



**WEB  
PROGRAMMING**

# **PROJECT BLOG SITE**



**[HTTPS://AYONTAKUR.GITHUB.IO/BLOGSITE/](https://ayonthakur.github.io/blogsite/)**



# Team Members



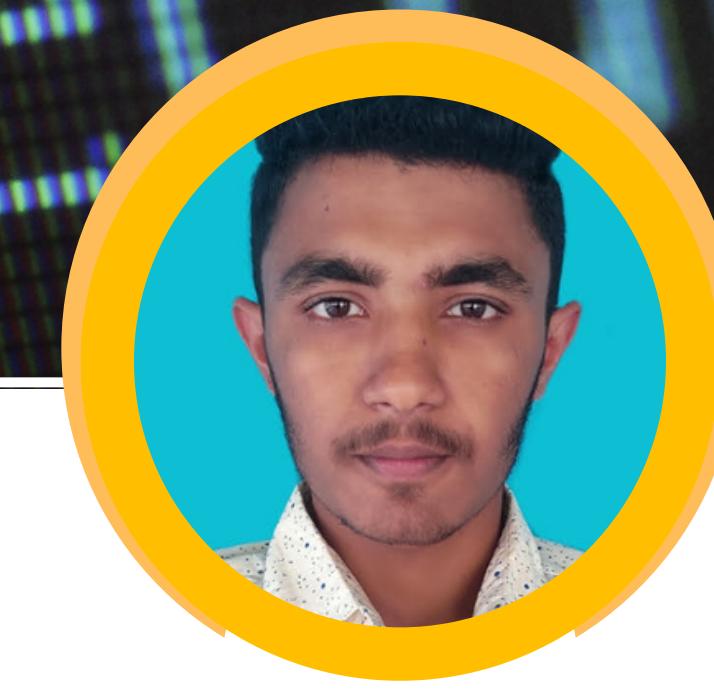
**Ayon Debnath**

*Leader*

Department

CSE

ID:CSE2201025009

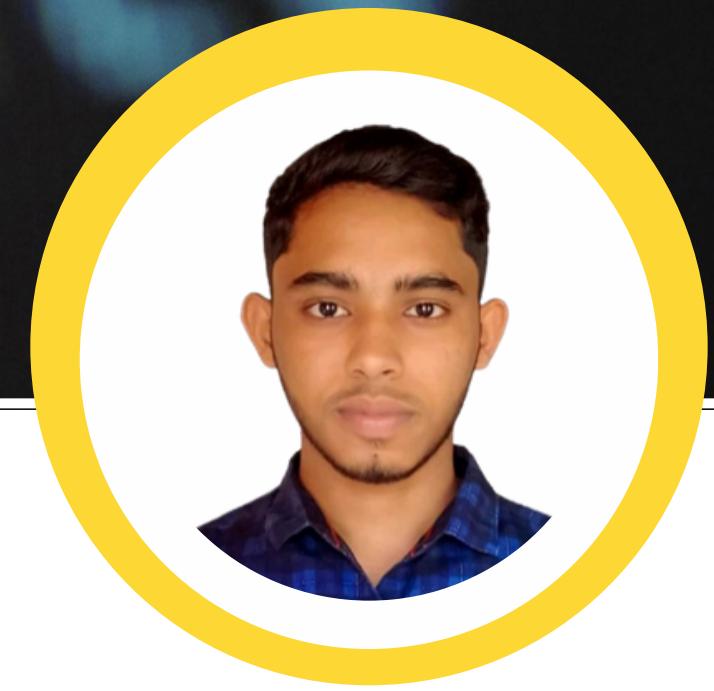


**Zubayar Hossain**

Department

CSE

ID:CSE2201025075

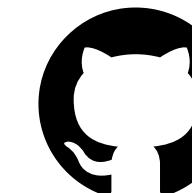


**Mustafizur Rahaman**

Department

CSE

ID:CSE2201025070



<https://github.com/ayonthakur/blogsite>

# Blog Site

## on Cyber Security



<https://github.com/ayonthakur>



# Page

- Home
- About
- Gallery
- Video
- Contact Us

# Home Page



A screenshot of a website titled "cyber security". The navigation bar includes links for Home, About, Gallery, Video, Contact Us, and a red "Youtube" button. A yellow curved arrow points from the top left towards the "Home" link. The main content area features a section on SQL injection with a laptop icon and a diagram of XSS (Cross-Site Scripting) attacks. It also includes sections on LFI (Local File Inclusion) vulnerability and a general introduction to cyber security.

**DCSS**

Home About Gallery Video Contact Us Youtube

## cyber security

Know about cyber security and be safe from cyber world

**TYPES OF SQL INJECTION Attack Examples**

**What is Sqlinjection**

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.

**Cross Site Scripting(XSS)**

The diagram illustrates an XSS attack. An "Attacker" sends a malicious payload via a "WEB APPLICATION" to a "Server". The server then serves this payload to "Client 1" and "Client 2". The payload contains malicious scripts that interact with a "DB" (Database). The payload is shown as: `INSERT ... <script>alert(1)</script>`, `text=<script>alert(1)</script>`, `<html> Comments <script>alert(1)</script> <html>`, and `SELECT ... <script>alert(1)</script>`.

**LFI VULNERABILITY**

The diagram shows an "Attacker" modifying a file path on a "WEB APPLICATION" to include a local file, such as `https://example.in?php=etc/passwd`. The application then serves this modified file to a "Client". The client's browser displays the contents of the local file, which in this case is the server's password file. The attack steps are: STEP 1 MODIFY, STEP 2 INJECT PAYLOAD IN SERVER, and STEP 3 RESULTS ON BROWSERS.

**Local File Inclusion**

(LFI) allows an attacker to include files on a server through the web browser. This vulnerability exists when a web application includes a file without correctly sanitising the input, allowing an attacker to manipulate the input and inject path traversal characters and include other files from the web server.

- Menu Bar
- Button
- Container
- `<nav> ....</nav>`
- `<div class=" " " ..</div>`

Responsive  
100%

Button

# About Page





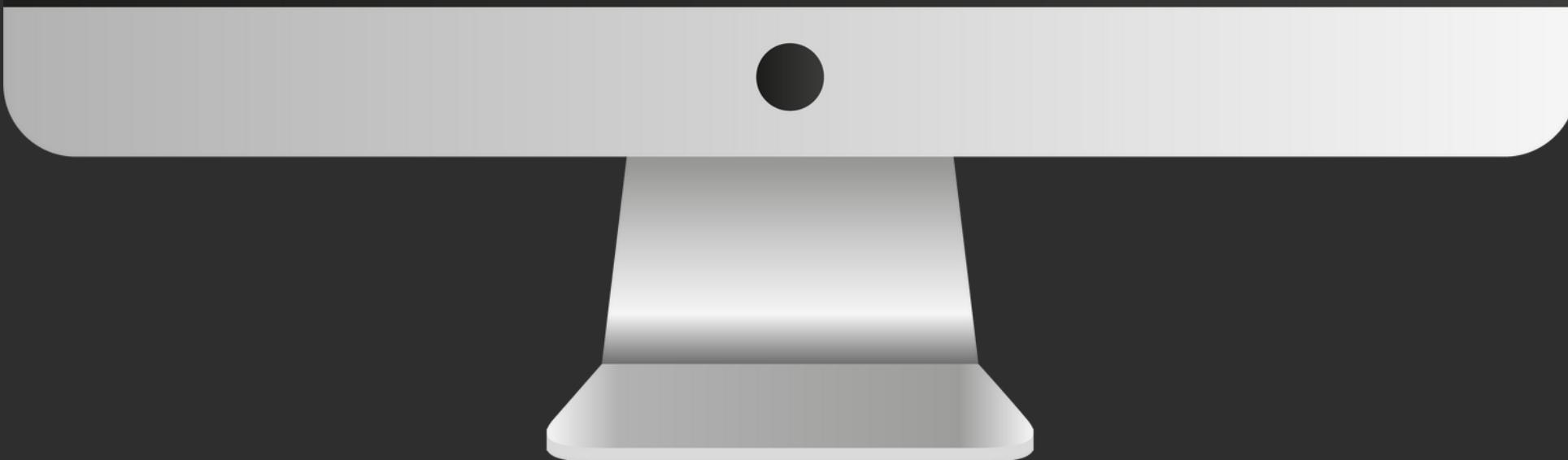
**Debnath Cyber Security Service**

## About Us

**Developer & Designer**

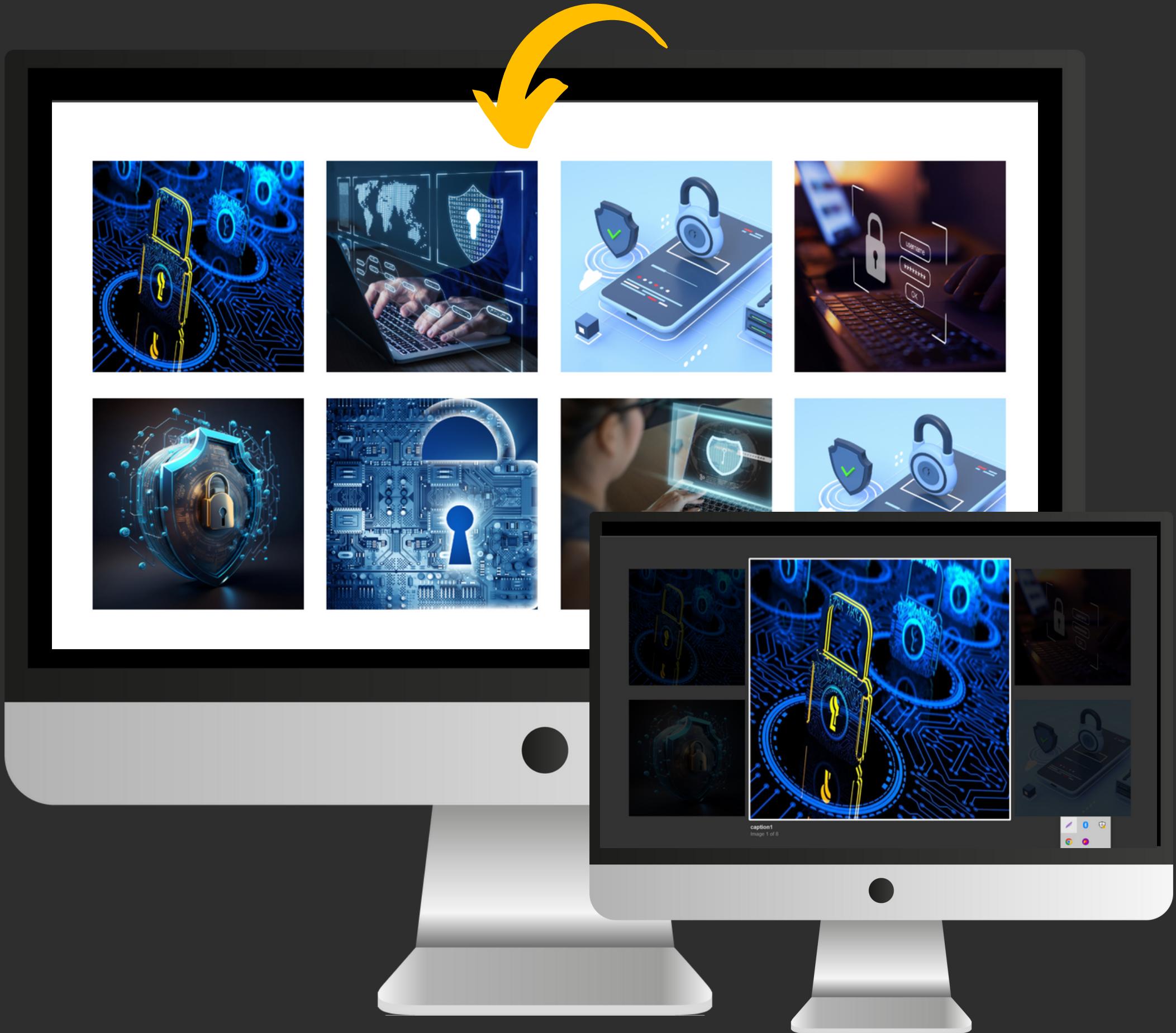
Hi sir/mam, we provide **ethical hacking, website security, malware removing service**. We are good at my job. We will recover WordPress hacked websites and make secure themes from future attacks. I also make website as you need .I will try to provide my best service. 100% client satisfaction is my prime goal.

[Let's Talk](#)



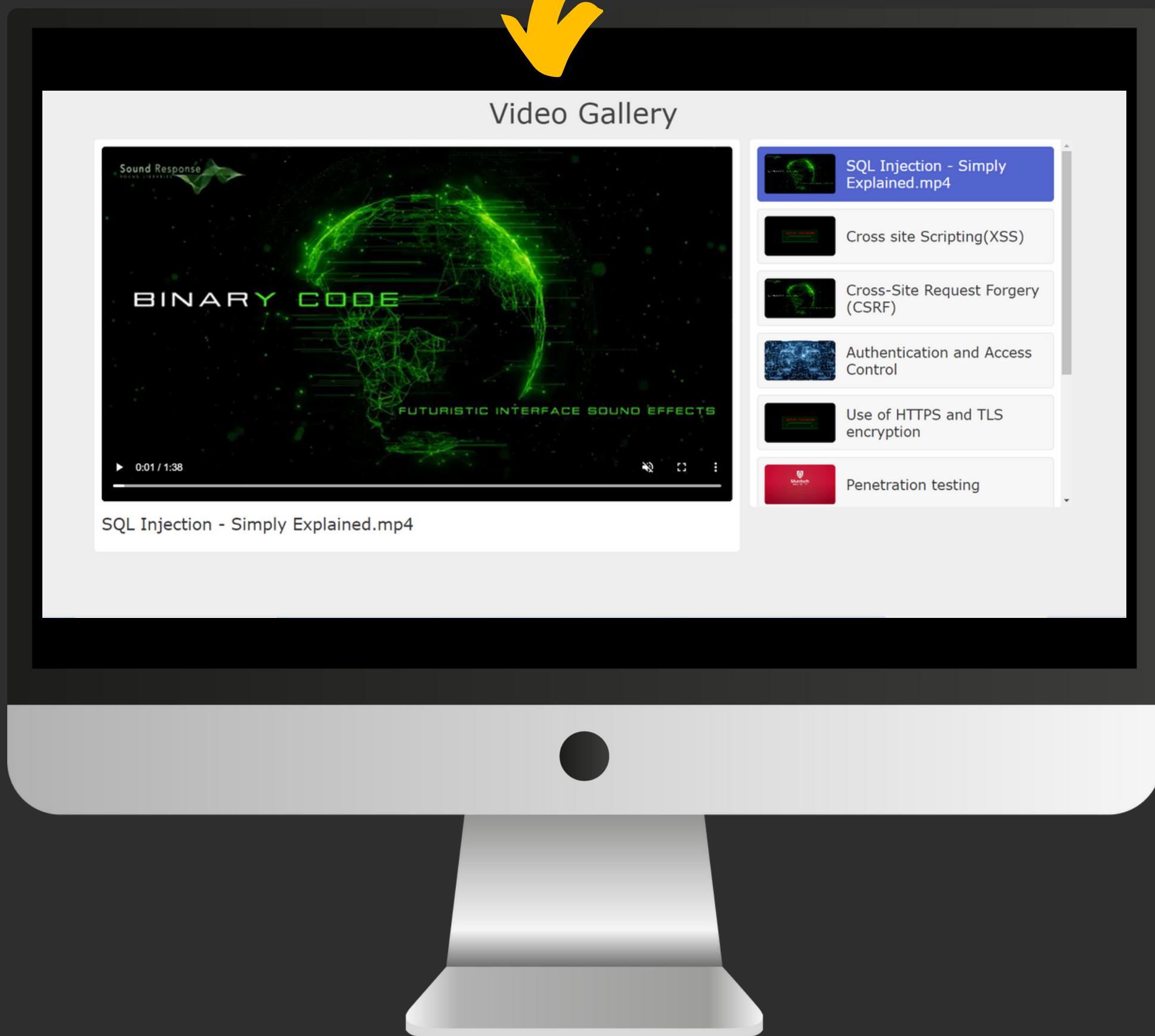
- **<section>.....</section>**
- **<div class=" " " >.. </div>**
- **h1 ,h5**
- **Button**
- **Container**
- **Responsive**

# Gallery Page



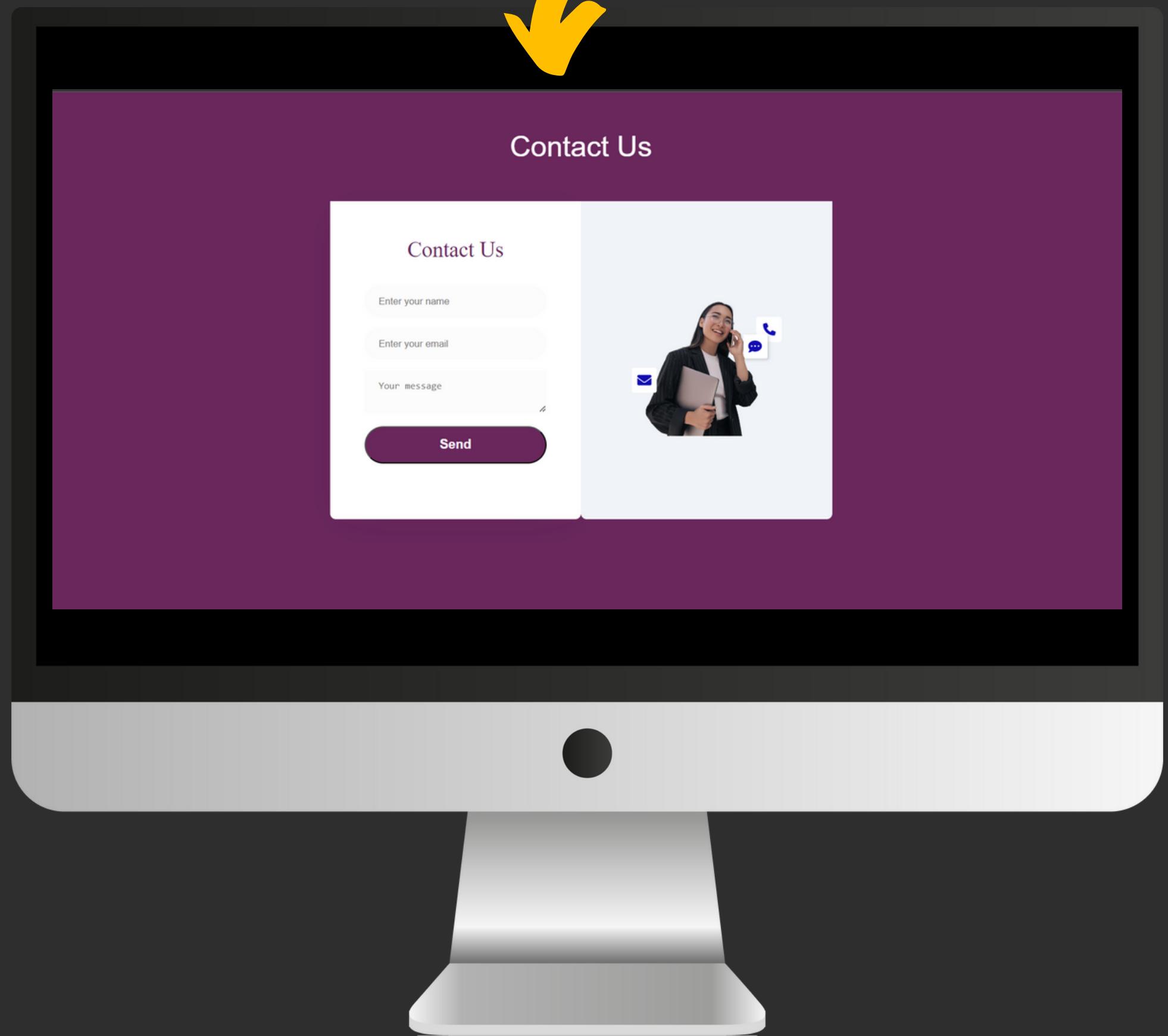
- Container
- `<div class="" .. ></div>`
- `<a href="" data-lightbox="" data-title=""> {hyperlink}`
- Lightbox (slide-show) **javascript**
- Responsive

# Video Page



- Container
- **<video src=" " controls muted autoplay></video>**
- **document.querySelectorAll('')**
- **JavaScript ( Video playlist)**
- **100% Resposive**

# Contact us Page



- **h1**
- **<form>...</form>**
- **<input type="text" name=" " placeholder="Enter your name">**
- **<textarea>....</textarea>**
- **Button**

**Thank you**