PHP interpreter može biti izvor sigurnosnih problema, samim tim su glavne slabosti PHP jezika programeri i web dizajneri koji ugrožavaju sigurnost aplikacija lošim kodom. Za uklanjanje sigurnosnih propusta u PHP interpreteru dovoljno je redovno pratiti sigurnosna upozorenja i instalirati odgovarajuće sigurnosne apdejte, dok je za minimiziranje sigurnosnih propusta u samom kodu potrebno razumevanje osnovnih sigurnosnih problema koji proizilaze iz nepažljivog i površnog programiranja.

* Globalne varijable

Najuobičajeniji i najozbiljniji sigurnosni nedostatak PHP skripti i web aplikacija je slaba provera korisničkog unosa. Često je slučaj da se informacija dobijena od korisnika upotrebljava u daljem procesuiranju. Varijable u PHP jeziku ne moraju biti deklarisane, one se aumatski stvaraju prilikom prve upotrebe. Tip varijable nije potrebno odrediti, već se on bazira na kontekstu u kojem je ta varijabla iskorišćena.

<?php

if (autentikacija\_korisnika()) {

$auth = true;

}

...

if (!$auth) {

die("Potrebna je autorizacija!");

}

else

echo "Neka važna informacija...";

?>

U navedenom primeru kroz autentikaciju korisnika obavlja se provera unosa. Ukoliko je provera tačna, pojavljuje se promenljiva $auth koja specificira da je korisniku dozvoljeno da čita neke važne informacije. Napadač može metodom GET postaviti promenljivu na željeni iznos:

<http://aplikacija/admin.php?auth=1>

* Interakcija sa bazom podataka

PHP komunicira sa raznim bazama podataka jednostavnom upotrebnom skripti. Ovakva interakcija može da predstavlja sigurnosni problem. Vrlo često upiti namenjeni bazi podataka se slažu pomoću informacije koje korisnik unosi pomoću web forme:

<?php

if ($obnovi\_tabelu) {

$db->query('Update $tabela set ime=$ime');

}

?>

Ukoliko se ne proverava promenljiva $tabela, i da li je promenljiva $obnovi\_tabelu došla putem forme, promenljive se mogu postaviti putem GET metode na željene vrednosti:

http://www.primer.com/edit.php?obnovi\_tabelu=1&tabela=korisni

ci+set+provera%3Dabcd+where+korisnik%3D%27+administrator%27%23

* Načini zaštite PHP aplikacija

Ako se radi o velikom broju napada koji mogu naneti štetu, PHP omogućava vrlo lak broj konfiguracijskih opcija pomoću kojih se PHP aplikacija može uspešno zaštititi. Međutim, učitavanjem nekih opcija, programiranje u PHP jeziku se može uveliko otežati. Zato je PHP skripte potrebno zaštititi pažljivom kombinacijom odabranih konfiguracijskih stavki i praksom sigurnog programiranja. Neki od tih jeste rad sa pridruženim datotekama, filtriranje korisničkog unosa kao i onemogućavanje obrađivanja datoteka koje su izvan radnog direktorijuma aplikacije.