BEZPIECZEŃSTWO BAZ DANYCH POD KONTEM WPROWADZANYCH DANYCH

Wszystkie dane przesłane do skryptu przez użytkowników powinny być dokładnie filtrowane pod kątem obecności w nich kodu HTML i PHP, do tego celu należy używać funkcji:

htmlspecialchars() - zamienia wybrane znaki w wyrażeniu, na odpowiadające im zamienniki (tzw. encje), dzięki czemu te nie będą interpretowane przez przeglądarkę jako znacznik HTML i zostaną prawidłowo wyświetlone.
strip_tags() - usuwa ze stringu znaczniki HTML i PHP

Należy też sprawdzać typ danych przekazanych przez użytkownika do skryptu, jeśli oczekujemy zmiennej typu *int* (liczby) to sprawdzajmy czy rzeczywiście otrzymaliśmy liczbę. Służą do tego funkcje:

is_double(),is_float() //sprawdza czy zmienna jest liczbą rzeczywistą
is_int(),is_integer() //sprawdza czy zmienna jest liczbą całkowitą
is_string() //sprawdza czy zmienna jest ciągiem znaków

Atak **SQL Injection** wykorzystuje fakt że dane wpisane do formularza na stronie WWW (lub w inny sposób wysłane do serwera) nie są w żaden sposób walidowane pod kątem ich poprawności. Do tego dochodzi fakt że w zapytaniach SQL stringi należy zamknąć pomiędzy znakami apostrofu. Zatem jeżeli ktoś wpisze do formularza ciąg znaków zawierający m.in. apostrof, różne rzeczy mogą się przytrafić - od zwykłego błędu wykonania zapytania SQL, aż po wykasowanie wszystkich danych z bazy danych czy dysku serwera, albo włamania do innych maszyn w sieci!
Aby takim atakom zapobiec należy sprawdzać wszystkie dane pochodzące od użytkownika.
W przypadku bazy MySQL do tego celu należy stosować funkcję:

mysql_real_escape_string() - wstawia znak **** przed każdym **'** w stringu

Ponadto w swoim zapytaniu (w przypadku MySQL), niezależnie od typu danych obejmuj je w pojedynczych cudzysłowach, należy też dokładnie filtrować wszystkie dane pochodzące od użytkowników skryptu.

np. mając w formularzu pole do wpisywania imienia:
<input type=text name=imie>

po pobraniu

$imie=$_POST['imie'];
Przed wysłaniem wartości do bazy danych:

$imie=mysql_real_escape_string(htmlspecialchars(strip_tags($imie)));