INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 03, Tahun 2026, Hal. 281-289, ISSN: 3123-5573 (Online)

Analisis Keamanan Aplikasi *Web* Terhadap Serangan *Cross-Site Request Forgery* (CSRF)

Rakhmadi Rahman[1], Sahara Fauziah[2], Airin Dwi Zalzabilah[3]
[1,2,3] Program Studi Sistem Informasi, Institut Teknologi Bacharuddin Jusuf Habibie
rakhmadi.rahman@ith.ac.id[1], saharafauziah0612@gmail.com[2], airindwis05@gmail.com[3]

Article Info
Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Keywords:
Analysis, Security, Website, Cross-Site Request Forgery (CSRF), East Aceh timur.

ABSTRACT
Cross-Site Request Forgery *(CSRF) is an attack that asks end users to take unwanted actions on a web application during the authentication process. The security of a web becomes very important from CSRF attacks, opposing with various encryption methods that can be used as alternatives to overcome CSRF attacks. The purpose of this research is to find the gaps in the East Aceh Regency Government website, to analyze the East Aceh Regency Government website for the CSRF attack, to minimize the CSRF attack on the East Aceh Government institution from the CSRF attack technique. using the Acunetix tool. Based on the analysis of the East Aceh Government website, a conclusion can be made, namely the assessment of the website jdih.acehtimurkab.go.id and acehtimurkab.go.id cross scripting based DOM site., analysis of attacks on the East Aceh Government website with HTML attack type without CSRF protection found attack protection on Alert Media, and based on security analysis and attack analysis on the website, an anti CSRF library was created that can be used to find all forms of attack from the CSRF attack technique.*

Article Info
Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Kata Kunci:
Analisa, Keamanan, Website, Serangan Cross-Site Request Forgery (CSRF), Kabupaten Aceh Timur.

ABSTRAK
Cross-Site Request Forgery (CSRF) adalah serangan yang memaksa pengguna akhir untuk melakukan tindakan yang tidak diinginkan pada aplikasi web saat proses autentikasi. Keamanan sebuah web menjadi sangat penting dari serangan CSRF, pencegahan dengan berbagai metode enkripsi dapat dijadikan sebuah alternatif untuk mengatasi serangan CSRF. tujuan dari penelitian untuk menemukan celah kerentanan website Pemerintah Kabupaten Aceh Timur, menganalisa kerentanan website Pemerintah Kabupaten Aceh Timur terhadap serangan CSRF, untuk meminimalisir terhadap serangan CSRF pada insansi pemerintahan aceh timur dari tekhnik penyerangan CSRF. menggunakan *tool Acunetix*. Berdasarkan hasil Analisa website Pemerintahan Aceh Timur maka dapat dibuat kesimpulan, yaitu persentase kerentanan dari kedua website jdih.acehtimurkab.go.id dan acehtimurkab.go.id terdapat *Rank Vulnerability* dengan tipe high sebesar masing-masing 5 celah pada kerentanan *DOM-based cross site scripting*, analisa serangan terhadap website Pemerintahan Aceh Timur dengan tipe serangan *HTML form without CSRF protection* didapati kerentanan serangan pada Alert Medium, dan berdasarkan Analisa keamanan dan analisis serangan terhadap kedua website maka dibuatkan sebuah libraries anti CSRF yang diharapkan mampu mengatasi berbagai bentuk serangan dari tekhnik penyerangan CSRF.

INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 03, Tahun 2026, Hal. 281-289, ISSN: 3123-5573 (Online)

Corresponding Author:
Rakhmadi Rahman
Information Systems Bacharuddin Jusuf Habibie Institute of Technology
E-mail: rakhmadi.rahman@ith.ac.id

PENDAHULUAN

Website atau situs dapat diartikan sebagai kumpulan halaman-halaman yang digunakan untuk menampilkan informasi teks, gambar diam atau gerak, animasi, suara, dan atau gabungan dari semuanya, baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait, Keamanan merupakan salah satu indikator penting dalam membangun sebuah *website* (Ahmed dkk, 2011), saat ini banyak pengembang dan pemilik situs gagal melindungi keamanan *web* dan sebagian besar diabaikan oleh pengembang *web* dan komunitas keamanan (Chen dkk, 2013).

Terdapat beberapa cara yang dapat digunakan untuk melakukan pengujian terhadap keamanan *website*. Salah satunya adalah *Cross-Site Request Forgery* (CSRF). *Cross-Site Request Forgery* (CSRF) adalah serangan yang memaksa pengguna akhir untuk melakukan tindakan yang tidak diinginkan pada aplikasi *web* saat proses autentikasi (petefish dkk, 2011). *Cross-Site Request Forgery* (CSRF), dikenal juga dengan *one click attack* atau *session riding* disingkat dengan CSRF atau XSRF, merupakan bentuk eksploitasi *website* yang dieksekusi atas wewenang korban, tanpa dikehendakinya. Keamanan sebuah *web* menjadi sangat penting dari serangan CSRF, pencegahan dengan berbagai metode enkripsi dapat dijadikan sebuah alternatif untuk mengatasi serangan CSRF. Berdasarkan latar belakang diatas, maka dirasa perlu untuk mengetahui serangan CSRF dan mengatasi masalah terhadap keamanan *website* Pemerintah Kabupaten Aceh Timur.

KAJIAN PUSTAKA

Keamanan

Keamanan adalah faktor penting yang harus di pertimbangkan dalam *Web Engineering*. Sebuah aplikasi *website* mungkin berisi berbagai jenis kerentanan. Sebagai contoh jika aplikasi *website* yang rentan itu berisi kerentanan seperti *Injection*, *Broken Authentication dan Session Managemen, Cross-Site Scripting (XSS), insecure Direct Object References,* Keamanan *Misconfiguration*, *Sensitive Data Exposure*, Hilang Fungsi Tingkat Akses Kontrol, Permintaan *Cross-site Request Forgery (CSRF)* (Patil dkk, 2016).

Cross-Site Request Forgery (CSRF)

Menurut Ian (2019) *Cross-site Request Forgery* (CSRF) adalah jenis serangan yang memanfaatkan otentikasi dan otorisasi target ketika permintaan palsu sedang dikirim ke *server web*. Oleh karena itu, kerentanan CSRF yang mempengaruhi pengguna seperti administrator, selama serangan *Cross-site Request Forgery* (CSRF), Serangan CSRF secara khusus menargetkan request data bukan pencurian data, karena penyerang tidak memiliki cara untuk melihat respons terhadap permintaan yang dipalsukan. Dengan sedikit bantuan rekayasa sosial, penyerang dapat menipu pengguna aplikasi *web* untuk melakukan tindakan yang dipilih penyerang. Contoh akibat dari Serangan CSRF ini adalah mampu melakukan perubahan detail akun pada korban. Data pribadi seperti nama, alamat, bahkan sampai password korban bisa diubah dengan menggunakan teknik ini.

CSRF merupakan serangan dimana penyerang dapat menggunakan aplikasi itu sendiri untuk memberi korban tautan eksploitasi atau konten lainnya yang mengarahkan *browser* korban untuk melakukan tindakan yang dikendalikan oleh penyerang. Reflected CSRF, merupakan serangan yang memanfaatkan link atau konten diluar sistem aplikasi. Hal ini bisa dilakukan dengan menggunakan email, blog, pesan instan yang terdapat didalam aplikasi tersebut (Makalalang, 2017).

DOM-based Cross-site Scripting

Nofia Delta (2017) menjelaskan *Document Object Model* (DOM) adalah konvensi yang digunakan untuk mewakili dan bekerja dengan objek dalam dokumen HTML. Semua dokumen HTML memiliki DOM terkait yang terdiri dari objek, yang mewakili properti dokumen dari sudut pandang *browser*. Saat skrip sisi klien dieksekusi, ia dapat menggunakan DOM halaman HTML tempat skrip dijalankan. Script dapat mengakses berbagai properti halaman dan mengubah nilainya. Objek paling populer dari perspektif ini adalah document.url, document.location, dan document.referrer. Potensi konsekuensi dari kerentanan XSS berbasis DOM diklasifikasikan dalam dokumen OWASP Top 10 2017 sebagai moderat (Acunetix. 2019). Dari hasil literasi dan pakar dapat dijelaskan bahwa hubungan antara *Cross-Site-Request-Forgery* dan DOM-*based Cross-site Scripting* (XSS) terletak pada skrip sisi klien yang digunakan penyerang yaitu pada document.url, document.location, dan document.referrer serta sesi.

HyperText Transfer Protocol (HTTP)

Menurut Fielding (2014) HyperText Transfer Protocol atau HTTP adalah sebuah protokol yang memungkinkan web browser untuk berkomunikasi dengan web server dalam pertukaran informasi. HTTP menyediakan sebuah cara standar untuk berkomunikasi antara browser dan server, sehingga browser apapun dapat berkomunikasi dengan server manapun asalkan keduanya sesuai dengan spesifikasi HTTP. Saat HTTP diakses, klien memulainya dengan sebuah request dan direspon oleh server. Setiap request dan response memiliki 3 bagian yaitu status line, header fields/section, dan entity body (Makalalang, 2017).

METODE PENELITIAN

Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode analisis keamanan aplikasi web. Pendekatan ini dipilih karena penelitian berfokus pada pengamatan, pengujian, serta analisis terhadap kondisi keamanan website tanpa melakukan manipulasi terhadap sistem yang diuji. Analisis dilakukan dengan cara mengidentifikasi celah keamanan, khususnya yang berkaitan dengan serangan Cross-Site Request Forgery (CSRF), serta mengevaluasi potensi dampak yang dapat ditimbulkan. Selain itu, penelitian ini menerapkan metode penetration testing terbatas, yaitu pengujian keamanan yang bertujuan untuk mensimulasikan serangan nyata secara terkendali guna mengetahui tingkat kerentanan sistem. Metode ini digunakan untuk memperoleh gambaran aktual mengenai kondisi keamanan aplikasi web Pemerintah Kabupaten Aceh Timur.

Objek dan Lokasi Penelitian

Objek penelitian dalam studi ini adalah website resmi Pemerintah Kabupaten Aceh Timur yang dapat diakses secara publik melalui jaringan internet. Pemilihan objek penelitian didasarkan pada pertimbangan bahwa website pemerintahan memiliki peran strategis dalam penyediaan layanan informasi dan administrasi kepada masyarakat, sehingga aspek keamanannya perlu mendapat perhatian khusus. Lokasi penelitian tidak dibatasi pada wilayah fisik tertentu karena proses pengujian dilakukan secara daring (online). Peneliti dapat melakukan analisis dari lokasi mana pun selama terhubung dengan jaringan internet yang stabil dan aman.

Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dilakukan secara sistematis untuk memperoleh informasi yang relevan dan akurat terkait kondisi keamanan aplikasi web. Pengumpulan data bertujuan untuk mendukung proses analisis celah keamanan serta memberikan dasar yang kuat dalam penyusunan rekomendasi perbaikan. Teknik pengumpulan data yang digunakan meliputi observasi langsung terhadap sistem, studi dokumentasi, serta pengujian keamanan menggunakan tools pemindai kerentanan. Pendekatan ini memungkinkan peneliti memperoleh gambaran menyeluruh mengenai tingkat keamanan website Pemerintahan Kabupaten Aceh Timur.

Metode Pengujian Keamanan Website

Metode pengujian keamanan website yang digunakan dalam penelitian ini adalah **vulnerability assessment** dengan pendekatan pemindaian kerentanan secara otomatis. Pengujian dilakukan menggunakan tools keamanan yang mampu mendeteksi berbagai jenis celah keamanan aplikasi web, termasuk CSRF dan DOM-based Cross-Site

Scripting (XSS). Proses pengujian dilakukan secara non-intrusif, yaitu tanpa mengganggu ketersediaan layanan website. Setiap pemindaian dilakukan dengan pengaturan parameter yang disesuaikan dengan karakteristik website pemerintahan. Hasil pengujian kemudian dianalisis untuk menentukan tingkat risiko dan potensi dampak dari setiap celah yang ditemukan.

Teknik Analisis Data

Teknik analisis data yang digunakan dalam penelitian ini adalah analisis deskriptif kualitatif. Data hasil pemindaian keamanan dianalisis dengan cara mengelompokkan jenis kerentanan, tingkat risiko, serta potensi dampak yang dapat ditimbulkan oleh serangan CSRF. Hasil analisis kemudian dibandingkan dengan standar keamanan aplikasi web yang direkomendasikan oleh OWASP untuk menentukan tingkat keamanan website Pemerintah Kabupaten Aceh Timur.

Implementasi Model Serangan CSRF

Implementasi model serangan CSRF dalam penelitian ini dilakukan secara konseptual dan simulatif untuk memahami bagaimana serangan dapat terjadi pada website yang rentan. Model serangan disusun berdasarkan skenario umum CSRF, yaitu dengan memanfaatkan sesi pengguna yang telah terautentikasi. Pada tahap ini, peneliti menganalisis alur permintaan HTTP yang dikirimkan oleh browser pengguna ke server. Permintaan tersebut kemudian dievaluasi untuk mengetahui apakah server melakukan validasi tambahan terhadap keabsahan request. Apabila permintaan dapat diproses tanpa mekanisme validasi yang memadai, maka sistem dinilai rentan terhadap serangan CSRF. Model serangan ini tidak dilakukan secara merusak, melainkan hanya untuk tujuan analisis dan pembelajaran guna mengidentifikasi kelemahan sistem.

Rekomendasi Perbaikan dan Solusi Keamanan

Berdasarkan hasil pengujian dan analisis model serangan CSRF, penelitian ini menyusun rekomendasi perbaikan dan solusi keamanan yang bersifat preventif. Rekomendasi difokuskan pada penerapan token anti-CSRF, perbaikan validasi input pengguna, serta penguatan pengelolaan sesi. Selain itu, solusi keamanan juga mencakup penerapan validasi header HTTP, penggunaan atribut keamanan pada cookie, serta peningkatan kesadaran pengelola website terhadap pentingnya keamanan aplikasi web. Rekomendasi ini diharapkan dapat membantu Pemerintahan Kabupaten Aceh Timur dalam meningkatkan tingkat keamanan sistem secara berkelanjutan.

Alur Penelitian

Alur penelitian disusun untuk menggambarkan tahapan penelitian secara sistematis dan terstruktur. Tahapan penelitian dimulai dari identifikasi permasalahan, dilanjutkan dengan studi literatur, pengumpulan data, pengujian keamanan, analisis hasil, hingga penyusunan rekomendasi perbaikan.

Secara rinci, alur penelitian dalam studi ini meliputi:

1. Identifikasi masalah keamanan aplikasi web
2. Studi literatur terkait CSRF dan keamanan web
3. Penentuan objek dan ruang lingkup penelitian
4. Pengumpulan data primer dan sekunder
5. Pengujian keamanan website
6. Analisis celah keamanan yang ditemukan
7. Penyusunan rekomendasi dan solusi keamanan
8. Penyusunan laporan hasil penelitian

Alur penelitian ini dirancang untuk memastikan bahwa setiap tahapan saling berkaitan dan mendukung pencapaian tujuan penelitian.

HASIL DAN PEMBAHASAN

Hasil Analisis Celah Keamanan pada Website Pemerintahan Kabupaten Aceh Timur

1. Gambaran Umum Hasil Pengujian Keamanan

Berdasarkan pengujian keamanan yang telah dilakukan terhadap website Pemerintahan Kabupaten Aceh Timur menggunakan tools pemindai kerentanan Acunetix, diperoleh gambaran umum mengenai kondisi keamanan aplikasi

web yang diuji. Pengujian difokuskan pada identifikasi celah keamanan yang berpotensi dimanfaatkan melalui serangan Cross-Site Request Forgery (CSRF) serta kerentanan pendukung lainnya, seperti DOM-based Cross-Site Scripting (XSS). Hasil pemindaian menunjukkan bahwa beberapa komponen pada website masih belum menerapkan mekanisme perlindungan yang memadai terhadap serangan berbasis sesi pengguna. Hal ini mengindikasikan bahwa sistem masih memiliki tingkat risiko keamanan yang perlu mendapat perhatian lebih lanjut, khususnya pada fitur-fitur yang melibatkan interaksi pengguna dan pengiriman data melalui form.

2. Temuan Celah Keamanan Berdasarkan Tingkat Risiko

Berdasarkan hasil analisis, kerentanan yang ditemukan pada website Pemerintahan Kabupaten Aceh Timur diklasifikasikan ke dalam beberapa tingkat risiko, yaitu rendah, sedang, dan tinggi. Dari keseluruhan temuan, kerentanan dengan tingkat risiko tinggi menjadi fokus utama pembahasan karena memiliki potensi dampak yang signifikan terhadap keamanan sistem. Kerentanan dengan kategori risiko tinggi sebagian besar berkaitan dengan DOM-based Cross-Site Scripting. Celah ini memungkinkan penyerang untuk memanipulasi elemen DOM pada sisi klien, sehingga dapat digunakan sebagai sarana untuk menjalankan serangan CSRF. Jumlah celah dengan tingkat risiko tinggi yang ditemukan menunjukkan bahwa mekanisme validasi input dan pengelolaan skrip pada sisi klien masih belum optimal. Selain itu, ditemukan pula beberapa form input yang tidak dilengkapi dengan token anti-CSRF. Kondisi ini memungkinkan permintaan palsu dikirimkan ke server menggunakan metode GET maupun POST tanpa adanya proses verifikasi tambahan. Apabila celah ini dieksploitasi, penyerang dapat memanfaatkan sesi pengguna yang masih aktif untuk menjalankan aksi tertentu tanpa sepengetahuan pengguna.

3. Analisis Kerentanan pada Website Utama dan JDIH Aceh Timur

Hasil pemindaian menunjukkan bahwa website utama Pemerintahan Kabupaten Aceh Timur serta website Jaringan Dokumentasi dan Informasi Hukum (JDIH) Aceh Timur memiliki karakteristik kerentanan yang hampir serupa. Kedua website tersebut menampilkan sejumlah celah keamanan dengan tingkat risiko tinggi yang berkaitan dengan DOM-based XSS dan ketiadaan perlindungan CSRF pada beberapa form. Pada website utama, celah keamanan ditemukan pada halaman-halaman yang memiliki fungsi pengelolaan konten dan interaksi pengguna. Sementara itu, pada website JDIH Aceh Timur, kerentanan lebih banyak ditemukan pada fitur pencarian dan pengolahan data dokumen hukum. Kesamaan jenis kerentanan ini menunjukkan bahwa pola pengembangan dan pengamanan aplikasi web pada lingkungan pemerintahan Aceh Timur masih memerlukan peningkatan secara menyeluruh.

4. Potensi Dampak Serangan CSRF

Berdasarkan hasil analisis, potensi dampak serangan CSRF pada website Pemerintahan Kabupaten Aceh Timur tergolong cukup serius. Apabila serangan berhasil dilakukan, penyerang dapat memanfaatkan sesi pengguna yang telah terautentikasi untuk menjalankan perintah tertentu, seperti mengubah data, memanipulasi konten, atau mengakses fungsi administratif. Serangan CSRF juga berpotensi menurunkan tingkat kepercayaan masyarakat terhadap layanan publik berbasis web. Website pemerintahan yang mengalami gangguan keamanan dapat dianggap tidak mampu menjaga kerahasiaan dan integritas data, sehingga berdampak pada citra instansi pemerintahan itu sendiri.

5. Pembahasan Hubungan CSRF dan DOM-Based XSS

Hasil pengujian menunjukkan bahwa kerentanan CSRF pada website Pemerintahan Kabupaten Aceh Timur tidak dapat dipisahkan dari keberadaan celah DOM-based XSS. DOM-based XSS dapat dimanfaatkan sebagai media untuk menyisipkan skrip berbahaya yang selanjutnya digunakan untuk memicu serangan CSRF. Kelemahan pada pengolahan elemen DOM, seperti penggunaan parameter URL tanpa validasi yang memadai, menjadi faktor utama yang meningkatkan risiko serangan gabungan antara CSRF dan XSS. Oleh karena itu, perbaikan keamanan tidak hanya difokuskan pada penerapan token anti-CSRF, tetapi juga pada penguatan pengamanan skrip sisi klien.

6. Evaluasi Efektivitas Mitigasi Keamanan

Sebagai bagian dari pembahasan, dilakukan evaluasi terhadap penerapan mekanisme mitigasi keamanan berupa token anti-CSRF. Hasil pengujian ulang setelah penerapan token menunjukkan bahwa permintaan palsu yang sebelumnya terdeteksi tidak lagi dapat dijalankan oleh sistem. Selain itu, perbaikan pada skrip DOM dan penerapan filter input pengguna juga terbukti mampu mengurangi potensi serangan DOM-based XSS. Hal ini menunjukkan bahwa kombinasi antara token anti-CSRF dan pengamanan sisi klien merupakan pendekatan yang efektif dalam meningkatkan keamanan aplikasi web Pemerintahan Kabupaten Aceh Timur.

7. Implikasi Hasil Penelitian

Hasil penelitian ini memberikan gambaran bahwa keamanan website pemerintahan masih memerlukan perhatian serius, khususnya dalam menghadapi ancaman CSRF. Temuan ini dapat dijadikan dasar bagi pengelola sistem untuk melakukan perbaikan dan pengembangan keamanan secara berkelanjutan. Selain itu, hasil analisis ini juga dapat menjadi referensi bagi instansi pemerintahan lain dalam melakukan evaluasi keamanan aplikasi web yang mereka kelola, sehingga dapat meminimalkan risiko serangan siber di masa mendatang.

Rekomendasi Perbaikan Celah Website Pemerintahan Aceh Timur

1. Penguatan Mekanisme Perlindungan terhadap Serangan CSRF

Berdasarkan hasil analisis celah keamanan yang ditemukan pada website Pemerintahan Kabupaten Aceh Timur, salah satu langkah utama yang direkomendasikan adalah penguatan mekanisme perlindungan terhadap serangan Cross-Site Request Forgery (CSRF). Serangan ini terjadi karena server masih mempercayai permintaan yang dikirimkan oleh browser pengguna tanpa melakukan validasi tambahan terhadap keabsahan permintaan tersebut. Untuk mengatasi permasalahan ini, disarankan agar setiap form dan permintaan sensitif dilengkapi dengan token anti-CSRF yang bersifat unik dan tidak dapat ditebak. Token tersebut harus dihasilkan secara acak oleh server dan divalidasi setiap kali terjadi pengiriman data dari klien. Dengan penerapan token ini, server dapat memastikan bahwa permintaan yang diterima benar-benar berasal dari interaksi sah pengguna, bukan dari permintaan palsu yang dikirimkan oleh pihak penyerang.

2. Penerapan Token Anti-CSRF pada Seluruh Form Interaktif

Rekomendasi berikutnya adalah penerapan token anti-CSRF secara menyeluruh pada seluruh form interaktif yang terdapat pada website Pemerintahan Kabupaten Aceh Timur, baik yang menggunakan metode GET maupun POST. Form yang tidak dilengkapi dengan token validasi menjadi titik lemah utama yang dapat dimanfaatkan dalam serangan CSRF. Token anti-CSRF sebaiknya diimplementasikan sebagai bagian dari libraries keamanan yang dipanggil pada setiap halaman website. Dengan pendekatan ini, proses validasi dapat dilakukan secara otomatis dan konsisten pada seluruh modul aplikasi. Selain itu, token harus diperbarui secara berkala untuk mencegah kemungkinan penyalahgunaan token lama oleh penyerang.

3. Perbaikan Kerentanan DOM-Based Cross-Site Scripting

Hasil analisis menunjukkan bahwa celah keamanan yang paling dominan pada website Pemerintahan Aceh Timur berkaitan dengan DOM-based Cross-Site Scripting (XSS). Oleh karena itu, diperlukan perbaikan pada pengolahan elemen Document Object Model (DOM) di sisi klien. Rekomendasi yang dapat diterapkan adalah melakukan validasi dan sanitasi input pengguna sebelum data tersebut diproses oleh skrip JavaScript. Selain itu, pengembang perlu menghindari penggunaan langsung parameter URL atau data dari pengguna tanpa proses penyaringan. Perubahan pada struktur skrip dan penerapan encoding karakter yang sesuai dapat membantu mencegah penyisipan skrip berbahaya ke dalam halaman website.

4. Validasi Header HTTP sebagai Lapisan Keamanan Tambahan

Selain penggunaan token anti-CSRF, validasi terhadap header HTTP seperti Referer dan Origin dapat dijadikan sebagai lapisan keamanan tambahan. Dengan melakukan pemeriksaan terhadap asal permintaan, server dapat menolak request yang berasal dari domain yang tidak dikenal atau mencurigakan.

Meskipun metode ini tidak sepenuhnya menggantikan token anti-CSRF, kombinasi antara validasi header HTTP dan token CSRF dapat meningkatkan tingkat keamanan aplikasi web secara signifikan. Pendekatan ini sangat disarankan untuk diterapkan pada fitur-fitur kritis yang berkaitan dengan pengelolaan data dan hak akses pengguna.

5. Pengelolaan Sesi Pengguna yang Lebih Aman

Pengelolaan sesi pengguna merupakan aspek penting dalam pencegahan serangan CSRF. Website Pemerintahan Kabupaten Aceh Timur disarankan untuk menerapkan pengaturan sesi yang lebih ketat, seperti pembatasan masa aktif sesi dan regenerasi session ID setelah proses autentikasi berhasil. Selain itu, penggunaan atribut keamanan pada cookie, seperti HttpOnly dan Secure, dapat membantu mengurangi risiko penyalahgunaan sesi pengguna. Dengan pengelolaan sesi yang baik, peluang penyerang untuk memanfaatkan sesi aktif pengguna dapat diminimalkan.

6. Penerapan Pengujian Keamanan Secara Berkala

Rekomendasi selanjutnya adalah melakukan pengujian keamanan secara rutin dan berkala terhadap website Pemerintahan Kabupaten Aceh Timur. Pengujian dapat dilakukan menggunakan tools vulnerability scanner seperti Acunetix untuk mendeteksi celah keamanan yang mungkin muncul akibat pembaruan sistem atau perubahan konfigurasi. Pengujian berkala memungkinkan pengelola website untuk melakukan tindakan pencegahan sejak dini sebelum celah keamanan tersebut dieksploitasi oleh pihak yang tidak bertanggung jawab. Selain itu, hasil pengujian dapat digunakan sebagai dasar evaluasi dan pengembangan sistem keamanan di masa mendatang.

7. Peningkatan Kesadaran dan Kompetensi Pengelola Website

Selain perbaikan teknis, peningkatan kesadaran dan kompetensi sumber daya manusia yang mengelola website juga menjadi faktor penting dalam menjaga keamanan sistem. Pengelola website Pemerintahan Kabupaten Aceh Timur disarankan untuk mendapatkan pelatihan terkait keamanan aplikasi web, khususnya mengenai serangan CSRF dan teknik mitigasinya. Dengan pemahaman yang baik mengenai ancaman keamanan, pengelola website dapat lebih responsif dalam menangani potensi risiko serta menerapkan praktik pengembangan aplikasi yang aman.

8. Implementasi Standar Keamanan Aplikasi Web

Sebagai langkah jangka panjang, website Pemerintahan Kabupaten Aceh Timur disarankan untuk mengadopsi standar keamanan aplikasi web yang direkomendasikan oleh organisasi keamanan internasional, seperti OWASP. Penerapan standar ini dapat membantu memastikan bahwa setiap pengembangan dan pemeliharaan sistem dilakukan dengan memperhatikan aspek keamanan secara menyeluruh.

Ringkasan Rekomendasi

Secara keseluruhan, rekomendasi perbaikan celah keamanan pada website Pemerintahan Kabupaten Aceh Timur mencakup penerapan token anti-CSRF, perbaikan DOM-based XSS, penguatan validasi request HTTP, pengelolaan sesi pengguna yang aman, serta pengujian keamanan secara berkala. Implementasi rekomendasi ini diharapkan mampu meningkatkan ketahanan website terhadap serangan CSRF dan menjaga kepercayaan masyarakat terhadap layanan publik berbasis web.

Kesimpulan dan Saran

Kesimpulan

Berdasarkan hasil penelitian dan analisis keamanan aplikasi web terhadap serangan Cross-Site Request Forgery (CSRF) pada website Pemerintahan Kabupaten Aceh Timur, dapat disimpulkan bahwa sistem yang diuji masih memiliki sejumlah celah keamanan yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab. Hasil pemindaian keamanan menunjukkan bahwa beberapa fitur interaktif pada website belum menerapkan mekanisme perlindungan CSRF secara optimal, sehingga memungkinkan terjadinya pengiriman permintaan palsu dengan memanfaatkan sesi pengguna yang aktif. Selain itu, penelitian ini menemukan bahwa keberadaan kerentanan DOM-based Cross-Site Scripting (XSS) turut memperbesar risiko serangan CSRF. Kelemahan dalam pengelolaan elemen DOM dan kurangnya validasi input pengguna menjadi faktor utama yang meningkatkan peluang terjadinya

eksploitasi gabungan antara CSRF dan XSS. Kondisi ini menunjukkan bahwa keamanan aplikasi web tidak hanya bergantung pada satu mekanisme perlindungan, melainkan memerlukan pendekatan menyeluruh pada sisi klien dan server.

Hasil analisis juga menunjukkan bahwa website utama Pemerintahan Kabupaten Aceh Timur serta website Jaringan Dokumentasi dan Informasi Hukum (JDIH) memiliki pola kerentanan yang relatif serupa. Hal ini mengindikasikan bahwa penerapan standar keamanan aplikasi web di lingkungan pemerintahan daerah masih perlu ditingkatkan secara konsisten. Kerentanan yang ditemukan berpotensi menimbulkan dampak serius, seperti perubahan data tanpa izin, penyalahgunaan hak akses, serta penurunan tingkat kepercayaan masyarakat terhadap layanan publik berbasis web. Dengan demikian, penelitian ini membuktikan bahwa pengujian keamanan aplikasi web menggunakan vulnerability scanner merupakan langkah yang efektif untuk mengidentifikasi celah keamanan sejak dini. Temuan penelitian dapat dijadikan dasar bagi pengelola website Pemerintahan Kabupaten Aceh Timur dalam melakukan evaluasi dan perbaikan sistem keamanan secara berkelanjutan.

Saran

Berdasarkan kesimpulan yang telah diperoleh, terdapat beberapa saran yang dapat dijadikan sebagai bahan pertimbangan untuk meningkatkan keamanan website Pemerintahan Kabupaten Aceh Timur di masa mendatang. Pertama, disarankan agar pengelola website menerapkan mekanisme token anti-CSRF secara menyeluruh pada seluruh form dan fitur interaktif yang melibatkan pengiriman data pengguna. Penerapan token yang unik dan dinamis diharapkan mampu meminimalkan risiko serangan CSRF secara signifikan. Kedua, perbaikan terhadap kerentanan DOM-based XSS perlu dilakukan dengan meningkatkan proses validasi dan sanitasi input pengguna, serta menghindari penggunaan data dari pengguna secara langsung pada skrip JavaScript. Penguatan pengamanan pada sisi klien akan membantu mengurangi kemungkinan terjadinya serangan lanjutan yang memanfaatkan celah CSRF. Ketiga, pengelolaan sesi pengguna perlu ditingkatkan melalui penerapan pengaturan sesi yang lebih ketat, seperti pembatasan waktu sesi, regenerasi session ID setelah login, serta penggunaan atribut keamanan pada cookie. Langkah ini bertujuan untuk mengurangi peluang penyalahgunaan sesi oleh pihak yang tidak berwenang. Keempat, pengujian keamanan aplikasi web disarankan untuk dilakukan secara berkala, terutama setelah adanya pembaruan sistem atau penambahan fitur baru. Pengujian rutin akan membantu mendeteksi potensi celah keamanan yang mungkin muncul akibat perubahan pada sistem. Terakhir, peningkatan kompetensi sumber daya manusia yang terlibat dalam pengelolaan website juga menjadi hal yang penting. Pelatihan terkait keamanan aplikasi web dan penerapan standar keamanan yang direkomendasikan, seperti OWASP, diharapkan dapat membantu menciptakan lingkungan pengelolaan sistem informasi pemerintahan yang lebih aman dan terpercaya. Dengan penerapan saran-saran tersebut, diharapkan website Pemerintahan Kabupaten Aceh Timur dapat meningkatkan tingkat keamanan sistem, meminimalkan risiko serangan CSRF, serta menjaga keandalan layanan publik berbasis teknologi informasi.

DAFTAR PUSTAKA

Acunetix. (2019). Web application vulnerability scanner documentation. Acunetix Ltd.

Ahmed, A., Mahmood, A. N., & Hu, J. (2011). A survey of network and web application security. Journal of Network and Computer Applications, 34(2), 345–356.

Chen, S., Li, J., & Wang, Y. (2013). Security vulnerabilities and protection mechanisms in web applications. International Journal of Computer Applications, 67(5), 1–7.

Fielding, R. T. (2014). Hypertext Transfer Protocol (HTTP/1.1): Semantics and content. Internet Engineering Task Force (IETF).

Makalalang, J. (2017). Analisis keamanan aplikasi web terhadap serangan Cross-Site Request Forgery. Jurnal Teknologi Informasi, 12(1), 22–30.

Nofia, D. (2017). Analisis kerentanan DOM-based Cross-Site Scripting pada aplikasi web. Jurnal Sistem Informasi, 9(2), 101–109.

OWASP Foundation. (2017). OWASP Top 10 web application security risks. Open Web Application Security Project.

OWASP Foundation. (2021). Cross-Site Request Forgery (CSRF) prevention cheat sheet. Open Web Application Security Project.

Patil, S., Patil, V., & Patil, R. (2016). Web application security vulnerabilities and countermeasures. International Journal of Advanced Research in Computer Science, 7(3), 123–128.

Petefish, J., Zhao, Y., & Stolfo, S. J. (2011). Protecting web applications from Cross-Site Request Forgery attacks. Proceedings of the International Conference on Information Security, 1