



Pemograman Web

2022/2023 Genap

Febri Damatraseta Fairuz, S.T., M.Kom



Rules in class room

- **MATERIAL AND ASSIGNMENT**
Materi, pengumpulan Tugas, dan Informasi kelas menggunakan **LMS** dan **GITHUB**.

Source code :

<https://github.com/FebryFairuz/IBIK-20222023-GENAP-PW>

Rules in class room



- **ATTENDANCE**
 - Minimum 30 minutes (setelah jadwal) sudah hadir diruangan dan bisa absen.
 - Maximum **ALPHA** sebanyak 5x, Jika melewati batas **AUTO RETAKE SUBJECT**.
- **ASSESSMENT**

Tugas Individu/Kelompok , Quiz (3x), Praktikum.

Rules in class room

- **EXAMINATION TEST**
UTS : Tertulis & Open Book

UAS : PROJECT FINAL & COMPREHENSIVE
KELOMPOK Minim 4 orang



Materials

01 Introduction

Type of Website and Web Security

02 Web Components

HTML, CSS, JS,
Web Dinamic

03 Monolith

Architecture model of
Monolith

04 PHP Framework

Introduction about
Laravel

05 Dev 1

Route, Session and layout

06 Dev 2

Create, Update and
Delete

Materials

07

React & Laravel

Combine React
Framework & Laravel

08

Project Phase 1

Introduction the themes
of project using UML

09

Project Phase 2

Progres 1

10

Project Phase 3

Progres 2

11

Project Final 1

Final Presentation
Test Compre

12

Project Final 2

Final Presentation
Test Compre



01

Website Introduction

You can enter a subtitle here if you need it



Website

World Wide Web (WWW)

Pengertian

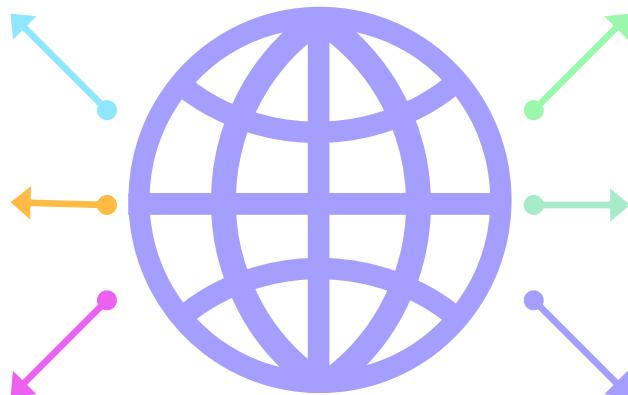
Merupakan sekumpulan dokumen, gambar-gambar, dan bentuk resources yang lainnya yang dihubungkan melalui hyperlinks dan URLs.

Internet

Sebuah sistem komunikasi global yang menghubungkan komputer-komputer dan jaringan-jaringan komputer di seluruh dunia.

Protocol

TCP/IP (Transmission Control Protocol Internet Protocol) merupakan cara standar untuk memaketkan dan menyelamatkan data komputer (sinyal elektronik) sehingga data tersebut dapat dikirim ke komputer yang lain.



HTTP

Adalah protokol yang menentukan aturan yang perlu diikuti oleh web browser dalam meminta dan mengambil suatu dokumen dan oleh web server dalam menyediakan dokumen yang diminta web browser.

URL

Digunakan untuk menentukan lokasi informasi pada suatu web server.

DNS

Adalah suatu sistem penamaan standar komputer-komputer di internet dengan tujuan untuk mempermudah pengelolaan server komputer internet



Website Transferring Data



Internet

Memiliki koneksi kedalam jaringan interkoneksi seperti menggunakan telepon, fyber-optic atau wireless

HTTP

Memerintahkan untuk mengirim kode pengiriman data (POST) kedalam tuan rumah

TCP/IP

Menerima kode POST permintaan

URL

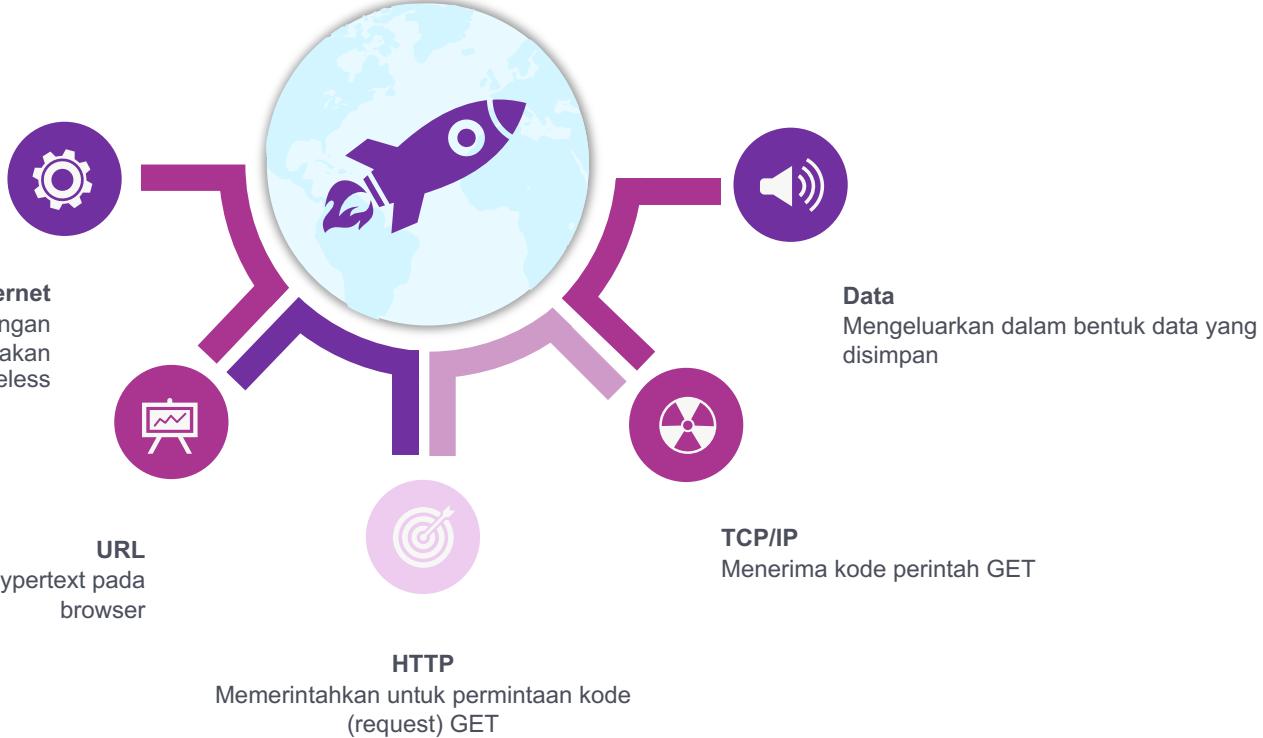
Mengeluarkan hasil data dalam bentuk url

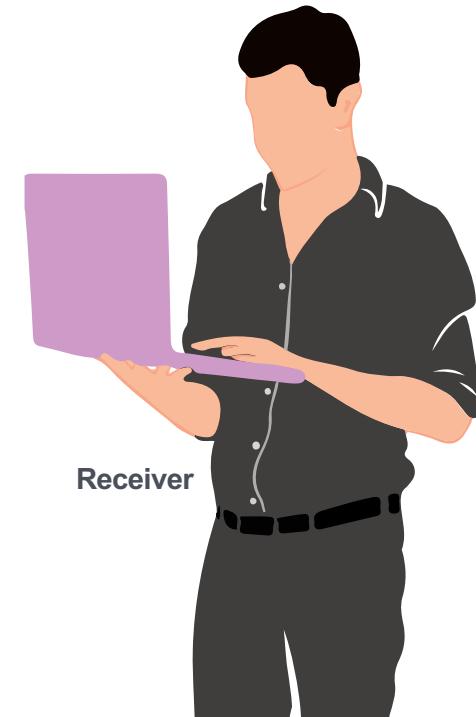
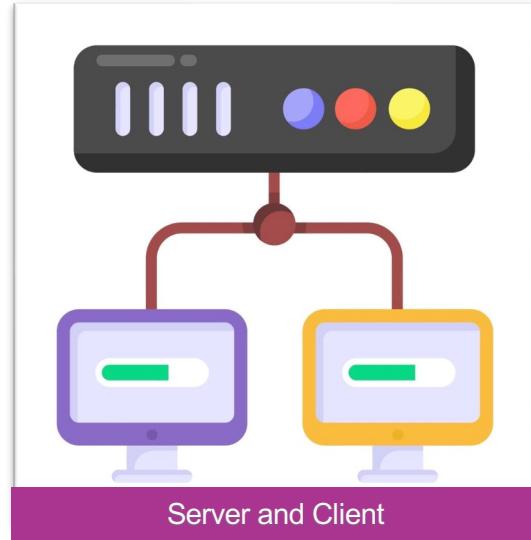
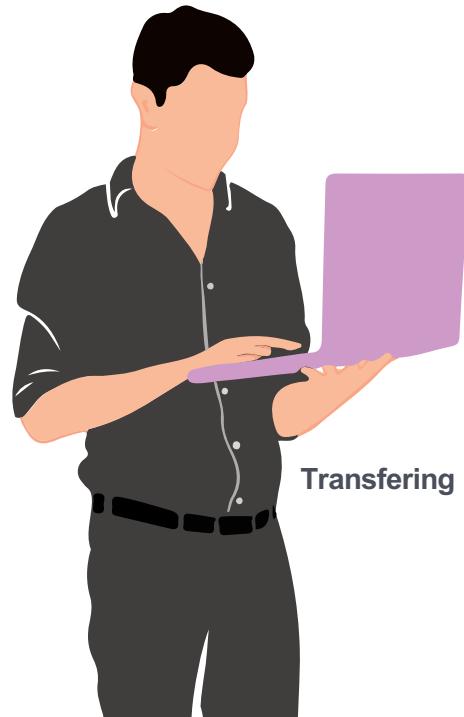
FTP

Memasukan data kedalam server



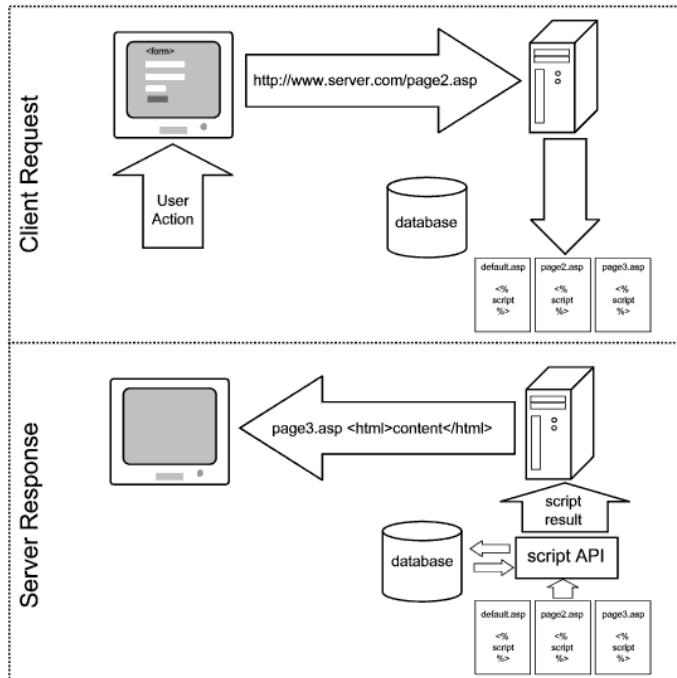
Website Receiving Data





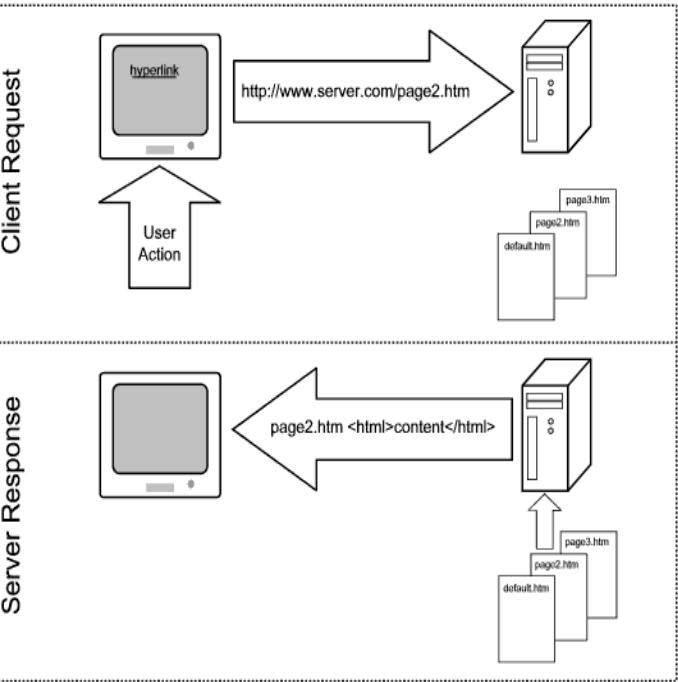


Server side programming



Web server melakukan *parse* dan eksekusi sehingga *script embedded* kedalam halaman web

Contoh: Perl, ASP, JSP, PHP, JAVA, Phyton



Client side programming

Web browser melakukan parse dan eksekusi sehingga script embedded kedalam halaman web

Contoh: JavaScript, HTML, VBScript



Types of Websites

01



Website Statis

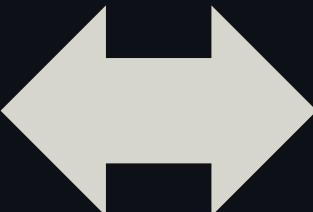
website yang kontennya konstan atau tidak berubah

02



Website Dinamic

website yang kontennya selalu di-update secara berkala





Static Website



Types of Websites

Website

Built with a minimal no. of tools and need only **static HTML** files, **CSS** styles, & possibly **JavaScript**.



Dynamic Web App



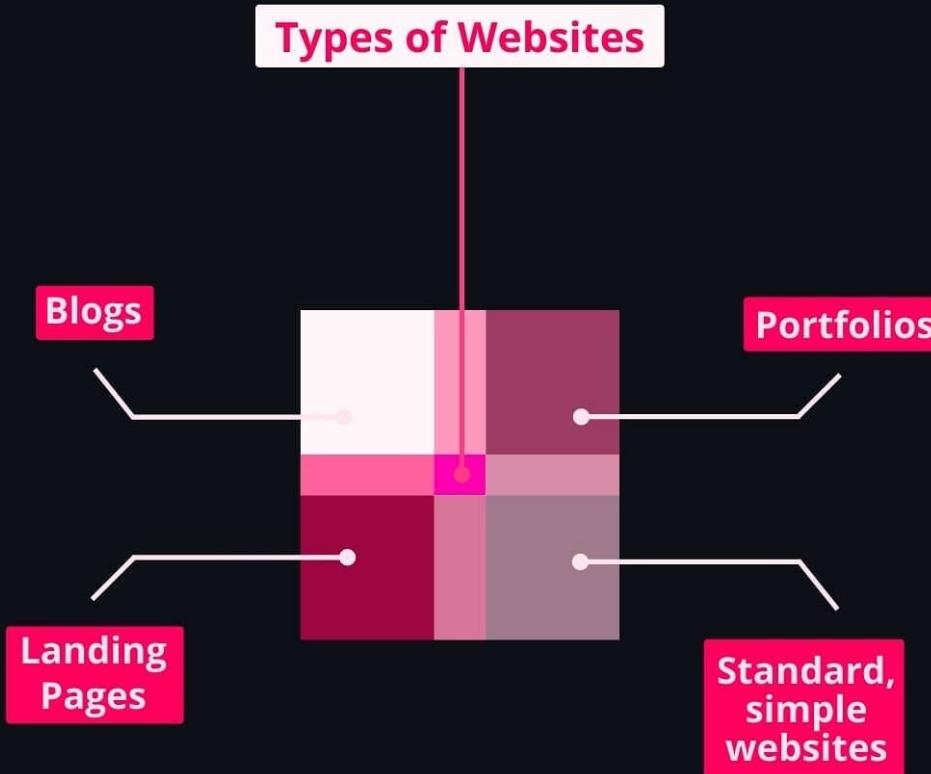
Web App

Web applications, except **frontend**, require **complex backend**, which is built using various technologies.



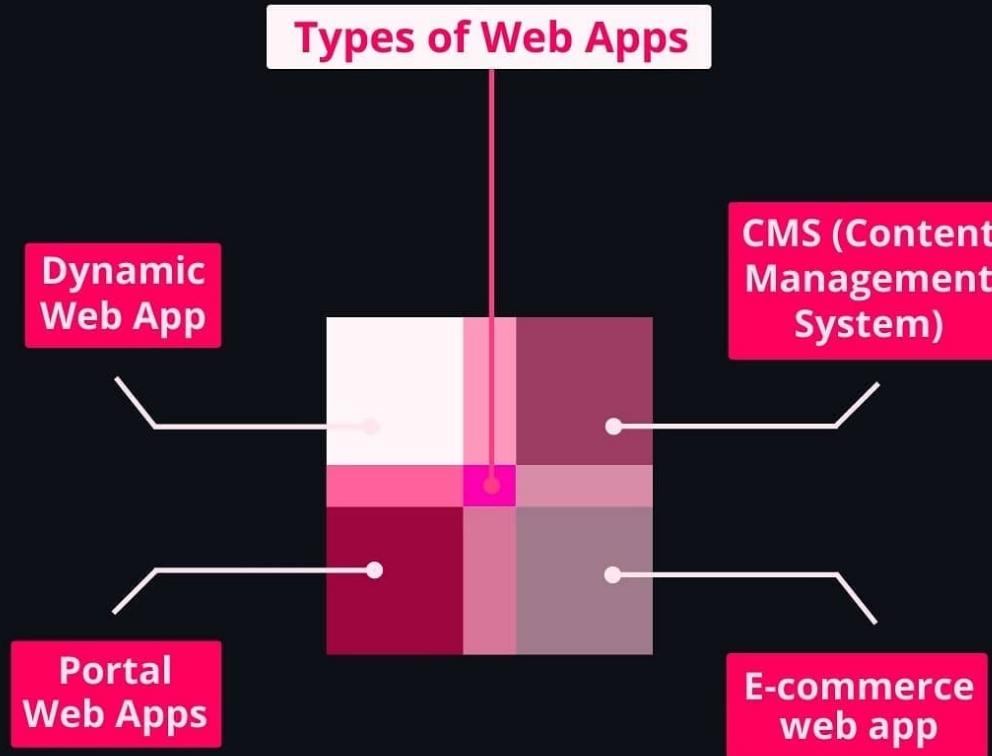


Types of Websites





Types of Websites





Types of Websites

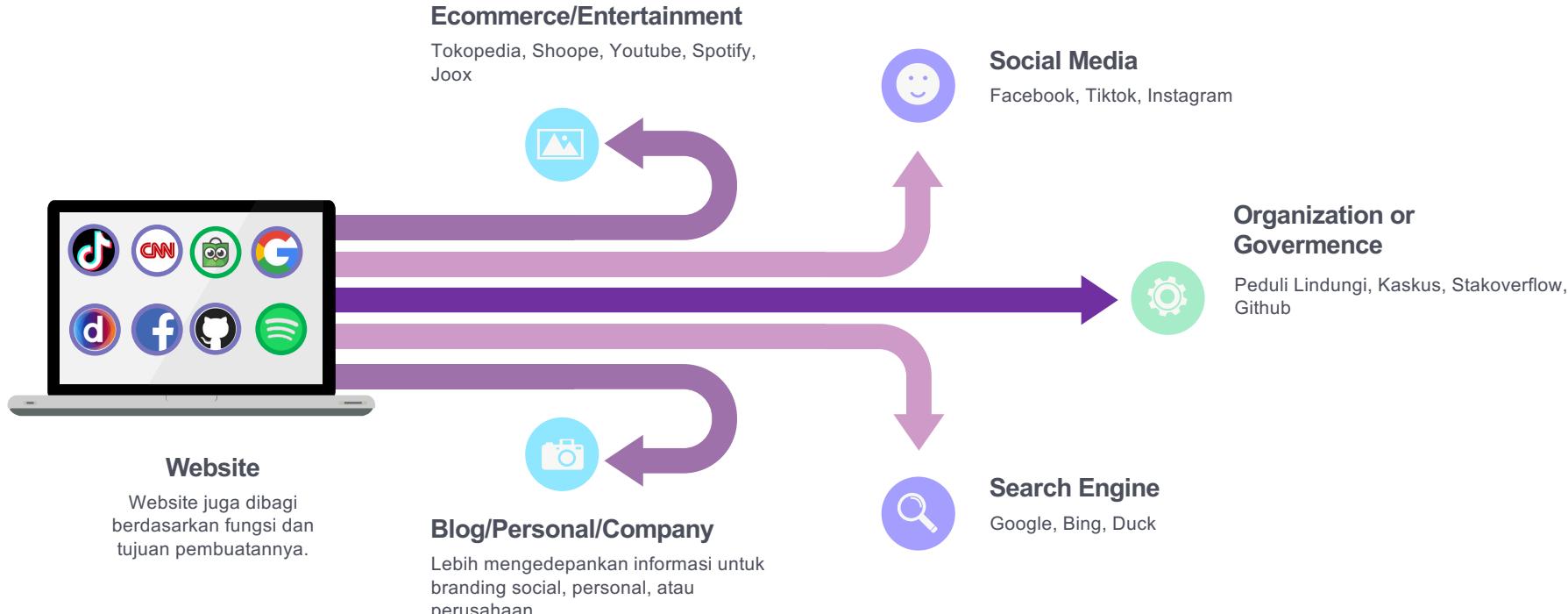
Websites do not need to set up a verification process because users do not interact with the content.



Web app, where users can create content, transmit sensitive information, & send private messages, authorization is required



Types of Websites by function





Timeline Website

1991



Web 1.0

Pada timeline ini website hanya bersifat **READ-ONLY**. User merupakan konsumen utama

Web 1.0
Layaknya seperti media penyimpanan informasi seperti Buku namun sudah digital

Web 2.0
Era website sudah muncul media seperti video, suara, social media, dan AI.

Web 3.0
Era website menggunakan teknologi blockchain dan cetralization. Mulai muncul uang digital, seperti NFT

2022-now

2004



Web 2.0

Era ini mengedepankan 'iklan' sebagai consumer utamanya. Dengan menjual data User kepada media. Kelemahan era ini ialah tidak adanya privacy. User pada era ini adalah Product.

2014



Web 3.0

User adalah pemilik dari setiap konten. Kelebihannya adanya scaming identitas



02

Developer Principles & Language

Type of developer & programming language



**Kampus
Merdeka**
INDONESIA JAYA



Web Designer / Frontend Developer

Menganalisa website

Creative & Artistic

Menggunakan otak
kanan

Designer

Salary \$64 USD



Web Developer / Backend Developer

Membangun website

Functional & Logical

Menggunakan otak kiri

Programmer

Salary \$70 USD



Programming Language

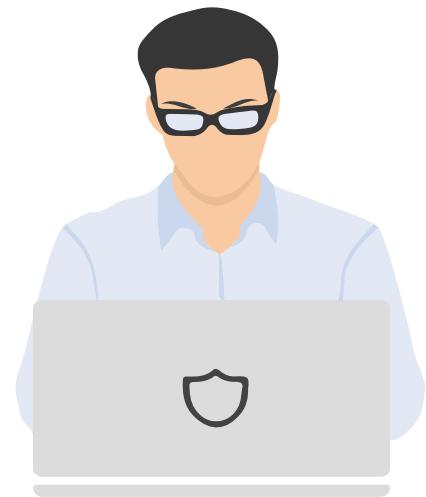
Base on Web Programming



Kampus
Merdeka
INDONESIA JAYA

Programming Language

Base on Programmer Web



Fullstack-Developer



Programming Language

Base on Programmer Web

Front-end	Back-end
FRONT-END LANGUAGES   	BACK-END LANGUAGES    
FRONT-END FRAMEWORKS    	BACK-END FRAMEWORKS    
USER ADMINISTRATION Part of website user can see and interact with.	ADMIN ADMINISTRATION In this everything happen behind the scene admin level.
DATABASE No database needed. Data stored in root directory.	DATABASE Database is needed and web server to manage data in DB.
APPLICATION Client Side Application.	APPLICATION Server Side Application.



Front End Dev

Skill Basic

HTML, JS, CSS,
UI / UX

Monolith

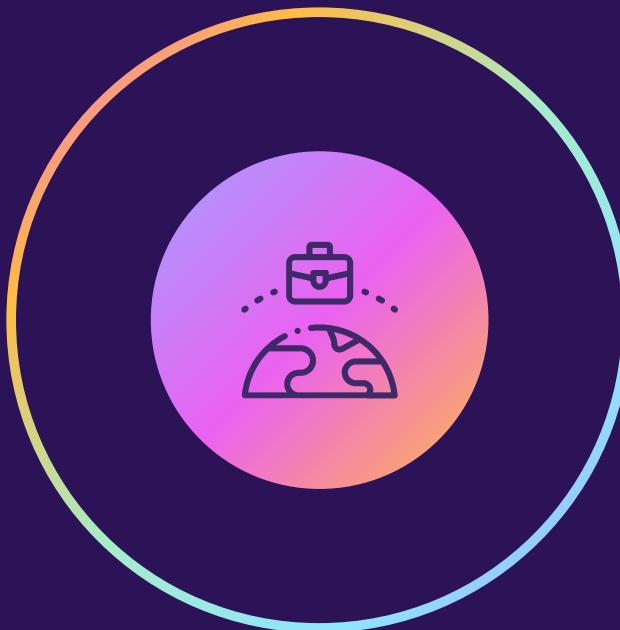
Apps yang dibangun
dalam 1 codebase

Web Apps

Frontend
Frameworks

Web Designer

Adobe XD, Figma,
Photoshop,
Illustrations





UI / UX

User Interface (UI)

Merupakan desain antarmuka yang fokus pada keindahan dari sebuah tampilan, dan pemilihan warna yang baik. Tujuannya, untuk membuat tampilan situs lebih enak dipandang mata dan pengunjung pun jadi betah berlama-lama.



User Experience (UX)

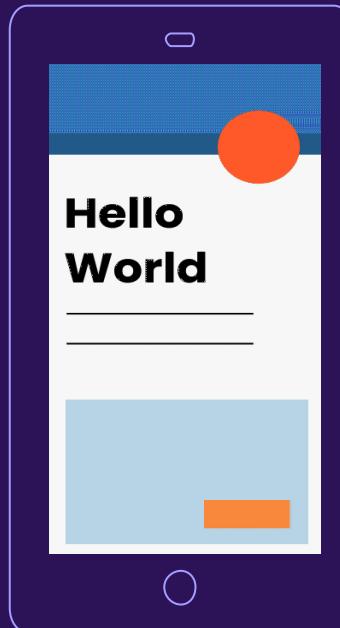
Merupakan proses meningkatkan kepuasan pengguna aplikasi tertentu melalui kegunaan dan kesenangan yang diberikan dalam interaksi antara pengguna dan produk. UX bertanggung jawab terhadap aplikasi yang bisa digunakan dengan mudah, sehingga tidak membingungkan pengguna. UX mencakup keseluruhan komponen elemen dari suatu aplikasi.

UI Principles

UI Principles

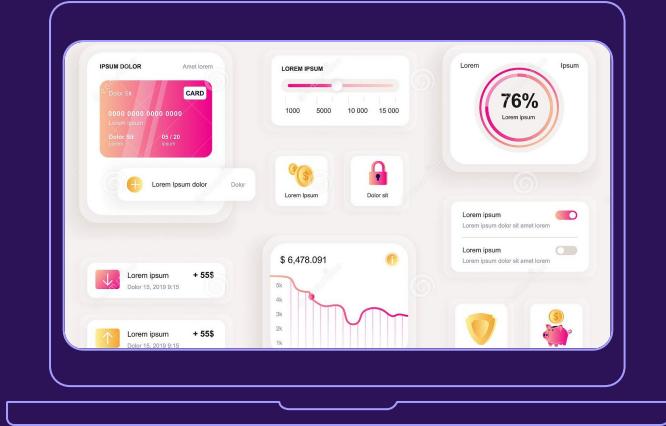
COLORS

Pelajari dasar-dasar warna dan psikologi warna. Warna pada aplikasi biasanya terbagi menjadi tiga buah kategori yaitu Warna **Primer**, **Sekunder** dan **Tersier**.



UI Principles

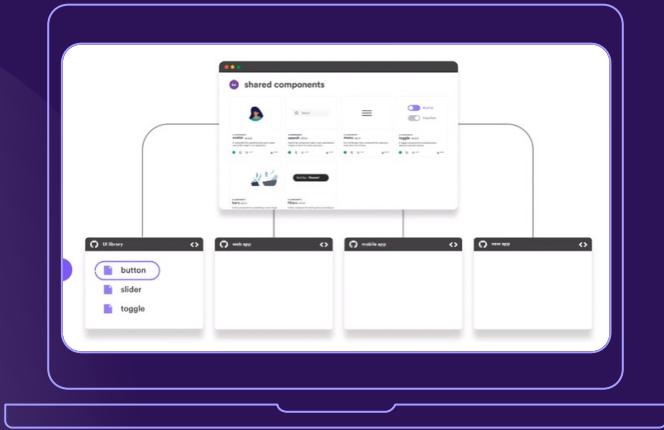
Kampus
Merdeka
INDONESIA JAYA



BALANCE

Membuat desain yang seimbang dengan memperhatikan *CONTRAST* dan *TYPOGRAPHY* seperti tentunya memilih font huruf yang mudah dibaca

UI Principles



Kampus
Merdeka
INDONESIA JAYA



CONSISTENT

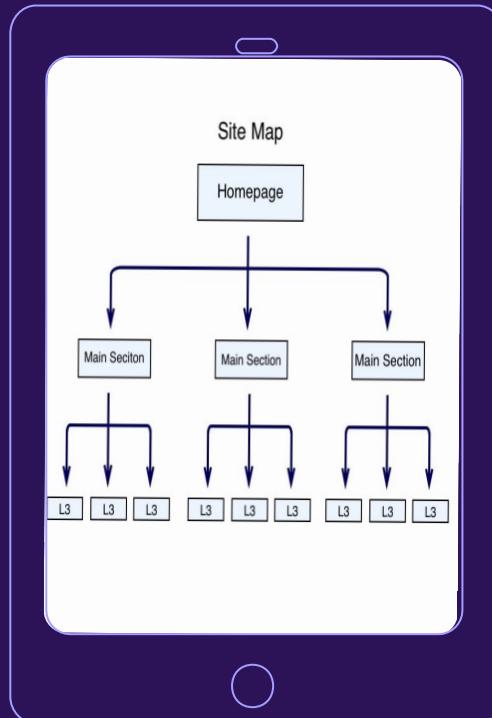
Konsisten terhadap bentuk komponen layout
dari 1 frame ke frame lain.
Dan konsisten terhadap framework / library yang
digunakan

UX Principles

UX Principles

Hierarchy

1. Information architecture
2. Visual hierarchy



UX Principles

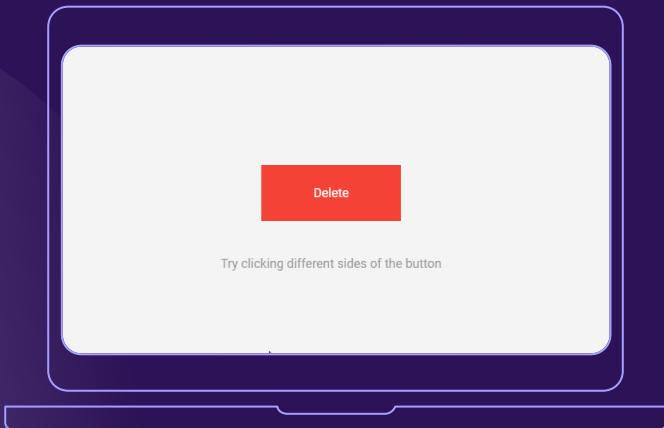
Kampus
Merdeka
INDONESIA JAYA



CONSISTENCY

Memiliki pola standart layout antar product.

UX Principles



Kampus
Merdeka
INDONESIA JAYA



CONFIRMATION

Mencegah terjadinya kesalahan informasi pada aplikasi adalah salah satu tujuan utama dari UX

UX Principles

User Control

Membantu pengguna dengan mudah untuk mundur atau kembali ke halaman awal atau tidak jadi melakukan transaksi.



UX Principles

Kampus
Merdeka
INDONESIA JAYA



ACCESSIBILITY

Merancang sebuah product yang dapat digunakan oleh banyak orang termasuk para disabilitas dengan sangat mudah

W3C and WAI

Programming Language



Client Side Programming

HTML



Hypertext Markup Language

bahasa markup standar yang digunakan untuk membuat halaman website dan aplikasi web.

Bahasa ini hanya bisa digunakan untuk menambah elemen dan membuat struktur konten

CSS



Cascading Style Sheets

berguna untuk menyederhanakan proses pembuatan website dengan mengatur elemen yang tertulis di bahasa markup.

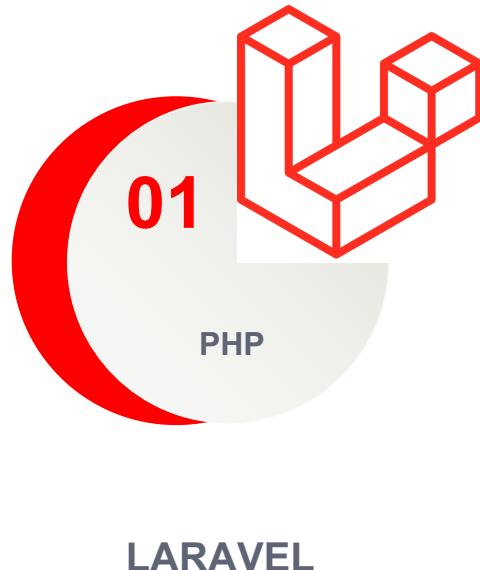
CSS dipakai untuk mendesain halaman depan atau tampilan website



JS

Javascript

digunakan untuk membuat situs dengan konten website yang dinamis dan interaktif. Bahasa pemrograman yang hanya bekerja dari sisi klien



Server Side Programming

Laravel adalah framework berbasis bahasa pemrograman PHP yang bisa digunakan untuk membantu proses pengembangan sebuah website agar lebih maksimal. Dengan menggunakan Laravel, website yang dihasilkan akan lebih dinamis.

Framework Laravel menggunakan struktur MVC (Model View Controller). MVC merupakan model aplikasi yang memisahkan antara data dan tampilan berdasarkan komponen aplikasi. Dengan adanya model MVC, pengguna Laravel menjadi lebih mudah dalam mempelajari Laravel. Serta menjadikan proses pembuatan aplikasi berbasis website menjadi lebih cepat.



Server Side Programming

MySQL merupakan sistem manajemen database yang bersifat open-source yang menggunakan perintah dasar atau bahasa pemrograman yang berupa structured query language (SQL) yang cukup populer di dunia teknologi.

SQL sendiri menjadi bahasa yang dipakai di dalam pengambilan data pada relational database atau database yang terstruktur. Dengan kata lain, MySQL merupakan database management system yang menggunakan bahasa SQL sebagai bahasa penghubung antara perangkat lunak aplikasi dengan database server.



**Kampus
Merdeka**
INDONESIA JAYA



PHP

Version 8.0.0



Composer

Version 2.5.4



Laravel

Version 10



VSCode

Text editor untuk code yang bersifat gratis buatan dari Microsoft



Browser Chrome

Aplikasi browser yang dikembangkan oleh google



Firefox

Aplikasi browser yang dikembangkan oleh Yayasan Mozilla

Programming Tools



03

Website

Security

You can enter a subtitle here if you need it



Web Security

Pengertian

Web security yang juga dikenal sebagai "cyber security" ini pada dasarnya berarti melindungi situs web atau aplikasi web dengan mendeteksi, mencegah, dan menangani ancaman dunia maya seperti hacker.

Tujuan

sebagai sistem tindakan perlindungan dan protokol yang dapat melindungi situs web atau aplikasi web kamu dari peretasan atau dimasuki oleh personel yang tidak berwenang.

Web Server

Security website biasanya dipasang pada server dari rumah website tersebut.



Data

Setiap komponen selalu dilindungi dengan berbagai protocol Ketika user melakukan request data.

Keamanan Deklaratif

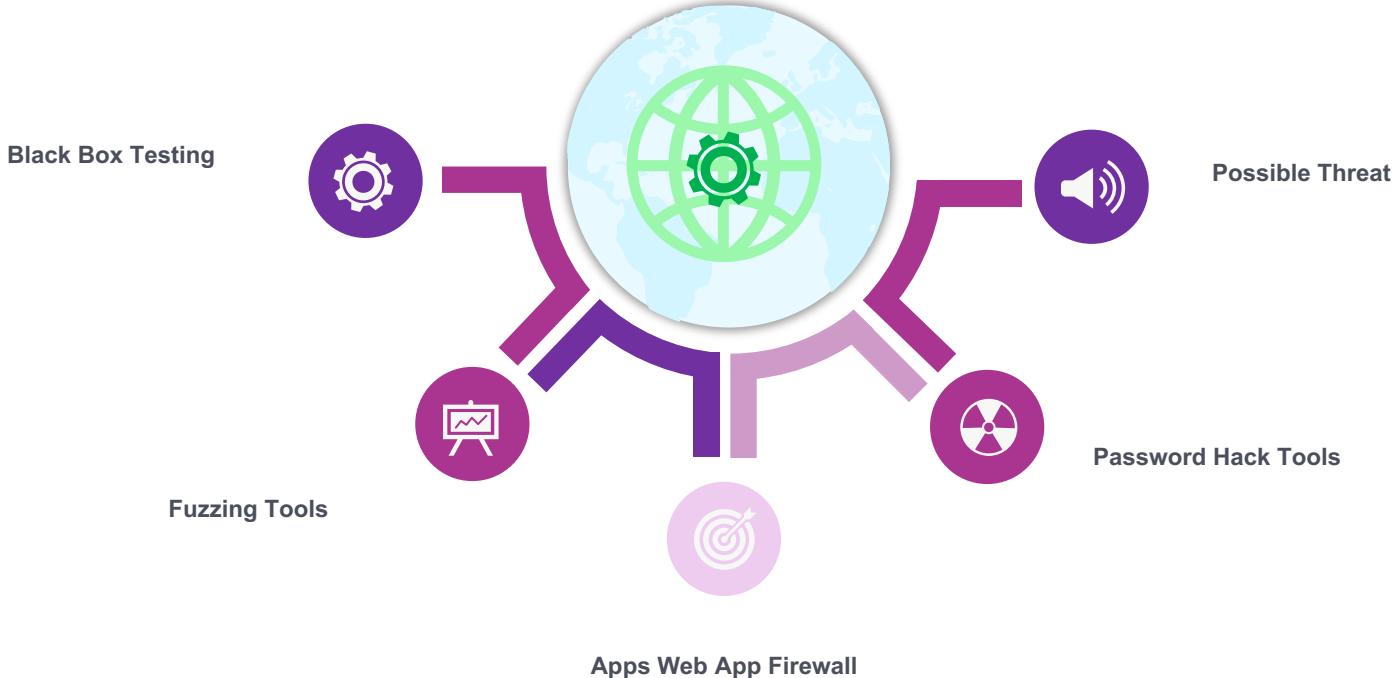
Keamanan ini diatur oleh system, hanya perlu menyiapkan sebuah script untuk mengeksekusinya.

Keamanan Program

Seluruh keamanan pada program sepenuhnya diatur oleh pembuat program.



Type of Web Security





Web Security - Threats

Cross-Site Scripting (XSS)

Metode ini adalah kerentanan yang memungkinkan penyerang memasukkan skrip sisi klien ke halaman web untuk mengakses informasi penting secara langsung, meniru identitas pengguna, atau mengelabui pengguna agar mengungkapkan informasi penting.

SQL Injection

Penyerang menggunakan SQI untuk mendapatkan akses ke informasi yang tidak sah, mengubah atau membuat izin pengguna baru, atau memanipulasi atau menghancurkan data sensitif.

Deface

ulah peretas yang masuk ke sebuah website dan mengubah tampilannya. Perubahan tersebut bisa meliputi semua halaman atau di bagian tertentu saja. Contohnya, font website diganti, muncul iklan mengganggu, hingga perubahan konten halaman secara keseluruhan.



Malware

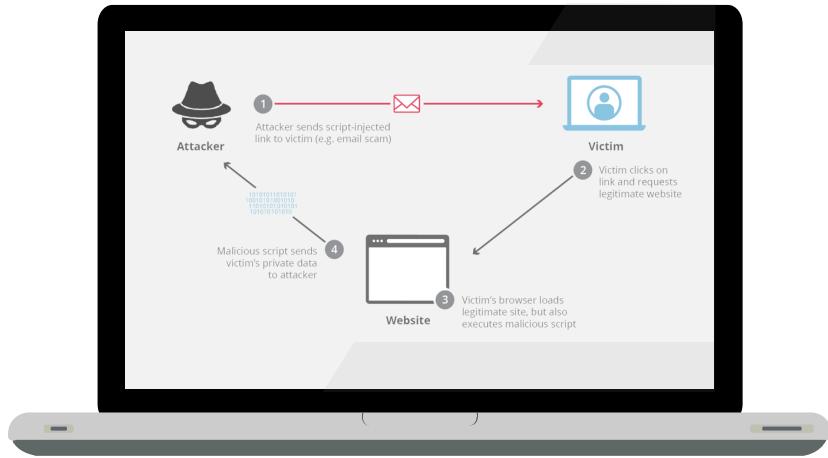
malicious software dalam kata bahasa inggris yang berarti program berbahaya. Malware adalah sebuah program yang didesain oleh hackers untuk mengeksplorasi dan merusak perangkat, server, maupun jaringan.

Buffer Overflow

anomali yang terjadi saat perangkat lunak menulis data ke ruang yang ditentukan dalam memori yang disebut buffer. Kapasitas buffer yang meluap menyebabkan lokasi memori yang berdekatan ditimpak dengan data.



Web Security - Threats



Contoh serangan dari XSS ialah seperti pencurian data dengan mengirimkan sebuah link website yang berisi script mencurigakan tanpa diketahui oleh korban. Setelah korban mengklik link tersebut ternyata data pribadi (seperti username dan password) dari korban atau target telah diambil atau dimiliki oleh sang pengirim link tersebut, yg disebut sebagai Attacker.

Serangan ini sering disebut dengan Phising Attacker.



Web Security – Threats

Cross-Site Scripting (XSS)

Contoh serangan XSS

01

Mengirim parameter kedalam URL

Menyisipkan parameter kedalam URL. Ini biasanya terjadi pada website yang tidak memiliki tingkat keamanan yg baik.



<https://kis.ibik.ac.id/login.php?username=32312342323&password=abc@123>

Menerka-nerka akun korban dengan cara mengirimkan parameter kedalam URL



Web Security – Threats

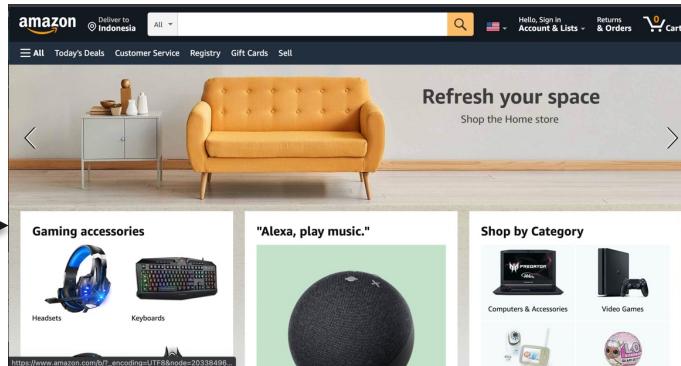
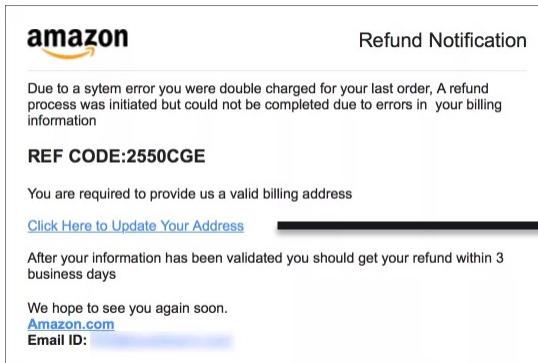
Cross-Site Scripting (XSS)

Contoh serangan XSS

02

Email Phising

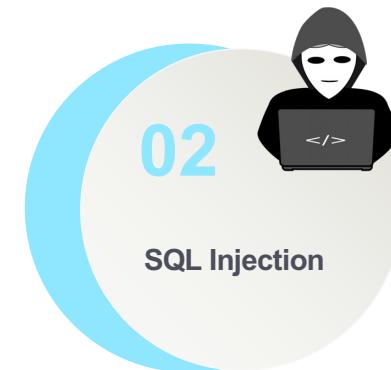
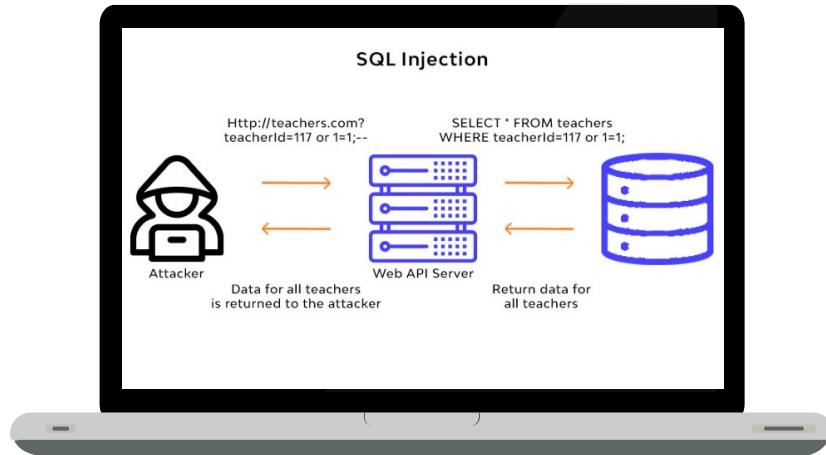
Teknik dari Social Engineering yang banyak digunakan oleh para peretas untuk mengelabui korban. Peretas mengirimkan sebuah email dengan judul yang menarik untuk dibuka oleh korban, biasanya berkaitan dengan finansial ataupun periklanan (hadiah, voucher, diskon, dll).



Yang seharusnya situs resmi Amazon ialah <https://www.amazon.com/> namun ketika di klik oleh korban alamatnya ialah <http://www.amazon.org/>



Web Security - Threats



SQL Injection adalah salah satu teknik yang menyalahgunakan celah keamanan yang ada di SQL pada lapisan basis data suatu aplikasi. Celah ini terjadi karena input dari user tidak difilter secara benar dan dalam pembuatannya menggunakan form yang salah. Jadi sampai saat ini SQL Injection masih menjadi favorit hacker untuk melakukan serangan pada website. Apalagi sekarang ini hacking melalui jaringan internet sudah tidak semudah zaman dulu.



Web Security – Threats

SQL Injection

Dampak SQL Injection

01

Bypass Otentikasi

Jika berhasil masuk kedalam sistem, hacker akan mudah melakukan bypass tanpa perlu menggunakan username dan password yang benar untuk bisa mendapatkan akses. Cukup dengan memasukan script SQL Injection pada form yang masih terbuka.

02

Pencurian Informasi

Hacker memungkinkan untuk mengambil semua informasi yang ada pada website terutama informasi yang bersifat sensitif seperti username dan password.

03

Delete Data

SQL Injection memungkinkan untuk hacker menghapus semua data yang tersimpan di database, jika sudah terjadi seperti ini dan tidak ada backup database maka akan sangat berbahaya. Jadi Anda perlu melakukan backup data secara berkala untuk tujuan keamanan data.

Modify Data

Selain menghapus data, hacker dengan mudah mengubah data yang tersimpan di database sehingga menyebabkan data tidak valid. Jadi Anda perlu memiliki backup data jika sewaktu-waktu data dirubah oleh orang yang tidak bertanggung jawab.

04



Web Security – Threats

SQL Injection

Cara mencegah SQL Injection

01

Menyesuaikan Form Inputan

Cara paling sederhana ialah dengan menyesuaikan inputan data dengan tipe data yg dimiliki dari masing-masing field pada table di database. Contoh: inputan nomor telpon bisa dibuat isiannya hanya dalam bentuk Number, dan membuat validasi karakter khusus pada setiap form inputan

Name:

KTP:

Normal Form

Name:

KTP:

Abnormal Form



Bisa diisi dengan query SQL



Web Security – Threats

SQL Injection

Cara mencegah SQL Injection

02

Mematikan error handler pada SQL

Jika terjadi error, Anda perlu mematikan fitur notifikasi pesan error yang keluar dari SQL Server. Jika sampai ada, ini bisa menjadi celah bagi hacker untuk melakukan eksplorasi lebih dalam percobaan SQL Injection.

The screenshot shows a browser window with the URL `/ViewGallery.aspx?CatID=2'`. The page displays an error message: "Server Error in '/' Application." followed by the technical details of the exception. The error message is: "Unclosed quotation mark after the character string '2' . Incorrect syntax near '2' ." The "Description" section states: "An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code." The "Exception Details" section shows: "System.Data.SqlClient.SqlException: Unclosed quotation mark after the character string '2' . Incorrect syntax near '2' ." The "Source Error" section shows the C# code from line 29 to 33:

```
Line 29:     SqlDataAdapter da = new SqlDataAdapter(cmd);
Line 30:     DataSet ds = new DataSet();
Line 31:     da.Fill(ds);
Line 32:     DataList1.DataSource = ds;
Line 33:     DataList1.DataBind();
```

The "Source File" is `g:\pleskvhhosts\angellybybid.in\ViewGallery.aspx.cs` and the "Line" is 31. The "Stack Trace" section shows the full stack trace of the exception, starting with "[SqlException (0x80131904): Unclosed quotation mark after the character string '2' .] Incorrect syntax near '2' .]" and listing several method calls from the System.Data.SqlClient namespace.



Web Security – Threats

SQL Injection

Cara mencegah SQL Injection

04

Setting Privilege

Hal ini juga dapat dilakukan dengan cara membuat user khusus yg dapat digunakan pada setiap aplikasi yang terkoneksi kedalam database. Contohnya user yg hanya diberikan akses untuk *read-only* saja

Edit privileges: User account 'user@321'@'localhost'

⚠ Note: You are attempting to edit privileges of the user with which you are currently logged in.

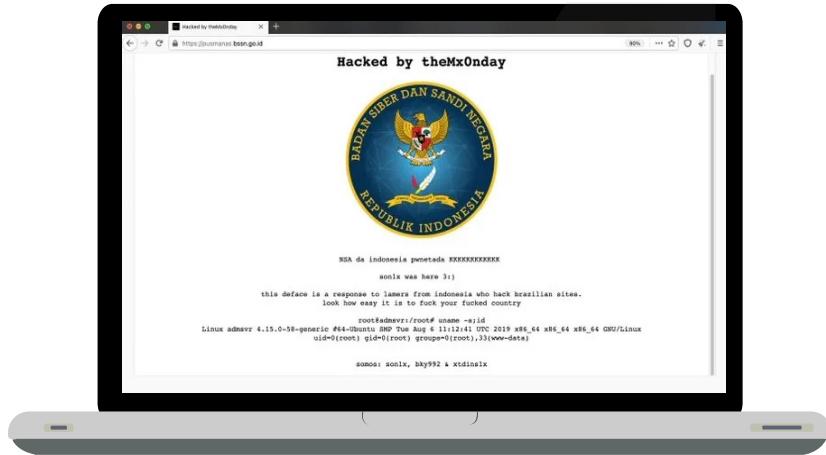
Global privileges Check all

Note: MySQL privilege names are expressed in English.

Category	Privileges
Data	<input checked="" type="checkbox"/> SELECT <input type="checkbox"/> INSERT <input type="checkbox"/> UPDATE <input type="checkbox"/> DELETE <input type="checkbox"/> FILE
Structure	<input type="checkbox"/> CREATE <input type="checkbox"/> ALTER <input type="checkbox"/> INDEX <input type="checkbox"/> DROP <input type="checkbox"/> CREATE TEMPORARY TABLES <input type="checkbox"/> SHOW VIEW <input type="checkbox"/> CREATE ROUTINE <input type="checkbox"/> ALTER ROUTINE <input type="checkbox"/> EXECUTE <input type="checkbox"/> CREATE VIEW <input type="checkbox"/> EVENT <input type="checkbox"/> TRIGGER
Administration	<input type="checkbox"/> GRANT <input type="checkbox"/> SUPER <input type="checkbox"/> PROCESS <input type="checkbox"/> RELOAD <input type="checkbox"/> SHUTDOWN <input type="checkbox"/> SHOW DATABASES <input type="checkbox"/> LOCK TABLES <input type="checkbox"/> REFERENCES <input type="checkbox"/> REPLICATION CLIENT <input type="checkbox"/> REPLICATION SLAVE <input type="checkbox"/> CREATE USER
Resource limits	<p>Note: Setting these options to 0 (zero) removes the limit.</p> <p>MAX QUERIES PER HOUR <input type="text" value="0"/></p> <p>MAX UPDATES PER HOUR <input type="text" value="0"/></p> <p>MAX CONNECTIONS PER HOUR <input type="text" value="0"/></p> <p>MAX USER_CONNECTIONS <input type="text" value="0"/></p>
SSL	<input checked="" type="radio"/> REQUIRE NONE <input type="radio"/> REQUIRE SSL <input type="radio"/> REQUIRE X509 <input type="radio"/> ENCRYPTED



Web Security - Threats



Deface website sering dilakukan untuk pengujian awal keamanan website. Peretas bisa saja melakukan aksi lebih jauh seperti pencurian data, dan sebagainya. Akibat yang ditimbulkan dari aksi deface website cukup serius. Apalagi jika website tersebut digunakan untuk tujuan bisnis. Kredibilitas Anda benar-benar dipertaruhkan.

Deface website sebagian besar terjadi karena adanya celah keamanan di sebuah website. Akses masuk peretas bisa dari berbagai pintu.



Web Security – Threats

Deface

Contoh kasus Deface

01

Melalui Form Inputan

Ini merupakan cara peretasan deface paling umum dilakukan oleh para peretas Junior. Dengan cara menyusupi sebuah script melalui form inputan. Terutama form yang memiliki field upload type file.



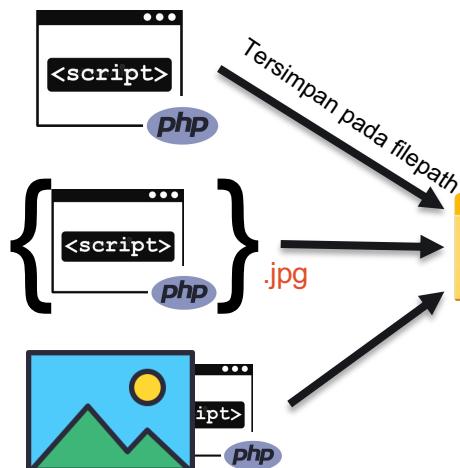
Name:
Febry D F

Upload:
Choose file No file chosen

Submit

Normal Form

Upload file



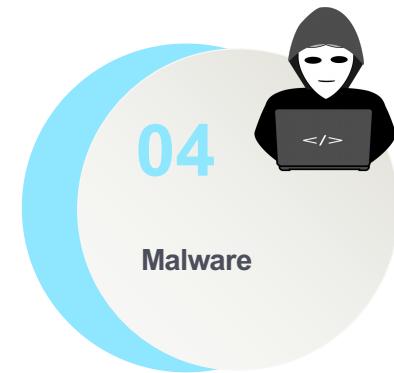
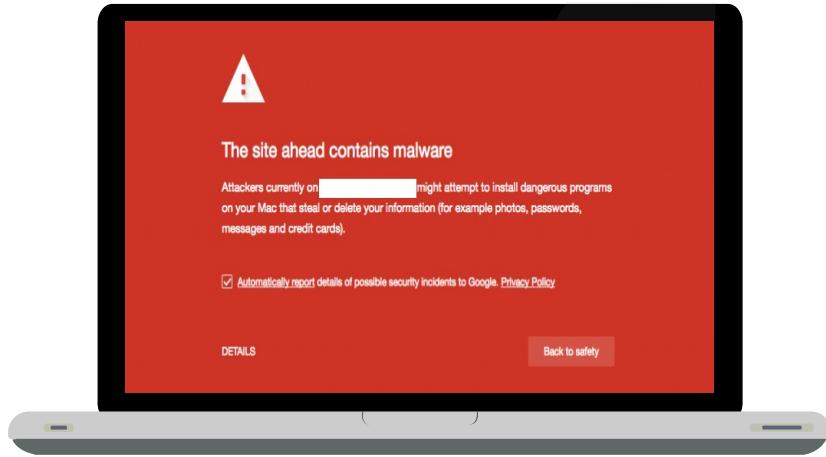
execute file

Get DATA atau
Get Source Code
atau
Merubah website





Web Security - Threats



Singkatan dari Malicious Software, artinya sendiri adalah sebuah software yang dirancang dengan tujuan untuk membahayakan, menyusup, atau merusak sebuah komputer.

Bagi website yang terkena malware, Google akan memasang tulisan "The site ahead contains harmful programs" atau "The site ahead contains malware" saat ada yang mencoba mengaksesnya.

Ada banyak malware yang berbahaya namun jenis malware yang paling umum termasuk *virus*, *keylogger*, *worm*, *trojan*, *ransomware/crypto-malware*, *bot/botnet*, *adware* dan *spyware*, serta *rootkit*.



Web Security – Threats

Malware

Dampak Malware

01

Menampilkan iklan

Jika website sudah terkena salah satu virus malware, maka hal yang paling mudah diketahui ialah munculnya iklan yang tidak sesuai dengan website.

The screenshot shows the homepage of detikcom. At the top, there are several advertisements for the 'Baru Galaxy A03'. One ad on the left features a phone with a small red notification bubble. Another ad in the center shows a tire, and another on the right shows a blue generator. The navigation bar includes links for detikNews, detikFinance, detikHot, detikKinet, detikSport, detikOto, detikTravel, detikFood, detikHealth, Wolipop, 20Detik, Daerah, Live TV, Adsmart, Foto, detikX, Sepakbola, Pasangmata, Hikmah, Edukasi, berbuatbaik.id, and Live Streaming MotoGP. Below the navigation, there are five news thumbnails: 'Dikonfirmasi WHO, Seberapa Bahaya Varian Gabungan Delta-Omicron?', 'Salah Tolak Kontrak Baru dari Liverpool, Gajinya Tak Cocok!', 'Rudy Salim Teseret Arus Kasus Indra Kenz', 'Adnan/Mychelle Tersingkir, Wakil Indonesia di German Open 2022 Habis!', and 'Pandemi Sudah 2 Tahun, Belum Pernah Tes COVID? Orang-orang Ini Ungkap Alasannya'.



Web Security – Threats

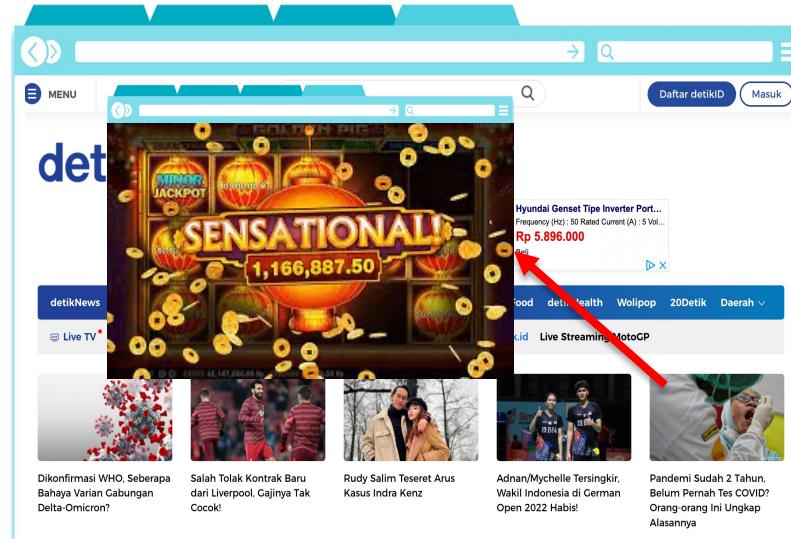
Malware

Dampak Malware

02

PopUp Ads Malware

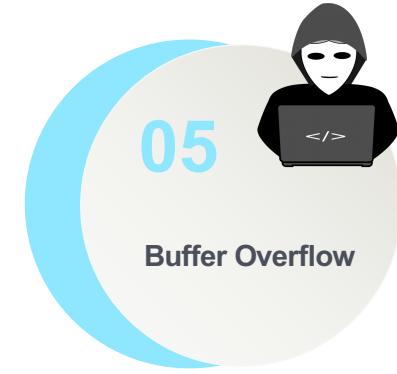
Ads Malware ini adalah termasuk malware injected, jadi dari scriptnya tersendiri sudah terinfeksi, ketika dideploy di website maka malware tersebut akan berjalan otomatis. Ads ini bekerja jika Anda membuka website yang terinfeksi kemudian akan diredirect ke website asing.





Web Security - Threats

```
(...TEXT,...text) section
_main:
0000000100000f10      55          pusha    %rbp
0000000100000f11      48 89 e5    movq    %rsp, %rbp
0000000100000f14      48 83 ec 30  subq    $0x30, %rsp
0000000100000f18      31 c0        xorl    %eax, %eax
0000000100000f1c      48 89 d0    movl    %eax, %edi
0000000100000f20      48 bd 0d 7e  testl    %edi, %edi(%rbp), %esi
0000000100000f20      48 8b bd 09 00 00 00  movl    %esi(%rbp), %rcx ## literal pool symbol address: __stack_chk_guard
0000000100000f27      48 89 d0    movl    %rcx, %rcx
0000000100000f2a      48 89 fd 48  movq    %rcx, -0x8(%rbp)
0000000100000f2e      c7 45 dc 00 00 00 00  movl    $0x0, -0x24(%rbp)
0000000100000f35      48 8d 0d 70 00 00 00  leaq    0x70(%rbp), %rcx ## literal pool for: "/bin/sh"
0000000100000f3c      48 89 4d e0    movq    %rcx, -0x20(%rbp)
0000000100000f40      48 c7 45 e8 00 00 00 00  movq    $0x0, -0x18(%rbp)
0000000100000f48      48 89 cf    movw    %rcx, %rdi
0000000100000f4d      48 89 04 00 00 00 00 00  movl    %rdi, %eax ## symbol stub for: _execve
0000000100000f52      48 8b 0d b7 00 00 00 00  movl    $0x70(%rbp), %rcx ## literal pool symbol address: __stack_chk_guard
0000000100000f59      48 8b 09    movq    (%rcx), %rcx
0000000100000f5c      48 8b 55 f8    movq    %rdx, %rdx
0000000100000f60      48 39 d1    cmpq    %rdx, %rcx
0000000100000f63      89 45 d8    movl    %eax, -0x20(%rbp)
0000000100000f66      0f 85 08 00 00 00  jne     0x100000f74
0000000100000f6c      31 c0        xorl    %eax, %eax
0000000100000f72      48 83 c4 30  addq    $0x30, %rsp
0000000100000f73      c3          retq    %
0000000100000f74      48 83 00 00 00 00  callq  0x100000f7c ## symbol stub for: __stack_chk_fail
0000000100000f79      9f 0b  ud2
```



05

Buffer Overflow

situasi di mana program yang sedang berjalan mencoba untuk menulis data di luar buffer memori yang tidak dimaksudkan untuk menyimpan data ini. Ketika ini terjadi kita berbicara tentang situasi buffer overflow atau buffer overrun. Suatu penyanga memori adalah suatu area dalam memori komputer (RAM) yang dimaksudkan untuk menyimpan data sementara. Buffer semacam ini dapat ditemukan di semua program dan digunakan untuk menyimpan data untuk input, output dan pemrosesan.

Biasanya serangan ini menggunakan SHELLCODE



Web Security – Threats

Buffer Overflow

Dampak Buffer Overflow

01

Performa tidak stabil

Ketika terjadi limpahan buffer memori dan data ditulis di luar buffer, program yang sedang berjalan dapat menjadi tidak stabil, crash atau mengembalikan informasi yang korup.

02

Pencurian Informasi

Peretas dapat mengambil alih kendali host seperti melakukan eskalasi hak istimewa atau lebih buruknya lagi. Penyerangan ini menggunakan kode arbitrer, dengan cara menyuntikan code kedalam bufferd

03

Denial of Service (DoS)

Serangan Denial of Service dapat dilakukan ketika mereka hanya menjalankan program yang macet. Karena buffer overflows vulnerabilities dapat terjadi dalam perangkat lunak, serangan DoS tidak hanya terbatas pada layanan dan komputer.



**Kampus
Merdeka**
INDONESIA JAYA

Web Security – Threats

Buffer Overflow

Cara mencegah Buffer Overflow

01

Menggunakan OS yg tepat

Mitigasi yang efektif adalah sistem operasi modern yang melindungi area memori tertentu agar tidak ditulis atau dieksekusi. Ini akan mencegah penyerang menulis kode arbitrer ke memori ketika terjadi buffer overflow.





Web Security – Threats

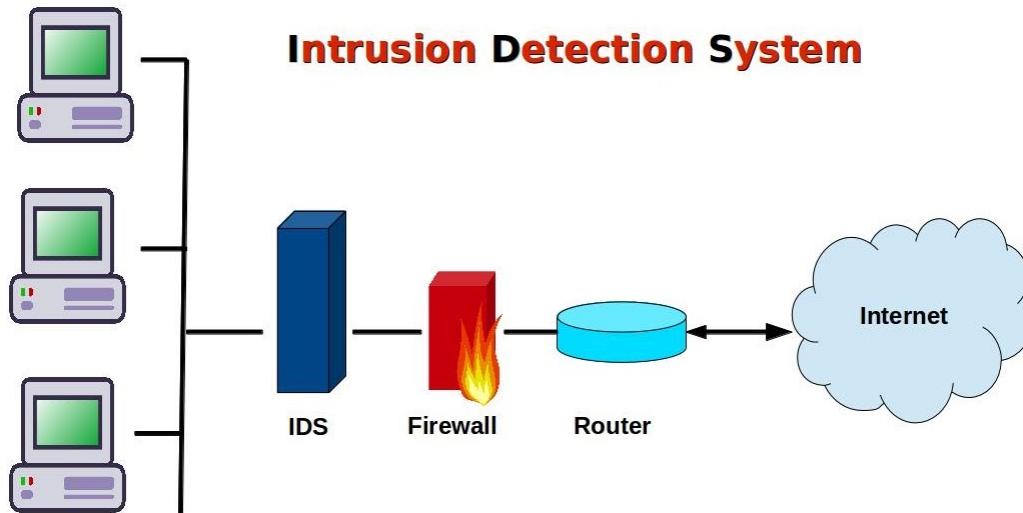
Buffer Overflow

Cara mencegah Bufferd Overflow

02

Menggunakan Intrusion Detection System (IDS)

Untuk menganalisis lalu lintas jaringan. IDS mampu mendeteksi tanda tangan dalam lalu lintas jaringan yang diketahui dapat mengeksploitasi kerentanan buffer overflow. IDS dapat mengurangi serangan dan mencegah payload dari mengeksekusi pada sistem yang ditargetkan.



QUIZ

1

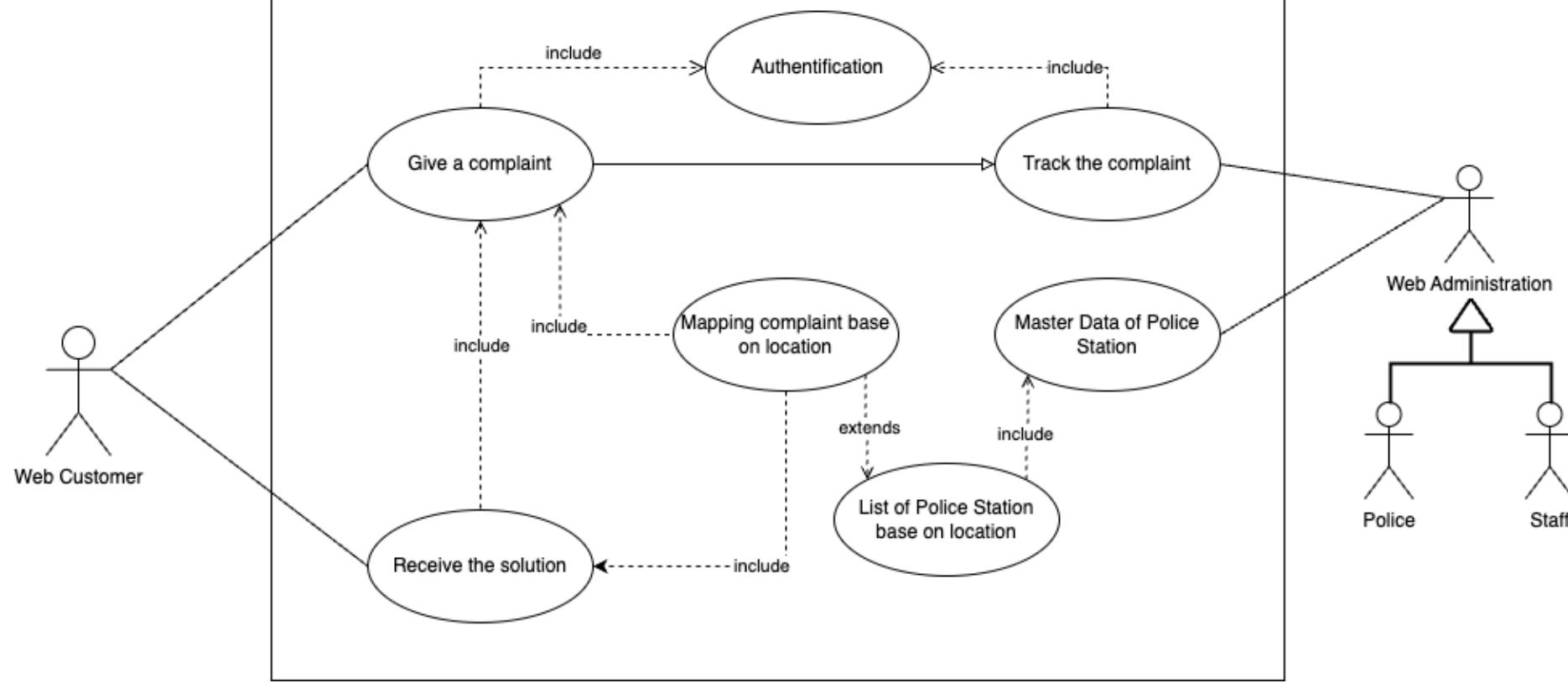


Isilah jawaban quiz dibawah ini
dengan mengirimkan email ke
febrid@ibik.ac.id dengan subject

PW-TI-20-[PA/KA]-QUIZ-1-NPM

Dikumpulkan Sabtu 04 Maret
2023 pukul 15.00

Use Case - Web Apps LAPOR PAK!!





1. Buatlah satu buah halaman mock up aplikasi Web yang menggambarkan business process sesuai dengan Use Case tersebut. (Sketch online: Figma, Auto Draw, dll)
2. Dari mock up soal nomor 1 buatlah Story Board dari page tersebut.
3. Pertimbangkan layout, fitur dan fasilitas (UI/UX) apa saja yang akan anda masukan namun tidak menghilangkan transaksi utama yg ada di Use Casenya

Thanks