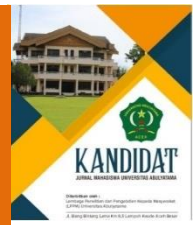
Available online at : http://jurnal.abulyatama.ac.id/index.php/kandidat
ISSN 2715-3126 (Online)
Universitas Abulyatama
Kandidat : Jurnal Riset dan Inovasi Pendidikan



Analisa Keamanan Website Terhadap Serangan *Cross-Site Request Forgery* (CSRF)

Rusdiana[1], Banta Cut[2], Sanusi[2]
[1]Mahasiswa Program Studi Sistem Informasi, Fakultas Teknik, Universitas Abulyatama, Aceh Besar, 23372, Indonesia.
[2] Dosen Program Sistem Informasi, Fakultas Teknik, Universitas Abulyatama, Aceh Besar, 23372, Indonesia.
*Email korespondensi: dianarusdi123@gmail.com

Diterima 29 Agustus 2019 ; Disetujui 7 Oktober 2019; Dipublikasi 19 Oktober 2019

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.*

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

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

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

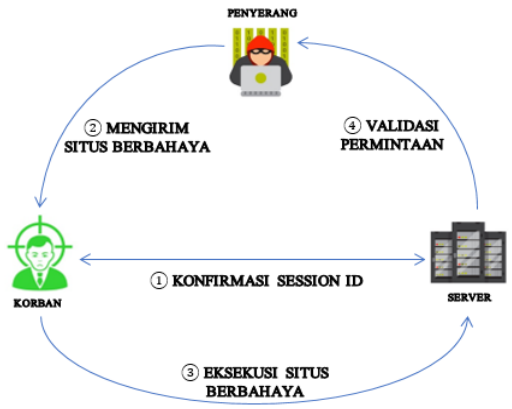
Keamanan

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).



Gambar 1. Gambaran umum CSRF.

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.

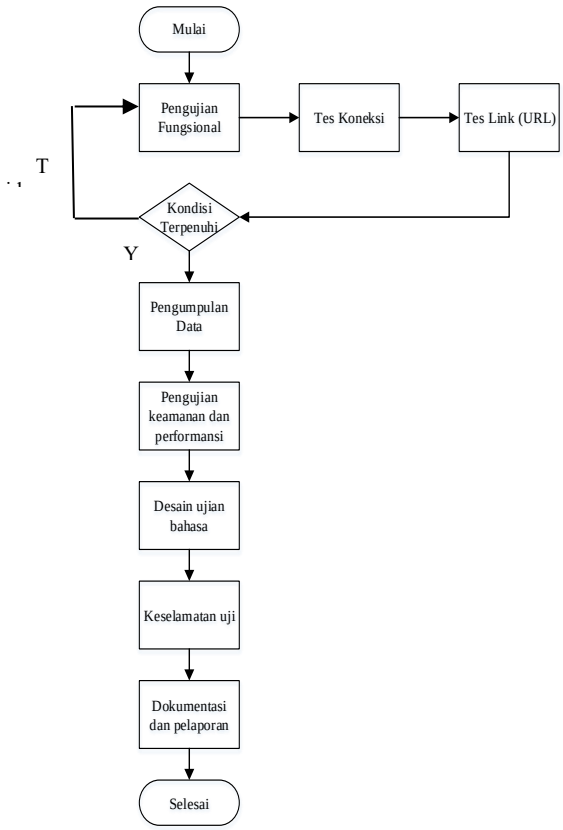
HyperText Transfer Protocol (HTTP)

Menurut Fielding (2014) *HyperText Transfer Protocol* atau HTTP adalah sebuah protokol yang memungkinkan *web browser* untuk berkomunikasi dengan *web server* dalam pertukaran in*form*asi. 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

Penyerangan dari *Cross-Site Request Forgery* (CSRF) yang didapat dari hasil *scanner* dengan menggunakan *tool* Acunetix. Pada serangan *cross site request forgery*, penyerang mengganggu integritas sesi pengguna dengan *website* melalui memasukkan *network request* lewat *browser* pengguna. Peraturan keamanan *browser* memperbolehkan *website* untuk mengirimkan HTTP *requests* kepada setiap alamat jaringan. Peraturan ini memperbolehkan penyerang untuk mengontrol content yang ditampilkan oleh *browser* untuk menggunakan *resource* yang tidak dinyatakan dibawah kekuasaannya (penyerang) (Firdaus, 2017).

Flowchart Data Analisa



Gambar 2 Flowchart Data Analisa

Metode Pengumpulan Data

Metode penelitian yang digunakan sebagai berikut :

1. Metode pengumpulan data sekunder. Mengumpulkan data-data yang berasal dari buku-buku *literature*, dokumen, dan sumber kepustakaan.

Tabel 1. Website Pemerintahan Daerah Aceh Timur

No	Nama Instansi
1.	Website Pemerintahan Aceh Timur
2.	Jaringan Dokumentasi dan Informasi Hukum Aceh Timur

2. Mencari sumber lain yang berhubungan dengan objek penelitian.

Teknik Pengambilan Data

Purposive sampling digunakan untuk teknik pengumpulan data untuk mempermudah dalam proses pencarian data sampel. *Purposive sampling* adalah teknik pengambilan sampel yang bukan berdasarkan atas random tetapi didasarkan atas adanya tujuan tertentu. Setiap sampel yang diambil dari populasi dipilih dengan sengaja berdasarkan tujuan dan pertimbangan tertentu.

1. Lokasi Analisis

   Analisis ini dilakukan pada website Pemerintahan Daerah Aceh Timur yang websitenya bisa di akses secara umum. Penulis boleh berada dimana saja untuk melakukan analisis asalkan harus terkoneksi dengan jaringan *internet*.

2. Populasi Analisis

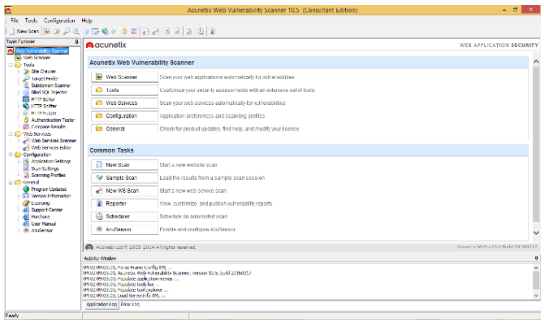
Tabel 2. Website Pemerintahan yang dianalisis

No	Nama Instansi
1.	LPSE Aceh Timur
2.	Dinas Kebudayaan, Pariwisata dan Olahraga Aceh Timur
3.	Website Pemerintahan Aceh Timur
4.	BAPPEDA Aceh Timur
5.	BPBD Aceh Timur
6.	Jaringan Dokumentasi dan Informasi Hukum Aceh Timur
7.	Aplikasi Dokumen Aceh Timur
8.	Webmail Aceh Timur

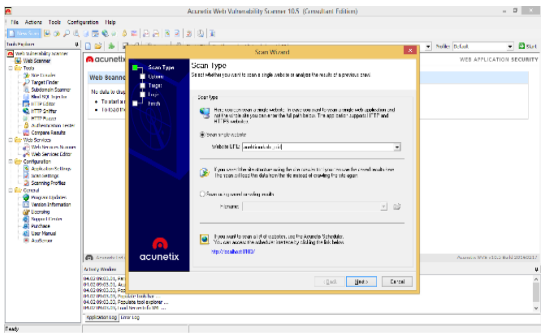
3. Sampel Analisis

Rancangan Analisis Pengujian

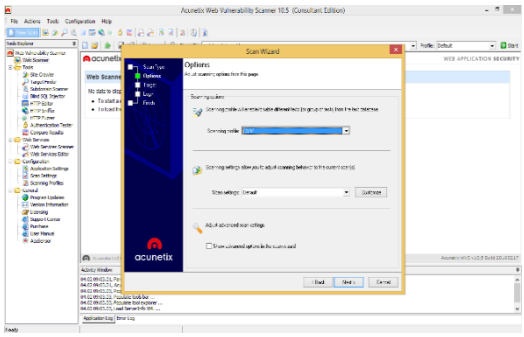
Pada tahap ini mulai dilakukan pengujian terhadap keamanan *website* Pemerintah Kabupaten Aceh Timur. Berikut ini langkah-langkah melakukan analisa :



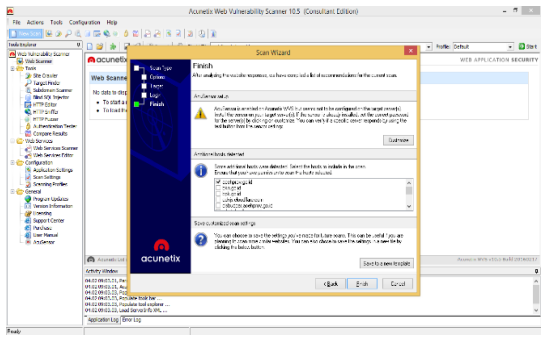
Gambar 3. Tampilan awal pada aplikasi Acunetix



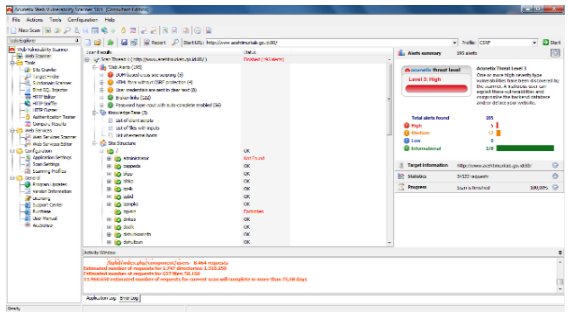
Gambar 4. tampilan analisis dengan menambah target website yang di-scan.



Gambar 5. Tampilan mengisi *scanning profile*



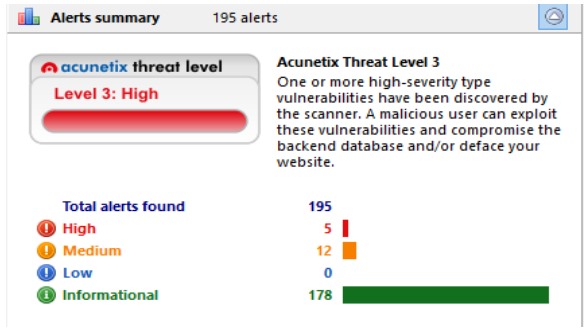
Gambar 6. Tampilan informasi analisa melakukan pengaturan terhadap host yang di-scan.



Gambar 7. menampilkan hasil dari analisis CSRF.

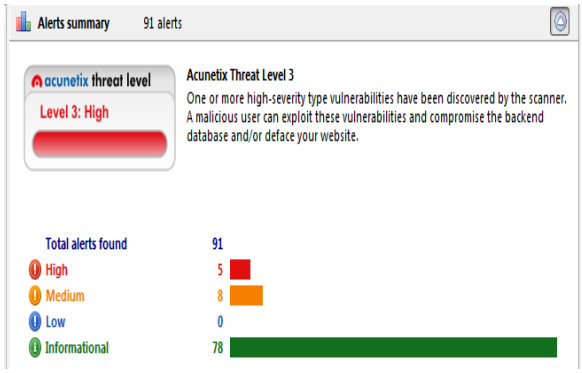
HASIL DAN PEMBAHASAN

Hasil Analisis Celah Keamanan Pada *Website* Pemerintahan Aceh Timur



Gambar 8. Hasil temuan celah *Website* acehtimurkab.

Berdasarkan hasil scanning pada bab sebelumnya website yang memiliki kerentanan alert high yang didapati pada website acehtimurkab dan jdih.acehtimurkab dengan jumlah *instance* sebesar 5 (lima)



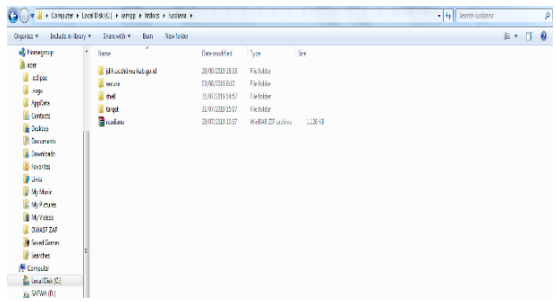
Gambar 9. Hasil temuan celah *Website* jdih.acehtimurkab.

Rekomendasi dan Solusi Prototyping Perbaikan Celah

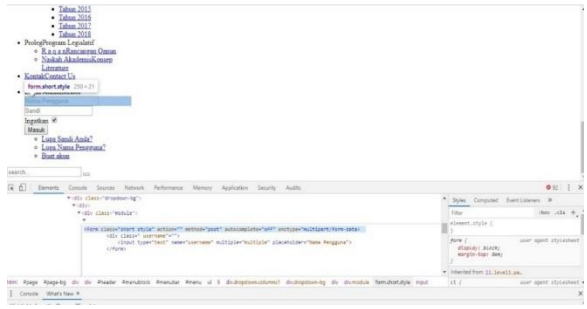
Rekomendasi perbaikan akan dibagi menjadi 2 bagian berdasarkan pada dimana celah *website* yang telah diuji sebelumnya dan membuat sebuah *libraries tools* agar dapat menangani masalah penyerangan CSRF. Penulis membuat sebuah aplikasi testing sebagai aplikasi guna untuk mencegah serangan terjadi pada *website*. Aplikasi dimaksud dapat menangani keseluruhan serangan CSRF baik dari sisi *browser* maupun terhadap tipe pengiriman _GET dan _POST pada sebuah form.

Implementasi Serangan dengan Model CSRF

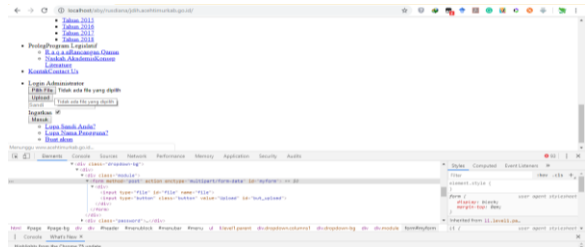
Untuk pengujian implementasi serangan dengan model CSRF bervariasi dan disesuaikan dengan target dan model dari *framework website* sendiri. Pada ujicoba ini, penulis menggunakan Teknik *deface* dengan memanfaatkan penggunaan *shell* yang telah disediakan. Penulis menyiapkan beberapa target, *shell*, *index defacer*, dan halaman *form* yang telah dimasukkan filter terhadap kesalahan dan file yang bisa diakses.



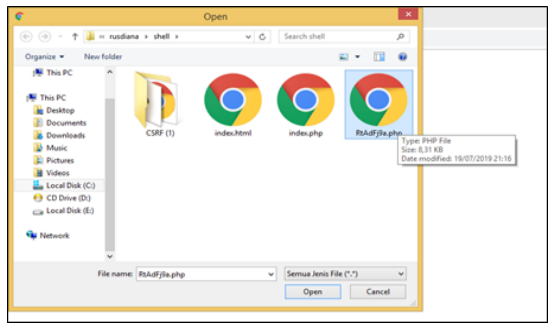
Gambar 10. Bahan Persiapan



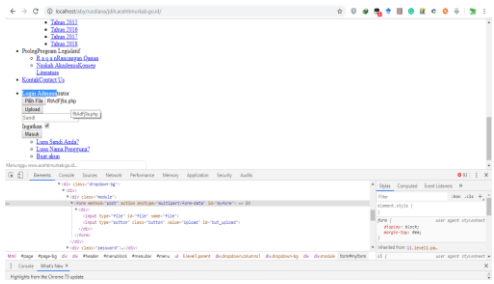
Gambar 11. *DOM-based* Target Website



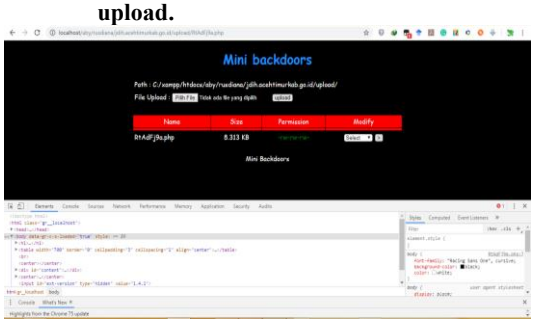
Gambar 12. Hasil perubahan *DOM-based* Target Website



Gambar 13. Pemilihan Shell sebagai backdoor



Gambar 14. *Shell* sebagai *backdoor* telah berhasil di upload.



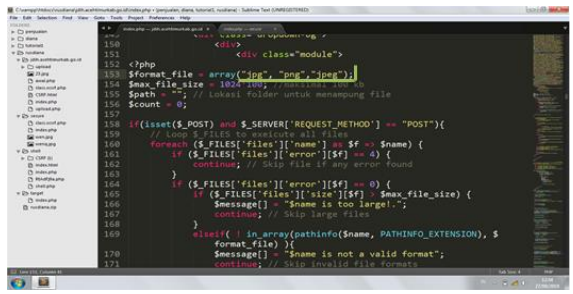
Gambar 15. Shell backdoor diakses

Gambar 16. Hasil *backdoor* Serangan CSRF

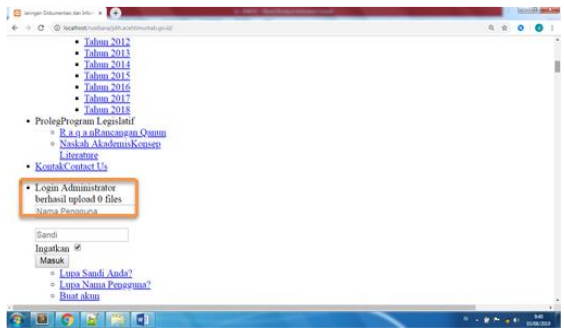
Rekomendasi Perbaikan Celah *Website* Pemerintahan Aceh Timur

Berikut penulis rumuskan rekomendasi perbaikan terhadap *website* Pemetintahan Aceh Timur berdasarkan celah yang telah ditemukan pada tahap Pencarian Celah.

Serangan DOM XSS sulit dideteksi oleh alat deteksi dan pencegahan serangan dari sisi server. Payload berbahaya biasanya tidak sampai menyerang server dan karenanya tidak dapat disanitasi pada sisi server. DOM-*based* merupakan kerangka atau elemen dari sebuah *webiste* dimana penyerangan CSRF bisa menggunakan kelemahan dari DOM-*based* tersebut. Untuk mencegah DOM XSS, dapat melakukan perubahan pada skrip serta harus memfilter karakter dari input pengguna.



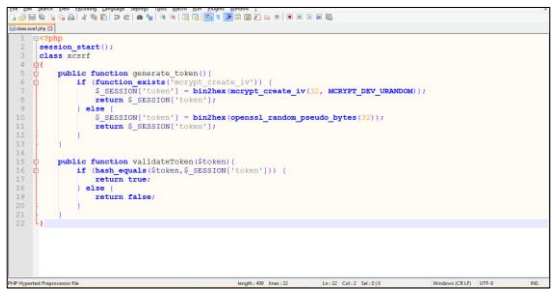
Gambar 17. Hasil coding yang sudah diperbaiki



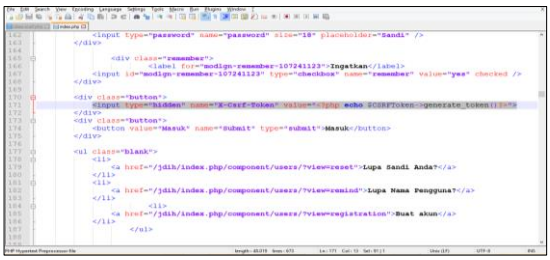
Gambar 18. Hasil perbaikan website

Penggunaan Token Anti CSRF

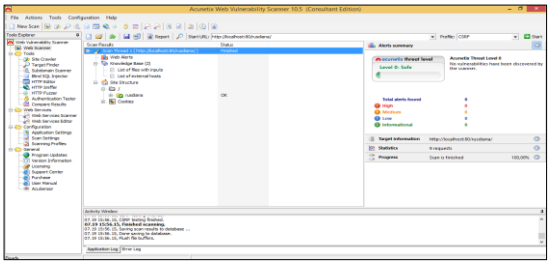
Token *anti* CSRF merupakan solusi terhadap berbagai serangan CSRF. Dalam hal ini *libraries anti* CSRF dipanggil dalam suatu halaman *website* dan selanjutnya *libraries* akan bekerja menfilter kode-kode serangan CSRF.



Gambar 19. Pengkodean Token Anti CSRF



Gambar 20. Pengkodean Token Anti CSRF pada *File* JDIH



Gambar 21. Hasil Pengujian setelah dimasukkan Token Anti CSRF

Gambar diatas adalah hasil pengujian setelah dimasukkan token anti CSRF, dimana setelah dilakukan proses scenning hasilnya tidak ditemukan lagi serangan CSRF karena telah di masukkan token anti CSRF.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil Analisa terhadap *website* Pemerintahan Aceh Timur maka dapat dibuat kesimpulan, yaitu:

1. Hasil analisa terhadap keamanan *website* Pemerintahan Aceh Timur, maka dihasilkan bahwa persentase kerentanan dari kedelapan *website* terbesar dengan *Rank Vulnerability* dengan tipe high pada *website* Aceh Timur sebanyak 5 (lima) yaitu pada kerentanan *DOM-based cross site scripting*.
2. Analisa serangan terhadap *website* Pemerintahan Aceh Timur dengan tipe serangan *DOM-based cross site scripting* didapati bahwa kerentanan serangan pada Alert High.
3. Berdasarkan Analisa keamanan dan analisis serangan terhadap *website* pemerintahan Aceh Timur maka dibuatkan sebuah *token* anti CSRF yang diharapkan mampu mengatasi berbagai bentuk serangan dari tekhnik penyerangan CSRF dan Untuk mencegah DOM XSS, dapat melakukan perubahan pada skrip serta harus memfilter karakter dari input pengguna.

Saran

Beberapa yang harus dihindari dari hal yang tidak diinginkan terhadap *web server* pada saat melakukan *penetration testing*, diantaranya:

1. Sebaiknya *library anti CSRF* yang telah penulis gunakan pada *prototipe test* serangan CSRF sebagai tambahan pendukung keamanan website.
2. Melakukan perbaikan terhadap analisa pada *website* Pemerintahan Aceh Timur menggunakan tool acunetix dan melakukan pengujian setiap periodik dan Pengembangan keamanan *website* Pemerintahan Aceh Timur.

DAFTAR PUSTAKA

Acunetix. (2019). *DOM XSS: An Explanation of DOM-based Cross-site Scripting*. https://www.acunetix.com/blog/articles/dom-xss-explained/. 12 April 2019 (16:56).

Ahmed, A.S. and Laud, P. (2011). May. Formal Security analysis of OpenID with GBA protocol. *In International Conference on Security and Privacy in Mobile Information and Communication Systems* (pp. 113-124). Springer, Berlin, Heidelberg.

Chen, C., Mitchell, C.J. and Tang, S. (2013). Ubiquitous one-time password service using the Generic Authentication Architecture. *Mobile Networks and Applications, 18*(5). pp.738-747.

Firdaus, T.R. (2017). Keamanan Aplikasi Web Melalui Penerapan Cross Site Request Forgery (CSRF). *ITEj (Information Technology Engineering Journals).* 1(2).

Fielding, R. and Reschke, J., 2014. Hypertext transfer protocol (HTTP/1.1): Message syntax and routing (No. RFC 7230).

Ian, M. (2019). What is Cross-site Request Forgery?. https://www.acunetix.com/blog/articles/cross-site-request-forgery/. 14 Februari 2019 (22:22).

Makalalag, R. and Najoan, X.B. (2017). Kajian Implementasi Cross Site Request Forgery (CSRF) Pada Celah Keamanan Website. *Jurnal Teknik Informatika Universitas Sam Ratulangi, 12*(1).

Nofia Delta, E. (2017). Performance Test Dan Stress Website Menggunakan Open Source Tools. *Jurnal Manajemen Informatika, 6*(1).

Petefish, P., Sheridan, E. and Wichers, D. (2011). Cross-site request forgery (csrf) prevention cheat sheet.

Patil, D.K. and Patil, K. (2016). Automated Clientside Sanitizer for Code Injection Attacks. *International Journal of Information Technology and Computer Science, 8*(4), pp.86-95.