Programování v PHP

Katedra softwarového inženýrství
Fakulta informačních technologií
České vysoké učení technické v Praze

Security - základní informace
BI-PHP

```
<!DOCTYPE html>
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
        <title>Zakladni informace k zabezpečení aplikace</title>
    </head>
    <body>
        <?php
            // Dulezite body pro zabezpeceni:

            // nastaveni serveru - prava apod, omezeni informaci o web
            // serveru, operacnim systemu a PHP (nezpristupnovat phpinfo)

            // desinfekce vstupu od uzivatele - test a upravy vstupnich dat,
            // eliminujici nebezpecne hodnoty

            // priklady utoku pres vstupni data:

            // 1. program v PHP provadi volani programu (na serveru), jehoz
            // jmeno se udava primo jako vstupni hodnota, popr. se zadavaji
            // parametry spoustenych programu; uzivatel muze zadat
            // napr. prikazy OS pro vymaz souboru!

            // 2. skriptovani pres weby (cross-site scripting, script
            // injection)- viz dale

            // 3. SQL injection - jako vstupni data se zadaji SQL prikazy
            // (nebo jejich casti) a ty PHP program zretezi do nove
            // vykonavanych SQL prikazu na databazi
            // (napr.: Select * From Zam Where ZamID = <hodnota_ze_vstupu>
            // a uzivatel zada jako <hodnota_ze_vstupu> 1; Delete From Zam!!)

            // nasleduje ukazka script injection - vkladani JavaScriptu (bod 2)

            $vstup = isset($_GET["vstup"])?$_GET["vstup"]:"";
        ?>


        <form action="securityInfo.php" method="get">
            <h1>Ukazka script injection</h1>
            <h2>Zadejte do textoveho pole:<br>
                "&gt;&lt;script type="text/javascript"&gt;
                 alert("Zlomyslny script!!");
                 &lt;/script&gt;&lt;span id="nic</h2>
            <h2>Mohl by byt zadan daleko horsi script!!</h2>
            <!-- Vubec se netestuje to, co uzivatel vlozil!! -->
            <input type="text" name="vstup" size="80"
                   value="<?php echo $vstup; ?>"><br><br>
            <input type="submit" name="submit" value="Proved">
        </form>
```

```
        <?php
            // Zamezeni temto problemum:

            // testovat (desinfikovat) vstupni data, zda obsahuji to, co maji
            // mozno pouzit funkce, urcene k temto ucelum:
            // - escapeshellargs - obklopi parametr apostrofy a vnitrni
            //   apostrofy zdvoji
            // - escapeshellcmd - predradi escape char pred metaznaky shellu:
            //   $#;() ...
            // - htmlentities - prevod & -> &amp, < -> &lt; ...
            // - strip_tags - vymaze tagy HTML
            // - addslashes - vlozi pred ';" a NULL char znak \
            // - od verze PHP 5.2 lze pouzit rozsireni Filter pro validovani
            //   a "sanitaci" dat - napr. filter_var("123",FILTER_VALIDATE_INT)
            // - lze pouzit i predpripravene balicky pro vytváření formularu
            //   a validaci dat - napr. HTML_QuickForm2
            // pro vytvareni SQL prikazu pouzivat parametrizovane (prepared)
            // prikazy nebo volat stored procedury a funkce
        ?>
    </body>
</html>
```