



Pemrograman Web

2022/2023 Genap

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



Classroom Rules

SCHEDULE:

PB Sabtu, 10.15 – 12.45 Room 404
PA Sabtu, 13.15 – 18.30 Room 303

The last 30 minutes of the schedule will be Q&A for Attendee and Score (No quizzes)



Classroom Rules

SCHEDULE:

KA Sabtu, 20.30 – 22.00 Room 401

The last 30 minutes of the schedule will be Q&A for Attendee and Score (No quizzes)

Base on Warek 1 use **BLENDED LEARNING**:
Offline : 4 meetings (2 before Mid exam and 2 after Mid Exam)
Online : 10 meetings (Google Meet on GCalendar)





Classroom Rules

BLANDED LEARNING TOOLS:

Gmett (on GCalendar)
VS Code install Live Share
GITHUB

Classroom Rules



- **ASSESSMENT**
 - Tasks are **individual** or **group**, submission deadline 1 week
 - Midterm Exam (UTS)
- **Final Exam (UAS)**
 - Project's Group
 - 3 times Presentations (Intro, Progress, Final)
 - Individual testing and comprehensive

*Attendee < 12 ineligible

Agenda

01 **Introduction**

Type of Website and Web Security

02 **Web Tech**

Monolithic Architecture
Laravel ^10

03 **UI/UX I**

CSS Framework
JQUERY

04 **UI/UX II**

Web Responsive and adaptive design

05 **Memory**

Authentications & Authorizations

06 **Resume**

Resume material,
Project Group

Agenda

07
Exmination

Midterm Exam

08
Project Phase 1

Topic, Research Method,
UML, Wireframe

09
Project Phase 1

Topic, Research Method,
UML, Wireframe

10
Project Phase 2

Progress
PW & PPB

11
Project Phase 2

Progress
PW & PPB

12
Project Final

Testing and
Comprehensive

Agenda

13

Project Final

Testing and
Comprehensive

14

Final Exam

Final Exam



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, fiber-optic atau wireless

HTTP

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

TCP/IP

Menerima kode POST permintaan

URL

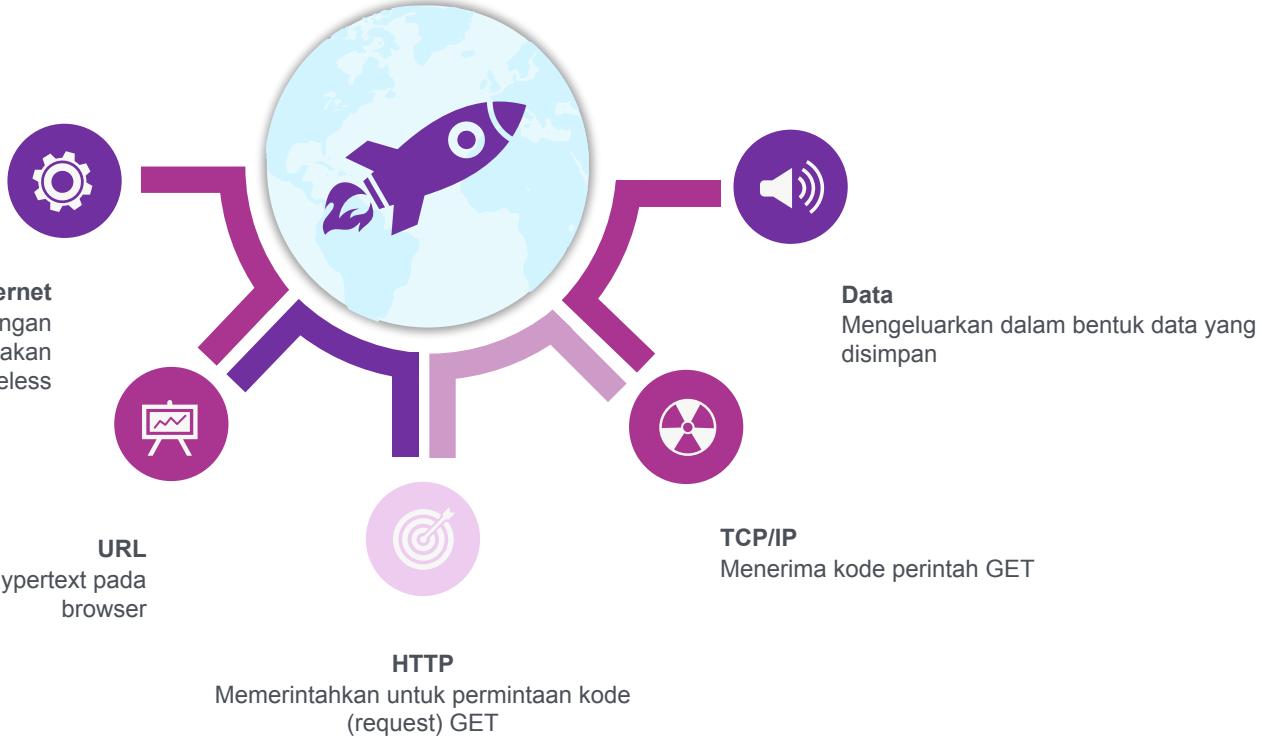
Mengeluarkan hasil data dalam bentuk url

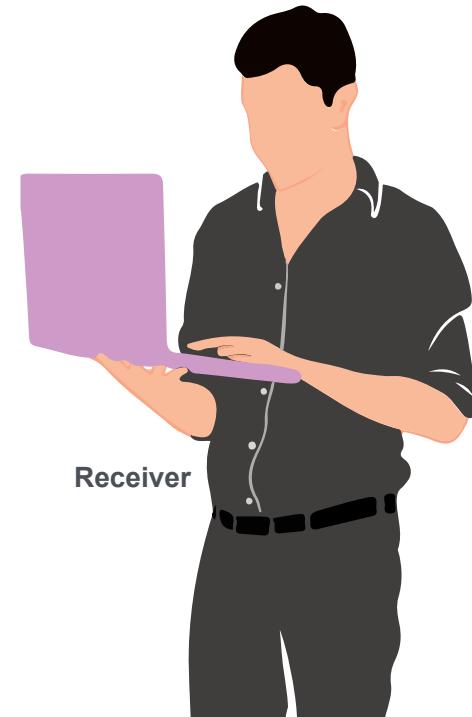
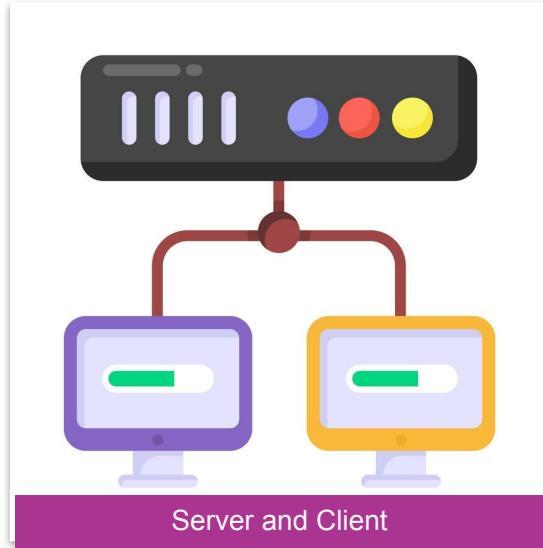
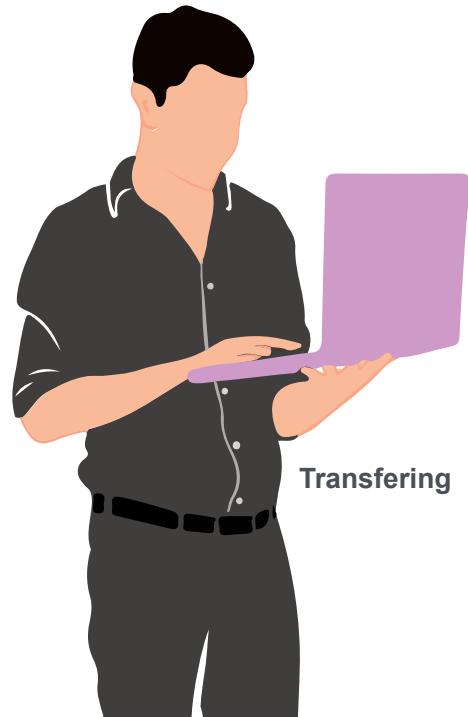
FTP

Memasukan data kedalam server



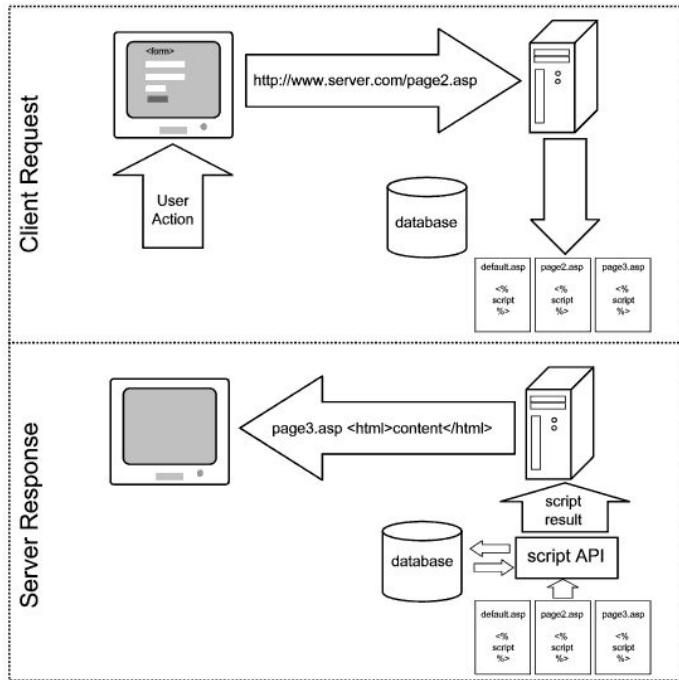
Website Receiving Data





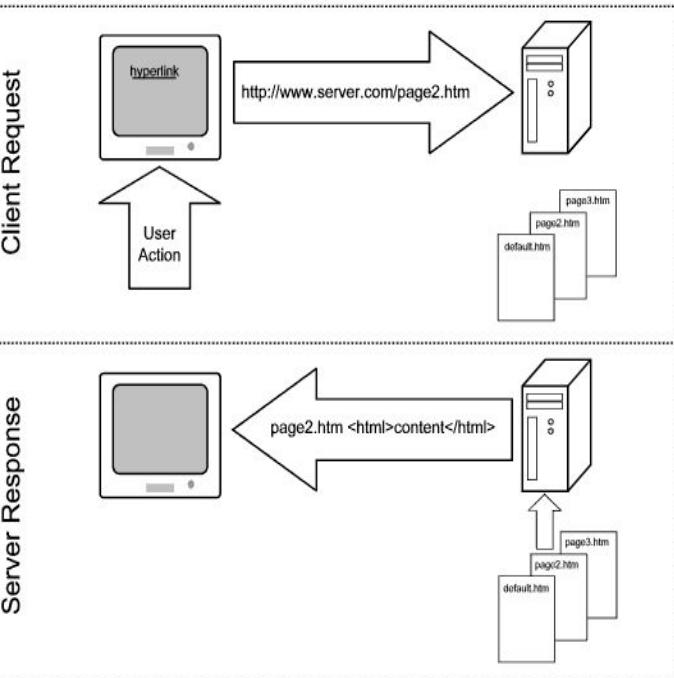


Server side programming



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



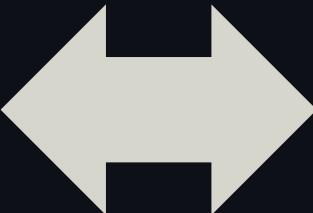
Types of Websites

01



Website Statis

website yang kontennya konstan atau tidak berubah



02



Website Dinamic

website yang kontennya selalu di-update secara berkala



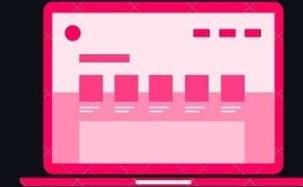
Static Website



Types of Websites

Website

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



Dynamic Web App



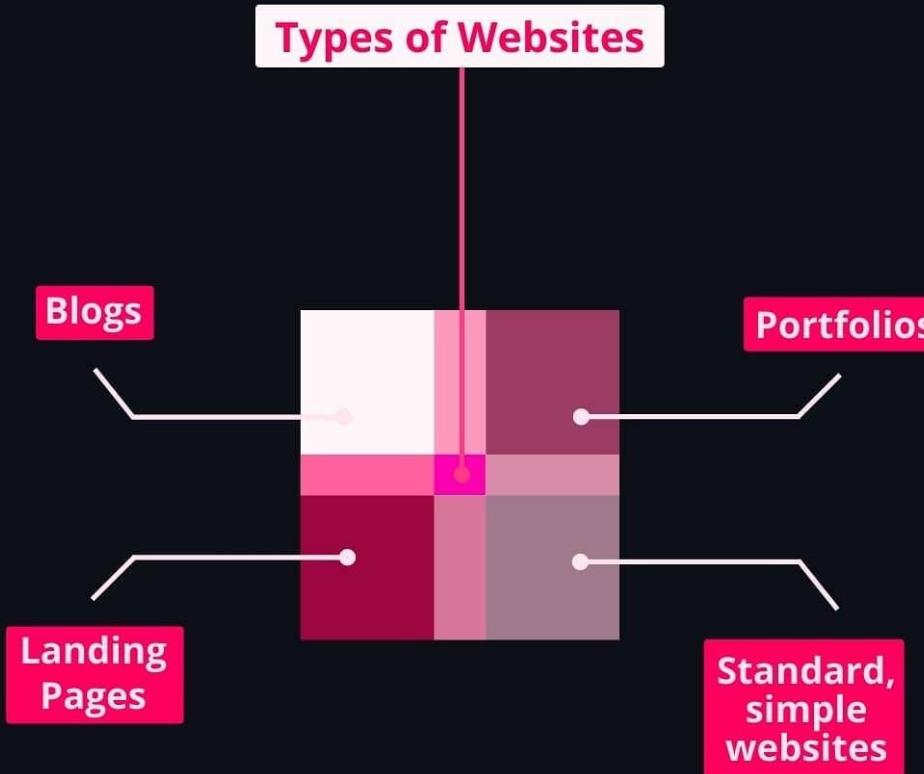
Web App

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



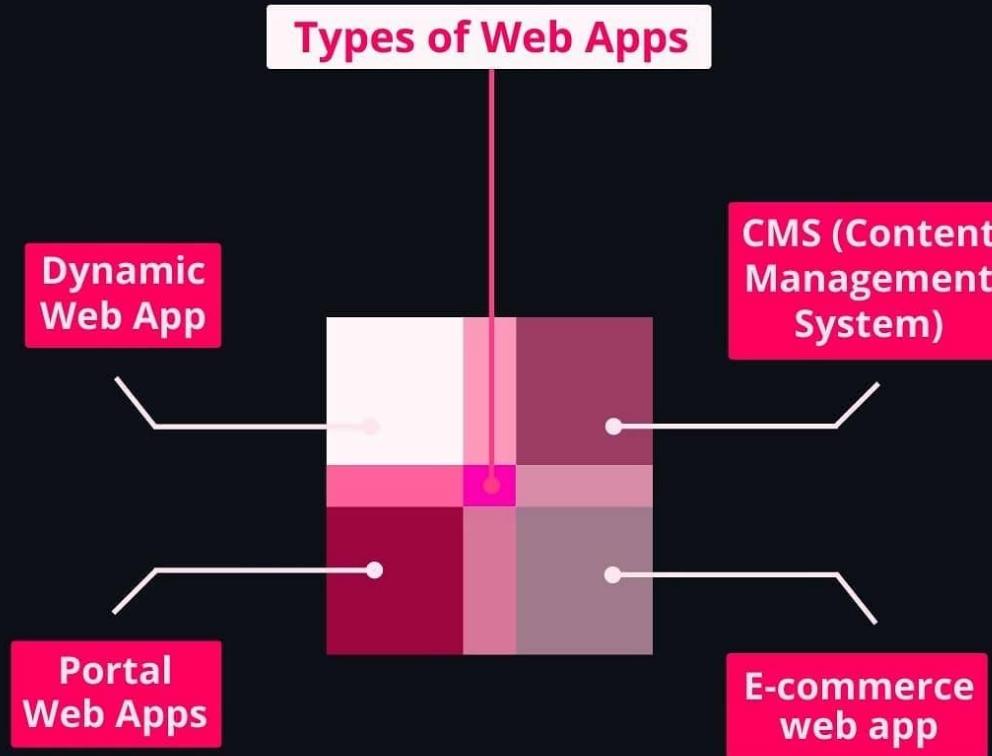


Types of Websites





Types of Websites





Types of Websites

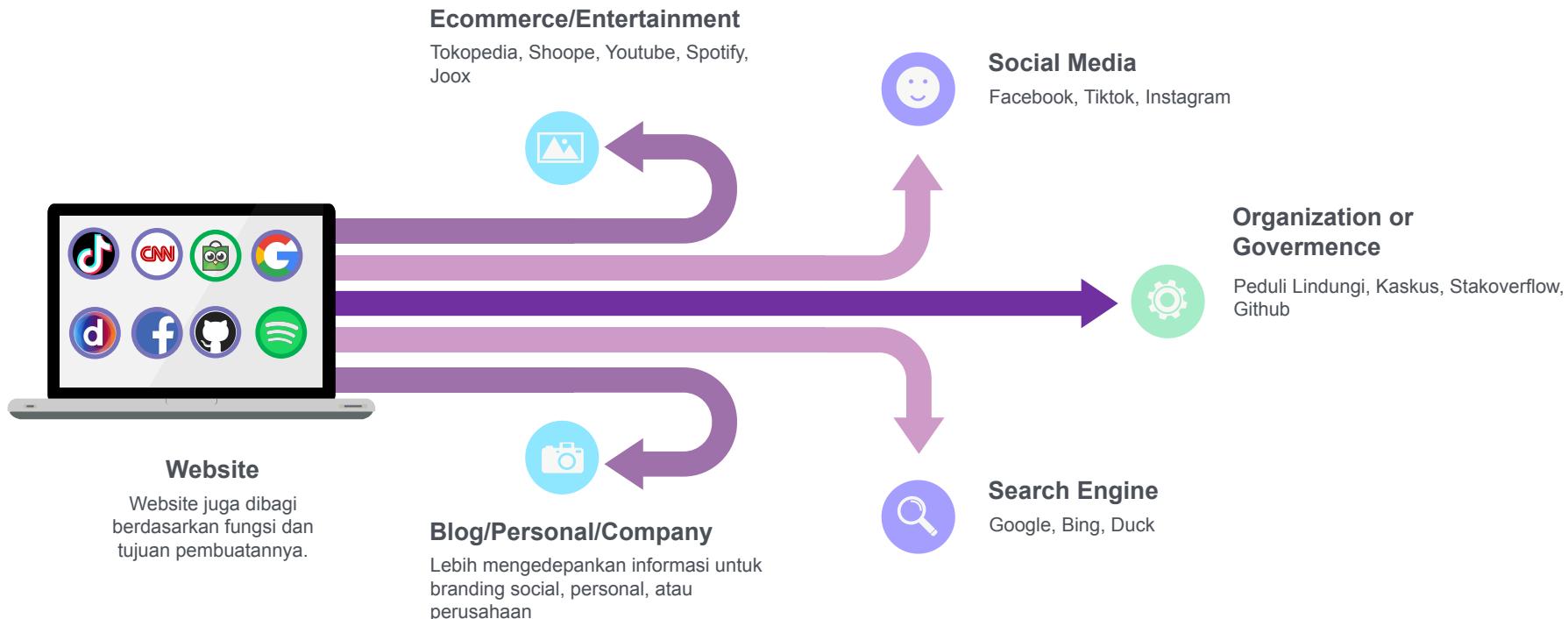
Websites do not need to set up a verification process because users do not interact with the content.



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 centralization. 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. Kelemahannya 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



Programming Language

Base on Web Programming



Web Developer / Backend Developer

Membangun website

Functional & Logical

Menggunakan otak kiri

Programmer

Salary \$70 USD

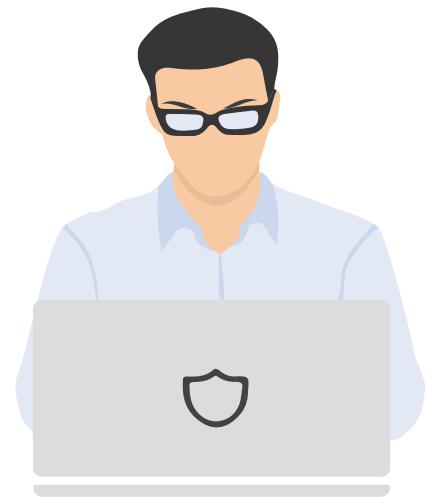




Kampus
Merdeka
INDONESIA JAYA

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

Kampus
Merdeka
INDONESIA JAYA



Skill Basic

HTML, JS, CSS,
UI / UX

Monolith

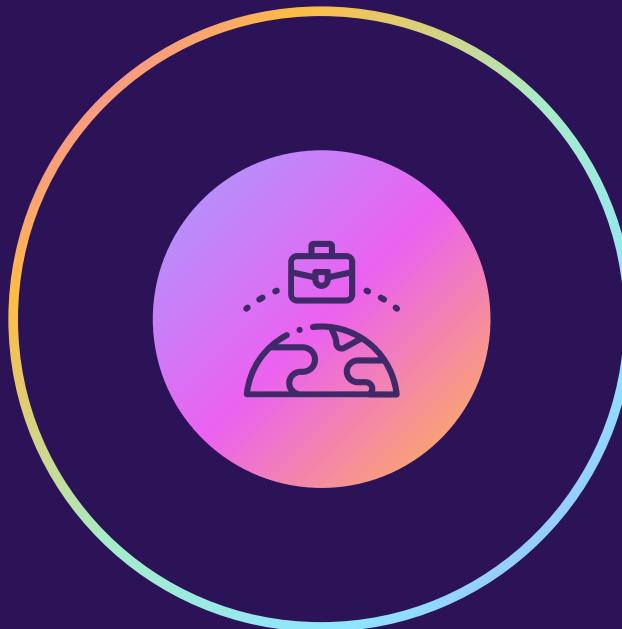
Apps yang dibangun
dalam 1 codebase

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.



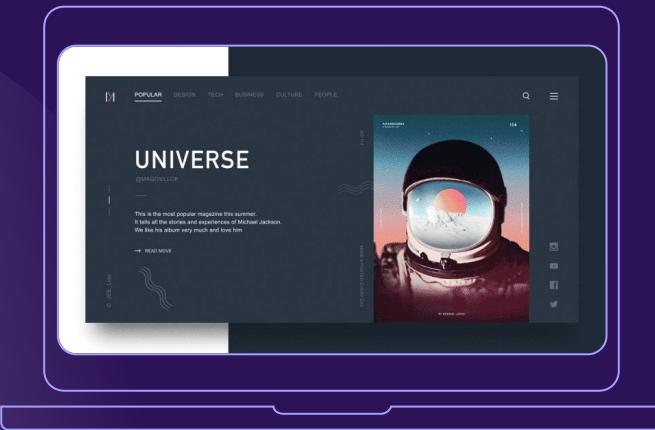
User Experience (UX)

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



Kampus
Merdeka
INDONESIA JAYA



COLORS

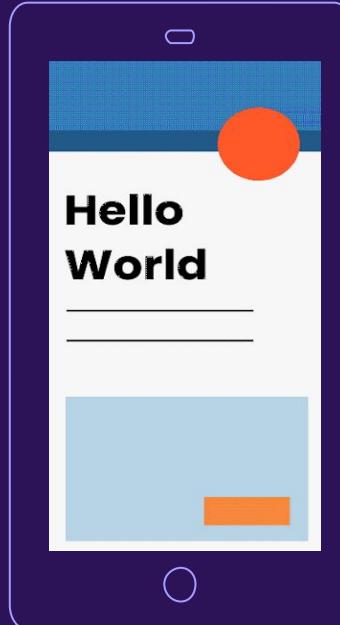
Pelajari dasar-dasar warna dan psikologi warna. Warna pada aplikasi biasanya terbagi menjadi tiga buah kategori yaitu Warna **Primer**, **Sekunder** dan **Tersier**.



UI Principles

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

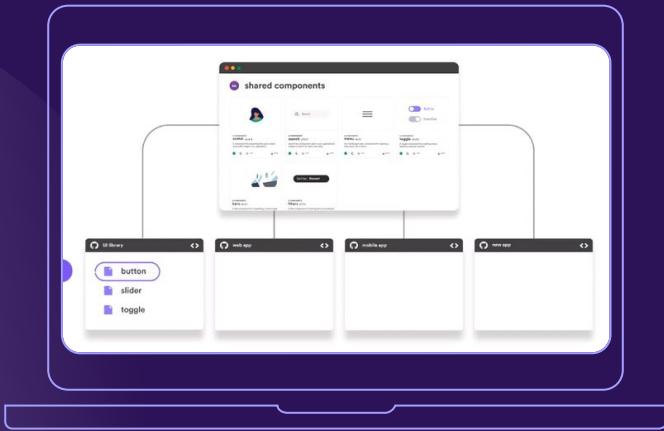


BALANCE

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

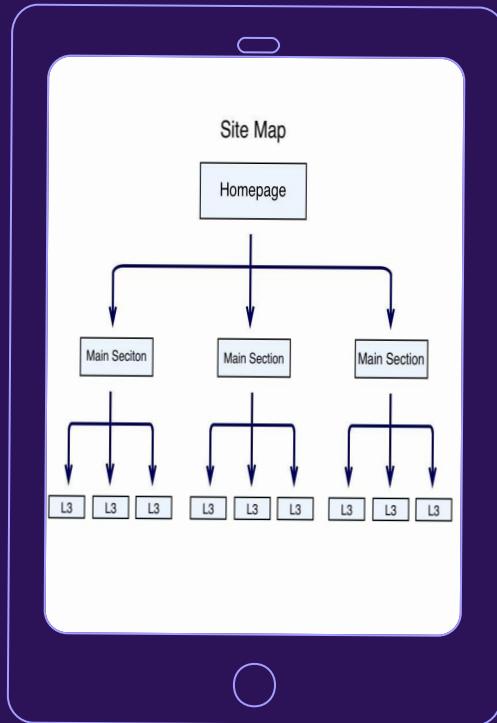
UX Principles

UX Principles

Hierarchy

1. Information architecture
2. Visual hierarchy

Kampus
Merdeka
INDONESIA JAYA



UX Principles

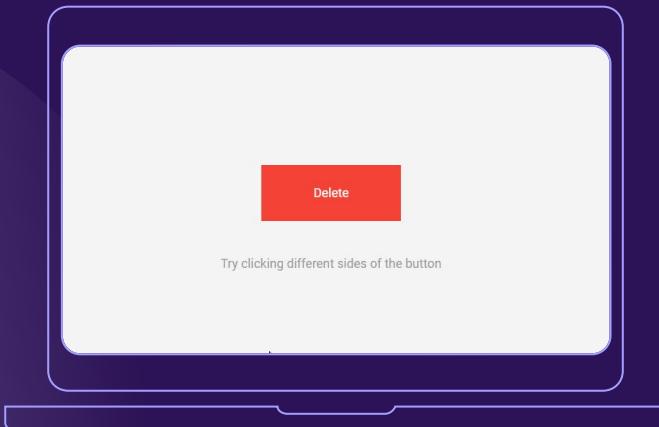
Kampus
Merdeka
INDONESIA JAYA



CONSISTENCY

Memiliki pola standart layout antar product.

UX Principles



Kampus
Merdeka
INDONESIA JAYA



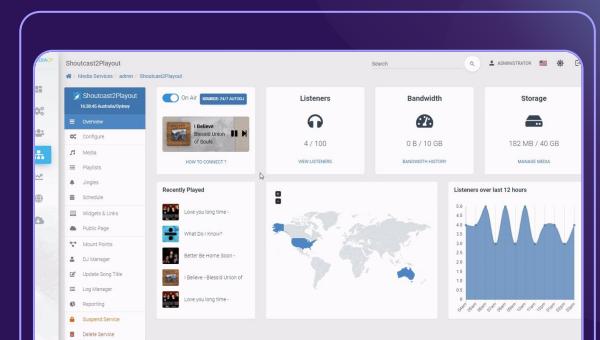
CONFIRMATION

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

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



03

JS

Javascript

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



Hypertext Markup
Language

Programming Language

HTML merupakan struktur utama dalam membangun sebuah website

Memiliki 140 tag HTML

Versi 5 merupakan versi terbaru dari HTML yg dikenalkan pada tahun 2014 dimana memiliki beberapa semantic baru seperti `<article>`, `<header>`, `<footer>`

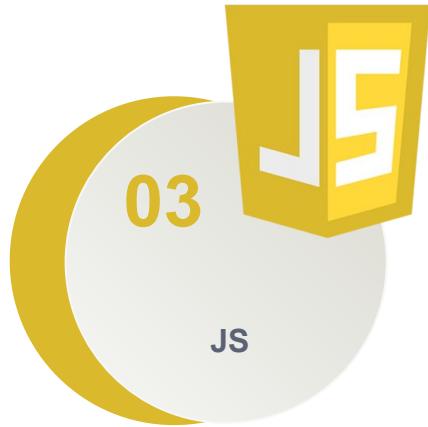


Cascading Style Sheets

Programming Language

CSS merupakan bagian dari pengembangan struktur website untuk mengatur tampilannya.

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

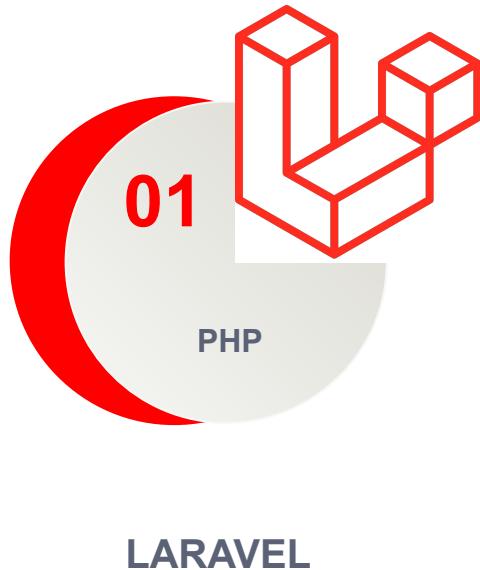


Javascript

Programming Language

JS merupakan bahasa pemrograman yang paling banyak digunakan dalam pengembangan website, aplikasi, game, dan lainnya.

JavaScript sendiri sebenarnya biasanya dikolaborasikan dengan HTML dan CSS. Di mana HTML digunakan untuk membuat struktur website dan CSS untuk merancang style halaman website. Lalu, JavaScript berperan menambahkan elemen interaktif untuk meningkatkan engagement pengguna.



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



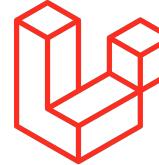
PHP

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

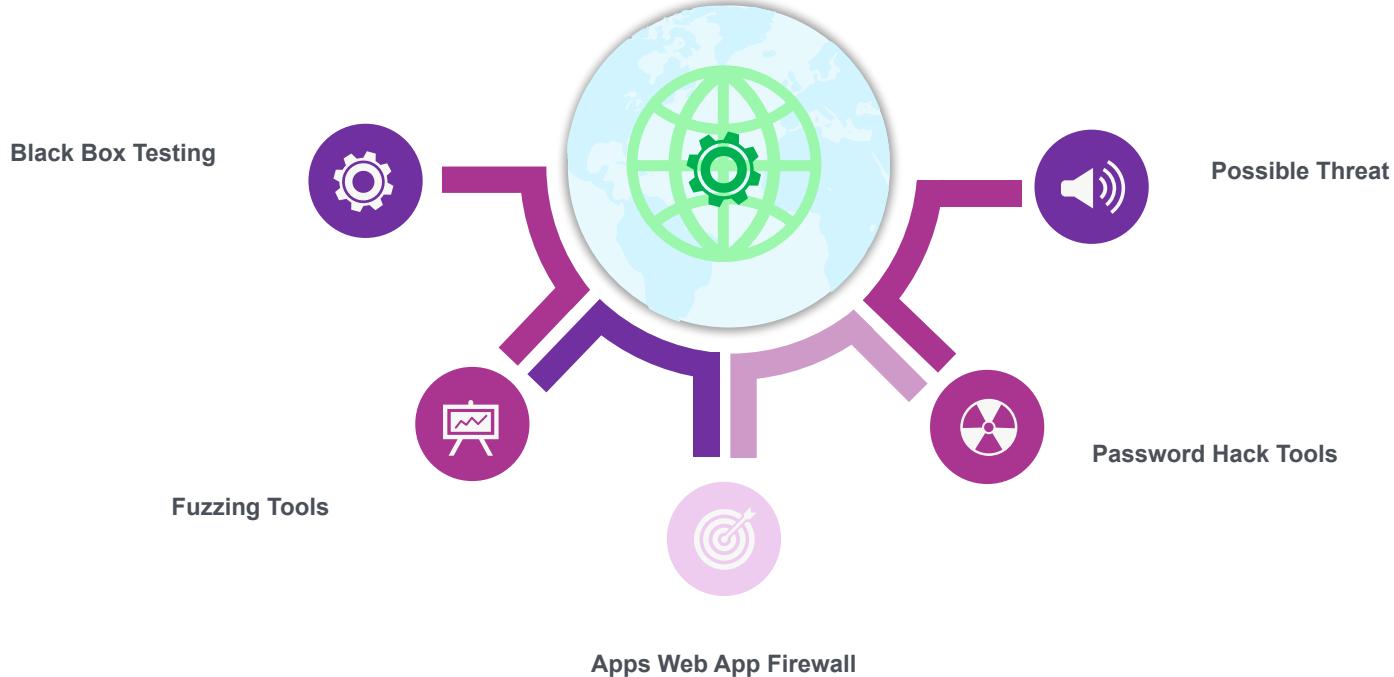
Keamanan ini diatur oleh system, hanya perlu menyiapkan sebuah script untuk mengeksekusinya.

Keamanan Program

Seluruh keamanan pada program sepenuhnya diatur oleh pembuat program.



Type of Web Security





Web Security - Threats

Cross-Site Scripting (XSS)

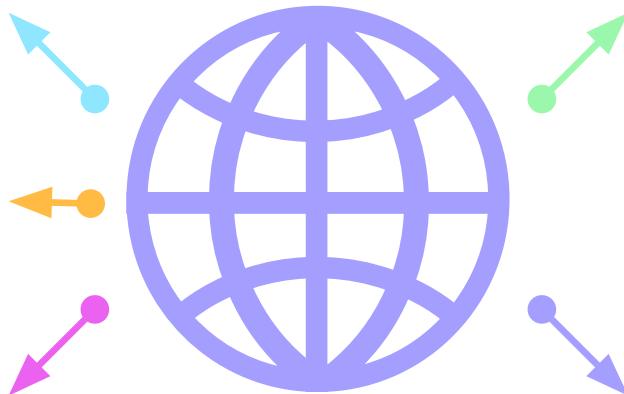
Metode ini adalah kerentanan yang memungkinkan penyerang memasukkan skrip sisi klien ke halaman web untuk mengakses informasi penting secara langsung, meniru identitas pengguna, atau mengelabui pengguna agar mengungkapkan informasi penting.

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

alah 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

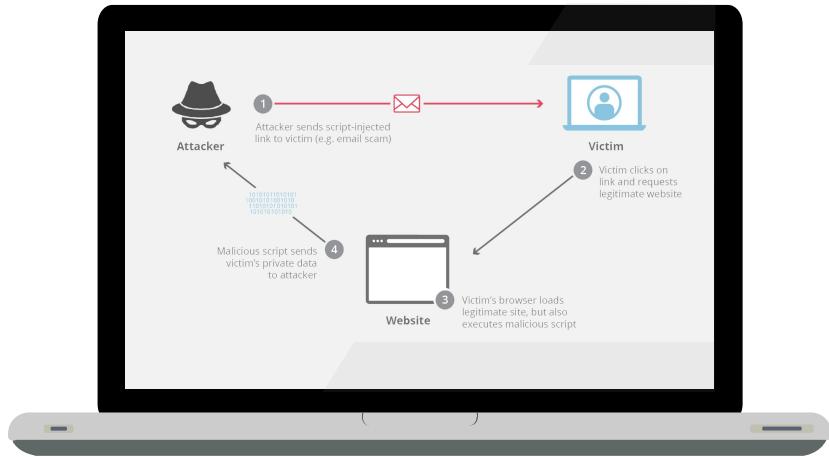
malicious software dalam kata bahasa inggris yang berarti program berbahaya. Malware adalah sebuah program yang didesain oleh hackers untuk mengeksplorasi dan merusak perangkat, server, maupun jaringan.

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

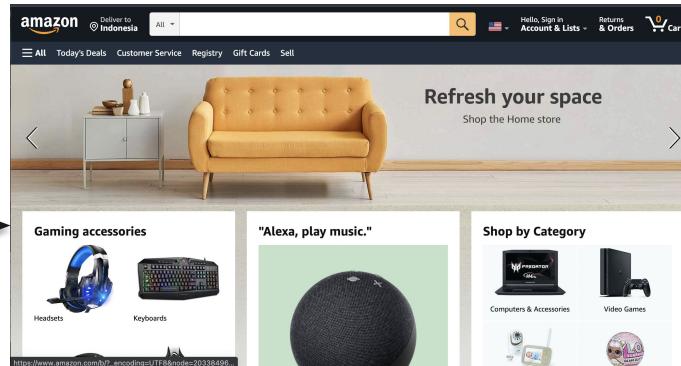
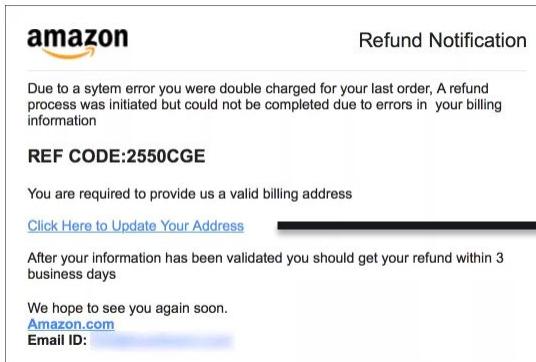
Cross-Site Scripting (XSS)

Contoh serangan XSS

02

Email Phising

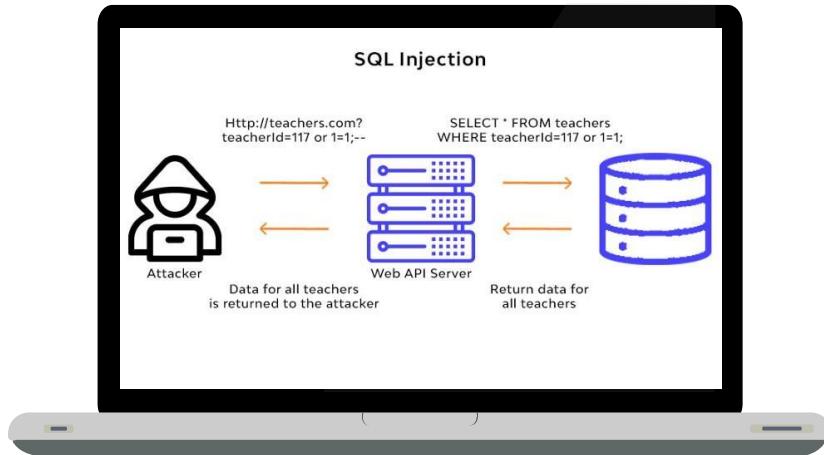
Teknik dari Social Engineering yang banyak digunakan oleh para peretas untuk mengelabui korban. Peretas mengirimkan sebuah email dengan judul yang menarik untuk dibuka oleh korban, biasanya berkaitan dengan finansial ataupun periklanan (hadiah, voucher, diskon, dll).



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.

04

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.



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 includes: "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 specifies: "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/angellybid.in/ViewGallery.aspx.cs` and the "Line" number is 31. The "Stack Trace" section shows the full stack trace of the exception, starting with the error at line 31 and extending up to the `SqlClient.SqlCommand.FinishExecuteReader` method.

```
[SqlException (0x80131904): Unclosed quotation mark after the character string '2' .
Incorrect syntax near '2' .]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +2582782
System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +6033430
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +297
System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj, Boolean asyncClose) +59
System.Data.SqlClient.SqlDataReader.TryConsumeMetaData() +59
System.Data.SqlClient.SqlDataReader.get_MetaData() +91
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString, Boolean isInternal, Boolean forDescribeParam, Boolean describe) +283
System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async, Int32 timeout, Task& result, Boolean& mustCloseConnection) +162
System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async) +140
System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, Boolean returnStream) +166
System.Data.SqlClient.SqlCommand.ExecuteDbDataReader(CommandBehavior behavior) +125
System.Data.Common.DbCommand.ExecuteReader() +102
DataList1.DataBind() +91
g:/pleskvhhosts/angellybid.in/ViewGallery.aspx.cs:31]
```



Web Security – Threats

SQL Injection

Cara mencegah SQL Injection

04

Setting Privilege

Hal ini juga dapat dilakukan dengan cara membuatkan 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.

Data	Structure	Administration	Resource limits
<input checked="" type="checkbox"/> SELECT	<input type="checkbox"/> CREATE	<input type="checkbox"/> GRANT	MAX QUERIES PER HOUR <input type="text" value="0"/>
<input type="checkbox"/> INSERT	<input type="checkbox"/> ALTER	<input type="checkbox"/> SUPER	MAX UPDATES PER HOUR <input type="text" value="0"/>
<input type="checkbox"/> UPDATE	<input type="checkbox"/> INDEX	<input type="checkbox"/> PROCESS	MAX CONNECTIONS PER HOUR <input type="text" value="0"/>
<input type="checkbox"/> DELETE	<input type="checkbox"/> DROP	<input type="checkbox"/> RELOAD	MAX USER_CONNECTIONS <input type="text" value="0"/>
<input type="checkbox"/> FILE	<input type="checkbox"/> CREATE TEMPORARY TABLES	<input type="checkbox"/> SHUTDOWN	
	<input type="checkbox"/> SHOW VIEW	<input type="checkbox"/> SHOW DATABASES	
	<input type="checkbox"/> CREATE ROUTINE	<input type="checkbox"/> LOCK TABLES	
	<input type="checkbox"/> ALTER ROUTINE	<input type="checkbox"/> REFERENCES	
	<input type="checkbox"/> EXECUTE	<input type="checkbox"/> REPLICATION CLIENT	
	<input type="checkbox"/> CREATE VIEW	<input type="checkbox"/> REPLICATION SLAVE	
	<input type="checkbox"/> EVENT	<input type="checkbox"/> CREATE USER	
	<input type="checkbox"/> TRIGGER		

SSL

REQUIRE NONE

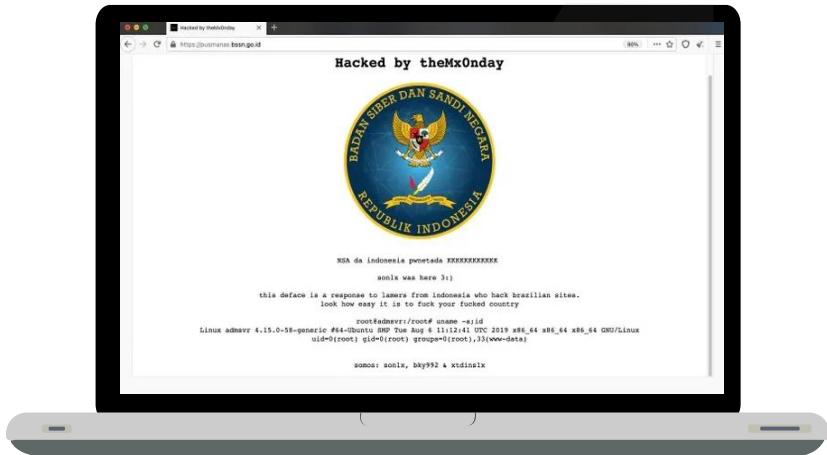
REQUIRE SSL

REQUIRE X509

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.



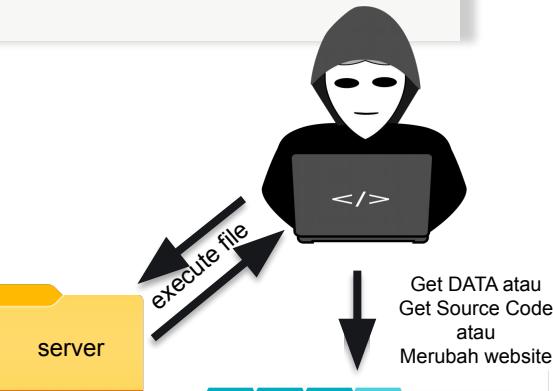
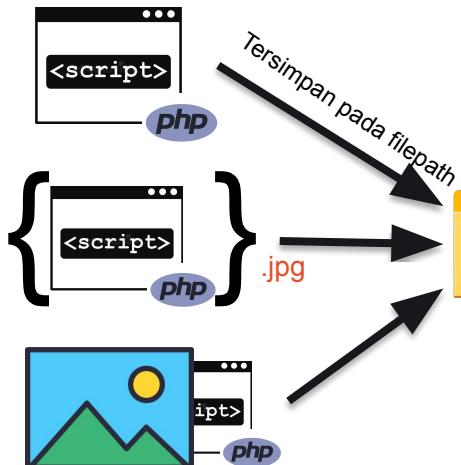
Name:
Febry D F

Upload:
Choose file No file chosen

Submit

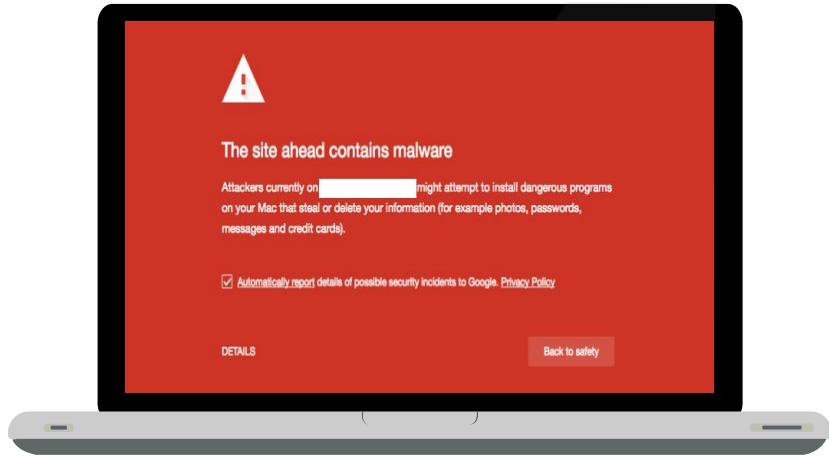
Normal Form

Upload file





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/cryptomalware, 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 is a navigation bar with 'MENU', a search bar, and buttons for 'Daftar detikID' and 'Masuk'. Below the header, there are several news thumbnails. Interspersed among these are several advertisements. On the left side, there's an ad for 'Baru Galaxy A03' from Samsung Indonesia. In the center, there's an ad for 'GT Radial Ban Mobil Radial Cham...' and another for 'Hyundai Genset Tipe Inverter Port...'. On the right side, there's another ad for 'Baru Galaxy A03' from Samsung Indonesia. The ads are clearly labeled with 'AD' and show various products like tires and generators.



Web Security – Threats

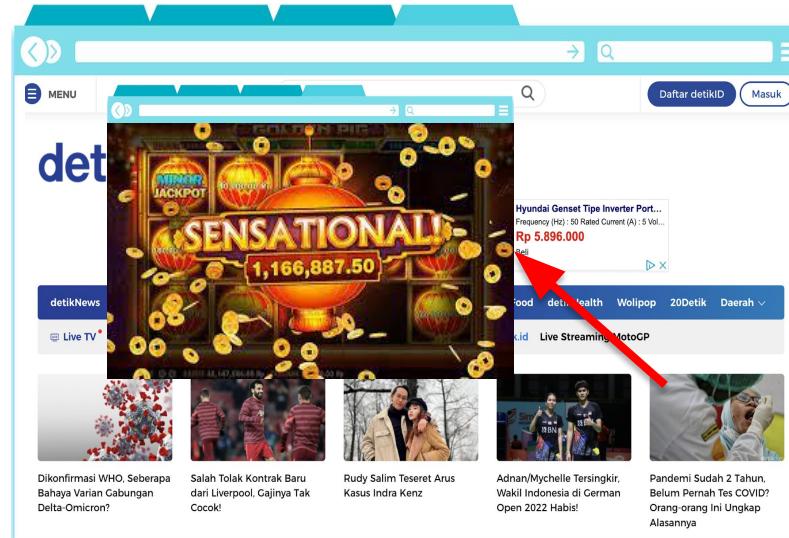
Malware

Dampak Malware

02

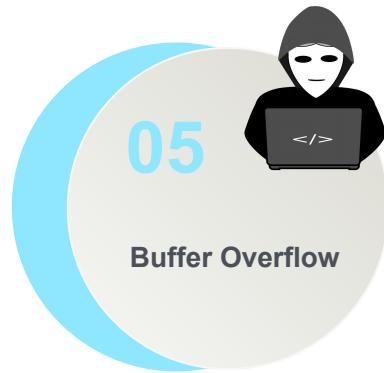
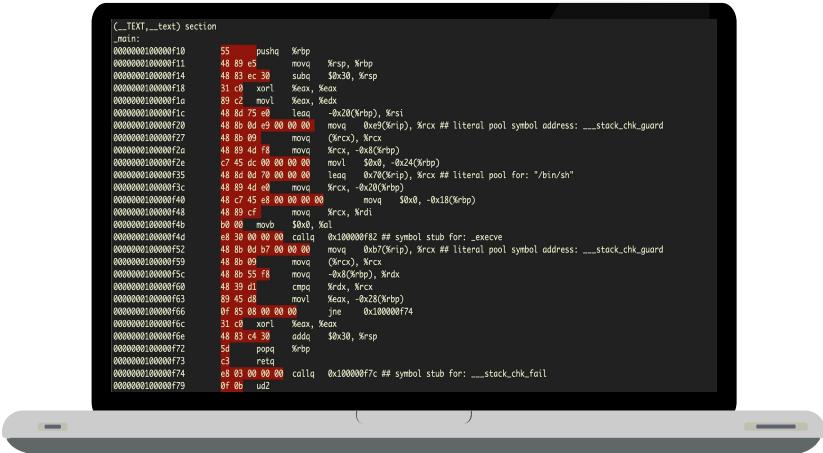
PopUp Ads Malware

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



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.



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

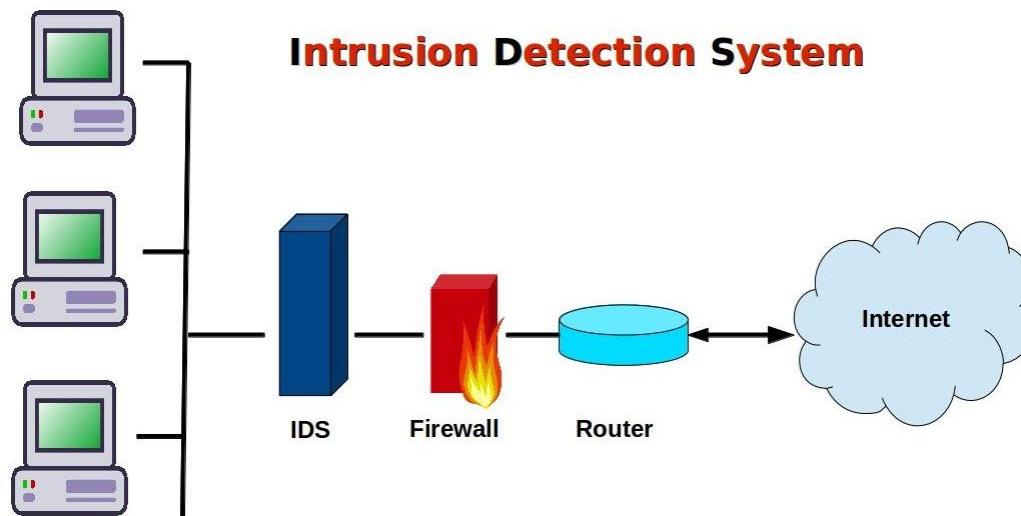
Buffer Overflow

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.



Thanks