acunetix

Affected Items Report

Acunetix Security Audit

21 May 2025

Generated by Acunetix

Scan of https://dev.e-office.semarangkab.go.id/

Scan details

Scan information	
Start time	21/05/2025, 14:51:58
Start url	https://dev.e-office.semarangkab.go.id/
Host	https://dev.e-office.semarangkab.go.id/
Scan time	1 minutes, 11 seconds
Profile	Full Scan

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	9
High	0
Medium	3
Low	1
Informational	5

Affected items

Web Server	
Alert group	**HTML form without CSRF protection**
Severity	Medium
Description	This alert requires manual confirmation Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser. Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.
Recommendations	Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary. The recommended and the most widely used technique for preventing CSRF attacks is know as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well designed anti-CSRF system involve the following attributes. • The anti-CSRF token should be unique for each user session • The session should automatically expire after a suitable amount of time • The anti-CSRF token should be a cryptographically random value of significant length • The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm • The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent) • The server should reject the requested action if the anti-CSRF token fails validation When a user submits a form or makes some other authenticated request that requires a Cookie, the anti-CSRF token should be included in the request. Then, the web application will then verify the existence and correctness of this token before processing the request. If the token is missing or incorrect, the request can be rejected.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**HTML form without CSRF protection**
Severity	Medium
Description	This alert requires manual confirmation Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser. Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.
Recommendations	Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary. The recommended and the most widely used technique for preventing CSRF attacks is know as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well designed anti-CSRF system involve the following attributes. • The anti-CSRF token should be unique for each user session • The session should automatically expire after a suitable amount of time • The anti-CSRF token should be a cryptographically random value of significant length • The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm

	• The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent) • The server should reject the requested action if the anti-CSRF token fails validation When a user submits a form or makes some other authenticated request that requires a Cookie, the anti-CSRF token should be included in the request. Then, the web application will then verify the existence and correctness of this token before processing the request. If the token is missing or incorrect, the request can be rejected.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**Password field submitted using GET method**
Severity	Medium
Description	This page contains a form with a password field. This form submits user data using the GET method, therefore the contents of the password field will appear in the URL.Sensitive information should not be passed via the URL. URLs could be logged or leaked via the Referer header.
Recommendations	The password field should be submitted through POST instead of GET.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**Cookie(s) without Secure flag set**
Severity	Low
Description	This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.
Recommendations	If possible, you should set the Secure flag for this cookie.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**Email address found**
Severity	Informational
Description	One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
Recommendations	Check references for details on how to solve this problem.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	**Password type input with auto-complete enabled**
Severity	Informational
Description	When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with

	local access could obtain the cleartext password from the browser cache.
Recommendations	The password auto-complete should be disabled in sensitive applications. To disable auto-complete, you may use a code similar to: `<INPUT TYPE="password" AUTOCOMPLETE="off">`
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Password type input with auto-complete enabled**
Severity	Informational
Description	When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.
Recommendations	The password auto-complete should be disabled in sensitive applications. To disable auto-complete, you may use a code similar to: `<INPUT TYPE="password" AUTOCOMPLETE="off">`
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Password type input with auto-complete enabled**
Severity	Informational
Description	When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.
Recommendations	The password auto-complete should be disabled in sensitive applications. To disable auto-complete, you may use a code similar to: `<INPUT TYPE="password" AUTOCOMPLETE="off">`
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Password type input with auto-complete enabled**
Severity	Informational
Description	When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.
Recommendations	The password auto-complete should be disabled in sensitive applications. To disable auto-complete, you may use a code similar to: `<INPUT TYPE="password" AUTOCOMPLETE="off">`
Alert variants	
Details	Not available in the free trial

Not available in the free trial

Scanned items (coverage report)

https://dev.e-office.semarangkab.go.id/
https://dev.e-office.semarangkab.go.id/asset
https://dev.e-office.semarangkab.go.id/asset/e-office
https://dev.e-office.semarangkab.go.id/asset/e-office/css
https://dev.e-office.semarangkab.go.id/asset/e-office/css/css-assets.css
https://dev.e-office.semarangkab.go.id/asset/e-office/css/style.css
https://dev.e-office.semarangkab.go.id/asset/e-office/fonts
https://dev.e-office.semarangkab.go.id/asset/e-office/fonts/flaticon-magicay
https://dev.e-office.semarangkab.go.id/asset/e-office/fonts/flaticon-magicay/flaticon.css
https://dev.e-office.semarangkab.go.id/asset/e-office/fonts/fontawesome
https://dev.e-office.semarangkab.go.id/asset/e-office/fonts/fontawesome/css
https://dev.e-office.semarangkab.go.id/asset/e-office/fonts/fontawesome/css/all.css
https://dev.e-office.semarangkab.go.id/asset/e-office/fonts/fontawesome/webfonts
https://dev.e-office.semarangkab.go.id/asset/e-office/fonts/fontawesome/webfonts/fa-brands-400.woff2
https://dev.e-office.semarangkab.go.id/asset/e-office/fonts/fontawesome/webfonts/fa-regular-400.woff2
https://dev.e-office.semarangkab.go.id/asset/e-office/fonts/fontawesome/webfonts/fa-solid-900.woff2
https://dev.e-office.semarangkab.go.id/asset/e-office/images
https://dev.e-office.semarangkab.go.id/asset/e-office/images/files
https://dev.e-office.semarangkab.go.id/asset/e-office/images/general-elements
https://dev.e-office.semarangkab.go.id/asset/e-office/images/general-elements/bg-patterns
https://dev.e-office.semarangkab.go.id/asset/e-office/images/general-elements/bg-patterns/grid
https://dev.e-office.semarangkab.go.id/asset/e-office/images/general-elements/bg-patterns/texture
https://dev.e-office.semarangkab.go.id/asset/e-office/images/general-elements/favicon
https://dev.e-office.semarangkab.go.id/asset/e-office/images/general-elements/section-separators
https://dev.e-office.semarangkab.go.id/asset/e-office/images/kolaborasi
https://dev.e-office.semarangkab.go.id/asset/e-office/js
https://dev.e-office.semarangkab.go.id/asset/e-office/js/functions.js
https://dev.e-office.semarangkab.go.id/asset/e-office/js/jquery.ajaxchimp.min.js
https://dev.e-office.semarangkab.go.id/asset/e-office/js/jquery.easing.min.js
https://dev.e-office.semarangkab.go.id/asset/e-office/js/jquery.fitvids.js
https://dev.e-office.semarangkab.go.id/asset/e-office/js/jquery.js
https://dev.e-office.semarangkab.go.id/asset/e-office/js/jquery.magnific-popup.min.js
https://dev.e-office.semarangkab.go.id/asset/e-office/js/jquery.mb.YTPlayer.min.js
https://dev.e-office.semarangkab.go.id/asset/e-office/js/jquery.stellar.js
https://dev.e-office.semarangkab.go.id/asset/e-office/js/jquery.validate.min.js
https://dev.e-office.semarangkab.go.id/asset/e-office/js/jquery.waypoints.min.js
https://dev.e-office.semarangkab.go.id/asset/e-office/js/jRespond.min.js
https://dev.e-office.semarangkab.go.id/asset/e-office/js/owl.carousel.min.js
https://dev.e-office.semarangkab.go.id/asset/e-office/js/simple-scrollbar.min.js
https://dev.e-office.semarangkab.go.id/captcha
https://dev.e-office.semarangkab.go.id/data
https://dev.e-office.semarangkab.go.id/data/logo
https://dev.e-office.semarangkab.go.id/robots.txt