

PMPS - Patient Medical Profile System

Front-End Security Mechanisms

JavaScript-based Data-Validation

- Validating user inputs at real-time
- Indicating and removing invalid inputs from forms
- Invalid inputs also include injection attack string

PHP-based API Functions

- Data-validation layer
- Transmitting encrypted Login JSON request over TCP port to Back-End
- Receiving, decrypting ,validating and authenticating Login JSON response
- Encoding a JSON request per an API function
- Transmitting encrypted JSON request over TCP port to Back-End
- Receiving encrypted JSON response which matches the request
- Decrypting and validating JSON response attributes and setting session variables accordingly
- Print retrieved data on a specific webpage
- Each API function is being processed independently of other functions (unique .php file)

PHP-based Restricted Views

- Access to restricted views is based on session variables and additional authentication mechanisms
- An additional data-validation layer
- Access to relevant API functionality presented is restricted base on type of permission

Front-End Structure

Login Process and Interface

- index.php

Login Authentication

- auth.php

JavaScript Validation:

- initialValidation.js

PHP Validation

- validation.php

Restricted Views:

- home_emt.php
- home_doctor.php
- home_admin.php

Logout Interface

- logout.php

Additional API Functions (JSON Communication)

- retPatInfo.php
- addPat.php
- modPatInfo.php
- modPatName
- remPat.php

Design Elements

- style.css
- jquery.placeholder.js