Web

Introduction

Web application security

→ arrangements particularly with the security of sites, web apps, and web administration

→ applies particularly to internet and web frameworks

Security Threats → Virus threat
→ Hackers
→ phishing

Virus :- works by inserting itself into an app
→ data destruction
→ Altering data

Hacker or predator :- not computer, people
→ Skilled comp expert with technical skills who uses his/her abilities to gain unauthorised access to systems or networks in order to commit crimes

Phishing :- OWASP (Charitable foundation) open Web App Security Project
Brings awarness about web security.

Top 10 Vulnerabilities

---

(1) Injection :- malicious code or data is inserted into an app..

(*) Diff b/w Injection attack and Virus attack?

→ Injection attack involves the insertion of malicious code or data into an application's input field.

but virus attack involve the introduction of malicious software onto a user's system.

→ Injection target is an app but virus target is a system or device.

(2) Broken Authentication and Session Management

means, authentication mechanism of a web app fail to adequately verify the identity of users, leading to unauthorized access or other security breaches

refers to the process of maintaining and controlling a user's interaction with a web app during a specific period of time or "session"

(3) Sensitive Data Exposure

If app is not given the adequate protection to the sensitive data, → it can be exposed include password, credit card data etc

(4) XML External Entity :- (Extensible Markup Language)

(DoS attack)

file format used to store data

XXE → (target only XML parsers and processors)

allows an attacker to inject unsafe XML entities into a web app that process XML data

→ If this happen, the attacker can read local files on the server.

(5) Broken access control :-

occurs when an application does not properly enforce restrictions on what authenticated users are allowed to do.

(*) Difference b/w Sensitive Data exposure and Broken access control.

→ Sensitive data ~~breach~~ exposure, can occur due to poor encryption practices, improper storage or other weakness in data handling.

Eg:- Storing password in plaintext, using weak encryption algorithm, or not encrypting data in transit

→ Broken access control can occur when ~~due to~~ users can access unauthorised resources or perform actions they should not have permission to do

(6) Security Misconfiguration :-

occurs when a system, app, or network is not properly configured to implement effective security measures.

(7) Cross-Site Scripting :- (XSS)

(CSP) ~~occurs in w~~. It involves an attacker injecting malicious scripts (typically JAVA) into web pgs viewed by other users.

→ To prevent can use mechanisms like CSP

CSP → Content Security Policy.

security feature to help protect websites and web applications from various attacks like XSS.

CSP is to control and limit the sources from which content, such as scripts, Style Sheets, images and other resources

(8) Insecure Deserialization :-

refers to the process of reconstructing serialized data into objects without implementing proper security checks and precautions.

Attackers can introduce malicious payloads into ~~sta~~ serialized objects, potentially leading to execution of unauthorized code

(9) Using Components with know Vulnerability

Components with known vulnerability could be the o.s itself, or some internal issues with the system or even a library used by one of these plugins, making this a very frequent finding.

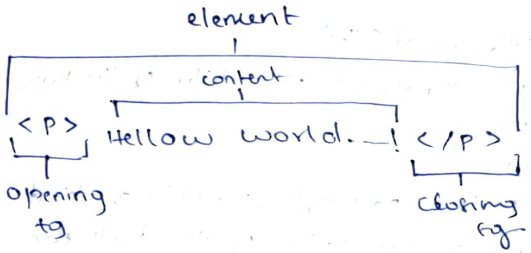
DoS (denial of service) attack is a cyber attack that makes a computer or other device unavailable to its intended user.

Serialization :- process of converting a data structure or object into a format that can be easily stored, transmitted, or reconstructed at a later time

(10) Insufficient Logging & Monitoring :-

an app or sys does not adequately record or ~~system doesn't~~ monitor security-related events and activities.

HTML



The Body

<body> ⟶ opening tag

</body> ⟶ closing tag.

Input

<body>

<P>what's up, doc? </P> ⟶ what's up, doc?

</body>

Output

child of <body>

parent

HTML Structure

when an element is contained inside another element. The child element is said to be nested inside of the parent element

The relationship b/w elements and their ancestor and descendent element is known as hierarchy

Eg:- <body> ⟶ Grandparent

 ⟶ parent

Siblings (children of)

<h1> Sibling to P, also grandchild of body </h1>

<P> Sibling to h1, but also grandchild to body </P>

</body>

Input

```
<body>
  <h1>Hello World</h1>
  <p>This paragraph is a child of the body element
  </p>
  <div>
    <p>This paragraph is a child of the div element
    and a grandchild of the body element</p>
  </div>
</body>
```

output

Hello World

This paragraph is a child of the body element

This paragraph is a child of the div element and a grandchild of the body element.

Headings

<h1> - used for main headings. All other used for subheadings.

Divs - short for "division" or a container that divides the page into sections

- div's can contain any text or other HTML elements, such as links, images or videos.

Remember always add two spaces of identation when you nest elements inside of for better readability.

Attributes :-

If we want to expand an element's tag, we can do so using an attribute.

Attributes are made of the following two parts.

→ The name of the attribute.

→ The value of the attribute

One commonly used attribute is the `id`

we can use the id attribute to specify diff content (such as `<div>`s) eg:- you have a content of bears in your file then the content is coded as `<div id:bears>` just to know the content is about

Displaying Text

→ Paragraphs `<p>` contain plain text

→ `<span>` contain short pieces of text or other HTML.

They are used to separate small pieces of content that are on the same line as other content

Styling Text :-

The `<em>` tag emphasizes text, while the `<strong>` tag highlights important text

→ The `<em>` tag will generally render as italic emphasis

→ `<strong>` will generally render as bold emphasis

Line Breaks :-

If you are interested in modifying the spacing in the browser, you can use HTML's line break element `<br>`. It is only composed of a starting tag.

Unordered List :-

In HTML, you can use an unordered list tag `<ul>` to create a list of items in no particular order.

The `<ul>` element should not hold raw text and won't automatically format raw text

into an unordered list of items.
Individual list items must be added to the unordered list using the <li> tag.

Ordered List

Each item is numbered. remaining is just like unordered list

Images :-

The <img> tag allows you to add an image to a web page. The <img> tag is a self-closing tag. Note that the end of the <img> tag has a forward slash /.
The <img> tag has a required attribute called src. src is set to location of image

Image Alt :-

The alt attribute, which mean alternative text, brings meaning to the images on our site. the alt is used just like src. The value of alt should be a description of the image

Videos :-

The <video> element requires a src attribute with a link to the video source
the <video> element requires an opening and a closing tag.
After the src attribute, the width & height attributes are used to set the size of the video displayed in the browser
The controls attribute instruct the browser to include basic video controls such as pausing and playing.
The text, video not supported, between the opening and closing video tags will only be displayed if the browser is unable to load the image

HTML DOCUMENT STANDARDS

Preparing for HTML

it's time to learn how to set up an HTML file we can let web browsers know that we are using HTML by starting our document with a document type declaration:

<!DOCTYPE html>

It must be the first line of code in your HTML doc

extension → .html

The <html> tag

To creat HTML structure and content, we must add opening and closing <html> tags after declaring <!DOCTYPE html>.

The Head :-

The <head> element contains the metadata for a web page. Metadata is information about the page that isn't displayed directly on the web page

Page Title :-

A browser's tab displays the title specified in the <title> tag. The <title> tag is always inside of the <head>

Where does the Title Appear?

Linking to Other web pages

You can add links to a web page by adding an anchor element (`<a>`) and including the text of the link in b/w the opening & closing tags.

Eg:- `<a>This is A link To wikipedia</a>`

The anchor element in the above example is incomplete without the `href` attribute (hyperlink reference)

`<a href = "link" >This is A link To wikipedia</a>`

Opening links in a New Window :-

The `target` attribute specifies how a link should open.

For a link to open in a new window, the `target` attribute requires a value of `_blank`. The `target` attribute can be added directly to the opening tag of the anchor element.

Linking to Relative Page :-

Many sites also link to internal web pages like Home, About and Contact.

When making multipage static website, web developers often store HTML files in the root directory, or a main folder where all the files for the project are stored

Eg:- Project - folder /
- about.html
- contact.html
- index.html

The files are stored in the same folder, we can link web pages together using a relative path

`<a href = "./contact.html"> Contact </a>`

In this eg; `<a>` is used as relative path to link from the current HTML file to the `contact.html`

`./` in `./contact.html` tells the browser to look for the file in the current folder

Linking At Will :-

Its possible to turn images into links by simply wrapping the `<img>` element with an `<a>` element

Eg:- `<a href = "text link" target = "_blank">`

Prickly Pear `</a>`

↓

```
<a href = "text link" target = "_blank">
<img src = "*.jpg" alt = "A red prickly
pear fruit" /></a>
```

Linking to Same page

In order to link to a target on the same page, we must give the target an `id`.

Whitespace :

Programmers use two tools to visualize the relationship b/w elements : Whitespace and Indentation.

CSS

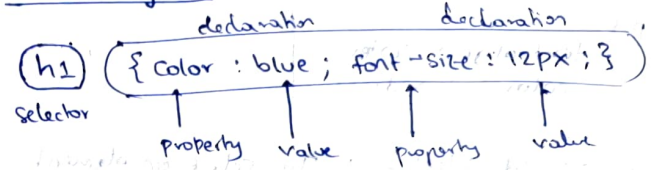
→ Used to style an HTML Doc

→ describes how HTML elements should be displayed

→ stands for Cascading Style Sheets

A CSS rule consists of a **selector** and a **declaration block**

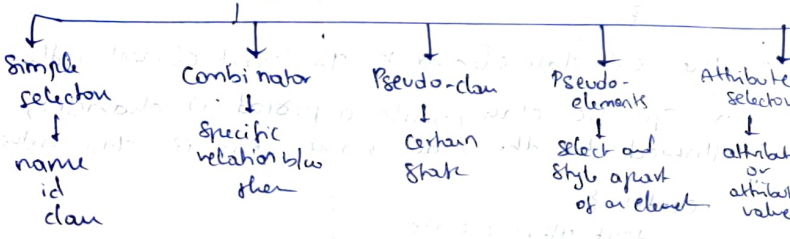
CSS Syntax



→ The selector points to the HTML element you want to style

→ declaration block contains one or more declarations separated by semicolons

CSS Selectors



1. The CSS element selector → <p> <h>
2. The CSS id selector → like
3. The CSS class selector → like →

(*) The only diff b/w them is that "id" is unique in a page and can only apply to at most one element, while "class" selector can apply to multiple elements.

④ Eg:-

```
p.centre {
    text align : centre;
    color : red;
}
```

In this ex. only <p> elements with class="centre" will be red and centre alligned.

① The CSS element selector

all <p> element on the page will be centre alligned & red color

```
p {
    text align : center;
    color : red;
}
```

② The css id selector :- To select an element with a specific id, write a hash (#) character, followed by the id of the element.

```
#Para 1 {
    text-align : center;
    color : red;
}.
```

③ The CSS class selector :- To select elements with a specific class, write a period (.) character, followed by the class name. Eg: if class = centre

```
.center {
    text.align : center;
    color : red;
}
```

④

```
p.cCenter {
    text-align : center;
    color : red;
}
```

In this example only <p> elements with class="centre" will be red & centre.

⑤

```
<p class = "center large">
```

In this example the <p> element will be styled ~~accordly~~ according to class="center" and to class="large".

⑥ The CSS Universal selector :-

The universal selector (*) select all HTML elements on the page.

```
* {
    text-align : center;
    color : blue;
}
```

⑦ The CSS Grouping selector :-

The grouping selector selects all the HTML elements with the same style definitions.

```
h1, h2, p {
    text-align : center;
    color : red;
}
```

How to Add CSS :-

three ways to insert CSS
- External CSS
- Internal CSS
- Inline CSS

External CSS

Each HTML page must include a reference to the external style sheet file inside the `<link>` element, inside the `<head>` section.

→ An external style sheet can be written in any text editor, and must be saved with a .css extension

→ The external CSS file should not contain any HTML tags

"mystyle.css"

```
body {
    background-colour : light blue;
}
h1 {
    colour : navy;
    margin-left : 20px;
}
```

NOTE: margin-left : 20 px; ⟶ Incorrect
margin-left : 20px; ⟶ correct

Internal CSS :- used if one single HTML page has a unique style.

The internal style is defined inside the <style> element, inside the head section.

```
<head>
<style>
body {
    background-color : linen;
}
h1 {
    color : maroon;
    margin-left : 40px;
}
</style>
</head>
```

Inline CSS :- used to apply a unique style for a single element.

→ add the style attribute to the relevant element

→ The style attribute can contain CSS property.

```
<h1 style = "color: blue; text-align : center;">
    This is a heading
</h1>
```

External style sheet

eg:-

```
<!DOCTYPE html>
<html>
<head>
<link rel="stylesheet" href = "mystyle.css">
</head>
  :
```

What style will be used when there is more than one style specified for an HTML element?

Priority order :-
1. Inline style.
2. Ext & Int style sheets
3. Browser default

CSS comments :-

CSS comments are not displayed in the browser, but they can help document your source code

→ A CSS comment is placed inside the <style> element, and starts with /* & ends with */

```
/* This is a single line comment */
```

→ You can add comments wherever you want

<!-- These paragraphs will be red --> HTML comment

/* Set text color to red */ → CSS comment

CSS colors :-

Predifined color names
- Tomato
- orange
- Dodger Blue
- Medium SeaGreen
- Gray
- SlateBlue
- Violet
- LightGray.

RGB ; HEX ; HSL ; RGBA ; HSLA value

Value represent (Red, Green, Blue light)

Each parameter defines intensity of color b/w 0 & 225

CSS Background Color :- You can set Background colour

```
<h1 Style = "background-color : DodgerBlue;">
        Hellaworld </h1>
<p  Style = "background-color : Tomato;"> lorem
        ipsum ... </p>.
```

CSS Text Color :- You can add color to text.

```
<h1 Style = "color : tomato;"> Hello world </h1>
```

CSS Border Color :-

```
<h1 Style = " border : 2px solid tomato; ">
        Hello world </h1>
```

- RGB → (Red, Green, Blue)
- RGBA → (Red, Green, Blue, Alpha) → colour intensity like half transparent.
- HEX → #RRGGBB (hexadecimal integer specify the components of the colour)
  - #000000 → Black
  - #ffffff → white
- 3 digit HEX value → #RGB
- HSL → (Hue, Saturation, Lightness)
  - Hue: degree of color wheel 0 to 360; 0 → red; 120 → green; 240 → blue
  - Saturation: % value, 0% shade of gray; 100% full colour
  - Lightness: % value; 0% black; 50% middle; 100% white
- HSLA → (Hue, Saturation, Lightness, alpha)

CSS Backgrounds :-

① **CSS background colour :-** background-color — specifies bgcolor of element

```
body {
    background-color : light blue;
}
```

opacity/transparency :- 0.0 → 1.0 (transparent → opacity)

opacity

```
div {
    background-color : green;
    opacity : 0.3;
}
```

② **CSS background image :-**

```
body {
    background-image : url("paper.gif");
}
```

background-repeat : → repeat x . :- horizontal repeat
→ repeat y :- vertical repeat
no repeat

background-position right top : etc

③ CSS background Attachment

background-Attachment → should scroll or fixed.

④ CSS background Shorthand :-

To shorten the code, it is also possible to specify all the background properties in one single property.

background : red url( ) no-repeat right top

The order of the property value

1. bg-color
2. bg-image
3. bg-repeat
4. bg-attachment
5. bg-positions

What is OT? (Operational Technology)

use of hardware & software to monitor and control phy process, device, infrastructure.

What is OT security?

Gartner defined

" Practice and technologies used to
- (a) protect people, assets & info
- (b) monitor and/or control phy devices, process & events
- (c) Initiate static change to enterprise OT sys.

→ **OT Cyber security** was not necessary because OT systems are not connected to internet

→ Unlike traditional IT, which deals with data & information systems, OT is focused on the control and automation of physical process

→ OT security is a specialized field that aims to safeguard the technology used in industrial and critical infrastructure settings, recognizing the unique challenges and risks associated with these environments.

→ OT network report to the COO
IT " " CIO

Components of OT :-

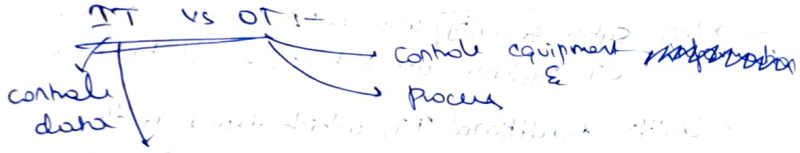
ICS, includes diff type of devices, systems, controls & networks that manage a variety of industrial process.
The most common are SCADA & DCS

SCADA :- System collect data from distributed sensors & send it to a central computer that controls data

DCS :- used to manage local controllers or devices of production system in one location.

IIOT Devices :-

* Smallest components of OT are sensors, monitors, actuators etc. These sensors are example of IIOT.



What is IT-OT convergence :-

→ With IT-OT integration, the data collected by phy equipment and IIOT device can be used to identify problems or increase efficiency.

→ OT component like control system, SCADA etc being connected to IT components like processor, storage and system management

→ OT is not secure because when it is connected to IT network it immediately exposes the OT networks

Why are OT networks at risk ?

Internet connectivity introduces ease of operability, but apart from those benefits, this transformation has exposed the system to vulnerabilities that cannot be stopped by an armed guards. This can cause destruction of these highly valuable machines, as was proven in the Stuxnet

Problems :- (1) Direct Internet connections
(2) Insecure passwords
(3) Unnecessary Exposure
(4) Outdated O.S.

Challenges in OT threat Detection :-

There are few challenges in OT threat detection.

(1) Lack of bespoke skills :- Limited cybersecurity skills & Lack of knowledge in SOC security operation centre

(2) Changing adversarial tactics :- Threats are continously changing & advancing.

(3) Disparate tool sets :- No single tool or sensor can provide visibility into all threats

(4) Passive, manual tooling :-

(5) Old equipment, exposed endpt :-

In context of ICS/SCADA OT, protocols are sets of rules and convention that define how devices and systems communicate with each other over a network.

Level 2 protocols :-

6LoWPAN :- [IPv6 over Low Power Personal Area Networks] is an network protocol used for communication b/w smaller and low power devices with limited processing capacity, it is mainly used for home & building automation

Here, Smaller & low power devices with limited processing. refers to resource-constrained devices : eg:-

1. Microcontrollers (used in embedded Sys)
2. Wireless Sensor Nodes (used in wireless sensor network (WSNs) & IOT)
3. RFID tags (Radio-Frequency Identification used in tracking)
4. Smartcards (credit cards)
5. Wearable devices
6. Environmental Monitoring Devices.
7. Remote control with (TV remote etc)

DNP3 :- [Distributed Network protocol 3]

used to interconnect components within process automation systems. It is widely used communication protocol in the utility and energy sector, particularly in the control of electric and water distribution system.

DNS/DNSSEC :- [Domain Name System] / [Domain Name System Security Extensions]

Protocol used on internet to translate human-readable domain names into numerical IP address.

is an extension to DNS protocol. It introduces cryptographic techniques to add an extra layer of security to DNS.

DNSSEC is a crucial technology used to improve the security of DNS.

FTE [Fault Tolerant Ethernet]

→ The focus is on minimizing downtime and disruption caused by network failures.

→ FTE is designed to quickly and efficiently handle network fault or failure

→ A "node" typically refers to a device or network endpoint that is part of the ethernet network. Nodes can be computers, servers, switches, routers etc

→ LAN Local Area Network

IEC 60870-5-101/104 : This is an extension of the IEC 101 protocol with some modifications in transport, network, link & phy layer services. This is for communication b/w control station and substation through the standard TCP/IP network

SOAP [Simple Object Access Protocol] is a messaging protocol containing a set of rules to administrate data transfer b/w client and server using the XML message format

What is accen control?

Accen control is a security measure used to regulate and mange who has permision to accen specific resources, areas, or information within a system, organization, or physical space.

There are two type of accen control → Physical
→ Logical

① Physical :- limit accen to compuses, buildings, room etc

② Logical :- limits connections to computer networks, system file & data

- Authentication → username, pass, biometrics, smartcards, multifactor
- Authorization → eg: a user might have read only accen to a document, while a administrator has full accen to edit.
- Multifactor Authentication (MFA) → require 2 or more authentication factors ~~is often~~

Why is accen control?

The goal of accen control is to minimize the security risk of unauthorized accen to physical & logical systems.

→ Widely used accen control → Role-based AC

MAC is a strict accen control model used in high-security Mandatory environments, such as goverment or military systems

DAC owners or administrators of the protected system, Discretionary data or resources set the policies defining who or what is authorised to accen to resource

RBAC accen to computer resources based on individuals etc or groups with defined busines functions

What is Principle of least Privilege? (POLP)

It is the idea that at any user, program or procen should have only the bare minimum privileges necessary to perform its function

→ can also proffered as Principle of min privilege (PUMP)

Principle of least authority (POLA)

How PLP work?

→ works by allowing only enough accen to perform the required job

→ Implementing the POLP helps contain compromises to their area of origin, stopping them from spreading to the system at large.

Benefits of the Principle of least P.

Better security
minimum attack surfac
Limited malware propagation
Better stability

What is ICS?

Industrial control system, there are specialized system used in various industries to control and manage critical infrastructure procen and operation.

S.No	Name	Year	Place	Type	Why
1	Triton	2017	Saudi petrochem plant	Malware attack	lead an explosion on release of toxic gas purposefully to cause loss of life
2.	Taiwan's state owned energy company	—	CPC corp in Taiwan, a national asset in charge of oil delivery & liquid natural gas	Ransomware attack	station unable to use payment used VIP card payment apps.
3.	Israeli water sys	2020	Israeli	cyberattack	designed to compromise the ICS command & control sys for Israeli pumping station, sewer sys etc
4.	Nippon Telegraph & Telephone (NTT)	—	The data breach leaked data of 621 corporate clients and hybrid in nature, in that it was committed both from the cloud and on-site		
5.	Moderna	—	China a company at the forefront of covid-19 vaccine development		it was revealed the hackers have been terrorizing hundreds of enterprises & govt agencies