Biblioteki kryptograficzne

Atroszczyk Dominika, Daria Shevchenko

Założenia języka

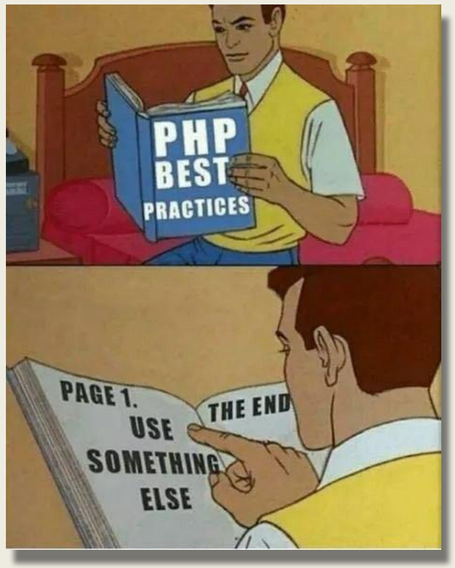
Hypertext Preprocessor

skryptowy język programowania

strony internetowe

aplikacji internetowe

- Język interpretowany: kod PHP jest wykonywany na serwerze, a wynikowy HTML jest przesyłany do przeglądarki użytkownika.
- Możliwe jest tworzenie dynamicznych stron internetowych, które mogą dostosowywać się do potrzeb użytkownika i generować zawartość na podstawie danych z bazy danych lub innych źródeł.



Historia

Stworzone w 1994 roku przez Rasmusa Lerdorfa jako zestaw skryptów CGI (Common Gateway Interface) do obsługi stron osobistych.

- Początkowo nazywane "Personal Home Page Tools"
- Udostępnienie koda PHP publicznie doprowadziło do rozwoju społeczności programistów, którzy przyczynili się do rozwoju języka.
- W 1997 roku wydano pierwszą oficjalną wersję PHP 3.0, która wprowadziła wiele nowych funkcji i udoskonaleń

Rasmus Lerdorf

Struktura i elementy

Kod PHP jest umieszczany wewnątrz znaczników **<?php** i **?>**. Pozwala to na oddzielenie kodu PHP od kodu HTML.

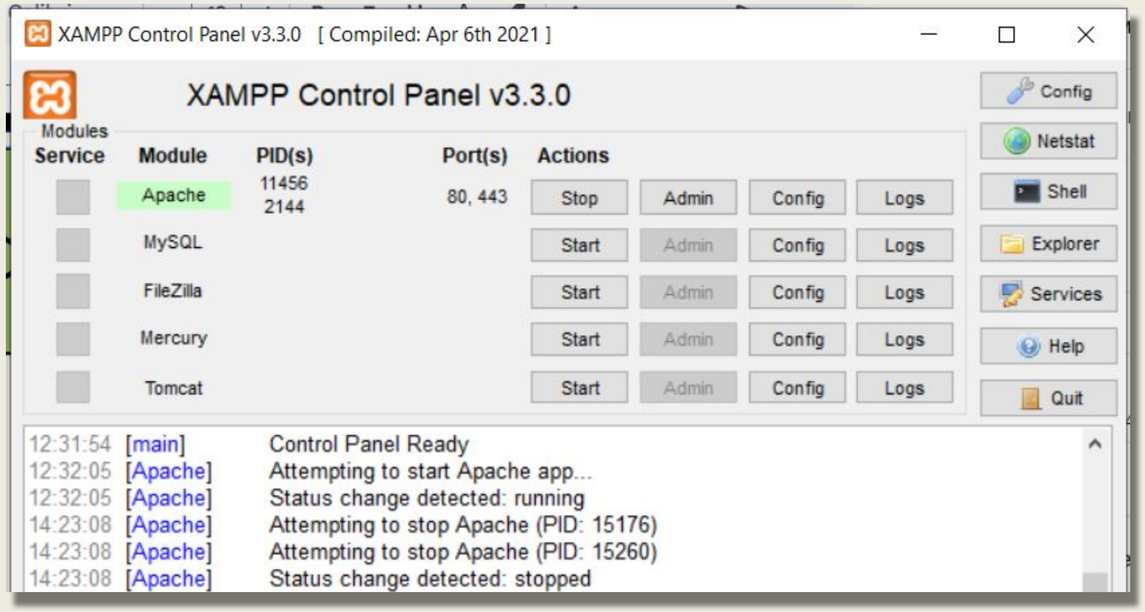
Podstawowe elementy składni PHP:

- **Zmienne** - mogą przechowywać różne typy danych.
- **Funkcje** - istnieje opcja tworzenia własnych funkcji.
- **Warunki i pętle** - if, else, switch; for, while, foreach

```
1  <!DOCTYPE html>
2  <html lang="pl">
3  <head>
4      <meta charset="UTF-8">
5      <meta name="viewport" content="width=device-width, initial-scale=1.0">
6      <title>How to plant</title>
7  </head>
8  <body>
9      <h1>Bamboo world!</h1>
10     <?php
11         $flower = 'red';
12         echo '<h3>flowering ' . $flower . '</h3>';
13     ?>
14 </body>
15 </html>
```

- **Obsługa plików** - manipulacja plikami na serwerze: odczyt, zapis, usuwanie, modyfikowanie.
- **Tablice w PHP** - są strukturami danych, które pozwalają przechowywać wiele wartości w jednej zmiennej.

Przygotowanie do realizacji zadań



- Serwer XAMPP to narzędzie, które umożliwia łatwe uruchomienie lokalnego serwera internetowego na komputerze osobistym
- Zawiera interpreter PHP, który jest potrzebny do interpretowania i wykonywania kodu PHP

1. Działania w ciałach skończonych

Wykonać obliczenia w ciele GF(p), zmieniając rząd wielkości p (p jest liczbą pierwszą)
Obliczenia wykonywane są na numerach indeksów: 335901 oraz 331156

10<p<100

p zapisana na 2048 bitach

1. bcmath wbudowana w PHP biblioteka służy do operacji na bardzo dużych liczbach i zapełnia większą poprawność obliczeniową
2. phpseclib3 pobrana z internetu biblioteka do generowania dużych liczb pierwszych

2. Generator liczb pseudolosowych

W trakcie tysiąca powtórzeń generujemy liczby z zakresu od 0 do 9 i przedstawiamy, ile razy każda liczba się pojawiła. Istnieją cztery różne sposoby generowania

1. *mt_rand()* (the Mersenne Twister Random Number Generator)
2. rand()

- funkcje wbudowane w PHP, generują liczby pseudolosowe
- niebezpieczne do używania w kryptografii
- seed można zmieniać
- funkcje *mt_rand()* i rand() są różne, ale zmiana seeda jednej z nich wpłynie na seed drugiej

	mt_rand()	rand()
0	101	86
1	100	95
2	83	104
3	103	113
4	92	101
5	117	96
6	110	111
7	104	103
8	94	92
9	96	99

Tablica wystąpień poszczególnych liczb z zakresu 0-9 losowania liczb w pętli 1000 powtórzeń

2. Generator liczb pseudolosowych

3. *random_int()* z automatycznie ustawianym seedem

- funkcja jest uważana za bezpieczną kryptograficznie
- nie pozwala na zmianę seeda
- jest wbudowana w PHP
- generuje losowe liczby z ograniczeniami na podstawie danego seeda.

	mt_rand()	rand()	random_int()
0	101	86	97
1	100	95	107
2	83	104	92
3	103	113	107
4	92	101	112
5	117	96	107
6	110	111	105
7	104	103	84
8	94	92	92
9	96	99	97

Tablica wystąpień poszczególnych liczb z zakresu 0-9 losowania liczb w pętli 1000 powtórzeń

2. Generator liczb pseudolosowych

4. Generator losowy z biblioteki PHP

- Randomizer to wysokiej klasy API służące do generowania losowości
- jest najbezpieczniejszą metodą do generowania losowych wartości
- jako jedyny z badanych jest funkcją z biblioteki
- Może korzystać z różnych silników do generowania losowości, w tym tych o charakterze kryptograficznym.

	mt_rand()	rand()	random_int()	\Random\Randomizer->getInt()
0	101	86	97	110
1	100	95	107	90
2	83	104	92	100
3	103	113	107	118
4	92	101	112	95
5	117	96	107	79
6	110	111	105	81
7	104	103	84	112
8	94	92	92	89
9	96	99	97	126

Tablica wystąpień poszczególnych liczb z zakresu 0-9 losowania liczb w pętli 1000 powtórzeń

2. Generator liczb pseudolosowych

Ciekawe zjawisko!

mt_rand() i rand() korzystają z różnych algorytmów generujących liczby losowe. Jednakże, jeśli zmienisz seed jednej z tych funkcji, automatycznie zmieni się również seed drugiej funkcji. W rezultacie otrzymujemy różne losowe wartości, co stanowi ciekawe zjawisko.

Generator losowy z seedem ustawionym na aktualny czas, powoduje, że każde odświeżenie strony generuje nowe losowe wartości. Wartości będą takie same w ciągu każdej sekundy. Gdybyś zatrzymał zegarek na tej samej godzinie, seed pozostałby taki sam, a generowane wartości pozostałyby identyczne.

	mt_rand() with seed = 5	rand() with seed = 5	rand() with seed = time()
0	87	122	128
1	101	102	96
2	107	79	73
3	98	99	94
4	104	102	98
5	103	99	105
6	97	105	114
7	114	88	96
8	88	95	93
9	101	109	103

Tablica wystąpień poszczególnych liczb z zakresu 0-9 losowania liczb w pętli 1000 powtórzeń

3. Szyfrowanie i odszyfrowanie

```
$newpassphrase = openssl_random_pseudo_bytes(strlen($filetext));
```

Inicjacja: zainicjowanie odpowiedniej biblioteki do generowania kluczy kryptograficznych

Generacja losowych bajtów: algorytm AES-128 wymaga klucza o długości 128 bitów, co odpowiada 16 bajtom. Więc trzeba wygenerować 16 losowych bajtów, które będą służyć jako klucz

Algorytm AES - 128:

- zaawansowany algorytm szyfrujący
- jeden z najbardziej bezpiecznych standardów szyfrowania
- szyfr symetryczny -> do szyfrowania i odszyfrowania używa się ten sam klucz o długości 128 bitów

4. Funkcja skrótu

Użyta wbudowana w PHP biblioteka hash do obliczenia skrótu dwóch podobnych wiadomości z plików, gdzie zmieniamy jedną literę:

*“T**o** wiadomość do zaszyfrowania”*
*“T**a** wiadomość do zaszyfrowania”*

Biblioteka oferuje wiele różnych algorytmów, ale przedstawimy skróty dla pierwszych 15: md, sha oraz whirlpool.

Nieważne, który algorytm użyjesz, skróty zawsze będą się różnić, nawet gdy zmienimy tylko jedną literę w tekście.

Źródła

Co to jest PHP

Father of PHP

AES - szyfr blokowy z kluczem symetrycznym

PHP manual

Biblioteki dla PHP