Security Assessment dengan Indonese Framework

Apa itu Security Assessment ?

Security Assessment adalah pengujian sebuah system untuk melihat seberapa tinggi tingkat keamanannya dari serangan kejahatan dunia maya (Cyber Crime). Biasanya ketika seorang developer program/aplikasi selesai membuat aplikasinya, langkah selanjutnya adalah melakukan pengujian terhadap kerentanan aplikasi dari serangan Cyber.

Apa itu Indonese Framework ?

Internet Domain & Network Security atau disingkat INDONESE adalah sebuah Framework (metode/cara/langkah) sederhana yang dibuat oleh IDSIRTII dan Kemenkominfo dengan tujuan melakukan Analisa kekuatan sebuah website dari serangan dunia maya. Framework ini akan melihat seberapa rentankah website dilihat dari DNS Server, Email Server, Web Server dan Informasi artikel web. Tools yang digunakan semuanya berbasis online, sehingga mudah digunakan oleh orang awam yang memiliki pemahaman minim tentang Cybersecurity.

Bagaimana Teknik Penilaiannya ?

Teknik penilaian menggunakan poin skala seperti 0 sampai 5, atau 0 sampai 10, atau menggunakan penilaian skala 100. Dari hasil pengujian (DNS, Email, Web) dilakukan rata-rata nilai, kemudian akan diperoleh hasil seberapa baguskan website tersebut dalam hal keamanan Cyber.

Proses penilaian, Anda dapat menetapkan Nilai sesuai hasil pengujian. Masing-masing penilai akan berbeda memberikan nilainya dengan objeck yang sama.

Daftar Poin Penilaian dan Toolsnya

No	Pengujian	Komponen Pengujian	Keterangan	Tools
1	DNS Server	Whois & DNS Record Test	Digunakan untuk melihat kapan, dimana, siapa, DNS tersebut dibuat. Ini digunakan untuk melihat legalitas DNS terdaftar.	whois.pandi.id centralops.net robtex.com
		Authoritative DNS Server Test	Digunakan untuk melihat siapa yang berwenang mengeluarkan DNS tersebut	dnsinspect.com dnsstuff.com intodns.com dnssy.com dnscheck.pingdom.com
		Open DNS Resolver Test	Untuk melihat apakah DNS tersebut berpotensi/ mungkin dapat diattack dengan mudah atau tidak. Jika DNS terdaftar di web resolver tools, maka DNS tersebut mudah/rentan di attack	openresolver.com openresolver.nl
		Zone Transfer Attack	Untuk melihat apakah server DNS memiliki transfer state dengan Attacker ataukah tidak. Jika dalam pengujian Failed, berarti DNS aman dari daftar transfer attacker.	hackertarget.com/zone-transfer ultratools.com/tools/zoneFileDump
2	Email Server	Reverse DNS Test	Melihat apakah email yang terdaftar di DNS, DNS nya benar-benar terdaftar ataukah palsu	dnsinspect.com internet.nl
		MX Connection Test	Mail Exchanger (MX) merupakan cara untuk melihat apakah email memiliki format Send-Reply ataukah hanya	mxtoolbox.com dnsstuff.com/mstc

			Send saja. Pengujian ini digunakan untuk melihat apakah Email tersebut digunakan untuk Spam ataukah tidak.	
		Email Blacklist & RBL Test	Realtime Blackhole List (RBL) merupakanpengujian untuk melihat apakah server email memiliki fasilitas spamming ataukah tidak. Email Blacklist untuk melihat reputasi Mail Server	mxtoolbox.com
		Open Relay Test	Untuk mengetahui konfigurasi SMT Email Server. Ini untuk melihat apakah email tersebut dapat dimiliki orang lain ataukah tidak (cek email ganda). Sering disebut Email Outgoing	unlocktheinbox.com/openrelaytest/
		SSL POP3 & IMAP Test	Digunakan untuk melihat konfigurasi Email server apakah email dapat dibuka dengan aplikasi ataukah tidak. Ini memungkinkan email diterima dari pengirim. Misal email dapat dibuka dan diakses dengan Outlook. Sering disebut Email Ingoing	wormly.com/test_pop3_mail_server
		Email Phising Test	Digunakan untuk melihat apakah email tersebut berpotensi disisipi phising ataukah tidak	anonymailer.net emkei.cz
3	Web Server	Website Analysis	Sama dengan DNS test. Pengujian ini sebenarnya menguji alamat website. DNS (Domain Name Service merupakan fasilita yang berguna merubah IP Address ke alamat URL	dnsinspect.com
		Security Header	Untuk melihat konfigurasi header sebuah website. Pengujian ini akan menunjukkan nilai point dalam bentuk	securityheaders.io httpsecurityreport.com

			A,B,C,D, E, F bahkan R seberapa bagus konfigurasi header aplikasi web dalam mencegah terjadinya serangan	
		Web Server Risk Rating Test	Untuk melihat apakah website masuk dalam kategori fraud dan phising	pentest-tools.com/website-vulnerability-scanning/web-server-scanner sitecheck.sucuri.net
		Website Vulnerability	Untuk melihat apakah website masuk ke dalam daftar website yang mudah diserang/exploit.	sitecheck.sucuri.net exploit-db.com
		Malware Detection	Untuk melihat apakah aplikasi website mengandung malware ataukah tidak.	quttera.com

Contoh Laporan Security Assessment

A. Tim Security Assessment

Tim	1. Hendro Wijayanto 2. 3.
Hari, Tanggal	Senin, 07 Januari 2019
Website yang di Assessment	**sinus.ac.id**

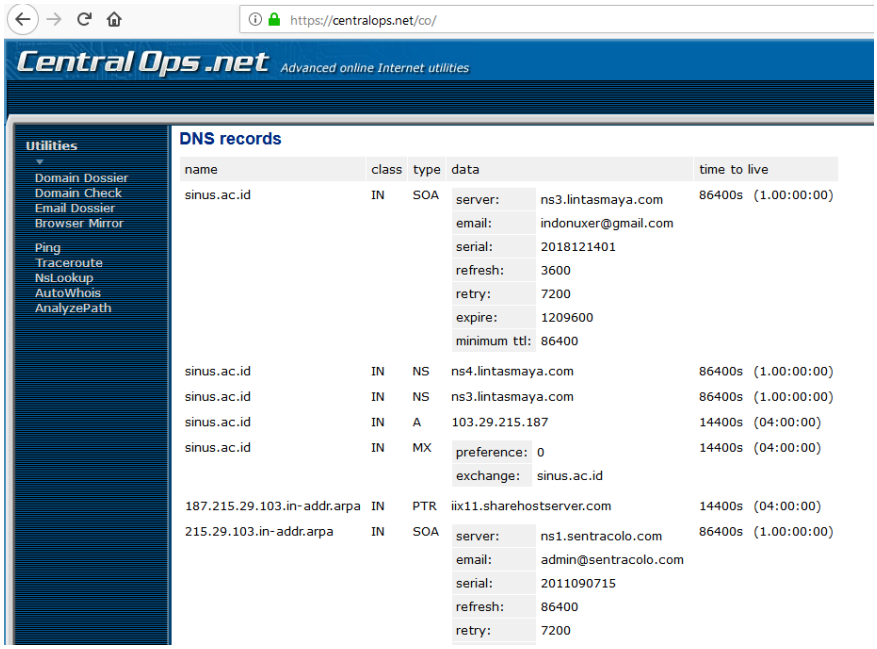
B. Proses Pengujian

1. DNS Server

1.1. Whois & DNS Record Test

Tools yang digunakan : https://centralops.net

Hasil :

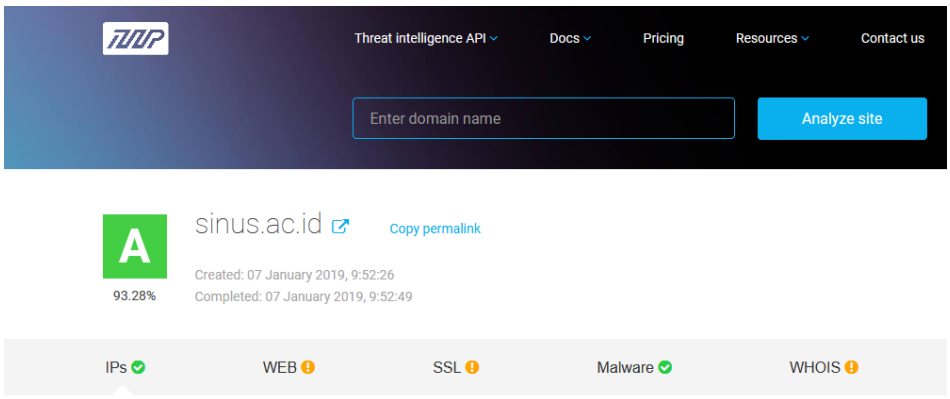


Dari hasil diatas terlihat bahwa sinus.ac.id terdaftar di domain hosting yang dikelola oleh lintasmaya.com. dengan IP terdaftar 102.29.215.187. Ini dikatakan bahwa domain tersebut ditemukan dan terdaftar resmi.

1.2. Authoritative DNS Server Test

Tools yang digunakan : http://dnsinspect.com/

Hasil :



Dari hasil pengujian didapat nilai A atau 93,28%. Jika dikonversi ke poin 0 sampai 5, kurang lebih masuk di rentan poin 4.8

1.3. *Open DNS Resolver Test*

Tools yang digunakan : http://openresolver.com

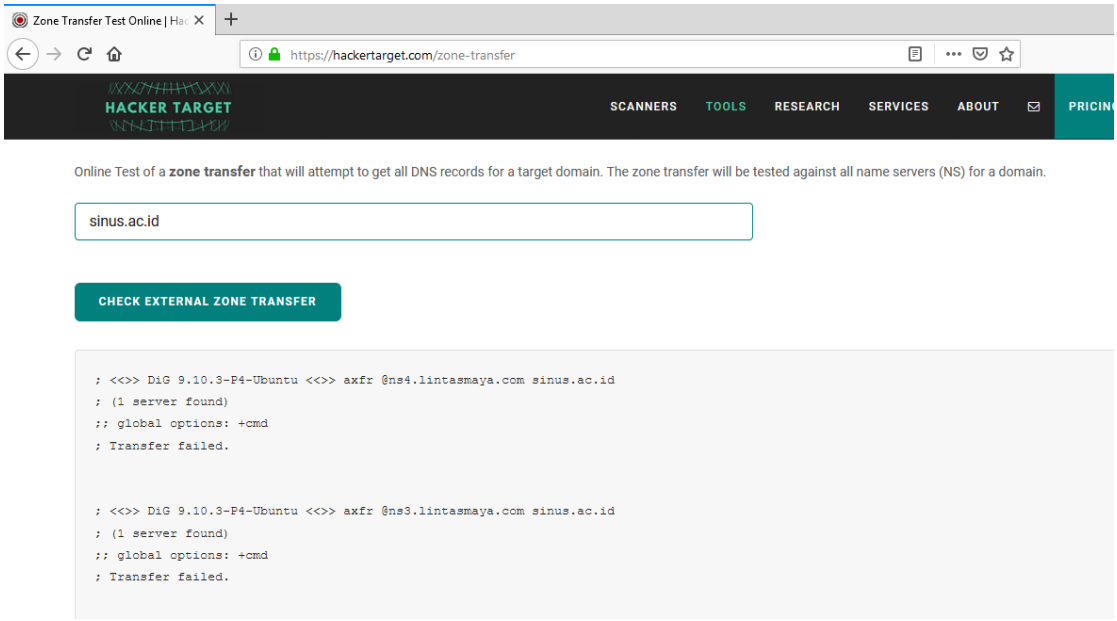
Hasil :

Dari hasil pengujian bahwa DNS Server sinus.ac.id tidak terdeteksi sebagai DNS Server yang berpotensi diserang.

1.4. *Zone Transfer Attack*

Tools yang digunakan : https://hackertarget.com/zone-transfer

Hasil :



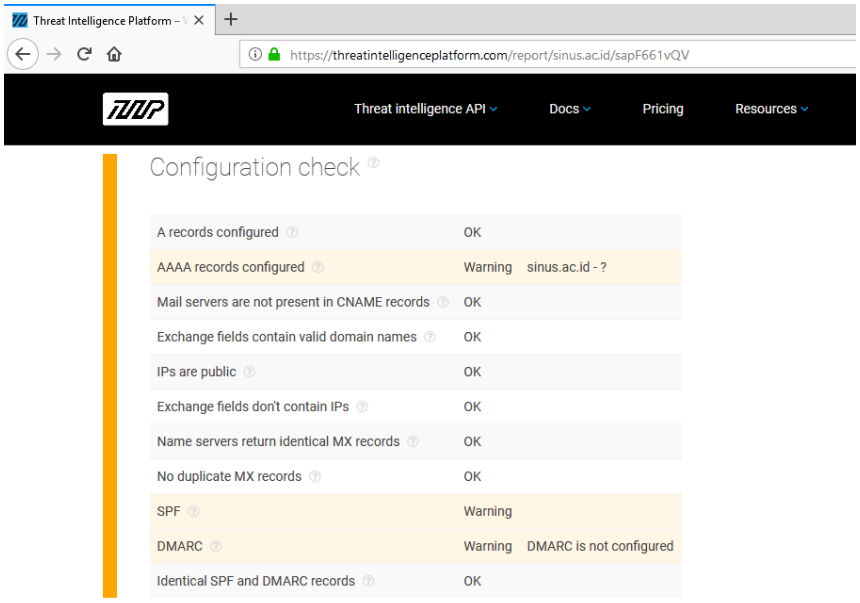
Dari hasil pengujian, server sinus.ac.id menggunakan system operasi Ubuntu. Dimana di konfigurasi DNS server Zone Transfer failed, artinya hanya orang tertentu saja yang dapat mengakses DNS server tersebut.

2. *Email Server*

2.1. *Reverse DNS Test*

Tools yang digunakan : https://internet.nl/

Hasil :

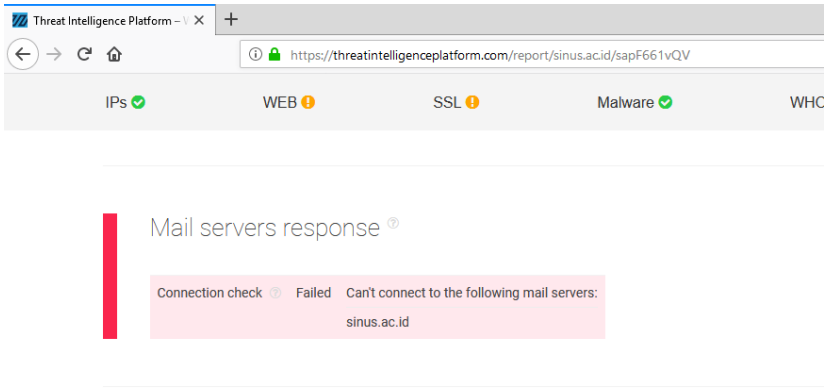


Terdapat beberapa permasalahan konfigurasi Mail Server, diantaranya DMARC (Domain-based Message Authentication Reporting and Conformance) yang merupakan validasi mail server belum terkonfigurasi, SPF (Sender Policies Framework) juga terdapat permasalahan konfigurasi.

2.2. *MX Connection Test*

Tools yang digunakan : https://internet.nl/

Hasil :

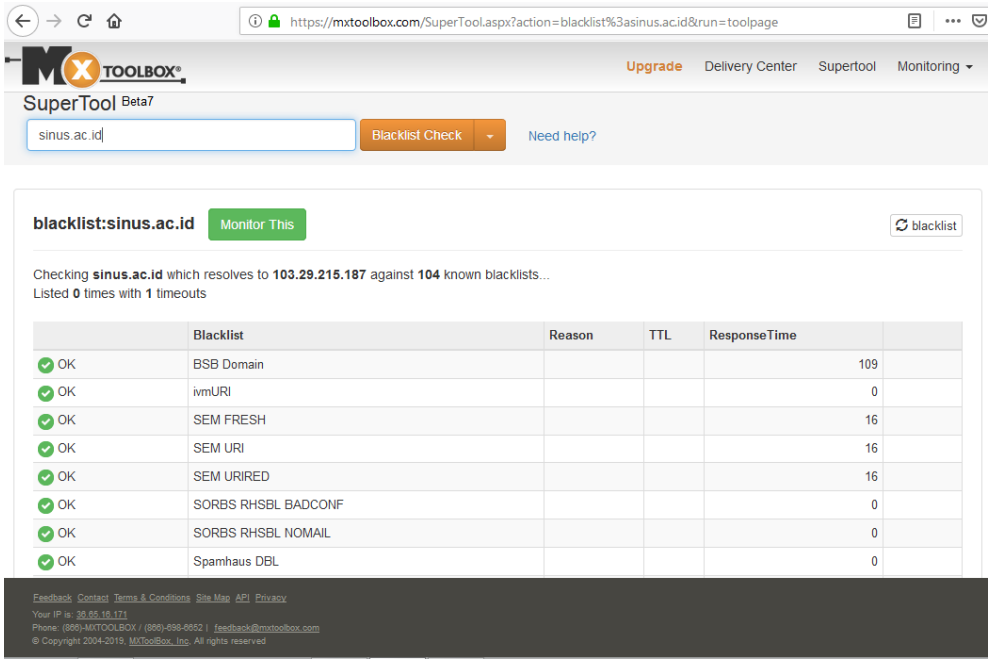


Dari hasil pengujian, Mail Server mengalami failed connection. Hal ini dikarenakan mungkin terjadi permasalahan konfigurasi Mail Server, atau memang sengaja dinonaktifkan.

2.3. *Email Blacklist & RBL Test*

Tools yang digunakan : https://mxtoolbox.com/blacklists.aspx

Hasil :

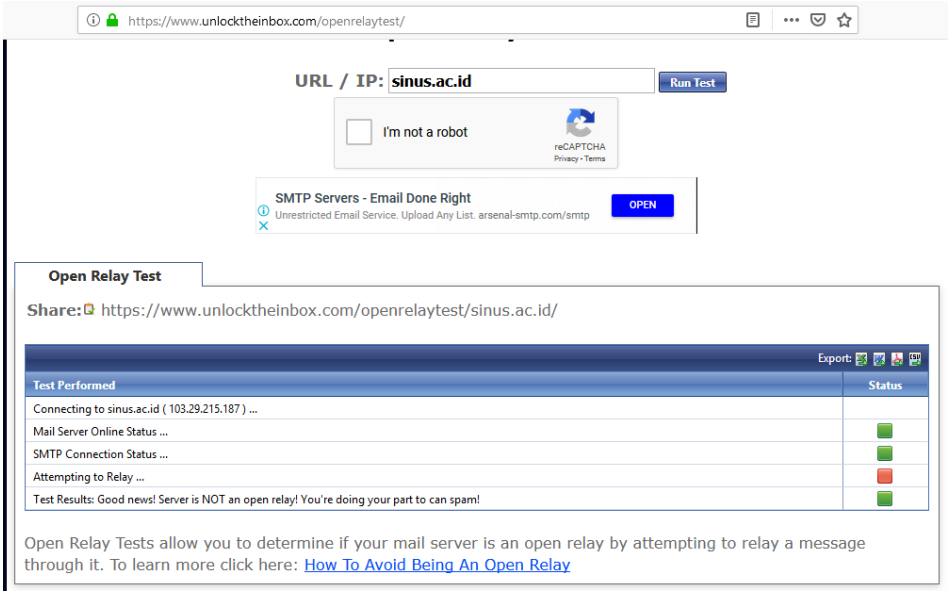


Dari hasil pengujian Mail Server yang digunakan memiliki reputasi yang baik. Hal ini biasanya dikarenakan aplikasi Mail Server selalu update. Akan tetapi dari pengujian ada beberapa layanan Blacklist yang memasukkannya ke dalam Daftar Blacklist (akan Nampak di daftar paling bawah)

2.4. *Open Relay Test*

Tools yang digunakan : https://www.unlocktheinbox.com/openrelaytest/

Hasil :

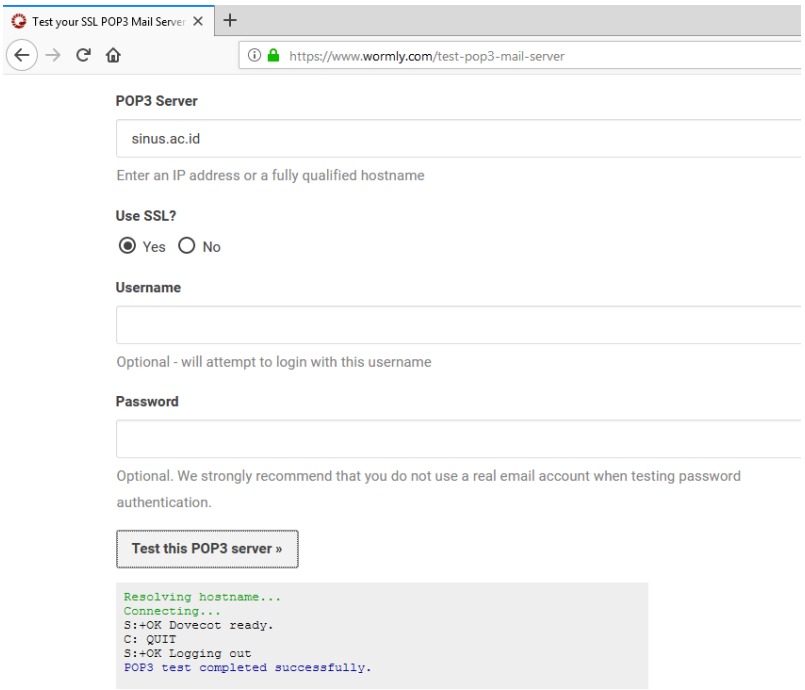


Dari hasil pengujian didapat bahwa “Server is NOT an open relay” yang berarti konfigurasi mail server untuk open relay tidak tersedia/terbuka. Tetapi hal ini masih memungkinkan email yang terdaftar digunakan untuk spaming

2.5. SSL POP3 & IMAP Test

Tools yang digunakan : https://www.wormly.com/test-pop3-mail-server

Hasil :

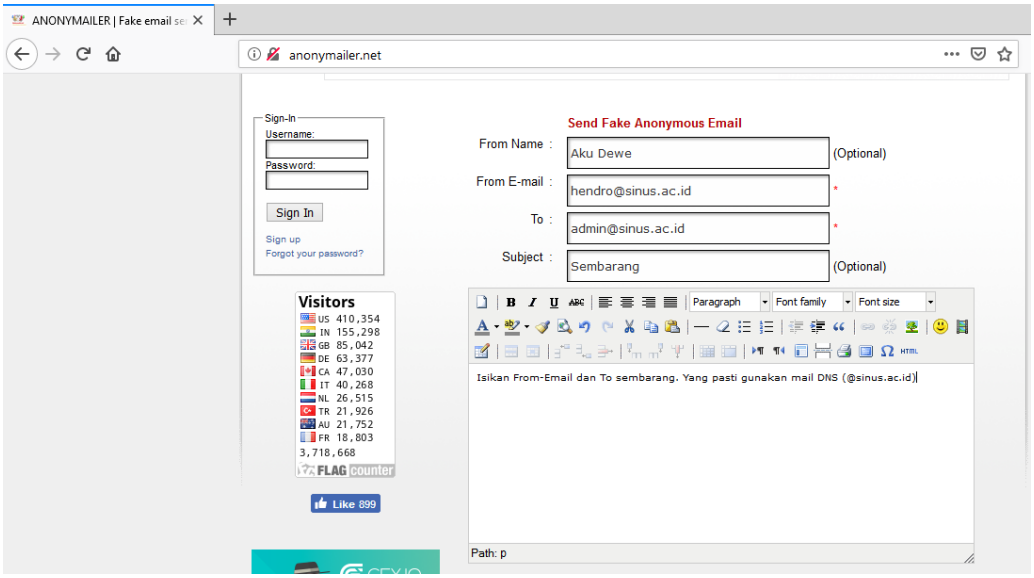


Mail Server mendukung layanan POP3 dan IMAP

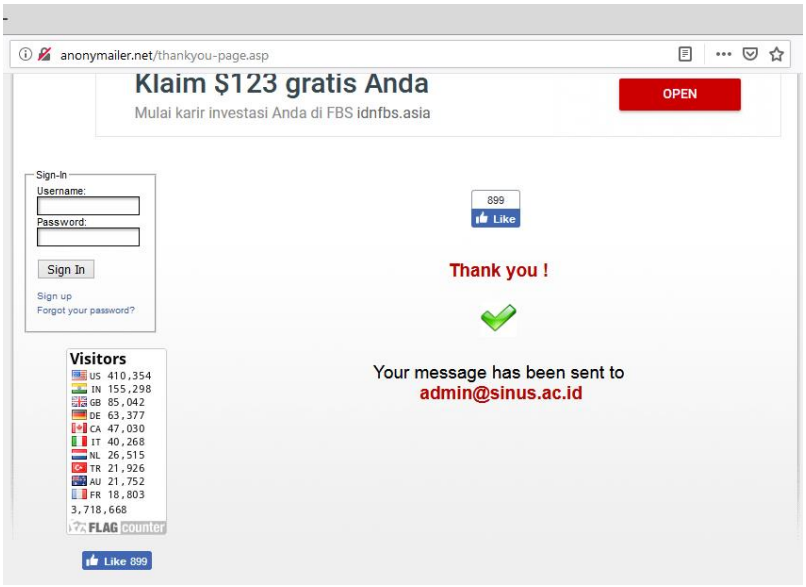
2.6. Email Phising Test

Tools yang digunakan : http://anonymailer.net/

Di pengujian ini wajib melakukan pengiriman pesan. Pengirim atau penerima dapat menggunakan email acak, yang pasti DNS email menggunakan DNS yang akan di uji (misalnya : @sinus.ac.id)



Hasil :



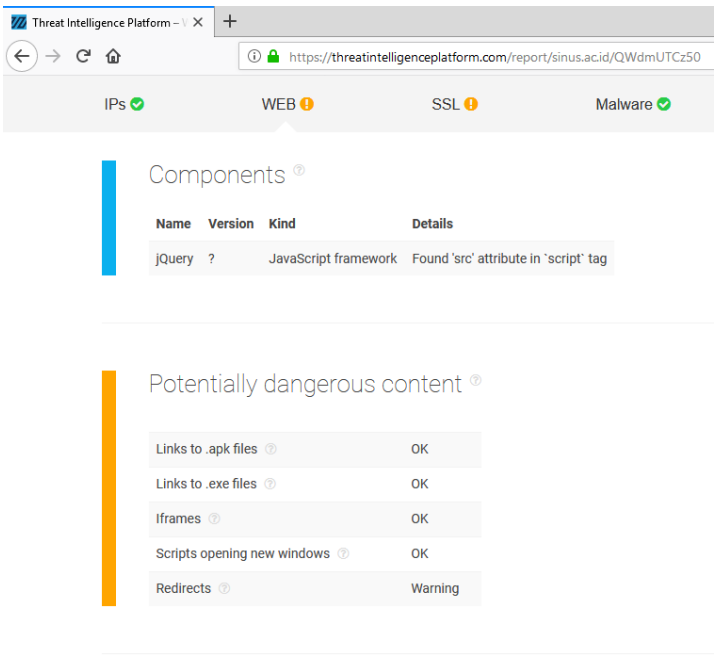
Dari hasil pengujian diperoleh hasil bahwa mail server sinus.ac.id berpotensi dapat digunakan untuk mengirimkan email palsu. Sangat rentan sekali oleh serangan Phising

3. *Web Server*

3.1. *Website Analysis*

Tools yang digunakan : http://dnsinspect.com/

Hasil :

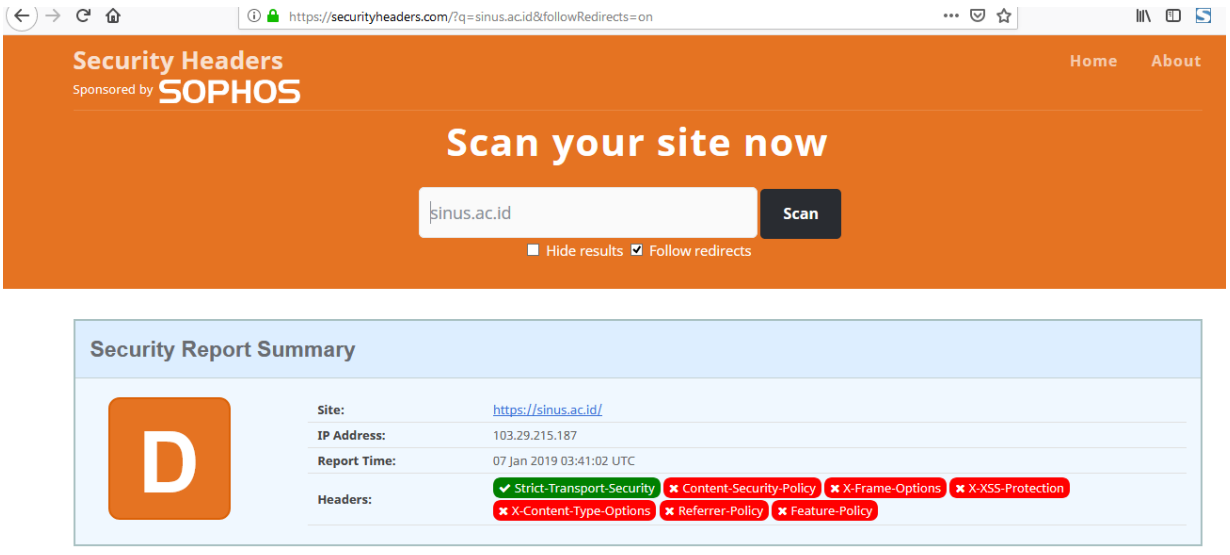


Dari hasil pengujian, konten ternyata mengandung beberapa file dan konfigurasi yang berpotensi terjadinya serangan malware. Seperti terdapatnya file EXE dan APK serta beberapa link redirect ke sistem

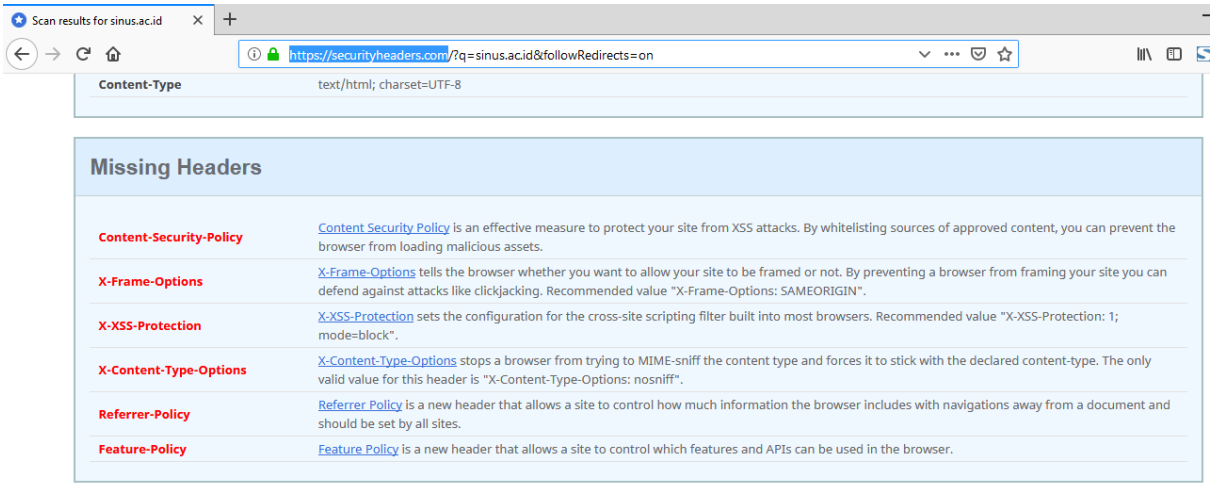
3.2. *Security Header*

Tools yang digunakan : https://securityheaders.com

Hasil :



Dari hasil pengujian, Nilai sinus.ac.id dilihat dari Security header ternyata menempati poin D. Point yang ada adalah A,B,C,D,E,F dan R.

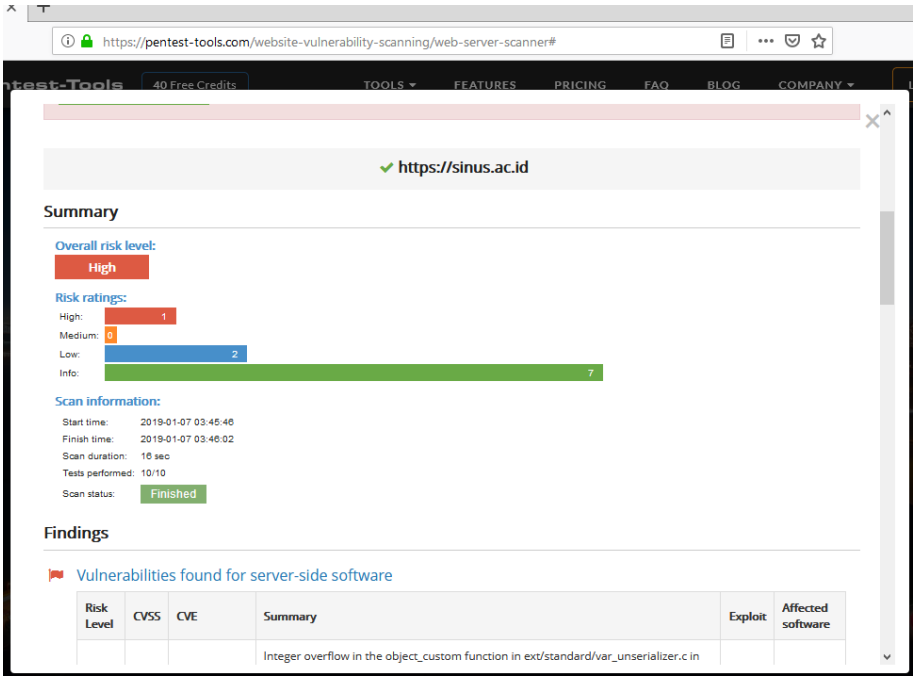


Beberapa konfigurasi script yang belum di optimalisasi dan berpotensi terjadi serangan

3.3. *Web Server Risk Rating Test*

Tools yang digunakan :

Hasil :

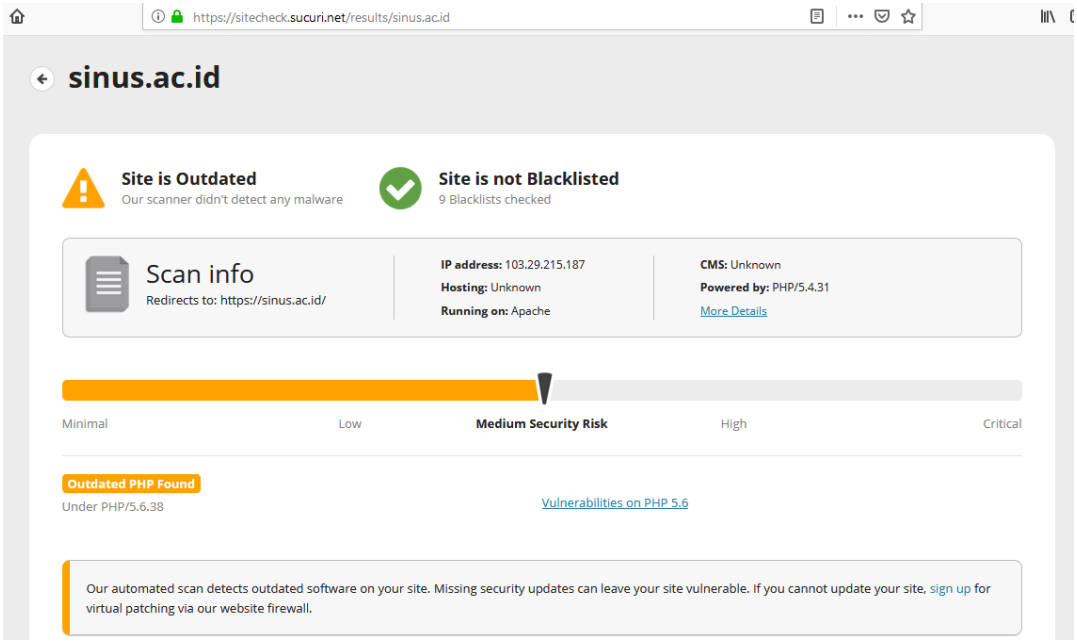


Dari hasil pengujian memiliki rata-rata kerusakan yang tinggi. Hal ini terjadi karena versi PHP dan aplikasi web server tidak update (analisis tidak terlihat di screenshoot karena berada di bawah)

3.4. *Website Vulnerability*

Tools yang digunakan : https://sitecheck.sucuri.net

Hasil :

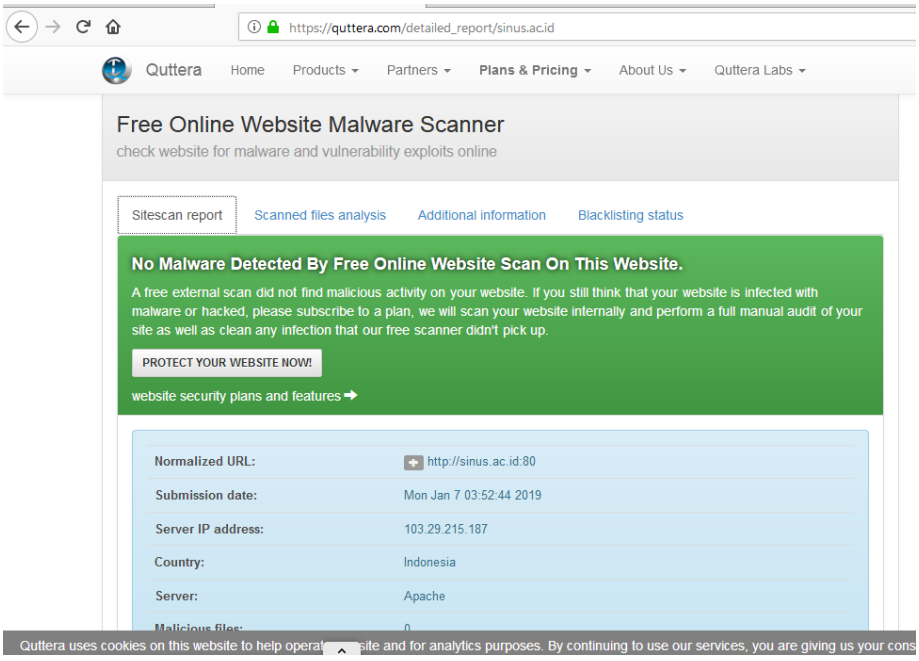


Dari hasil pengujian didapat tingkat kemungkinan terjadi serangan web sinus.ac.id di level medium.

3.5. *Malware Detection*

Tools yang digunakan : https://quttera.com/

Hasil :



Dari hasil pengujian tidak ditemukan malware di dalam script/file didalam aplikasi web sinus.ac.id

C. Penilaian

Dalam penilaian security assessment ini, menggunakan penilaian dengan skala 0 sampai 5, dimana rentan skalanya :

Skala	Keterangan
4 sampai 5	Sangat Aman
3 sampai 3.9	Aman
2 sampai 2.9	Cukup
1 sampai 1,9	Rentan
0 sampai 0.9	Sangat Rentan

No	Pengujian	Komponen Pengujian	Nilai
1	DNS Server	Whois & DNS Record Test	5
		Authoritative DNS Server Test	4.8
		Open DNS Resolver Test	5
		Zone Transfer Attack	5
		Rata-rata	**4.95**
2	Email Server	Reverse DNS Test	2
		MX Connection Test	2
		Email Blacklist & RBL Test	4.7
		Open Relay Test	3
		SSL POP3 & IMAP Test	5
		Email Phising Test	1
		Rata-rata	**2.95**
3	Web Server	Website Analysis	2.5
		Security Header	2
		Web Server Risk Rating Test	2
		Website Vulnerability	2.5
		Malware Detection	5
		Rata-rata	**2.8**

D. Kesimpulan

Dari hasil Security Assessment diperoleh hasil dan kesimpulan sebagai berikut :

1. Dari penilaian, tingkat keamanan website sinus.ac.id sebesar 3.57 dari total nilai 5. Dari hasil tersebut dapat dikatakan secara keseluruhan website sinus.ac.id berada di

posisi Aman dari serangan kejahatan dunia maya. Akan tetapi hal ini tidak serta merta website tersebut tidak mungkin diserang. Mengingat tidak ada sistem yang benar-benar secure selama terkoneksi dengan jaringan.

2. Beberapa hal yang perlu dilakukan adalah melakukan peningkatan versi/update, memperbaiki beberapa konfigurasi server dan melakukan patch header website.
3. Dari hasil analisis ini diperlukan beberapa tools untuk masing-masing pengujian agar dapat membandingkan antara tools satu dengan yang lain dalam memberikan kesamaan penilaian.

UJIAN AKHIR SEMESTER GANJIL 2019

KEAMANAN SISTEM INFORMASI

TAKE HOME

1. Take Home
2. **Kelompok Maksimal 2 Mahasiswa**
3. Dikumpulkan dalam bentuk **Hardfile (TANPA JILID)** pada saat UAS hari H Keamanan Sistem Informasi
4. Format laporan sesuai dengan contoh
5. Objek analisis/website adalah website akademik/universitas **selain sinus.ac.id.** (Karena sudah digunakan untuk contoh)
6. Terdapat 4 bagian laporan yaitu **A. Tim Security Assessment**, **B. Proses Pengujian**, **C. Penilaian** dan **D. Kesimpulan**
7. Masing-masing analisis boleh menggunakan tools lebih dari satu. Atau menggunakan tools yang lain
8. Hal yang kurang paham dapat ditanyakan lewat Whatsapp 08562565414
9. **Pada saat pengumpulan laporan hari H UAS, sertakan fotocopy sertifikat Seminar Cyber Security**