**BAB II**

**TINJAUAN PUSTAKA**

**2.1 WEBSTIE**

*Website* merupakan sebuah kumpulan halaman-halaman *web* beserta file-file pendukungnya, seperti file gambar, video, dan file digital lainnya yang disimpan pada sebuah *web server* yang umumnya dapat diakses melalui internet. Atau dengan kata lain, *website* adalah sekumpulan folder dan file yang mengandung banyak perintah dan fungsi fungsi tertentu, seperti fungsi tampilan, fungsi menangani penyimpanan data, dsb (Hartono,2014).

WWW adalah suatu program yang ditemukan oleh Tim Berners-Lee pada tahun 1991 Awalnya Berners-Lee hanya ingin menemukan cara untuk menyusun arsip-arsip risetnya Untuk itu, beliau mengembangkan suatu sistem untuk keperluan pribadi Sistem itu adalah program peranti lunak yang diberi nama Enquire Dengan program itu, Berners-Lee berhasil menciptakan jaringan yang menautkan berbagai arsip sehingga memudahkan pencarian informasi yang dibutuhkan Inilah yang kelak menjadi dasar dari sebuah perkembangan pesat yang dikenal sebagai WWW (Andriyanto, 2014).

*Website* pada era sekarang ini digunakan hampir seluruh kalangan baik pribadi maupun perusahaan, instansi pemerintah, instansi non pemerintah, organisasi, komunitas, dan dll yang digunakan untuk memberikan informasi dan layanan yang mempermudahkan orang lain sehingga tidak menggunakan cara yang manual lagi seperti menempelkan informasi pada mading atau mengharuskan orang yang memberlukan layanan pergi ke tempat penyedia layanan tersebut.

**2.1.1 HTTP**

HTTP (*Hypertext Transfer Protocol*) adalah suatu *protokol* yang digunakan untuk mentransfer dokumen/halaman dalam WWW (World *Wide Web*). HTTP mendefinisikan bagaimana suatu pesan dapat diformat dan dikirimkan dari *client* ke *server* atau sebaliknya. HTTP mengatur aksi apa saja yang harus dilakukan oleh *web server* dan *web browser* sebagai respon atas perintah-perintah yang ada pada protokol HTTP ini (Seprtian, 2011).

**2.1.2 HTTPS**

*Hypertext Transfer Protocol Secure* memiliki pengertian yang sama dengan http hanya saja https memiliki kelebihan fungsi di bidang keamanan (*secure*). Dengan menggunakan *Secure Socket Layer* (SSL) atau *Transport Layer Security* (TLS) sebagai *sublayer* di bawah http aplikasi layer yang biasa. Teknologi https protokol mencegah kemungkinan “dicurinya” informasi penting yang dikirimkan selama proses komunikasi berlangsung antara *user* dengan *web server* atau sebaliknya (Zabar dan Novianto, 2015).

**2.1.3 WEB SERVER**

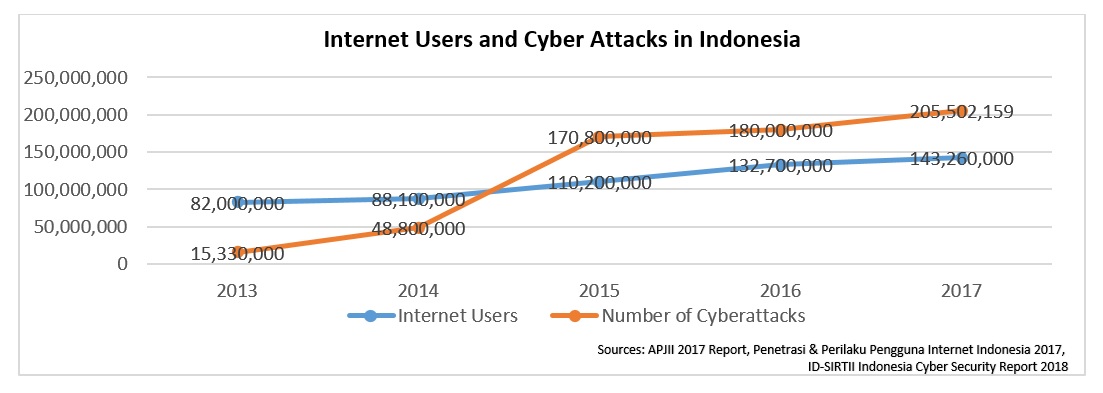
*Web server* merupakan *software* yang memberikan layanan data yang berfungsi menerima permintaan HTTP atau HTTPS dari klien yang dikenal dengan *browser web* dan mengirimkan kembali hasilnya dalam bentuk halaman - halaman web yang umumnya berbentuk dokumen HTML. Cara kerja dari *web server* sebenarnya sangat mudah kita pahami. Contoh paling mudah seperti berikut; kita akan membuka sebuah halaman *website*, Proses yang akan terjadi pada *browser* adalah *browser* akan membentuk *koneksi* dengan *web server*, meminta halaman *website* dan menerimanya. *Web server* kemudian mengecek permintaan tersebut apakah tersedia atau tidak. Apabila tersedia, maka *web server* akan mengirimkan data kepada *browser*. Apabila permintaan tidak ditemukan atau terjadi error maka *web server* akan mengirimkan pesan error kepada *browser*. Pembentukan koneksi, permintaan data, penerimaan data dari *browser* ke *web server* diatur dalam sebuah kode RFC2616. RFC2616 mencantumkan status web server dalam bentuk kombinasi tiga angka yang memiliki arti berbeda-beda. Status ini muncul di peramban saat kita mengakses web server tertentu (Suhesti, 2008).

**2.2 KEAMANAN WEBSITE**

Keamanan web, sangat erat kaitannya dengan jaringan, karena untuk mengakses sebuah website pasti dibutuhkan koneksi jaringan. Saat ini sangat pesat sekali perkembangan teknologi website, jaringan dan bermacam ancaman keamanan yang dihadapi, seperti ancaman terhadap kerahasiaan yang sering dihadapi adalah hacker, Masquerader,virus virus dari internet maupun dari media transfer data seperti flasdisk, hardisk eksternal, melalui jaringan LAN, download file tanpa proteksi, Trojan horse, Aktifitas user yang tidak terotorisasi dan masih banyak lagi ancaman keamanan yang kadang tidak kita sadari (nimda, 2012).

Catatan ID-SIRTII adalah pada 2014, ada 48,8 juta serangan cyber di Indonesia. Serangan tersebut kebanyakan diakibatkan oleh adanya aktivitas "malware" sebanyak 12.007.808 insiden. Serangan akibat adanya celah keamanan sebanyak 24.168 kasus, kebocoran rekam jejak atau "record leakage" 5.970 kasus. Ada juga serangan melalui "password harvesting" atau "phising" sebanyak 1.730 kasus dan serangan akibat kebocoran domain sebanyak 215 kasus. Dari angka tersebut, menurut ID-SIRTII, laman pemerintah atau beralamat go.id paling banyak diserang peretas(Veren, 2016)

Menurut data 2017 APJII didapatkan bahwa perbandingan jumlah pengguna internet dan juml ah cyber attack selama lima tahun mengalami penambahan setiap tahunnya. Samakin tinggi jumlah pengguna internet semakin banyak cyber attack yang terjadi, jumlah tertinggi terjadi pada tahun 2017 dengan jumlah pengguna internet 143.250.000 jiwa dan terjadi cyber attack dengan jumlah serangan 205,502,159.



Gambar 2.1 Penetrasi dan perilaku pengguna internet indonesia 2017

Menurut Direktur Deteksi Ancaman BSSN Sulistyo (2019), 225,9 juta serangan siber yang masuk ke Indonesia 2018. Kita bisa melihat kebanyakan 40% malware makanya ada teknologi khusus kita kerja sama dengan HoneyNet.

**2.2.1 OWASP (OPEN WEB APPLICATION SECURITY PROJECT)**

OWASP Foundation (Slide Tinjauan Umum) adalah asosiasi profesional anggota global dan terbuka untuk siapa saja yang tertarik untuk mempelajari lebih lanjut tentang keamanan perangkat lunak. Bab-bab lokal dijalankan secara independen dan dipandu oleh Chapter\_Leader\_Handbook (Yoseman,2018).

Terdapat 10 celah keamanan website menurut OWASP , sebagai berikut (Nathasya, 2018) :

a. Injection

Serangan injection biasa terjadi jika ada data yang tidak terpercaya dikirim ke sebuah code interpreter melalui sebuah formulir input atau cara input data ke website lainnya. Misalnya, seorang hacker bisa memasukkan kode database SQL melalui sebuah formulir yang sebenarnya hanya meminta data plaintext. Kalau formulir input ini tidak diamankan dengan baik maka kode SQL nya bisa saja dijalankan. Ini adalah contoh serangan injection SQL. Nah, serangan injection ini bisa dicegah dengan memvalidasi dan membersihkan data yang dimasukkan oleh user. Validasi yang dimaksud disini adalah menolak data-data yang terlihat mencurigakan. Membersihkan data berarti menghapus semua data-data mencurigakan tersebut. Tidak hanya itu, admin database juga bisa meminimalkan jumlah informasi yang mungkin terexpose ke serangan injection.

b. Broken Authentication

Kelemahan pada sistem login bisa memberi hacker akses ke akun user. Tidak hanya itu mereka bisa menguasai seluruh sistem dengan meng-hack akun admin. Untuk memitigasi kelemahan authentication, Anda bisa menggunakan 2-factor authentication (2FA).

c. Sensitive Data Exposure

Jika sebuah website menyimpan data-data sensitive penggunanya, tentunya akan bahaya jika mereka tidak menjaga keamanannya. Untuk mengurangi kemungkinan pencurian data, Anda bisa mengenskripsi data-data sensitifnya. Developer juga harus memastikan bahwa website tidak menyimpan data-data sensitive yang sebenarnya tidak dibutuhkan.

d. XML External Entities

Ini adalah serangan ke website dan aplikasi yang menganalisa input XML. Input ini bisa mereferensikan entity external untuk mengetahui kelemahan yang ada pada input XMLnya. Entiti external yang dimaksud disini biasanya berupa unit penyimpanan, seperti misalnya hard drive. Analisa input XML bisa dibuat seakan-akan mereka mengirim data ke entity external yang tidak dipercaya, dimana mereka bisa mengirim data-data sensitive ke hackernya langsung. Cara terbaik untuk mengatasi XEE ini adalah dengan memiliki web app yang mengandung jenis data yang tidak terlalu kompleks.

e. Broken Access Control

Access control pada poin ini mengacu kepada sistem control yang mengakses informasi dan fungsionalitasnya. Access control yang rusak memungkinkan penyerang untuk melewati proses autorisasi dan melakukan hal-hal yang biasanya hanya bisa dilakukan oleh admin.

f. Security Misconfiguration

Kesalahan konfigurasi keamanan adalah kelemahan yang paling sering terjadi di antara kelemahan lain di daftar ini. Biasanya kesalahan terjadi jika Anda hanya menggunakan default konfigurasi tanpa melihat kebutuhan website.

g. Cross Site Scripting

Kelemahan cross site scripting akan terjadi pada web app jika web app tersebut menginjinkan user untuk menambahkan kode custom ke sebuah path URL atau ke website yang dilihat oleh user lain. Kelemahan ini biasa dimanfaatkan untuk menjalankan kode JavaScript yang berbahaya pada browser korban. Contohnya, jika seorang hacker mengirim email ke korban dengan mengatas namakan nama bank tersebut dan menyertakan link ke website bank tersebut, mereka bisa saja menaruh kode JavaScript berbahaya ke dalamnya. Kalau website bank tidak terlindungi dengan baik, nasabah Anda akan menjadi korban.

h. Insecure Deserialization

Untuk mengerti apa masalah dari kelemahan ini, kita harus mengerti dulu apa arti dari serialisasi dan deserialisasi. Serialisasi adalah proses dimana object diambil dari kode aplikasi dan di-convert ke format lain sehingga bisa digunakan untuk keperluan lain, misalnya menyimpan data ke sebuah disk. Deserialisasi berarti sebaliknya; meng-convert data yang sudah diserialisasi kembali object yang digunakan oleh aplikasinya. Insecure deserialization atau deserialisasi yang kurang aman bisa saja diserang dengan memanfaatkan data dari asal yang tidak dipercaya. Ini bisa menyebabkan terjadinya serangan DDoS. Untuk mencegah ini terjadi, Anda perlu melarang deserialisasi dari data yang tidak dipercaya.

i. Using Components With Known Vulnerabilities

Kebanyakan web developer menggunakan komponen seperti libraries dan frameworks di web app mereka. Komponen-komponen ini adalah kumpulan software yang menolong developers untuk bekerja dengan lebih efisien. Beberapa hacker biasa mencari kelemahan yang ada pada komponen-komponen ini agar mereka bisa melakukan serangan. Oleh karena itu, developer harus selalu memastikan bahwa komponen-komponen ini sudah diupdate agar tetap aman.

j. Insufficient Logging and Monitoring

Kebanyakan web app tidak mengambil langkah yang cukup untuk mendeteksi penembusan data. Rata-rata orang baru sadar kalau terjadi penembusan di website mereka setelah 200 hari. Ini tentunya memberikan penyerang banyak waktu untuk melakukan penyerangan. OWASP merekomendasikan developer untuk mengimplementasi logging dan monitoring serta rencana response insiden agar mereka tahu jika ada penyerangan yang terjadi pada aplikasi mereka.

**2.3 CERTIFIED ETHICAL HACKER (CEH)**

Ujian Certified Ethical Hacker (CEH) dikembangkan oleh Dewan Internasional Konsultan E-Commerce (EC-Council) untuk menyediakan sarana industri untuk mensertifikasi kompetensi profesional keamanan. Sertifikasi CEH diberikan kepada mereka yang telah mencapai tingkat pengetahuan dan keterampilan keamanan yang dibutuhkan untuk melakukan audit keamanan dan pengujian penetrasi sistem dan jaringan. Ujian CEH diperbarui secara berkala untuk menjaga sertifikasi berlaku untuk alat dan kerentanan peretasan terbaru. Ini diperlukan karena CEH harus terbiasa dengan serangan dan eksploitasi terbaru (Graves, 2010).

**2.3.1 PENETRATION TEST**

Penetration test adalah subkelas dari ethical hacking; itu terdiri dari serangkaian metode dan prosedur yang bertujuan menguji / melindungi keamanan organisasi. Penetration test terbukti membantu dalam menemukan kerentanan dalam suatu organisasi dan memeriksa apakah penyerang akan dapat mengeksploitasi mereka untuk mendapatkan akses tidak sah ke suatu aset (baloch, 2015) .

**2.4 ACUNETIX WEB VULNERABILITY SCANNER (WVS)**

Acunetix website application scanner merupakan perangkat lunak yang dikembangkan untuk melakukan scanning. Kelebihan dari tools ini adalah kemampuannya untuk memberikan solusi dari kelemahan yang ditemukan dan mengelola traceability dari setiap vulnerabilities tersebut. Selain itu, acunetix menyediakan fungsi-fungsi tambahan yang dapat digunakan untuk melakukan pengujian lebih lanjut terhadap website yang diuji (Robby, 2013).

Menurut Mamad (2018), dibawah ini adalah penjelasan tentang status bahaya (kerentanan) ditemukan :

Salah satu komponen kunci dari hasil scan adalah daftar semua kerentanan yang ditemukan dalam target pemindaian selama pemindaian. Tergantung pada jenis scan, ini dapat berupa Web Alerts atau Network Alerts, dan tanda dikategorikan menurut 4 tingkat keparahan:

a. High Risk Alert Level 3

Kerentanan dikategorikan sebagai yang paling berbahaya, yang menempatkan target scan pada risiko maksimum untuk hacking dan pencurian data.

b. Medium Risk Alert Level 2

Kerentanan disebabkan oleh server misconfiguration dan sitecoding yang lemah, yang memfasilitasi gangguan server dan intrusi.

c. Low Risk Alert Leve 1

Kerentanan berasal dari kurangnya enkripsi lalu lintas data atau jalur direktori pengungkapan.

d.Information Alert

ini adalah item yang telah ditemukan selama scan dan yang dianggap menarik, misalnya kemungkinan pengungkapan alamat internal IP atau alamat email, atau pencocokan string pencarian ditemukan di database Google Hacking, atau informasi tentang layanan yang telah ditemukan selama scanning.

**2.4 WEBSITE PRODI DI UNIVERSITAS SYIAH KUALA**

Pada Universitas Syiah Kuala terdapat 110 prodi yang terbagi dalam 11 fakultas. Terdapat 30 prodi yang tidak memiliki website dan 80 prodi yang memiliki website dengan 75 website aktif dan 5 website yang tidak aktif. Dalam penelitian ini dilakukan pengujian celah keamanan kepada setiap website yang aktif untuk mengetahui tingkat keamanan pada website prodi di Universitas Syiah Kuala.

Tabel 2.1 Website prodi di Universitas Syiah Kuala

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | Fakultas | Prodi | Website | Status |
| 1 | Ekonomi dan Bisnis | [Pemasaran](http://feb.unsyiah.ac.id/d3-pemasaran/) | - | - |
|  |  | [Perpajakan](http://d3perpajakan.feb.unsyiah.ac.id/) | http://d3perpajakan.feb.unsyiah.ac.id/ | Aktif |
| [Akuntansi](http://feb.unsyiah.ac.id/d3-akuntansi/) | - | - |
| [Perusahaan](http://feb.unsyiah.ac.id/d3-perusahaan/) | - | - |
| [Sekretari](http://feb.unsyiah.ac.id/d3-sekretari/) | - | - |
| [Keuangan dan Perbankan](http://feb.unsyiah.ac.id/d3-keuangan-dan-perbankan/) | - | - |
| [Ekonomi Manajemen](http://ekm.feb.unsyiah.ac.id/) | http://ekm.feb.unsyiah.ac.id/ | Aktif |
| [Ekonomi Akuntansi](http://eka.feb.unsyiah.ac.id/) | http://eka.feb.unsyiah.ac.id/ | Aktif |
| [Ekonomi Pembangunan](http://ekp.feb.unsyiah.ac.id/) | http://ekp.feb.unsyiah.ac.id/ | Aktif |
| [Ekonomi Islam](http://eki.feb.unsyiah.ac.id/) | http://eki.feb.unsyiah.ac.id/ | Aktif |
| [Magister Manajemen](http://mm.unsyiah.ac.id/) | http://mm.unsyiah.ac.id/ | Aktif |
| [Magister Akuntansi](http://magisterakuntansi.unsyiah.ac.id/) | http://magisterakuntansi.unsyiah.ac.id/ | Aktif |
| [Magister Ilmu Ekonomi](http://s2ie.unsyiah.ac.id/) | http://s2ie.unsyiah.ac.id/ | Aktif |
| [Doktor Ilmu Manajemen](http://feb.unsyiah.ac.id/s3-doktor-ilmu-manajemen/) | - | - |
| [Doktor Ilmu Ekonomi](http://feb.unsyiah.ac.id/s3-doktor-ilmu-ekonomi/) | - | - |
| 2 | Kedokteran hewan | Pendidikan Dokter Hewan | http://fkh.unsyiah.ac.id/ | Aktif |
|  |  | Magister Kesehatan Masyarakat Veteriner | - | - |
| 3 | Hukum | Ilmu Hukum | http://www.law.unsyiah.ac.id/ | Aktif |
|  |  | Magister Ilmu Hukum | http://www.mih.unsyiah.ac.id/ | Aktif |
| Magister Kenotariatan | http://mkenotariatanfh.unsyiah.ac.id/ | Aktif |
| Doktor Ilmu Hukum | http://dih.unsyiah.ac.id/ | Aktif |
| 4 | Teknik | Teknik Sipil | http://sipil.unsyiah.ac.id/ | Aktif |
|  |  | Teknik Mesin | http://mesin.unsyiah.ac.id/ | Aktif |
| Teknik Kimia | http://che.unsyiah.ac.id/ | Aktif |
| Arsitektur | http://arsitektur.unsyiah.ac.id/ | Aktif |
| Teknik Elektro | http://elektro.unsyiah.ac.id/ | Aktif |
| Teknik Industri | http://www.industri.unsyiah.ac.id/ | Aktif |
| Teknik Geofisika | http://geosciences.unsyiah.ac.id/ | Aktif |
| Teknik Pertambangan | http://www.tektambang.unsyiah.ac.id/ | Aktif |
| Teknik Geologi | http://geologi.unsyiah.ac.id/ | Aktif |
| Teknik Komputer | http://komputer.unsyiah.ac.id/ | Aktif |
| Perencanaan Wilayah Dan Kota | http://pwk.unsyiah.ac.id/ | Aktif |
| Magister Teknik Mesin | http://mtm.unsyiah.ac.id/ | Aktif |
| Magister Teknik Sipil | http://mts.unsyiah.ac.id/ | Tidak aktif |
| Magister Industri | http://mti.unsyiah.ac.id/ | Aktif |
| Magister Teknik Kimia | http://mche.unsyiah.ac.id/ | Tidak aktif |
| Magister Teknik Elektro | http://mte.unsyiah.ac.id/ | Aktif |
| 5 | Pertanian | Agribisnis | http://psa.unsyiah.ac.id/ | Aktif |
|  |  | Agroteknologi | http://agrotek.unsyiah.ac.id/ | Tidak aktif |
| Peternakan | http://pet.unsyiah.ac.id/ | Aktif |
| Teknik Hasil Pertanian | http://thp.unsyiah.ac.id/ | Aktif |
| Teknik Pertanian | http://tp.unsyiah.ac.id/ | Aktif |
| Ilmu Tanah | http://www.ilmutanah.unsyiah.ac.id/ | Aktif |
| Proteksi Tanaman | http://ptn.fp.unsyiah.ac.id/ | Aktif |
| Kehutanan | http://www.kehutanan.unsyiah.ac.id/ | Aktif |
| Magister Konservasi Sumberdaya Lahan | http://ksdl.unsyiah.ac.id/ | Aktif |
| Magister Agrotekoteknologi | http://magr.unsyiah.ac.id/ | Aktif |
| Magister Agribisnis | http://mab.unsyiah.ac.id/ | Aktif |
| Magister Teknologi  Industri Pertanian | - | - |
| Magister Peternakan | http://magister.pet.unsyiah.ac.id/ | Aktif |
| Doktor Ilmu Pertanian | http://dip.unsyiah.ac.id/ | Aktif |
| Budidaya Peternakan | http://d3fp.unsyiah.ac.id/ | - |
| Manajemen Agribisnis | http://d3fp.unsyiah.ac.id/ | - |
| Agroteknologi PPD Gayo Lues | - | - |
| Kehutanan PPD Gayo Lues | - | - |
| 6 | Keguruan dan Ilmu Pendidikan | Pend. Jasmani Kesehatan dan Rekreasi | http://penjaskesrek.fkip.unsyiah.ac.id/ | Aktif |
|  |  | Pend. Anak Usia Dini | http://paud.fkip.unsyiah.ac.id/ | Aktif |
| Pend. Kesejahteraan Keluarga | http://pkk.fkip.unsyiah.ac.id/ | Aktif |
| Pend. Guru Sekolah Dasar | http://pgsd.fkip.unsyiah.ac.id/ | Aktif |
| Pend. Bimbingan & Konseling | http://bks.fkip.unsyiah.ac.id/ | Aktif |
| Ilmu Pendidikan | http://ip.fkip.unsyiah.ac.id/ | Tidak aktif |
| Pend. Matematika | http://matematika.fkip.unsyiah.ac.id/ | Aktif |
| Pend. Fisika | http://fisika.fkip.unsyiah.ac.id/ | Aktif |
| Pend. Biologi | http://biologi.fkip.unsyiah.ac.id/ | Aktif |
| Pend. Biologi PSDKU Gayo Lues | http://psdkugayolues.unsyiah.ac.id/ | Aktif |
| Pend. Kimia | http://kimia.fkip.unsyiah.ac.id/ | Aktif |
| Pendidikan Ekonomi | http://ekonomi.fkip.unsyiah.ac.id/ | Aktif |
| Pend. Kewarganegaraan | http://ppkn.fkip.unsyiah.ac.id/ | Aktif |
| Pendidikan Sejarah | http://sejarah.fkip.unsyiah.ac.id/ | Aktif |
| Pendidikan Geografi | http://geografi.fkip.unsyiah.ac.id/ | Aktif |
| Pendidikan Sendratasik | http://seni.fkip.unsyiah.ac.id/ | Aktif |
| Pend. Bahasa & Sastra Indonesia | http://pbsi.fkip.unsyiah.ac.id/ | Aktif |
| Pend. Bahasa Inggris | http://english.fkip.unsyiah.ac.id/ | Aktif |
| 7 | Kedokteran | Pendidikan Dokter | - | - |
|  |  | Prodi Psikologi | - | - |
| Ilmu Penyakit Dalam | http://penyakitdalam.unsyiah.ac.id/ | Aktif |
| Ilmu Bedah | - | - |
| Ilmu Obgyn | - | - |
| Ilmu Kesehatan THT-KL | - | - |
| Pulmonologi | - | - |
| Anestesiologi | - | - |
| Kardiology | - | - |
| Ilmu Kesehatan Anak | - | - |
| Neurologi | http://neurologi.unsyiah.ac.id/ | Aktif |
| Ilmu Kesehatan Masyarakat | - | - |
| 8 | Matematika dan Ilmu Pengetahuan Alam | Matematika | http://math.unsyiah.ac.id/ind/ | Aktif |
|  |  | Fisika | http://fisika.unsyiah.ac.id/ | Aktif |
| Kimia | http://chem.unsyiah.ac.id/ | Aktif |
| Biologi | http://biologi.unsyiah.ac.id/ | Aktif |
| Informatika | http://informatika.unsyiah.ac.id/ | Aktif |
| Farmasi | http://farmasi.unsyiah.ac.id/ | Aktif |
| Statistika | http://stat.unsyiah.ac.id/ | Aktif |
| S2 Matematika | http://www.m-math.unsyiah.ac.id/ | Aktif |
| S2 Kimia | - | - |
| S2 Fisika | - | - |
| S2 Biologi | - | - |
| D3 Manajemen Informatika | http://d3-mi.unsyiah.ac.id/id/ | Aktif |
| D3 Teknik Elektronika | - | - |
| 8 | Ilmu Sosial dan Ilmu Politik | Ilmu Politik | http://ilmupolitik.fisip.unsyiah.ac.id/ | Aktif |
|  |  | Ilmu Komunikasi | http://ilkom.fisip.unsyiah.ac.id/ | Aktif |
| Sosiolog | http://sosiologi.fisip.unsyiah.ac.id/ | Aktif |
| Ilmu Pemerintah | http://ipm.fisip.unsyiah.ac.id/ | Aktif |
| 9 | Kelautan dan Perikanan | Ilmu Kelautan | http://www.kelautanperikanan.unsyiah.ac.id/ | Aktif |
|  |  | Budidaya Perairan | - | - |
| Pemanfaatan Sumber Daya Perikanan | - | - |
| 10 | Kedokteran Gigi | Kedokteran Gigi | http://fkg.unsyiah.ac.id | Tidak aktif |
| 11 | Keperawatan | Spesialis Keperawatan | http://www.fkep.unsyiah.ac.id/ | Aktif |
|  |  | Profesi Ners | - | - |
|  |  | Ilmu Keperawatan | - | - |
|  |  | Magister Keperawatan | - | - |