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:	3
Info:	53

Scan information:

Start time:	2023-06-27 16:58:12 UTC+03
Finish time:	2023-06-27 22:04:42 UTC+03
Scan duration:	5 hrs, 6 min, 30 sec
Tests performed:	56/56
Scan status:	Finished

Findings

Missing security header: X-Frame-Options

CONFIRMED

URL	Evidence
https://prod.kiss-demo.nl/.well-known/security.txt	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: Content-Security-Policy

CONFIRMED

URL	Evidence
https://prod.kiss-demo.nl/.well-known/security.txt	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

Server software and technology found

UNCONFIRMED

Software / Version	Category
Sectigo	SSL/TLS certificate authorities
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:

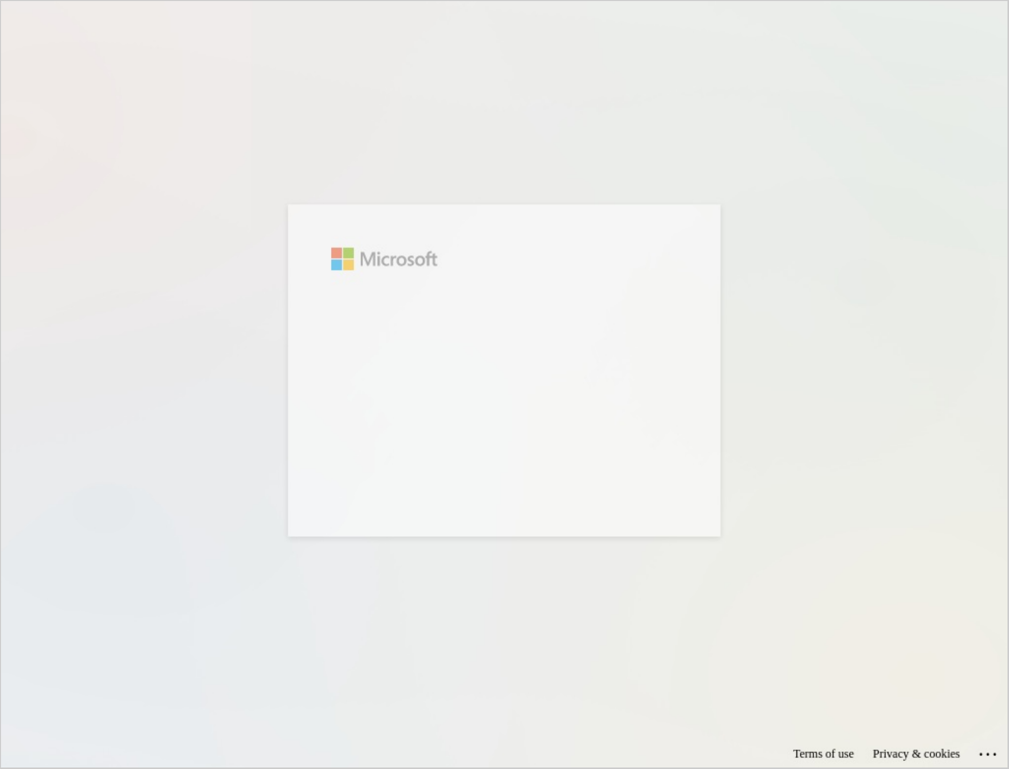

Figure 1. Website Screenshot

Login Interface Found

CONFIRMED

URL	Evidence
https://prod.kiss-demo.nl/	<input aria-describedby="loginHeader usernameError" aria-label="Enter your email, phone, or Skype." aria-required="true" class="form-control ltr_override input ext-input text-box ext-text-box" data-bind=" attr: { lang: svr.fApplyAsciiRegexOnInput ? null : 'en' }, externalCss: { 'input': true, 'text-box': true, 'has-error': usernameTextbox.error }, ariaLabel: tenantBranding.unsafe_userIdLabel || str['CT_PWD_STR_Username_AriaLabel'], ariaDescribedBy: 'loginHeader' + (pageDescription && !svr.fHideLoginDesc ? ' loginDescription usernameError' : ' usernameError'), textInput: usernameTextbox.value, hasFocusEx: usernameTextbox.focused, placeholder: $placeholderText, autocomplete: svr.fIsUpdatedAutocompleteEnabled ? 'username' : null," data-report-attached="1" data-report-event="Signin_Email_Phone_Skype" data-report-trigger="click" data-report-value="Email_Phone_Skype_Entry" id="i0116" maxlength="113" name="loginfmt" placeholder="Email, phone, or Skype" type="email"/> <input aria-hidden="true" class="moveOffScreen" data-bind="moveOffScreen, textInput: passwordBrowserPrefill" id="i0118" name="passwd" tabindex="-1" type="password"/> <input class="win-button button_primary button ext-button primary ext-primary" data-bind=" attr: primaryButtonAttributes, externalCss: { 'button': true, 'primary': true ... (truncated)
https://prod.kiss-demo.nl/api/challenge	<input aria-describedby="loginHeader usernameError" aria-label="Enter your email, phone, or Skype." aria-required="true" class="form-control ltr_override input ext-input text-box ext-text-box" data-bind=" attr: { lang: svr.fApplyAsciiRegexOnInput ? null : 'en' }, externalCss: { 'input': true, 'text-box': true, 'has-error': usernameTextbox.error }, ariaLabel: tenantBranding.unsafe_userIdLabel || str['CT_PWD_STR_Username_AriaLabel'], ariaDescribedBy: 'loginHeader' + (pageDescription && !svr.fHideLoginDesc ? ' loginDescription usernameError' : ' usernameError'), textInput: usernameTextbox.value, hasFocusEx: usernameTextbox.focused, placeholder: $placeholderText, autocomplete: svr.fIsUpdatedAutocompleteEnabled ? 'username' : null," data-report-event="Signin_Email_Phone_Skype" data-report-trigger="click" data-report-value="Email_Phone_Skype_Entry" id="i0116" maxlength="113" name="loginfmt" placeholder="Email, phone, or Skype" type="email"/> <input aria-hidden="true" class="moveOffScreen" data-bind="moveOffScreen, textInput: passwordBrowserPrefill" id="i0118" name="passwd" tabindex="-1" type="password"/> <input class="win-button button_primary button ext-button primary ext-primary" data-bind=" attr: primaryButtonAttributes, externalCss: { 'button': true, 'primary': true }, value: primary... (truncated)

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:

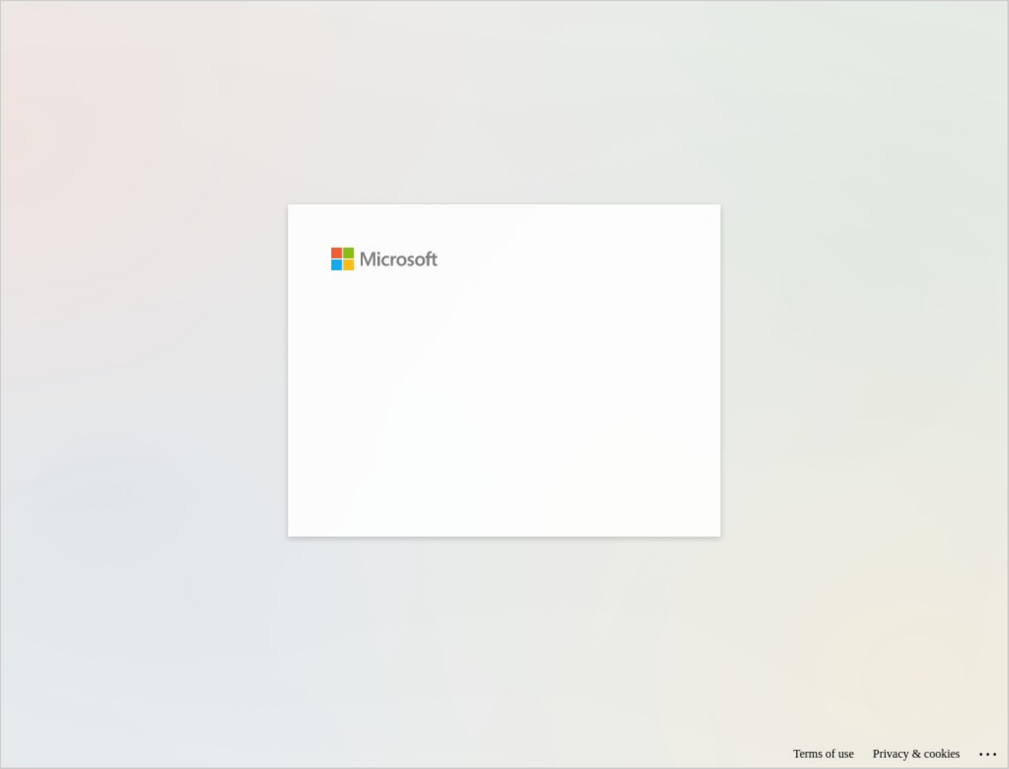

Figure 2. Login Interface

Spider results

URL	Method	Parameters
https://prod.kiss-demo.nl/	GET	Headers: User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

https://prod.kiss-demo.nl/api/challenge	GET	Headers:
		Referer=https://prod.kiss-demo.nl/
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

https://prod.kiss-demo.nl/api/me	GET	Headers:
		Referer=https://prod.kiss-demo.nl/
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

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.

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.

Searching for URLs in Wayback Machine.

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 - X-XSS-Protection.

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 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.

Nothing was found for Exposed Backup Files.

Nothing was found for Request URL Override.

Nothing was found for HTTP/1.1 Request Smuggling.

Scan coverage information

List of tests performed (56/56)

- ✓ Checking for website accessibility...
- ✓ Checking for website technologies...
- ✓ Checking for vulnerabilities of server-side software...
- ✓ Checking for client access policies...
- ✓ Checking for robots.txt file...
- ✓ Checking for missing HTTP header - X-Frame-Options...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ 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...
- ✓ Spidering target...
- ✓ Checking for login interfaces...
- ✓ Checking for administration consoles...
- ✓ Checking for interesting files... (this might take a few hours)
- ✓ Checking for information disclosure... (this might take a few hours)
- ✓ Checking for software identification...
- ✓ Searching for URLs in Wayback Machine...
- ✓ 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 - X-XSS-Protection...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ Checking for missing HTTP header - Feature...
- ✓ 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 secure password submission...
- ✓ Checking for sensitive data...
- ✓ Checking for Server Side Request Forgery...
- ✓ Checking for Open Redirect...
- ✓ Checking for PHP Code Injection...
- ✓ Checking for JavaScript Code Injection...
- ✓ 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...

Scan parameters

Website URL:	https://prod.kiss-demo.nl/
Scan type:	Full_scan_default
Authentication:	False

Scan stats

Unique Injection Points Detected:	3
URLs spidered:	3
Total number of HTTP requests:	13740
Average time until a response was received:	7ms
Total number of HTTP request errors:	53