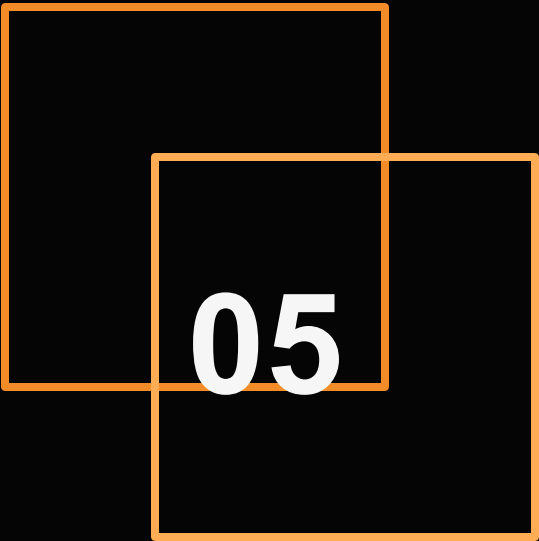


KEAMANAN SISTEM INFORMASI

Pertemuan 5

Authentication, Authorization, dan Accountability

Identitas yang benar, akses yang tepat, dan tindakan yang dapat ditelusuri



05

Posisi Pertemuan 5 dalam RPS



Sub-CPMK-3 · Konsep Authentication, Authorisation, dan Accountability

Minggu	Fokus pembelajaran	Status
1	Konsep dasar keamanan informasi	SELESAI
2	Keamanan sistem dan jaringan	SELESAI
3	Ancaman dan pengamanan jaringan	SELESAI
4	Hukum, kebijakan, privasi, dan regulasi	SELESAI
5	Authentication, Authorization, Accountability	SAAT INI

Target Pembelajaran



Kemampuan yang perlu ditunjukkan mahasiswa setelah pertemuan

01 Membedakan komponen AAA

Menjelaskan fungsi authentication, authorization, dan accountability pada sebuah sistem.

02 Menilai mekanisme login

Mengenali faktor autentikasi, MFA, sesi, dan kelemahan yang umum terjadi.

03 Menentukan hak akses

Memilih model kontrol akses dan menerapkan prinsip least privilege.

04 Menyusun bukti akuntabilitas

Menentukan peristiwa yang perlu dicatat dan informasi sensitif yang tidak boleh masuk log.

Model IAAA

Identity mendahului tiga komponen AAA



Urutan logis: kenali identitas, verifikasi, batasi akses, lalu catat aktivitas.

Perbedaan Authentication, Authorization, dan Accountability



Ketiga proses menjawab pertanyaan yang berbeda

Authentication

Pertanyaan:
Apakah Anda benar-benar pemilik identitas ini?

Contoh:
Password, OTP, passkey, atau biometrik.

Authorization

Pertanyaan:
Apakah identitas ini boleh melakukan tindakan tersebut?

Contoh:
Mahasiswa boleh melihat nilainya sendiri.

Accountability

Pertanyaan:
Dapatkah aktivitas pengguna ditelusuri?

Contoh:
Log mencatat pengguna, waktu, objek, dan hasil.

Berhasil login tidak berarti pengguna boleh mengakses seluruh data.

Siklus Hidup Identitas Digital



Identitas perlu dikelola sejak dibuat sampai aksesnya dihentikan

01

Daftar

Identitas dibuat dan informasi awal diperiksa

02

Aktif

Autentikator diberikan dan akses disetujui

03

Berubah

Peran, unit, atau kebutuhan akses diperbarui

04

Ditinjau

Hak akses dan aktivitas diperiksa berkala

05

Dicabut

Akun, token, dan sesi dihentikan

Akun yang tidak lagi diperlukan tetap menjadi risiko jika tidak dicabut.

Faktor Autentikasi



Multi-Factor Authentication (Autentikasi Multi-Faktor), menggunakan faktor yang berbeda, bukan dua bukti dari jenis yang sama



Tahu

Sesuatu yang diketahui

Password atau PIN



Punya

Sesuatu yang dimiliki

Token, ponsel, atau kunci keamanan



Diri

Sesuatu yang melekat

Sidik jari atau pengenalan wajah

Password + PIN masih satu faktor karena keduanya sama-sama diketahui.

Authentication Assurance Level



NIST SP 800-63B-4 membagi tingkat keyakinan autentikasi menjadi AAL1, AAL2, dan AAL3

AAL1

Keyakinan dasar

Satu faktor dapat digunakan. Cocok untuk risiko rendah.

AAL2

Keyakinan tinggi

Memerlukan dua faktor berbeda. Menuntut perlindungan lebih kuat.

AAL3

Keyakinan sangat tinggi

Menggunakan autentikator kriptografis dengan perlindungan yang lebih ketat.

PANDUAN AKTIVASI

Multi-Factor Authentication (MFA) dengan Microsoft Authenticator

Ikuti panduan berikut untuk mengaktifkan MFA dan meningkatkan keamanan akun Microsoft Anda

PANDUAN AKTIVASI

1 Login ke Akun Microsoft

Buka laman **office.com** dan login menggunakan akun Microsoft Tel-U yang anda miliki



2 Laman Aktivasi MFA

Laman ini merupakan proses awal aktivasi MFA



Pilih **Next** untuk melanjutkan pengaturan

3 Install Aplikasi

Install Aplikasi Microsoft Authenticator pada perangkat seluler Anda



4 Tambah Akun Work School

Add Work School Account pada aplikasi Microsoft Authenticator



5 Scan QR Code

Pilih opsi Scan QR Code lalu arahkan perangkat ke barcode di laman aktivasi



6 Notifikasi Approve MFA

Akan muncul notifikasi **Approve** baik dalam bentuk **Approve** atau **Matching Number** untuk konfirmasi penambahan akun.



7 MFA berhasil diaktifkan

Jika sudah muncul notifikasi **Authenticator Added**, proses aktivasi sudah berhasil.



MOHON DIPERHATIKAN!

- Jangan pernah menyetujui Notifikasi jika Anda tidak merasa melakukan login ke Microsoft
- Jangan menghapus Aplikasi Authenticator, jika terhapus maka perlu mengajukan reset MFA ke Service Desk



Panduan Aktivasi:

s.telkomuniversity.ac.id/aktivasisma

Butuh bantuan?

☎ 0823 1994 9941

📧 servicedesk.telkomuniversity.ac.id

Top 5 authenticator apps to use with WP 2FA



 melapress

1. Google Authenticator
2. Microsoft Authenticator
3. Authy
4. Autentikator LastPass Duo

Praktik Password Modern



Panjang, pemeriksaan terhadap password bocor, dan perlindungan serangan otomatis lebih penting daripada aturan rumit

01 Panjang minimum

Gunakan minimal 15 karakter untuk password sebagai faktor tunggal. Jika MFA wajib, minimal 8 karakter.

02 Password bocor

Tolak password yang ditemukan pada daftar password umum atau yang telah bocor.

03 Password manager

Izinkan paste dan dukung penggunaan password manager.

04 Serangan otomatis

Terapkan rate limiting, deteksi anomali, dan perlindungan percobaan berulang.

MFA dan Autentikasi Tahan Phishing



Tidak semua faktor kedua memberikan perlindungan yang sama

01 SMS atau OTP

Meningkatkan keamanan, tetapi masih dapat dicuri melalui phishing atau pengambilalihan nomor.

02 Aplikasi autentikator

Kode berbasis waktu lebih baik daripada password saja, tetapi masih dapat dimasukkan ke situs palsu.

03 Passkey atau security key

Menggunakan kriptografi kunci publik dan terikat pada situs yang benar.

Akun berisiko tinggi memerlukan autentikasi yang lebih tahan terhadap phishing.

Manajemen Sesi



Sesi mempertahankan status pengguna setelah proses login selesai



Login

Sistem memverifikasi
autentikator



Buat sesi

Server menerbitkan
session identifier



Gunakan

Identifier menyertai
permintaan berikutnya



Akhiri

Logout, kedaluwarsa,
atau pencabutan

Risiko utama

Session identifier yang dicuri dapat memberi akses meskipun penyerang tidak mengetahui password.

Keputusan Authorization



Izin akses ditentukan untuk subjek, tindakan, sumber daya, dan konteks tertentu

01

Subjek

Siapa yang meminta akses?

Mahasiswa 23001

02

Tindakan

Apa yang ingin dilakukan?

Melihat atau mengubah

03

Sumber daya

Objek mana yang diminta?

Nilai, KRS, atau profil

04

Konteks

Kondisi apa yang berlaku?

Waktu, lokasi, risiko

Keputusan akses harus diperiksa pada sisi server untuk setiap permintaan.

Model Kontrol Akses



Model dipilih berdasarkan kebutuhan organisasi dan karakter sumber daya

DAC

Pemilik objek menentukan siapa yang mendapat akses.

Berbagi dokumen

MAC

Akses mengikuti label dan klasifikasi yang ditetapkan pusat.

Data rahasia

RBAC

Hak akses melekat pada peran pekerjaan.

Dosen, mahasiswa, admin

ABAC

Keputusan memakai atribut subjek, objek, tindakan, dan konteks.

Akses adaptif

Least Privilege dan Default Deny



Akses diberikan secukupnya dan penolakan menjadi kondisi awal

LEAST PRIVILEGE

Pengguna hanya menerima izin yang dibutuhkan untuk menjalankan tugasnya.

Hak akses memiliki pemilik, alasan, masa berlaku, dan proses peninjauan.

DEFAULT DENY

Permintaan ditolak jika tidak ada aturan yang secara jelas mengizinkannya.

Aplikasi tidak mengandalkan menu tersembunyi atau keputusan pada sisi pengguna.

Eskalasi Hak Akses



Kelemahan authorization dapat memberikan akses horizontal atau vertikal

Horizontal

Pengguna mengakses sumber daya milik pengguna lain dengan tingkat peran yang sama.

Contoh:

Mahasiswa A mengubah ID pada URL lalu melihat nilai Mahasiswa B.

Vertikal

Pengguna memperoleh fungsi yang seharusnya hanya tersedia untuk peran lebih tinggi.

Contoh:

Mahasiswa membuka fungsi perubahan nilai milik dosen atau admin.

Accountability dan Audit Trail



Catatan aktivitas membantu rekonstruksi kejadian dan penentuan tanggung jawab

1

Siapa

user_id dan peran

2

Kapan

waktu tersinkron

3

Apa

tindakan dan objek

4

Dari mana

sumber atau perangkat

5

Hasil

berhasil atau gagal

Audit trail yang baik

lengkap, konsisten, terlindungi, memiliki retensi, dan dapat dikorelasikan antar sistem

Peristiwa yang Perlu Dicatat



Catat peristiwa keamanan tanpa menyimpan rahasia autentikasi

CATAT

- login berhasil dan gagal
- perubahan password atau MFA
- perubahan peran dan hak akses
- akses ke data sensitif
- tindakan administrator
- kegagalan pemeriksaan authorization

JANGAN CATAT

- password dalam bentuk apa pun
- OTP dan recovery code
- token sesi lengkap
- kunci privat atau secret key
- data pribadi yang tidak diperlukan
- informasi pembayaran lengkap

Tujuan logging menentukan tingkat detail, retensi, dan pihak yang boleh mengakses log.

Kegagalan IAAA pada OWASP Top 10:2025



TryHackMe menggabungkan tiga kategori untuk latihan pemula

01 A01 Broken Access Control

Pemeriksaan izin tidak konsisten atau tidak dilakukan pada sisi server.

Dampak: pengguna membaca atau mengubah sumber daya tanpa izin.

07 A07 Authentication Failures

Sistem gagal memverifikasi atau mengikat identitas secara andal.

Contoh: enumerasi, password lemah, dan kelemahan sesi.

09 A09 Logging & Alerting Failures

Aktivitas penting tidak tercatat atau tidak menghasilkan peringatan.

Dampak: serangan sulit dideteksi dan ditelusuri.

Ketiga kategori tersebut menjadi inti tugas praktik TryHackMe.

Studi Kasus Sistem Akademik



Tentukan akses yang tepat untuk setiap peran

Sumber daya	Mahasiswa	Dosen	Admin akademik
Profil mahasiswa	Lihat dan ubah milik sendiri	Lihat peserta kelas	Koreksi data administratif
KRS	Ajukan dan lihat milik sendiri	Setujui sebagai dosen wali	Kelola periode dan status
Nilai	Lihat milik sendiri	Isi mata kuliah yang diampu	Buka periode dan audit perubahan
Audit log	Tidak langsung	Lihat aktivitasnya sendiri	Akses terbatas sesuai tugas

Pertanyaan: pemeriksaan apa yang mencegah mahasiswa melihat nilai milik mahasiswa lain?

Tugas Praktik TryHackMe



Room: OWASP Top 10 2025: IAAA Failures

TUJUAN

Menguji secara langsung bagaimana kegagalan identity, authentication, authorization, serta logging memengaruhi keamanan aplikasi web.

Room resmi

<https://tryhackme.com/room/owasptopten2025one>

Dikerjakan berpasangan · satu akun per mahasiswa

BATAS ETIKA

Seluruh percobaan hanya dilakukan pada mesin atau situs latihan yang disediakan TryHackMe.

Dilarang mencoba teknik yang sama pada sistem kampus, website publik, atau target lain tanpa izin tertulis.

Bobot tugas: bagian dari penilaian Sub-CPMK-3 sebesar 5%

1

[Back to all walkthroughs](#)

OWASP Top 10 2025: IAAA Failures

Learn about A01, A07, and A09 in how they related to failures in the applied IAAA model.

30 min 74,300

[Save Room](#) [408 Recommend](#) [Connectivity](#) [Options](#)

Room progress: 22%

Task 1 Introduction

Task 2 What is IAAA?

Task 3 A01: Broken Access Control

Broken Access Control happens when the server doesn't properly enforce **who can access what** on every request. A common occurrence of this is **IDOR** (Insecure Direct Object Reference): if changing an ID (like `?id=7` to `?id=6`) lets you see or edit someone else's data, access control is broken.

View Site

In practice this shows up as horizontal privilege escalation (same role, other user's stuff) or vertical privilege escalation (jumping to admin-only actions) because the application trusts the client too much.

Start the static site attached to this task and play with the `accountID` value in the URL. So if you can identify which user has more 1 million in their account!

`https://bank.thm/accounts?id=7`

THM{Found.the.Millionare!}
Account ID: 7

Account Number
******6789**

Account Balance
\$ 1,234,567.89

Vulnerability Detected

This application contains an **Insecure Direct Object Reference (IDOR)** vulnerability. By simply changing the ID parameter in the URL, you can access other users' account information without proper authorization checks.

Try changing the `id` value in the URL bar above to view different accounts (1-10).

How to Fix This Vulnerability

- Implement proper authentication and authorization checks
- Verify that the authenticated user has permission to access the requested resource
- Use indirect references or encrypted tokens instead of predictable IDs
- Log and monitor access attempts to sensitive resources

Langkah Pengerjaan Tugas



Ikuti urutan dan simpan bukti sejak awal

- 01 Persiapan** Buat akun, tulis username, nama, NPM, dan anggota kelompok.

- 02 Selesaikan room** Kerjakan seluruh task pada OWASP Top 10 2025: IAAA Failures.

- 03 Ambil bukti** Simpan tangkapan layar progres dan interaksi penting. Tampilkan username.

- 04 Analisis** Petakan A01, A07, dan A09 ke komponen IAAA serta kontrol perbaikannya.

- 05 Refleksi** Setiap anggota menulis pelajaran pribadi dan satu usulan kontrol untuk sistem kampus.

Luaran & Rubrik Penilaian



Kumpulkan satu PDF kelompok dan bukti progres akun setiap anggota

Komponen	Kriteria	Nilai
Penyelesaian room	Progres akun masing-masing anggota terlihat dan dapat diverifikasi	25
Bukti praktik	Tangkapan layar relevan, diberi nomor, waktu, dan keterangan	20
Analisis IAAA	Pemetaan A01, A07, A09 serta penjelasan penyebab dan dampak	25
Usulan kontrol	Perbaikan authentication, authorization, logging, dan alerting	20
Refleksi individu	150 sampai 200 kata per anggota dan terkait pengalaman praktik	10

Jawaban flag tanpa bukti proses dan analisis tidak memperoleh nilai penuh. Dikumpulkan di Ilmu setiap mahasiswa

Ringkasan Pertemuan 5



AAA menghubungkan identitas, izin akses, dan bukti aktivitas

01 Authentication

Verifikasi identitas menggunakan autentikator dan tingkat keyakinan yang sesuai dengan risiko.

02 Authorization

Periksa izin pada sisi server untuk setiap tindakan dan terapkan least privilege.

03 Accountability

Catat peristiwa penting, lindungi log, dan gunakan alert untuk mendeteksi penyimpangan.

Exit ticket

Mengapa login yang berhasil belum cukup untuk melindungi data pada sistem akademik?

Pertemuan berikutnya: Evaluasi keamanan informasi menggunakan Indeks KAMI 5.0