

# PHP Knihovna: Zabezpečené stránky

**Občas je třeba omezit přístup na některé stránky, například placený obsah, administrace systému ap. Mnohým začátečníkům dělá zabezpečení problémy, tudíž jsem pro tyto případy vytvořil malou knihovnu, se kterou je zabezpečení hračka.**

Jedná se o jednoduchou knihovnu skládající se z několika souborů a není určena k ničemu jinému, než přihlášení, odhlášení a zabezpečení vybraných stránek. Předpokládá se, že uživatel ovládá základy PHP a MySQL. Kdo si chce upravit knihovnu dle svých požadavků, musí samozřejmě PHP a MySQL znát lépe. Ale vzhledem k tomu, že zdrojový kód je hustě komentován v češtině, tak budou i úpravy velice jednoduché.

V krátkosti vysvětlím význam souborů. V souboru `index.php` je přihlašovací formulář a skrytá část, ve které je odkaz na zabezpečenou stránku, v souboru `login_procesing.php` je zpracování informací, které přijdou z přihlašovacího formuláře, `safe.php` je určen k includování na každou stránku, kterou chceme zabezpečit. Musí být includován před jakýkoliv standardní výstup (stačí i prázdný řádek), protože používá přesměrování pomocí `Header: Location`. Soubor `login.php` obsahuje definici funkce `check_login()` a nastavení doby expirace. Vyznám souboru `logout` je jasný, stejně tak `DB_connect.php` a `close_dbconn.php`, `safe_page.php` je příklad zabezpečené stránky a `sha1.php` slouží k zahashování hesel, které chceme uložit do databáze uživatelů. Všechny soubory jsou ke stažení v jednom balíku spolu s tímto článkem v PDF.

Obecný princip asi nejlépe znázorní Vývojový diagram

Script je založen na `sessions`(odkaz), což je další kolekce proměnných podobně jako `GET` nebo `POST`, ale `SESSIONS` se uchovávají na serveru a u klienta je buď v `cookies` nebo v `URL session id`, které identifikuje danou kolekci na serveru. Pomocí `session` budeme uchovávat `ID` uživatele, jeho přihlašovací jméno a čas poslední aktivity.

Při pokusu o přístup k zabezpečené stránce se zkontroluje zda `session` existuje a zda existují všechny proměnné, jestli se od poslední aktivity nezměnila `IP` adresa a jestli neuplynula doba expirace (nastavitelná v souboru `login.php`). Pokud jsou splněny všechny podmínky, je uživatel puštěn dál, pokud něco nesedí, je přesměrován na stránku s přihlášením.

Kde zadá jméno a heslo. Formulář se odešle souboru `login_procesing.php` kde se zahashuje heslo a z databáze se vybere záznam, kterému odpovídá jak jméno tak heslo. Pokud je takový řádek jen jeden, vše je v pořádku a uživatel je přesměrován zpět na přihlašovací stránku, kde ale už není formulář k loginu, ale zabezpečený obsah. Pokud neexistuje žádný odpovídající účet, je uživatel přesměrován zpět na přihlášení, pokud nastane ještě jiná alternativa, která by nastat neměla, ale přesto je ošetřena, je uživatel přesměrován zpět na přihlášení s hlášením o chybě.

