JINTEKS (Jurnal Informatika Teknologi dan Sains) ISSN 2686-3359 (Online)
Vol. 4 No. 4, November 2022, hlm. 325 – 329

# ANALISIS KEAMANAN WEBSITE PRODI SISTEM INFORMASI UINSU MENGGUNAKAN METODE APPLICATION SCANNING

**Pria Mitra Purba[1], Azrah Cipta Amandha[2], Riyan Hidayah Purnama[3] , Ali Ikhwan[4]**
[1,2]Prodi Sistem Informasi, Sains Dan Teknologi, UIN Sumatera Utara Medan
*email*: priamitrapurba2@gmail.com[1*]

**Abstrak:** Perkembangan teknologi saat ini keamanan dalam setiap website lembaga atau instansi pastinya akan memberikan keamanan terbaik terutama dari segi interface hingga keamanan data. Website merupakan sebuah halaman informasi yang tersedia melalui jalur internet sehingga dapat diakses diseluruh dunia selama terkoneksi dengan jaringan internet. Website sendiri merupakan komponen atau kumpulan dari komponen yang terdiri dari teks,gambar,suara, dan animasi sehingga menarik untuk dikunjungi. Website prodi sistem informasi merupakan salah satu website yang mampu memberikan informasi akademik dan kebutuhan mahasiswa prodi sistem informasi uinsu. Oleh sebab itu, tentunya website ini memiliki keamanan tersendiri untuk mengolah data dan informasi yang ada.Web security atau keamanan web mengacu pada tindakan perlindungan protokol yang diadopsi oleh pengelola web untuk melindungi dan mengamakan data di situs web dan server agar tidak terpapar oleh penjahat dunia maya atau untuk mencegah eksploitasi situs web dengan cara apapun.

**Kata Kunci :** Website, Keamanan Website, Scan Keamanan

***Abstract:*** *The current technological developments on security in every agency or agency website will certainly provide the best security, especially in terms of interfaces and data security. The website is an information page that is available through the internet so that it can be accessed throughout the world as long as it is connected to the internet network. The website itself is a component or collection of components consisting of text, images, sound, and animation so that it is interesting to visit. The Information Systems Study Program website is one of the websites that is able to provide academic information and the needs of UINSU Information Systems Study Program students. Therefore, of course, this website has its own security for processing existing data and information. Web security refers to protocol protection measures adopted by web managers to protect and secure data on websites and servers so that they are not exposed to cybercriminals or to prevent exploitation of the website in any way.*

***Keywords*** **:** *Website, Website Security, Security Scan*

## PENDAHULUAN

Bersamaan terus menjadi meningkat nya teknologi system informasi digolongan publik, meningkat pula system yang dapat mempermudah warga buat mengakses serta mencari sesuatu data dalam wujud suatu situs. Teknologi informadi sebagai salah satu kedudukan berarti dalam sesuatu kegiatan industri, wadah guna menyokong kemampuan serta kegiatan.

Tetapi dalam pengurusan IT keamanan suatu web dalah perihal yang amat berarti. Efek keamanan jadi salah satu perihal yang terletak pada urutann terakhir dalam perihal– perihal yang dikira berarti. Serta apabilla mengganggu penampilan kerapkali di kurangi. perihal itu berbanding terbalik dengan terus menjadi banyak nya sela yang keamanan dari web itu.

Website sistem informasi merupakan salah satu website Prodi UIN Sumatera Utara dan website ini sendiri memberikan sajian informasi berupa agenda, opini mahasiswa serta profil prodi. Website ini sendiri didirikan sekitar 2 tahun yang lalu pada tahun 2021. Website prodi sistem informasi ini sendiri dapat diakses oleh semua orang. Dalam pengelolaannya website ini dikelola oleh 1 admin dan 1 operator yang mengelola segala informasi baik keamanan dalam website prodi.

Dalam aksesnya website ini tentu memiliki kelebihan dan kelemahannya. Kelebihannya yakni dapat diakses dengan cepat, aman, *traffic* tinggi, tampilan yang responsive. Sedangkan kelemahannya adalah informasinya kurang banyak, menu yang kurang banyak, dan beberapa data yang belum *update*, fitur kerjasama yang masih kosong, dan menu untuk membagikan langsung/*backline* kurang bagus.

Oleh karena itu penulis menawarkan solusi yakni dengan menganalisa website tersebut menggunakan application scannning . Dengan adanya analisa keamanan *website* Prodi SI UINSU, diharapkan mampu menjadi solusi bagi Prodi SI UINSU agar dapat meningkatkan keamanan *Website.*

## TINJAUAN PUSTAKA

Analisis adalah sebuah kegiatan untukmencari pola ataupun metode berasumsi yang berhubungan dengan pengetesan dengan cara analitis kepada suatu buat memastikan bagian, jalinan antar bagian, dan ikatan dengan totalitas. Analisa merupakan sesuatu upaya buat menguraikan sesuatu permasalahan jadi bagian- bagian( decomposition) alhasil lapisan wujud sesuatuyang dijabarkan itu nampak dengan nyata alhasil dapatdimengerti permasalahannya.

Analisis data adalah cara mencari serta menata dengan cara analitis informasi yang didapat dari hasil tanya jawab, memo alun- alun, serta pemilihan, dengan metode mengorganisasi informasi kedalam jenis, menjabarkan kedalam unit- unit melaksanakan sintesa, memilah mana yang berarti serta yang hendak dipelajari, serta membuat

 ISSN 2686-3359 (Online)

kesimpulan alhasil mudah dimengerti oleh diri sendiri ataupun orang lain.

Keamanan informasi dalam suatu web menjadi amat berarti. Keamanan data suatu web ialah salah satu prioritas yang amat penting untuk seorang website development. Bila seorang melalaikan keamanan itu hingga seseorang hacker bisa mengutip informasi berarti serta apalagi mangacak- acak bentuk website tersebut.

Vulnerability Asesment ialah kerangka kegiatan abstrak global yang seleksi, tercantum arti kerentanan yang memastikan resiko buat pengukuran. Perihal ini pula terkait pada tujuan konsumen hasil evaluasi, yang bisa berkisar dari hasrat buat menginformasikan kebijaksanaan global ataupun buat merujuk aksi ditingkat publik.

Vulnerability scanning merupakan aktivitas cara mendapatkan data vulnerability network dengan menggunakan bermacam tools jaringan scanning serta vulnerability scanner, semacam port yang terbuka, bugs aplikasi serta mengenali serangan-serangan yang hendak terjalin kepada kerentaan web yang terdapat, yang hendak berakibat lumayan kurang baik bila terjadi.

## METODE

Pada penelitian ini penulis menggunakan metode wawancara dan metode application scanning,. Dalam wawancara tentunya penulis telah mewawancarai yakni admin sekaligus menjabat sekretaris Prodi Sistem Informasi UIN Sumatera Utara Medan yaitu bapak Suendri, M.Kom.

Metode kedua yang digunakan adalah metode kuantitatif dimana penulis mencari berbagai macam sumber teori melalui buku, jurnal dan lain sebagainya.

Dan metode yang terakhir adalah metode kualitatif yakni menggunakan metode analisa menggunakan application web scanning. Pada pengujian ini periset hendak memakai tool berbentuk fitur lunak serta cara- cara khusus yang dipakai buat mencoba keamanan suatu web. Guna melaksanakan analisa keamanan web, aplikasi yang dipakai merupakan Acunetix web vulnerability scanner.

Pada langkah ini periset menekuni rancangan, metode, ataupun data dari bermacam pangkal semacam internet, novel, harian, ataupun postingan objektif yang lain yang berhubungan dengan jaringan komputer.

### *Vulnerability Scanning*

*1) Who. is*

*Who.is* bertujuan bermaksud buat mendapakan data hal suatu daerah, tujuan, Nomor. telepon, tujuan emil, bila daerah didaftarkan serta bila daerah itu bakal kadaluarsa.

*2) Nslookup*

*Nslookup* Yang bermaksud mengenali IP dari suatu domain.

*3) Scanning port*

*Scaning Port* Bermaksud untuk menyelidiki server ataupun host port terbuka.

### ***Result* Analisis**

Pada metode ini bertujuan untuk menganalisa rentannya keamanan dari web Sistem Informasi UINSU adapun tool yang digunakan yakni *tool Open Web Aplication Security Project* (OWASP), yang dapat mengindentifikasi kerentanan keamanan sebuah website.

### ***Remediation***

Langkah ini bermaksud guna megurangi efek kerentanan pada suatu web. Langkah ini ialah kesimpulan akhir, berbentuk bagan dari jumlah angka dari suatu riset yang sudah dicoba pengarang melaksanakan riset pada web Prodi Sistem Informasi UINSU.

Menurut (Digdo, 2017) beberapa orang senantiasa menyangkutkan antara tata cara Penetration Testing dengan tata cara Vulnerability Asesment. Ada pula perbandingan antara Tata cara Penetration Testing dengan Tata cara Vulnerability Asesment, ditunjukkan pada bagan berikut:

**Tabel 1. Perbedaan Metode *Penetration Testing* dan *Vunerability Asessment***

| NO | *Metode Penetration Testing* | *Metode Vulnerability Asesment* |
|---|---|---|
| 1 | Identifikasi Beberapa Celah Keamanan | Identifikasi semua Celah Keamanan |
| 2 | Pendekatan risiko IT | Pendekatan Bisnis dan Resiko IT |
| 3 | Pembuktian Secara Teknis | Pendekatan secara Teori |

Tabel 1. Perbedaan Metode PenetrationTesting dan Vulnerability Asesment

Pada gambar diatas terlihat jelas beberapa perbedaan antara PenetrationTesting dan Vulnerability Asesment. Oleh karena itu metode scanning yang penulis gunakan pada penelitian ini adalah metode Vulnerability Asesment.

 ISSN 2686-3359 (Online)

## HASIL DAN PEMBAHASAN

### Hasil Wawancara :

Berdasarkan hasil wawancara yang dilakukan bersama sekretaris Prodi Sistem Informasi UIN Sumatera Utara Medan yakni bapak Suendri, M.Kom didapati hasil sebagai berikut :

Website ini didirikan sekitar 2 tahun yang lalau, pada website si.uinsu.ac.id menggunakan software dan framework PHP- Laravel, Database Mongo DB, serta Apache. Keamanan yang digunakan ialah Anti CSRF yakni keamanan bawaan framework pada website tersebut.

Dalam pengelolaannya website ini memiliki beberapa fungsi yakni dapat melihat agenda, opini mahasiswa, informasi kemahasiswaan hingga profil prodi Sistem Informasi. Akses website ini juga dapat diakses oleh semua orang. Tata kelola pada website ini dikelola oleh 1 admin dan 1 operator yang mengelola.

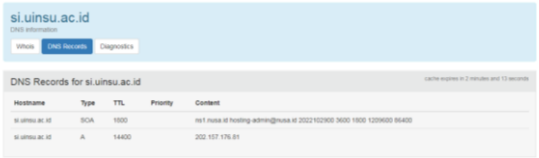
Website ini sendiri memiliki kelebihan yakni dapat diakses sangat cepat, aman, traffic nya juga tinggi, dan tampilan yang elegan serta responsive. Pada kekurangan yang terletak di website si.uinsu.ac.id ini sendiri informasinya kurang banyak atau belum banyak update dari informasinya sendiri, kemudian menu yang kurang banyak, dan beberapa data yang belum update, serta fitur kerjasama yang masih kosong dan menu untuk membagikan langsung atau backline kurang baik. Yang terakhir website ini sendiri sudah tersedia secara mobile/aplikasi dan tidak pernah mengalami ngelag.

### Analisa Metode Scanning :

Pengecekan Halaman *Website*

a. Cek Domain Melalui Who.is

Berdasarkan hasil analisa yang penulis ambil melalui website Who.is dengan domain sebagai berikut https://si.uinsu.ac.id/ maka didapati hasil sebagai berikut :

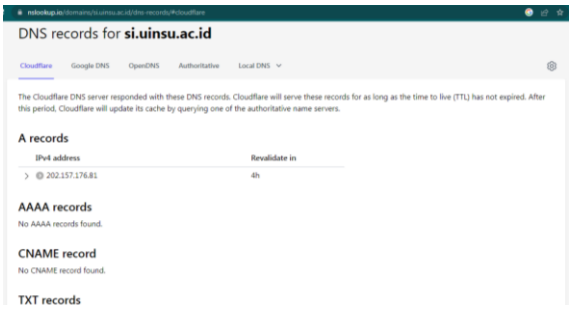



**Gambar 1.** *Hasil cek website https://si.uinsu.ac.id/*

Hasil gambar diatas menunjukkan bahwa pengambilan informasi domain dari website Prodi Sistem Informasi menggunakan who.is pada target yang sudah ditetapkan maka didapati informasi terkait domain, kemudian content serta type dari website itu sendiri.

b. Cek NsLookup

Pada hasil pengecekan ini didapatkan informasi IP terkait dari domain website Prodi Sistem Informasi. Berikut IP yang didapatkan :



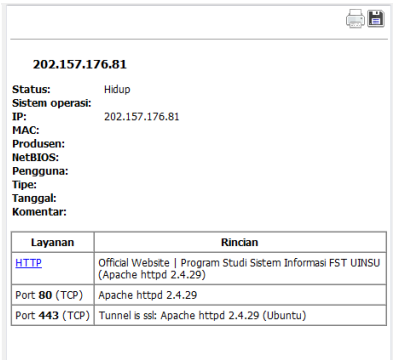

**Gambar 2.** *Hasil cek NsLookup Website SI*

Adapun hasil scanning port diatas, dapat dilihat bahwa alamat website dan Ip address pada website prodi Sistem Informasi UIN Sumatera Utara Medan. Pada hasil scanning di atas yang dilakukan melalui tools NsLookup pada website Prodi Sistem Informasi UIN Sumatera Utara maka menampilkan informasi IP sebagai berikut : “202.157.176.81”.

c. Scanning Port

Scanning port digunakan untuk melihat server atau port yang terbuka, dalam hal ini Tool yang digunakan yakni Tool advanced port scanner dan Network Mapper (NMAP). Hasil yang didapati dari scanning website tersebut adalah :

***Hasil scan Advanced Port Scanner :***




**Gambar 3.** *Hasil Scanning Advanced Port Scanner*

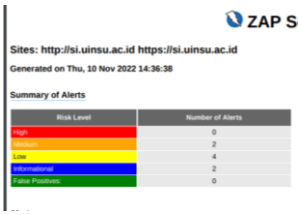
Hasil scan diatas menunjukkan bahwa beberapa port yang terbuka yakni untuk layanannya sendiri menggunakan HTTP dengan rincian Official Website | Program Studi Sistem Informasi FST UINSU menggunakan Apache httpd 2.4.29. Dan untuk port yang terbuka yakni ***Port 80*** dan ***Port 443.***

 ISSN 2686-3359 (Online)

**Hasil Penilaian Kerentanan Web**

Dalam hasil pengujian menggunakan Open Web Application Security Project(OWASP) didapati hasil sebagai berikut :

*Grafik Summary Of Alert :*




*Alert :*

Alerts

| Name | Risk Level | Number of Instances |
|---|---|---|
| Absence of Anti-CSRF Tokens | Medium | 83 |
| Missing Anti-clickjacking Header | Medium | 83 |
| Cookie No HttpOnly Flag | Low | 84 |
| Cookie Without Secure Flag | Low | 102 |
| Secure Pages Include Mixed Content | Low | 2 |
| X-Content-Type-Options Header Missing | Low | 91 |
| Information Disclosure - Sensitive Information in URL | Informational | 34 |
| Re-examine Cache-control Directives | Informational | 1 |

Hasil grafik diatas dijelaskan dalam tabel pengujian sebagai berikut yang telah dianalisa :

**Tabel 2.** Pengujian Analisa Website Prodi SI

| No | Alert | Risk | | |
|---|---|---|---|---|
| | | Medium | Low | Informational |
| 1 | Absence of Anti-CSRF Tokens | Y | | |
| 2 | Missing Anti-clickjacking Header | Y | | |
| 3 | Cookie No HttpOnly Flag | | Y | |
| 4 | X-Content-Type-Options Header Missing | | Y | |
| 5 | Cookie Without Secure Flag | | Y | |
| 6 | Secure Pages Include Mixed Content | | Y | |

Berdasarkan Tabel diatas diperoleh keterangan sebagai berikut :

1) **Absence of Anti-CSRF Tokens** => Tidak ada token Anti CSRF yang ditemukan dalam formulir pengiriman HTML.
2) **Missing Anti-clickjacking Heade** => Respons tidak menyertakan Kebijakan Keamanan Konten dengan arahan 'frame-ancestors' atau X-Frame-Options untuk melindungi dari serangan 'ClickJacking'.
3) **Cookie No HttpOnly Flag** => Cookie sudah disetel tanpa kode HttpOnly, yang berarti kalau cookie bisa diakses oleh JavaScript. Bila naskah beresiko bisa dijalani di laman ini, hingga cookie hendak bisa diakses serta bisa dikirim ke web lain. Bila ini merupakan cookie tahap, hingga pemalsuan tahap bisa jadi terjalin.
4) **X-Content-Type-Options Header Missing** => Header Anti-MIME-Sniffing X-Content-Type-Options tidak disetel ke 'nosniff'. Ini memungkinkan versi Internet Explorer dan Chrome yang lebih lama untuk melakukan sniffing MIME pada badan respons, yang berpotensi menyebabkan badan respons ditafsirkan dan ditampilkan sebagai tipe konten selain tipe konten yang dideklarasikan. Firefox versi saat ini (awal 2014) dan lawas akan menggunakan tipe konten yang dideklarasikan (jika ada yang disetel), daripada melakukan sniffing MIME.
5) **Cookie Without Secure Flag** => Cookie telah disetel tanpa tanda aman, yang berarti bahwa cookie dapat diakses melalui koneksi yang tidak terenkripsi.
6) **Secure Pages Include Mixed Content** => Halaman tersebut mencakup konten campuran, yaitu konten yang diakses melalui HTTP, bukan HTTPS.

**Hasil dan Rekomendasi aplikasi Owasp :**

**Tabel 3.** Rekomendasi Aplikasi Pengujian

| No | Nama Sistem | Jumlah |
|---|---|---|
| 1 | Absence of Anti-CSRF Tokens | 83 |
| 2 | Missing Anti-clickjacking Header | 83 |
| 3 | Cookie No HttpOnly Flag | 84 |
| 4 | X-Content-Type-Options Header Missing | 91 |
| 5 | Cookie Without Secure Flag | 102 |
| 6 | Secure Pages Include Mixed Content | 2 |

 ISSN 2686-3359 (Online)

Berdasarkan tabel diatas maka didapati lah solusi sebagai berikut :

a. Gunakan perpustakaan atau kerangka kegiatan yang ditilik yang tidak membolehkan kelemahan ini terjalin ataupun sediakan arsitektur yang membuat kelemahan ini lebih mudah buat diatasi. Misalnya, maanfaatkan paket anti CSRF semacam OWASP CSRFGuard. Pastikan aplikasi Anda bebas dari masalah skrip lintas situs, karena sebagian besar pertahanan CSRF dapat dilewati menggunakan skrip yang dikendalikan penyerang. Perhatikan bahwa ini dapat dilewati menggunakan XSS. Periksa header HTTP Referer untuk melihat apakah permintaan berasal dari halaman yang diharapkan. Ini dapat merusak fungsionalitas yang sah, karena pengguna atau proxy mungkin telah menonaktifkan pengiriman Perujuk karena alasan privasi.

b. Browser Web modern mendukung header HTTP Content-Security-Policy dan X-Frame-Options. Pastikan salah satunya disetel di semua halaman web yang ditampilkan oleh web atau aplikasi Kamu. Bila Kamu menginginkan laman dibingkai cuma oleh laman di server Kamu( mis. itu bagian dari FRAMESET) hingga Kamu hendak mau memakai SAMAORIGIN, bila tidak, bila Kamu tidak sempat menginginkan laman dibingkai, Anda wajib memakai DENY. Atau pertimbangkan untuk menerapkan arahan "frame-ancestor" Kebijakan Keamanan Konten.

c. Pastikan bahwa flag HttpOnly disetel untuk semua cookie.

d. Pastikan aplikasi/server web menyetel header Content- Type dengan pas, serta menyetel header X- Content- Type-Options ke nosniff buat seluruh laman website. Bila membolehkan, yakinkan kalau konsumen akhir memakai browser website yang cocok standar serta modern yang tidak melaksanakan sniffing MIME serupa sekali, ataupun yang bisa ditunjukan oleh aplikasi website atau server website buat tidak melaksanakan sniffing MIME.

e. Setiap kali cookie berisi informasi sensitif atau merupakan token sesi, maka cookie harus selalu diteruskan menggunakan saluran terenkripsi. Pastikan bahwa tanda aman diatur untuk cookie yang berisi informasi sensitif tersebut.

f. Halaman yang tersedia melalui SSL/TLS harus sepenuhnya terdiri dari konten yang dikirimkan melalui SSL/TLS.Halaman tidak boleh berisi konten apa pun yang dikirimkan melalui HTTP yang tidak terenkripsi. Ini termasuk konten dari situs pihak ketiga.

## KESIMPULAN DAN SARAN

Dari penjelasan diatas mengenai analisa yang telah dilakukan baik dengan wawancara dan berdasarkan hasil analisis website dengan menggunakan aplikasi web scanning maka didapati permasalahan yakni tidak adanya token Anti CSRF yang ditemukan dalam formulir pengiriman HTML, lalu Respons tidak menyertakan Kebijakan Keamanan Konten dengan arahan 'frame-ancestors' hingga permasalahan lainnya yang timbul ini dapat berdampak pada keamanan website Prodi Sistem Informasi

Dalam hal ini saran yang tepat untuk memperbaiki keamanan website prodi SI UIN Sumatera Utara adalah dengan meningkatkan software keamanan serta cookies yang tidak mudah dibobol atau dimasukin oleh penyusup manapun. Ini dapat meningkatkan kualitas serta performa website menjadi lebih baik.

## DAFTAR PUSTAKA

[1] Yudi Mulyanto., Dkk., 2021, *Analisis Keamanan Website Menggunakan Metode Vulnerability*, Jurnal Informatika Teknologi dan Sains, Jinteks, Sumbawa.
[2] Muhammad Farkhurozzi., 2021, *Analisa Keamanan Website Menggunakan Metode Footprinting dan Vulnerability Scanning pada Website Kampus*, Santika, Vol.2, Seminar Nasional Informatika Bela Negara, Depok.
[3] Imam Rialdi., Dkk., 2019, *Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assesment*, Jurnal Ilkom, Vol. 7 No.4, KEMENRISTEKDIKTI, No.30, Yogyakarta.
[4] Guntoro, G., Costaner, L., & Musfawati, M. (2020). Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning). *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *5*(1), 45. https://doi.org/10.29100/jipi.v5i1.1565.
[5] Ika yusnita sari, Muttaqin Muttaqin, J. J. (2020). keamanan data dan informasi. Yayasan Kita Menulis.