v 1.1

Programowanie Aplikacji WWW

Laboratorium
nr 6

Opracowane przez:
mgr inż. Artur Samojluk

UWM w Olsztynie

PHP – prosty CMS w naszej stronie WWW

część 1

Wstęp do ćwiczenia

PHP Hypertext Preprocessor – język skryptowy zaprojektowany do generowania dynamicznych stron internetowych w czasie rzeczywistym. Język PHP pozwala na programowanie zaawansowanych pełnoprawnych aplikacji. Można go stosować do generowania grafik (np. GTK+) lub do obliczeń arytmetycznych dla dużych liczb (np. biblioteka BC Math). PHP jest językiem kompilowanym po stronie serwera w czasie rzeczywistym. Oznacza to, że nie należy przeprowadzać wcześniej procesu kompilacji (cały czas pracuje się na otwartym kodzie). Składnia języka jest mieszanką zapożyczeń z C, Perl oraz Java. Ma szerokie możliwości konfiguracji, optymalizacji kodu i daje szeroki wachlarz gotowych bibliotek. Manual na stronie: https://www.php.net/

CMS - z ang. Content Management System (System Zarządzania Treścią). Jest to integralny element strony WWW pozwalający na samodzielne i darmowe, modyfikowania treści z poziomu przeglądarki internetowej. CMS pozwala na zarządzania treścią strony dla osób, które nie mają znajomości programowania ani uprawnień do części serwerowej (ftp) naszej aplikacji.

Ćwiczenie do wykonania.

TIP 1. W celu łatwiejszego zrozumienia zagadnienia, temat laboratorium został podzielony na kilka części. Jeżeli wiesz, potrafisz, rozumiesz zasady działania CMSa możesz zrealizować projekt od razu w całości.

Projekt proszę wysłać na e-mail spakowany zip lub rar w katalogu *imie_nazwisko_nr_indeksu.*

Zadanie 1. Oznacz projekt jako wersja v1.5, wykonaj poniższe czynności modyfikujące projekt. Utwórz katalog *admin* w swoim projekcie. W katalogu *admin*, utwórz plik *admin.php*

Zadanie 2. Uruchom z pomocą panelu XAMPP, bazy danych MySQL. Następnie uruchom opcje „admin” dla baz danych. Otworzy się środowisko do obsługi baz danych PHPmyAdmin. Następnie wykonaj czynności:

1. Utwórz bazę danych: *moja_strona*
2. Utwórz w bazie danych tabele: *page_list*
   Zdefiniuj pola (kolumny) tabeli ich typy: *id* -> autoincrement, start od 1, *page_title* -> varchar(255), *page_content* -> text, *status* -> INTEGER, domyślną wartość ustaw na 1.
3. Wprowadź do tabeli zawartość swoich podstron z użyciem PHPmyAdmin.

TIP 2. Opcjonalnie można w tabeli *page_list* dodać dodatkowe pole: alias –> varchar(20), UNIQUE, które pozwoli również na wyszukiwanie zawartości stron.

Zadanie 3. Połącz swoją stronę z bazą danych. Utwórz plik *cfg.php* w folderze głównym projektu. Plik zaimplementuj *cfg.php* wywołaj w metodzie *include()* na początku pliku index.php

```php
<?
   $dbhost = 'localhost';
   $dbuser = 'root';
   $dbpass = '';
   $baza = 'moja_strona';

   $link = mysql_connect($dbhost,$dbuser,$dbpass);
   if (!$link) echo '<b>przerwane połaczenie </b>';
   if(!mysql_select_db($baza)) echo 'nie wybrano bazy';
?>
```

TIP 3. Sprawdź jakie masz ustawioną domyślną nazwę użytkownika i hasło, zależnie od środowiska może być root/root lub jeszcze inaczej**.**

Zadanie 4. Utwórz plik showpage.php i użyj zapytania SELECT do wyświetlenia treści swojej strony WWW. Opakuj to odpowiednimi warunkami (zmodyfikuj warunki jakie miałeś w wersji 1.4 to includowania plików html.

```php
<?

function PokazPodstrone($id)
{
 //czyscimy $id, aby przez GET ktoś nie probował wykonać ataku SQL INJECTION
  $id_clear = htmlspecialchars($id);

   $query="SELECT * FROM page_list WHERE id='$id_clear' LIMIT 1";
    $result = mysql_query($query);
     $row = mysql_fetch_array($result);

   //wywolywanie strony z bazy
     if(empty($row['id']))
     {
       $web =  '[nie_znaleziono_strony]';
     }
     else
     {
       $web = $row['page_content'];
     }

  return $web;
}

?>
```

TIP 4. Podstawowym elementem optymalizacji wyszukiwania w bazach danych jest ustawienie odpowiedniej wartości parametru LIMIT. Jeżeli nie ma parametru limit, a w bazie jest np. milion rekordów, to nawet jak znajdzie ten dla nas najważniejszy – zapytanie będzie wykonywało się do samego końca bazy. Jest to niepotrzebne obciążenie, gdy wiemy, że wynik już został znaleziony.

TIP 5. W bazach MySQL, zapytanie LIMIT można użyć z dwoma parametrami, początku i końca – używa się to najczęściej do tworzenia stronicowania długich list rekordów.

TIP 6. Tu w naszej stronie pojawia się potencjalna luka w zabezpieczeniach, wszędzie tam gdzie są pobierane pola z POST lub GET, należy być czułym na zagrożenie. Ktoś może próbować podstawić inne parametry, a nawet całe kody skryptów i przejąć kontrolę nad stroną lub wykraść wrażliwe dane.