Task 1

1) Appropriate Authentication within system, all credentials must match.
2) Appropriate Authorization, access rights must be specified in order to access resources related to information security.
3) Data protection, the entire user's data prompted is secured.
4) Passwords must be encrypted, to protect the user's data.
5) No unrelated and redundant information must be stored into the system.
6) Images with specific formats are to be accepted when uploaded (format of .jpg/.png/.gif).
7) Images not greater than 2MB must be allowed to be uploaded.
8) Dynamic menu's Website loaded according to the user's role.
9) Appropriate and well implemented validations.
10) Symmetric and asymmetric algorithms implemented in system
11) Encryption of the connection string which connects the Database with the website
12) Encryption of any querystrings.
13) Appropriate Password hashing when registering and logging a user.

Task 2

Assets

ID	Name	Description	Trust Level
A1	User	Assets in "PicDo" Website	
A1.1	User's login data	User's credentials username and password. This asset requires protection in case of theft any another user would have access to everything he didn't have.	T2 Authenticated user T3 Database server admin
A1.2	User's personal data	User's personal data including contact information. Appropriate Protection is needed since personal data might be leaked to the wrong person such as contact number	T2 Authenticated user T3 Database server admin

ID	Name	Description	Trust Level
A2	User		
A2.1	Authenticated	User must log in the website before viewing any images he/she uploaded.	T2 Authenticated user
A2.2	Authenticated	The user could upload an image	T2 Authenticated User

ID	Name	Description	Trust Level
A3	Guest		
A3.1	Permissions	The guest can only see navigate through some pages of the website e.g. login, about us etc.	T1 Guest

ID	Name	Description	Trust Level
A4	Admin		
A4.1	Permissions	The Admin is allowed to view all the images of all the clients.	T3 Admin

ID	Name	Description	Trust Level
A6	Image		
A6.1	Download Image	The Client who uploaded the image is only allowed to download the image(and view it). Admin is also able to download it since he/she has access to the whole images.	T2 Authenticated User T3 Admin
A6.2	Upload Image	User is able to upload images in his own account and also the Admin.	T2 Authenticated User T3 Admin
A6.3	View Image	User is capable to view only the images he uploaded, also admin has the right to view all images uploaded by all users.	T2 Authenticated User T3 Admin

Trust Levels

ID	Name	Description
T1	Guest	A user who has authorizations and can view partial pages of the website.
T2	Authenticated user	A registered user who has correct credentials
T3	Admin	A user who can view all images regardless who uploaded it.

Entry Points

ID	Name	Description	Trust Level
E1	Login Page	This page allows users to input their email and password and access the website, with their role assigned.	T1 Guest T2 Authenticated User
E1.1	Login method	This Login method compares the user's credentials with the data stored in database and a session is created.	T1 Guest T2 Authenticated User T3 Admin
E2	Register Page	This page allows the guest to register himself or herself as a new user.	T1 Guest
E3	Upload Image	This method allows the user to upload Images	T2 Authenticated User

Threat Listing

ID	TR1
Name	Hacking Attempt
Description	Hacker attempts to log in without having a valid username and password
STRIDE	Tampering, Elevation of privilege
Entry Points	E1 - Login Page E1.1 - Login Method
Assets	A1 - User login
Mitigated/Strategy	Inspecting users logging details appropriately, and using strong passwords when the user registers.

ID	TR2
Name	Hacker Hacks inside by stealing Username and Password
Description	Hacker Manages to get another user’s credentials, Giving the hacker access to all data of the client.
STRIDE	Information disclosure, Tampering, Elevation of privilege
Entry Points	E1 - Login Page E1.1 - Login Method
Assets	A1.1 - User login A1.2 – User’s personal data
Mitigated/Strategy	Strong passwords enforced, encryption must take place, and db must be protected from external access.

ID	TR3
Name	User uploads an malicious file
Description	User tries to upload a file which is not .jpg/.png/.gif and greater than 2MB
STRIDE	Tampering
Entry Points	E3 – Upload Article
Assets	A6.4 – Uploaded Article
Mitigated/Strategy	Appropriate validation on both client and server side.

ID	TR5
Name	Buffer Overflow
Description	The designated attacker will excess this allocated space in the system, which will eventually lead to the extra data overwriting the data in other areas.
STRIDE	Information disclosure, Spoofing
Entry Points	E1 - Login Page E2 - Register Page
Assets	A1, A2, A3, A4, A5, A6, A7
Mitigated/Strategy	Response sizes are limited accepted by the DNS. Keep the buffer from overflowing by manually limiting its size.

ID	TR6
Name	unauthorized pages access.
Description	Attacker attempts to access pages by inputting directly the URL into address bar into the browser without having privileges to the system.
STRIDE	Tampering, Information disclosure
Entry Points	E3 - Upload Article, E4 - Publish article, E5 – Identifying Roles
Assets	A1 – User login, A6 - Article
Mitigated/Strategy	Validate roles and re-direct the user to another page when trying to access a web page which is not authorized.

ID	TR7
Name	Denial Of Service
Description	Attacker overwhelms the website with requests for loads of information, which results in slowing down the operation (system) or also brings it down completely.
STRIDE	Tampering, Repudiation, Spoofing
Entry Points	E1- Login Page , E2 – Register Page, E3 - Upload Article
Assets	A1, A2, A3, A4, A5, A6, A7
Mitigated/Strategy	

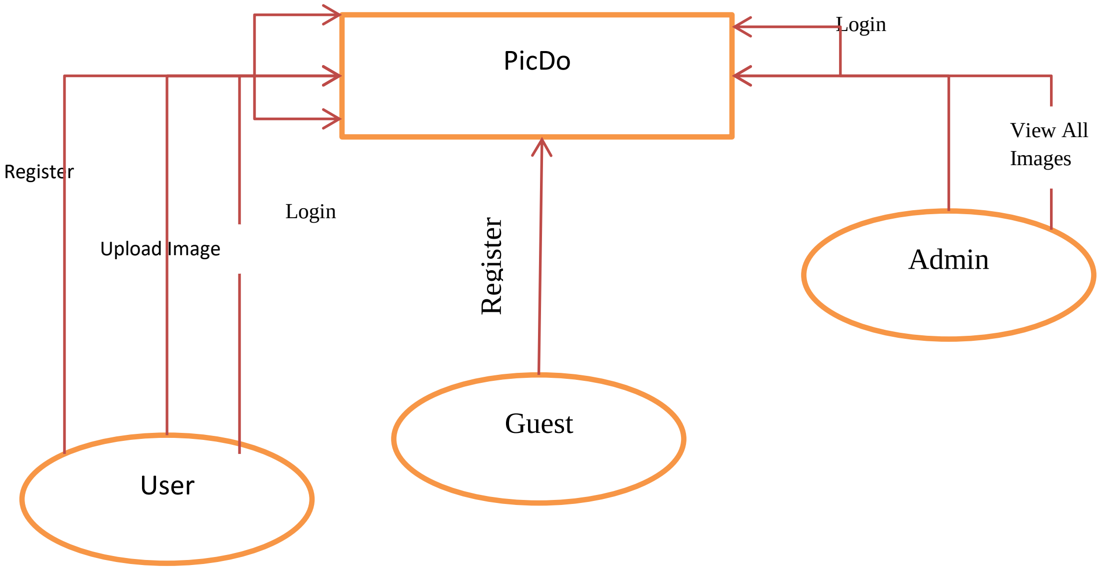
ID	TR9
Name	SQL Injection
Description	Inputting an SQL statement from the attacker into the website which can harm the website’s data.
STRIDE	Tampering, Denial of service
Entry Points	E2 – Register Page
Assets	A1 – Login User, A6 - Article
Mitigated/Strategy	Good validations both on client and server side. Also use secure libraries.

ID	TR10
Name	Session Hijacking
Description	Attacker will infiltrate into the session of another user, reading information as it passes between the user and the server.
STRIDE	Tampering, Information disclosure
Entry Points	E1 – Login Page
Assets	A1 – Login User
Mitigated/Strategy	Make sure that the login page is HTTPS. When the user logs in, set a secure cookie.

Ranking Threats

	High(3)	Medium(2)	Low(1)
Damage potential	TR6, TR7, TR9	TR1, TR2, TR3, TR5, TR10	
Reproducibility	TR1, TR2, TR7	TR3, TR5, TR6, TR9, TR10	
Exploitability	TR1, TR2, TR3,TR10	TR5, TR7, TR9	TR6,
Affected users	TR3, TR10	TR1, TR2, TR5, TR7	TR6, TR9
Discoverability	TR1	TR2, TR3, TR4, TR5, TR7, TR9, TR10	TR6

DFD


PicDo
Login
Register
Upload Image
Login
Register
View All Images
Admin
Guest
User