These files/folders usually contain sensitive information which may help attackers to mount further attacks against the server. Manual validation is required.

Recommendation:
We recommend you to analyze if the mentioned files/folders contain any sensitive information and restrict their access according to the business purposes of the application.

Classification:
CWE : CWE-200
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

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 - Feature.

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 secure password submission.

Nothing was found for sensitive data.

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 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.

Website is accessible.

Login Interface Found CONFIRMED

URL	Evidence
https://kissdevelopment-gatewayui.commonground.nu/	<input class="denhaag-textfield__input" name="username" type="text"/> <input class="denhaag-textfield__input" icon="[object Object]" name="password" type="password"/> <button class="denhaag-button denhaag-button--large" type="submit"><span class="denhaag-button__label">Send</span></button>

Details

Risk description:
An attacker could use this interface to mount brute force attacks against known passwords and usernames combinations leaked throughout the web.

Recommendation:
Ensure each interface is not bypassable using common knowledge of the application or leaked credentials using occasional password audits.

References:
https://pentest-tools.com/network-vulnerability-scanning/password-auditor
http://capec.mitre.org/data/definitions/16.html

Screenshot:

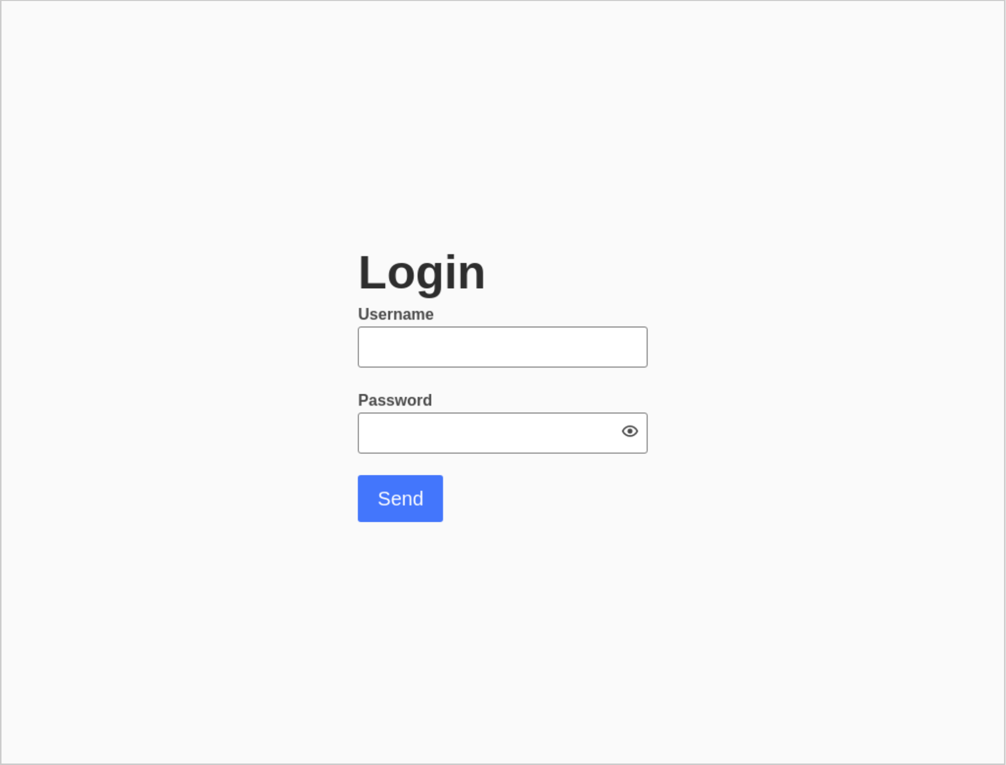


Figure 6. Login Interface

Spider results

URL	Method	Parameters
https://kissdevelopment-gatewayui.commonground.nu/	GET	Headers: User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36

https://kissdevelopment-gatewayui.commonground.nu/	GET	Query:
		password=Secure123456$
		username=1d3d2d231d2dd4
		Headers:
		User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36

https://kissdevelopment-gatewayui.commonground.nu/logs/	GET	Headers: User-Agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36

Nothing was found for vulnerabilities of server-side software.

Nothing was found for client access policies.

Nothing was found for robots.txt file.

Security.txt file is missing CONFIRMED

URL
Missing: https://kissdevelopment-gatewayui.commonground.nu/.well-known/security.txt

Details

Risk description:
We have detected that the server is missing the security.txt file. There is no particular risk in not creating a valid Security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation:
We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

References:
https://securitytxt.org/

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration

Nothing was found for outdated JavaScript libraries.

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 information disclosure.

Nothing was found for software identification.

Nothing was found for secure communication.

Nothing was found for directory listing.

Tool configuration details

The following tools were run to obtain the findings above:

Website Vulnerability Scanner

Scan parameters

Website URL	https://kissdevelopment-frontend.commonground.nu/
Scan type	Full_scan_default
Authentication	False

Scan information

Start time:	2022-12-16 15:54:21 UTC+02
Finish time:	2022-12-16 15:56:46 UTC+02
Scan duration:	2 min, 25 sec
Tests performed:	52/52
Scan status:	Finished

Website Vulnerability Scanner

Scan parameters

Website URL	https://kiss-dev.commonground.nu/
Scan type	Full_scan_default
Authentication	False

Scan information

Start time:	2022-12-16 15:54:25 UTC+02
Finish time:	2022-12-16 15:55:37 UTC+02
Scan duration:	1 min, 12 sec
Tests performed:	52/52
Scan status:	Finished

Website Vulnerability Scanner

Scan parameters

Website URL	https://kissdevelopment-gatewayui.commonground.nu/
Scan type	Full_scan_default
Authentication	False

Scan information

Start time:	2022-12-16 15:55:45 UTC+02
Finish time:	2022-12-16 15:58:51 UTC+02
Scan duration:	3 min, 6 sec
Tests performed:	52/52
Scan status:	Finished

Website Vulnerability Scanner

Scan parameters

Website URL	https://kissdevelopment-dimpact-gatewayui.commonground.nu/
Scan type	Full_scan_default
Authentication	False

Scan information

Start time:	2022-12-16 16:05:49 UTC+02
Finish time:	2022-12-16 16:09:29 UTC+02
Scan duration:	3 min, 40 sec
Tests performed:	52/52
Scan status:	Finished